CUVEX

CUVEX ACADEMY · 0.1

Учитесь. Разбирайтесь. Берите управление в свои руки.

Bitcoin и самостоятельное хранение средств шаг за шагом. Курс, руководство, словарь и упражнения доступны бесплатно и без регистрации. Вы сами выбираете, с чего начать.

Бесплатно · без регистрации

Все разделы

1. Подготовьте место для занятий
2. Цифровые деньги и проблема доверия
3. История и границы возможностей Bitcoin
4. Сатоши и расчёты без ошибок
5. Ваша модель угроз
6. Узлы, майнинг и консенсус
7. UTXO и сдача в транзакции
8. Мемпул, подтверждения и реорганизации
9. Комиссии, виртуальный размер и замена транзакций
10. Сети, адреса и платёжные запросы
11. Хеши, подписи и шифрование
12. Сид-фраза, дополнительная парольная фраза и пароль
13. Деривация ключей, xpub и дескрипторы
14. Выбор кошелька и модели хранения
15. Резервные копии, из которых можно восстановиться
16. Знакомство с Original и BIT
17. Генерация сид-фразы с помощью физической энтропии
18. Шифрование и расшифрование секрета с помощью Cuvex
19. Пороги доступа к зашифрованным данным и биометрия
20. Клонирование, хранение и проверка копий
21. Установка и защита Cuvex Desk
22. Привязка криптограмм и организация счетов WOW
23. Сопряжение Mirror и Desk
24. NFC через Mirror, USB-C и чтение QR-кодов
25. Публичные поставщики данных и собственный узел
26. Получение bitcoin и проверка адреса
27. Метки, заморозка и выбор UTXO
28. Подготовка и проверка платежа
29. Подписание с помощью Original и BIT
30. Завершение и передача транзакции в сеть, устранение сбоев
31. Какие сведения видны в Bitcoin
32. Разделение контекстов и управление сдачей
33. Конфиденциальность в сети, Tor и VPN
34. CoinJoin, Payjoin и их нынешние ограничения
35. Уроки реальных инцидентов

36. Создание идентичности и проверка контактов в чате
37. Запрос и оплата в сатоши через чат
38. Осознанная передача криптограмм
39. Восстановление чата и понимание его метаданных
40. Повседневные настройки и проверка разрешений
41. Проектирование кошелька с мультиподписью
42. Создание приглашений и предоставление ключей
43. Проверка политик в Mirror в произвольном порядке
44. Координация подписей и передача транзакции с мультиподписью в сеть
45. Восстановление и изменение кошелька с мультиподписью
46. Обновление прошивки по проверенной процедуре
47. Потеря, поломка и экстренное восстановление
48. Фишинг, служба поддержки и голосовое мошенничество
49. Конфиденциальность, законность и личный учёт
50. Наследование, преемственность и ежегодная тренировка
51. Цена, накопления и фундаментальный анализ
52. Выбор места для приобретения bitcoin
53. Счета, ордера и издержки исполнения
54. Свечи, индикаторы и искажения технического анализа
55. Маржинальные операции, фьючерсы и автоматизация
56. Lightning и другие уровни
57. Taproot, MuSig2 и постквантовая перспектива
58. Совместимость и выход из экосистемы производителя
59. Техническая лаборатория с regtest
60. Итоговый проект и план преемственности
61. Руководство учащегося
62. Словарь Bitcoin и самостоятельного хранения
63. Проверьте, чему вы научились

M01

Подготовьте место для занятий

Цель

Подготовьтесь к курсу, разберитесь в назначении трёх устройств и договоритесь, какие сведения нельзя передавать преподавателю.

Разберитесь в теме

Вы научитесь самостоятельно принимать решения о получении, хранении, расходовании и восстановлении bitcoin. Цель — уметь объяснить решение до его подтверждения. Курс можно читать самостоятельно. В голосовой беседе преподаватель разъясняет материал, задаёт вопросы и помогает на отдельных этапах. Ему не требуется видеть ваши активы или управлять устройствами.

Устройство Cuvex защищает секретные данные и позволяет авторизовать операции на своём экране. Desk на компьютере служит для работы с криптограммами, кошельками только для наблюдения, платежами и координацией. Mirror локально передаёт данные для поддерживаемых операций и сравнивает их. Он не подписывает транзакции и не служит самостоятельным кошельком. Доступные способы работы зависят от модели и версии.

По возможности выделите по одному экрану для курса и Desk. Держите телефон и Cuvex под рукой. Если экран один, переключайтесь между окнами и не включайте демонстрацию экрана по видеосвязи при вводе секретов. Звонок может закончиться до завершения упражнения. Делать паузы нормально. Сохраните только номер урока, достигнутый шаг и описание возникшей трудности.

Ни преподавателю-человеку, ни ИИ нельзя передавать сид-фразы, дополнительные парольные фразы BIP39, пароли, ключ чата (Clave Chat), PIN-коды, личные файлы или полные коды покупки. Им также не нужны ваш xpub, реальный дескриптор или адрес. Хотя по этим данным нельзя тратить средства, они раскрывают вашу активность. Опишите сообщение об ошибке и используйте вымышленные данные лаборатории.

Практика

1. Определите, какие компьютер, телефон и модель Cuvex у вас под рукой. Запишите их версии в личный блокнот.
2. Отделите учебную среду без средств от среды хранения реальных активов. Для упражнений не импортируйте сид-фразу действующего кошелька.
3. Откройте урок и найдите паузу, помощь и словарь. Если кто-либо попросит секретные данные, прекратите это взаимодействие.

Проверьте себя на практике

Объясните, кто подписывает, кто обращается к сети и кто переносит данные. Переходите дальше, когда сможете различать эти функции без подсказки.

Частый вопрос

Обязательно ли разговаривать с преподавателем каждый день? Нет. Можно заниматься самостоятельно, повторить занятие и обратиться за помощью только для конкретной операции. Доступ к курсу и остаток времени голосового сервиса — отдельные права.

Где сделать паузу

Урок L01 завершён. Устройства определены. В курсе не зафиксировано никаких секретных данных.

Преподаватель просит вашу сид-фразу, чтобы проверить, правильно ли вы её записали. Как вы поступите?

1. Медленно продиктую её.
2. Отклоню просьбу и проверю сид-фразу только в своей безопасной среде.
3. Отправлю только первые слова.

> **Показать ответ: Отклоню просьбу и проверю сид-фразу только в своей безопасной среде.**
> Учебному сервису нельзя передавать даже часть секрета.

M01

Цифровые деньги и проблема доверия

Цель

До открытия кошелька разберитесь, какую проблему решает Bitcoin.

Разберитесь в теме

Банковский остаток — запись, которую ведёт организация. Она проверяет личность клиента, решает, какие переводы провести, и ведёт учёт. Обычный цифровой файл легко скопировать: отправив фотографию, вы можете оставить себе копию. Чтобы цифровая единица служила деньгами, необходимо предотвратить её двойное расходование.

Bitcoin объединяет правила проверки, подписи и общую историю транзакций. Реестр не нужно целиком доверять одной организации: независимые участники могут проверить соответствие транзакции правилам. Ограниченность предложения зависит от дальнейшей проверки и принятия этих правил, а не от картинки монеты или котировки биржи.

При самостоятельном хранении меняется распределение ответственности. Вы можете тратить без разрешения кастодиана, но можете потерять доступ или средства, уничтожив все копии или подписав неверный платёж. Свобода действий не отменяет безопасности, координации, необходимости связи для передачи операции в сеть и соблюдения применимых обязанностей.

Различайте Bitcoin как сеть и протокол и BTC как денежную единицу. Другие сети также могут использовать термин «блокчейн», обладая иными свойствами. Обязательство компании под названием «bitcoin» не равнозначно выходу Bitcoin под контролем ваших ключей.

Практика

1. Сравните три ситуации: остаток в банке, остаток на бирже и UTXO под контролем ваших ключей.
2. Для каждой ситуации запишите, кто может помешать переводу и кто способен помочь, если вы забудете данные доступа.
3. Опишите, что произойдёт при копировании фотографии и при попытке дважды потратить один выход.

Проверьте себя на практике

Объясните своими словами, почему остаток и возможность подписывать — разные понятия. Технические термины заучивать не требуется.

Частый вопрос

Исчезают ли при самостоятельном хранении все посредники? Для покупки, запросов или общения вы можете выбирать сервисы. Важно, какими полномочиями они располагают и какие данные получают.

Где сделать паузу

Сохраните сравнение ответственности без названий реальных счетов.

Какую денежную проблему цифровая подпись сама по себе не решает?

1. Предотвращение попыток дважды потратить один и тот же выход.
2. Доказательство авторизации с помощью ключа.
3. Обнаружение изменения подписанного сообщения.

> **Показать ответ: Предотвращение попыток дважды потратить один и тот же выход.** Подписи подтверждают авторизацию. Правила и консенсус определяют порядок несовместимых трат.

История и границы возможностей Bitcoin

Цель

Поместите появление Bitcoin в исторический контекст и отделите факты от коммерческих повествований.

Разберитесь в теме

Документ Сатоши Накамото распространили в 2008 году, а сеть начала работать в 2009-м. В нём предложены электронные наличные для прямых расчётов между участниками на основе прежних идей криптографии, доказательства работы и цифровых денег. Для проверки программы или транзакции не нужно знать гражданскую личность Сатоши.

Развитие не сводится к односторонней замене правил компанией. Разработчики предлагают и проверяют изменения, операторы выбирают ПО, майнеры строят блоки, а пользователи и сервисы решают, что принимать. Такое распределение может приводить к разногласиям. Развилка сети и обновление приложения — разные вещи.

Узел может отклонить блок, нарушающий его правила, независимо от затраченной работы. Консенсус — не простое голосование по числу компьютеров. Запуск тысяч копий узла сам по себе не увеличивает полномочия. Аналогично, большинство майнеров не получает по этому основанию закрытый ключ пользователя.

У Bitcoin есть намеренные ограничения и компромиссы: ёмкость блока, затраты на проверку, переменное время подтверждения и публичный реестр. По умолчанию нет административного возврата платежей или полной конфиденциальности. Дополнительные уровни и приложения решают конкретные задачи ценой новых зависимостей.

Практика

1. Нанесите на шкалу времени первоначальный документ, запуск сети, внедрение SegWit и активацию Taproot. Проверяйте даты по источникам до публикации.
2. Отнесите фразы «компания гарантирует цену», «узел проверяет» и «майнер предлагает блок» к коммерческим обещаниям или техническим функциям.
3. Объясните одно преимущество и одну издержку отсутствия администратора, способного отменять платежи.

Проверьте себя на практике

Различайте правило консенсуса, локальную политику и решение компании. Используемое вами приложение не является всей сетью.

Частый вопрос

Всегда ли новейшее ПО меняет денежные правила? Нет. Выпуски также исправляют ошибки, улучшают производительность или изменяют локальные политики. Читайте примечания к версии и сведения о совместимости.

Где сделать паузу

Запишите одно проверяемое свойство и одно утверждение, для которого нужны дополнительные свидетельства.

Блок содержит трату без действительной авторизации. Может ли большинство майнеров сделать её действительной?

1. Да, если доля превысит 51 %.
2. Только если об этом объявит биржа.
3. Нет для узла, применяющего правила, по которым такая трата отклоняется.

> **Показать ответ: Нет для узла, применяющего правила, по которым такая трата отклоняется.**
> Накопленная работа сравнивается между вариантами истории, которые действительны по правилам узла.

M01

Сатоши и расчёты без ошибок

Цель

Переводите BTC в сатоши и обратно, проверяя суммы без опоры на котировку.

Разберитесь в теме

Один BTC равен 100 000 000 сатоши. «sat» — единица измерения, а не другая валюта. В базовой цепочке суммы учитываются целым числом сатоши. 0,001 BTC — это 100 000 sat, а 0,00001000 BTC — 1 000 sat. Десятичный разделитель зависит от языка интерфейса. Не добавляйте нули на глаз.

Котировка позволяет на данный момент пересчитать BTC в валюту вроде EUR или USD. Она не меняет контролируемое вами число сатоши. Если у вас 100 000 sat, при изменении цены их число остаётся прежним. В Desk курс показан как справочное значение с источником и датой. Устаревшая котировка может привести к ошибочному экономическому решению даже при правильном остатке BTC.

В платеже различайте сумму получателю, сетевую комиссию и полный расход. При отправке 50 000 sat с комиссией 600 sat из кошелька уйдёт 50 600 sat при отсутствии других собственных выходов. При отправке всего остатка чистая сумма получателю обычно меньше доступного остатка, поскольку нужно оплатить комиссию.

Примеры курса — арифметические упражнения, а не рыночные цены или рекомендуемые ставки. Перед подписанием проверьте на соответствующем экране единицу, сеть, получателя и полную стоимость. Голос может произнести «пятьдесят тысяч сатоши» и одновременно показать «50 000 sat». Нельзя выбирать сумму по сомнительной расшифровке.

Практика

1. Пересчитайте 250 000 sat в BTC: 0,0025 BTC. Пересчитайте 0,00025000 BTC в сатоши: 25 000 sat.
2. Рассчитайте отправку 75 000 sat с комиссией 900 sat. Полный расход равен 75 900 sat.
3. В симуляторе используйте 120 000 sat, перевод 70 000 и комиссию 1 000. Проверьте сдачу в 49 000 sat.

Проверьте себя на практике

Прочитайте сумму в BTC и sat и объясните, какая величина включает комиссию. При сомнении приостановите операцию.

Частый вопрос

Обязательно ли покупать целый bitcoin? Нет. Можно приобрести долю с учётом минимальных сумм и расходов поставщика.

Где сделать паузу

Сохраните только результаты упражнения.

У вас 80 000 sat, и вы хотите отправить весь остаток с комиссией 1 200 sat. Сколько получит адресат?

1. 80 000 sat.
2. 78 800 sat.
3. 81 200 sat.

> **Показать ответ: 78 800 sat.**
> В этом примере без других выходов получателю достаётся доступный для расходования остаток за вычетом комиссии.

M01

Ваша модель угроз

Цель

Выбирайте соразмерные меры против потери, кражи, обмана и раскрытия данных.

Разберитесь в теме

Безопасность — сохранение возможности действовать согласно своему намерению. Конфиденциальность — контроль над тем, кому известны ваши данные и связи. Доступность — возможность получить доступ в нужный момент. Недоступный всем сейф может быть недоступен и вам, а слишком удобная копия способна раскрыть лишнее.

Определите защищаемые активы, противников и случайные события. В активы входят ключи, копии, история, места хранения и идентичности контактов. Среди рисков — вредоносное ПО, фишинг, пожар, забывчивость, принуждение, поломка, смерть и собственные ошибки. Один инструмент не уменьшает их все.

В простой матрице укажите примерную вероятность, последствия и конкретную меру. Длинный пароль снижает риск подбора, но не исправит мошеннического получателя, которого вы сами одобрили. Две копии в одной сумке не спасают при её потере. Если устройства и копии мультиподписи контролирует один человек, общей точки отказа избежать не удалось.

Курс и преподаватель также входят в модель. Покупки, звонки, периоды соединения и прогресс могут создавать метаданные. Учебному сайту не следует запрашивать адреса или остатки для персонализации урока. Отсутствие обычной регистрации в Desk или Mirror не означает, что о вашей активности ничего не знают магазин, поставщик голосовой связи или третья сторона, которой направлен запрос.

Практика

1. Запишите три наиболее важных риска без сумм имущества и точных мест.
2. Выберите для каждого риска меры предупреждения, обнаружения и восстановления. Пример для потери карты: две раздельные копии, опись, пробное восстановление.
3. Различайте, какие люди и системы могут наблюдать покупку, звонок, запрос остатка и публичную транзакцию.

Проверьте себя на практике

Обоснуйте, какой конкретный риск уменьшает следующая мера. Не добавляйте сложности, которую не сможете поддерживать или объяснить наследникам.

Частый вопрос

Больше устройств всегда означает большую безопасность? Только если они уменьшают общие зависимости и вы можете проверить восстановление. Дополнительные устройства также требуют ухода и повышают вероятность путаницы.

Где сделать паузу

Храните план в личной документации. В курсе отметьте только «модель угроз рассмотрена».

Какая мера лучше всего снижает риск потерять все копии при пожаре в одном месте?

1. Изменить цвет карты.
2. Положить две копии в один ящик.
3. Хранить проверенные копии в местах с независимыми рисками.

> **Показать ответ: Хранить проверенные копии в местах с независимыми рисками.**
> Резервные копии должны пережить тот же инцидент, который угрожает оригиналу.

M02

Узлы, майнинг и консенсус

Цель

Объясните, что проверяют узлы и что даёт майнинг.

Разберитесь в теме

Полный узел получает блоки и транзакции, проверяет правила и поддерживает собственное представление о цепочке. Ему не приходится доверять остатку, показанному сайтом. Майнинг — предложение блоков с доказательством работы. Майнеры выбирают действительные транзакции и соревнуются в поиске допустимого блока.

Доказательство работы делает переписывание истории затратным. Когда есть несколько действительных ветвей, ориентируются на накопленную работу, а не просто считают блоки без учёта сложности. Интервалы меняются. Десять минут — целевое среднее, а не установленный срок следующего платежа.

Награда майнера состоит из субсидии и комиссий. Субсидия уменьшается по расписанию, привязанному к высоте блоков, а комиссии зависят от включённых транзакций. Высокая комиссия не делает ошибочную подпись действительной. Экономическая безопасность и стоимость атаки не придают недавнему платежу математическую необратимость.

Собственный узел уменьшает потребность обращаться к сторонним поставщикам и позволяет проверять данные. При этом нужно защищать ОС, доступ и соединение. Сам по себе запущенный узел не даёт этих преимуществ, если он не синхронизирован или приложение обращается к другому серверу.

Практика

1. Распределите задачи: проверка подписи, выбор транзакций блока, хранение вашей сид-фразы и решение о принятии платежа.
2. Объясните, почему утверждение «мои bitcoin хранит майнер» ошибочно.
3. В лабораторной сети наблюдайте высоту и синхронизацию. Не публикуйте данные доступа RPC.

Проверьте себя на практике

Опишите разницу между проверкой и предложением. Можно начать с аналогии, но в конце правильно назовите техническую функцию.

Частый вопрос

Нужно ли майнить, чтобы пользоваться Bitcoin? Нет. Для начала не обязателен и собственный узел, однако вы должны понимать, в какой степени доверяете поставщику.

Где сделать паузу

Запишите тип лабораторного поставщика без приватного URL.

Что даёт пользователю правильно настроенный полный узел?

1. Возможность проверять соблюдение правил принимаемой цепочкой.
2. Восстановление любого потерянного ключа.
3. Гарантию роста цены.

> **Показать ответ: Возможность проверять соблюдение правил принимаемой цепочкой.**
> Проверка и хранение средств — разные функции.

M02

UTXO и сдача в транзакции

Цель

Читайте транзакцию как расходование прежних и создание новых выходов.

Разберитесь в теме

UTXO — ещё не израсходованный выход предыдущей транзакции. Кошелёк вычисляет остаток, определяя контролируемые им выходы. Здесь нет универсального счёта, с которого вычитают сумму как в банковской таблице: вход указывает на предыдущий выход по идентификатору транзакции и позиции.

При расходовании UTXO используется целиком. При платеже меньше его стоимости обычно создаются выход получателю и выход сдачи под вашим контролем. При входе 120 000 sat, получателе на 70 000 и комиссии 1 000 сдача равна 49 000. Сумма входов должна равняться сумме выходов и комиссии.

Адрес не является UTXO и может получать несколько выходов. Он также не обязательно представляет человека. Идентификатор транзакции может быть публичным, но привязка к вашей личности или объяснение принадлежности выходов добавляет сведения, которых цепочка сама по себе не содержит.

Структура важна для конфиденциальности: объединение входов может указывать на общее управление, а сдача связывать последующие платежи. Из-за совместных транзакций это не универсальное доказательство. Coin control — осознанный выбор расходуемых выходов с учётом последствий их объединения.

Практика

1. Нарисуйте три вымышленных входа: 40 000, 60 000 и 200 000 sat. Используя только первые два, заплатите 70 000 с комиссией 1 000.
2. Проверьте, что сдача равна 29 000 sat и третий вход не участвует.
3. Повторите только с входом 200 000. Сдача составит 129 000. Сравните возможные издержки и связи, не предполагая равенства размеров транзакций.

Проверьте себя на практике

Найдите на схеме курса вход, получателя, сдачу и комиссию. Если не можете определить назначение выхода, не подписывайте реальную операцию.

Частый вопрос

Всё, что приходит в мой кошелёк обратно, — сдача? Нет. Возможен перевод на другой собственный адрес. Для классификации нужно знать политику и деривацию, а не угадывать по сумме.

Где сделать паузу

Сохраните вымышленную схему, а не снимок экрана с реальными активами.

Вход 100 000 sat создаёт выходы на 30 000 и 69 200 sat. Какова комиссия?

1. 69 200 sat.
2. 800 sat.
3. 30 000 sat.

> **Показать ответ: 800 sat.**
> 100 000 минус 99 200 равно 800 sat.

M02

Мемпул, подтверждения и реорганизации

Цель

Различайте подготовленную, переданную в сеть и подтверждённую транзакции.

Разберитесь в теме

Мемпул — локальный набор неподтверждённых транзакций, которые узел хранит по своей политике. Единого одинакового для всего мира мемпула нет. Если обозреватель показывает платёж, о нём знает этот сервис. Это не гарантирует принятия всеми узлами или подтверждения в определённый срок.

Подготовка PSBT ничего не передаёт в сеть. Подписание создаёт авторизацию. Завершение формирует транзакцию, пригодную для отправки. Публикация — попытка передать её в сеть. Подтверждение означает включение в блок цепочки, принятой вашим источником проверки. Второе подтверждение — ещё один блок сверху, а не вторая подпись получателя.

При реорганизации участок цепочки может замениться, и транзакция потеряет подтверждения или вернётся в ожидание. Для платежей с большими последствиями стороны обычно требуют больше подтверждений. Нет числа, устраняющего все риски при любых суммах и обстоятельствах.

Если Desk показывает сохранённое состояние, проверьте дату синхронизации. «Подтверждено» в старом снимке не обязательно отражает настоящее. Если перевод не отображается, сохраните его локальный идентификатор и проверьте публикацию и историю до новой подготовки. Нетерпеливый повтор может создать ещё один действительный платёж.

Практика

1. Расположите карточки по порядку: черновик, PSBT, подпись, итоговая транзакция, распространение, включение в блок.
2. Смоделируйте отключение после передачи в сеть. Решите, что проверить до повторной оплаты.
3. Объясните продавцу, почему отметка «оплачено» в чате не заменяет сетевой проверки.

Проверьте себя на практике

Укажите состояние операции, источник и дату сведений, не выдавая их за гарантию.

Частый вопрос

Отменяет ли закрытие Desk уже переданную транзакцию? Нет. Её могут хранить другие узлы и участники. Отмена локального черновика имеет другую область действия.

Где сделать паузу

Запишите состояние симуляции и не передавайте преподавателю реальные идентификаторы.

Компьютер теряет соединение сразу после нажатия кнопки передачи в сеть. Каков первый шаг?

1. Подготовить тот же платёж заново.
2. Удалить кошелёк.
3. Восстановить связь и проверить транзакцию и её входы.

> **Показать ответ: Восстановить связь и проверить транзакцию и её входы.**
> Отсутствие ответа не доказывает, что транзакция не распространилась по сети.

M02

Комиссии, виртуальный размер и замена транзакций

Цель

Оценивайте издержки, интерпретируйте sat на vbyte и разберитесь в RBF и CPFP.

Разберитесь в теме

Сетевая комиссия — разность сумм входов и выходов. Её конкурентоспособность обычно выражают в sat/vB, сатоши за виртуальный байт. Она напрямую не зависит от денежной стоимости перевода. Много входов могут удорожить небольшой платёж, а крупный платёж с малым числом входов может занимать меньше места.

При 200 vB и ставке 5 sat/vB комиссия равна 1 000 sat. До подписания она лишь оценочная, поскольку итоговый размер может зависеть от подписей и структуры. Desk предлагает ориентировочные варианты скорости и ручную ставку. Метка «быстро» не обещает подтверждения к определённому времени.

RBF — политика замены неподтверждённых транзакций при определённых условиях. Она позволяет предложить конфликтующую трату с более высокой комиссией. Политики узлов менялись, поэтому сигнал об отсутствии замены нельзя считать гарантией получения. Замена требует новой проверки и необходимых подписей.

При CPFP расходуют выход ожидающей транзакции, чтобы пакет из родителя и потомка стал привлекательнее для включения. Необходимы контроль подходящего выхода, соблюдение политик и оплата издержек. Это механизм Bitcoin. Наличие кнопки CPFP в версии Cuvex учащегося не предполагается.

Пыль — выход, слишком малый по применимым политикам и предполагаемым затратам на его расходование. Универсального порога для всех скриптов нет. Не выдавайте фиксированное число за правило консенсуса. Если сдача нецелесообразна, проверьте сумму, входы или перевод всего остатка и фактическую комиссию.

Практика

1. Рассчитайте 180 vB по 8 sat/vB: 1 440 sat. Проверьте, превышает ли это бюджет упражнения.
2. Сравните одну входную UTXO и десять входов. Объясните, почему одной суммы перевода недостаточно для оценки стоимости.

3. Смоделируйте ожидающую транзакцию и выберите ожидание, RBF или изучение CPFP без предположения об автоматической совместимости.

Проверьте себя на практике

Обоснуйте ставку, абсолютную комиссию и её отношение к сумме перевода. Не принимайте комиссию, которую не понимаете.

Частый вопрос

Гарантирует ли RBF отмену прежнего платежа? Нет. До подтверждения версии конкурируют, а распространение имеет значение. Не передавайте товары, полагаясь на обещание отмены.

Где сделать паузу

Сохраните решение упражнения и его обоснование.

Какова комиссия для 250 vB при ставке 4 sat/vB?

1. 1 000 sat.
2. 254 sat.
3. 4 % от отправленной суммы.

> **Показать ответ: 1 000 sat.**
> Произведение виртуального размера и ставки даёт оценку комиссии.

M02

Сети, адреса и платёжные запросы

Цель

До копирования или сканирования определите сеть, формат адреса и платёжные инструкции.

Разберитесь в теме

В mainnet переводят bitcoin с реальной стоимостью. Тестовые сети служат для разработки и обучения, но не взаимозаменяемы. Regtest — локальная сеть под управлением создателя лаборатории. У signet и testnet собственные правила и экосистемы. Поддержка одиночной подписи в signet не означает поддержки этой сети профилем мультиподписи Cuvex.

Адреса кодируют условия получения. В mainnet встречаются форматы с префиксами 1, 3, bc1q и bc1p. Префикс помогает распознать семейство, но не удостоверяет получателя, не гарантирует совместимости подписывающего устройства и не заменяет полной проверки формата.

QR-код — визуальный контейнер. Он может нести адрес, счёт, дескриптор или вредоносный текст. Сканирование не удостоверяет автора. Ссылка bitcoin: может включать сумму и сообщение. Современная спецификация BIP321 заменила BIP21, однако рассмотренная реализация Desk сохраняет терминологию и совместимость BIP21. Развитие стандарта само по себе не расширяет возможности приложения.

Счёт Lightning не является адресом базовой цепочки. Он может содержать срок действия и другие поля. Не вставляйте его в форму перевода по цепочке без совместимой процедуры. Токен с обозначением BTC в другой сети также не становится автоматически нативным bitcoin.

Практика

1. Распределите подписанные учебные образцы без действующих адресов для средств: адрес, URI bitcoin:, счёт Lightning и дескриптор.
2. Определите выбранную в лаборатории сеть. Рассмотренный профиль мультиподписи Cuvex поддерживает mainnet/regtest.
3. До реальной операции сравните весь текст запроса получателя через аутентифицированный канал.

Проверьте себя на практике

Умейте отклонить запрос с неизвестной сетью или способом оплаты и объяснить, что нужно проверить.

Частый вопрос

Можно ли отправить BTC через любую сеть, предлагаемую биржей? Нет. Сеть вывода должна совпадать с фактической сетью получения. Не выбирайте исключительно по наименьшей комиссии.

Где сделать паузу

Запишите только тип учебной сети.

Адрес получения с префиксом bc1 сам по себе не позволяет вывести BTC через другую токенную сеть. Что нужно проверить?

1. Изменить псевдоним получателя.
2. Убедиться, что вывод идёт в основной цепочке Bitcoin и все данные совпадают.
3. Ввести сид-фразу на бирже.

> **Показать ответ: Убедиться, что вывод идёт в основной цепочке Bitcoin и все данные совпадают.**
> Актив, сеть и способ получения должны быть совместимы.

M03

Хеши, подписи и шифрование

Цель

Различайте целостность, авторизацию и конфиденциальность.

Разберитесь в теме

Хеш-функция преобразует данные в отпечаток фиксированной длины. Сравнение с известным отпечатком помогает обнаружить изменения, но не шифрует файл и не устанавливает, кто его опубликовал. Если файл и хеш скачаны с одной скомпрометированной страницы, злоумышленник мог заменить оба.

Закрытый ключ позволяет создавать подписи, соответствующий открытый — проверять их. Подпись связывает авторизацию с конкретным сообщением по правилам алгоритма и не скрывает содержимое. В Bitcoin действительная подпись — часть условий расходования выхода.

Шифрование предназначено для того, чтобы читать содержимое мог лишь обладатель необходимых средств доступа. Аутентифицированное шифрование добавляет обнаружение изменений. В Cuvex криптограммы защищают секреты, подписанные транзакции авторизуют расходование, а шифрованные каналы переносят сообщения. Общая криптография не делает их равнозначными.

Человеческий пароль обычно пропускают через функцию выработки ключа перед криптографическим применением. «AES-256» описывает алгоритм и длину ключа, но не делает предсказуемый пароль стойким. Генерация, реализация, хранение, экран и восстановление участвуют в общей безопасности.

Сложный вид QR-кода также не гарантирует безопасности. Нужно знать его содержимое, создателя и то, что приложение собирается сделать с данными. До принятия действия попросите преподавателя объяснить цель без запроса приватных сведений.

Практика

1. Сопоставьте «обнаружить изменение файла», «скрыть сид-фразу» и «авторизовать платёж» с хешем, шифрованием и подписью.
2. Измените букву вымышленного текста и посмотрите, как меняется хеш. Не используйте секреты для демонстрации.
3. Объясните, как транзакция может одновременно быть публичной и подписанной.

Проверьте себя на практике

Опишите нужную вам гарантию и механизм, который её обеспечивает, не называя «зашифрованным» всё безопасное.

Частый вопрос

Удостоверяет ли хеш отсутствие ошибок в прошивке? Нет. Он идентифицирует байты при надёжном эталоне. Аудит, подпись производителя и физическое испытание отвечают на разные вопросы.

Где сделать паузу

Сохраните три соответствия из упражнения.

Какой механизм скрывает содержимое секрета?

1. Опубликовать имя файла.
2. Подписать без шифрования.
3. Правильно зашифровать с защищённым ключом.

> **Показать ответ: Правильно зашифровать с защищённым ключом.**
> Ни подпись, ни отпечаток сами по себе не обеспечивают конфиденциальности.

Сид-фраза, дополнительная парольная фраза и пароль

Цель

Не путайте различные секреты и данные доступа в системе.

Разберитесь в теме

Мнемоническая фраза BIP39 представляет энтропию и контрольную сумму словами из словаря. Стандартные длины — 12, 15, 18, 21 или 24 слова. Запоминающаяся фраза, строка песни или выбор слов человеком «наугад» не воспроизводят безопасную генерацию. Контрольная сумма обнаруживает часть ошибок, но не удостоверяет автора сида или то, что он никому больше не известен.

Дополнительная парольная фраза BIP39 участвует в выводе двоичного сида. Иная фраза может открыть совершенно другой, на вид пустой кошелёк. Сообщение о неверной фразе появляется не обязательно. Она не обязана быть словарным словом и не является буквально двадцать пятым словом.

Пароль криптограммы Cuvex защищает хранимый секрет, пароль Desk — локальное хранилище компьютера. PIN-код сопряжения авторизует сеанс связи. Ключ чата (Clave Chat) восстанавливает идентичность в мессенджере. Ничто из перечисленного не равнозначно сид-фразе, и знание одного значения не позволяет восстановить все остальные.

Хранение сид-фразы и дополнительной фразы в одной криптограмме может упростить восстановление, но устраняет разделение для того, кто её расшифрует. Раздельное хранение повышает требования к вам и наследникам. Решение нужно документировать и испытывать, а не выбирать по оценке преподавателя о «более продвинутом» варианте.

Практика

1. Подготовьте пять бумажных карточек без секретных значений: сид-фраза, дополнительная парольная фраза, пароль Cuvex, пароль Desk и ключ чата (Clave Chat).
2. Запишите, что восстанавливает каждая и что теряется при её утрате.
3. Спланируйте испытание с пустым кошельком. Вводите слова и дополнительную фразу без посторонних, а преподавателю сообщите только результат.

Проверьте себя на практике

Объясните, почему курс никогда не должен просить пароль для «проверки» знаний. Определите, какой секрет нужен вашей процедуре восстановления.

Частый вопрос

Можно ли сбросить дополнительную фразу по почте? В BIP39 такого механизма нет. Кастодиальный поставщик может восстанавливать доступ к учётной записи, но это другая модель.

Где сделать паузу

Запишите «виды данных доступа различены» без указания их значений.

После изменения одной буквы дополнительной парольной фразы BIP39 вы видите нулевой остаток. Как это объяснить?

1. Возможно, из другой парольной фразы выведен иной действительный кошелёк.
2. Сеть удалила средства.
3. Desk должен угадать исходную парольную фразу.

> **Показать ответ: Возможно, из другой парольной фразы выведен иной действительный кошелёк.**
> Другая парольная фраза может дать другой кошелёк без сообщения об ошибке.

M03

Деривация ключей, xpub и дескрипторы

Цель

Разберитесь, как описать кошелёк без передачи возможности расходования.

Разберитесь в теме

Иерархический кошелёк выводит много ключей из одного корня. Путь указывает выбранную ветвь. В mainnet для первого счёта SegWit с одной подписью по BIP84 обычно используется m/84'/0'/0', а для первого счёта с мультиподписью BIP48 P2WSH — m/48'/0'/0'/2'. Апостроф обозначает усиленную деривацию. Изменение счёта, сети или типа скрипта может дать другие адреса из той же мнемонической фразы.

xpub — расширенный открытый ключ, позволяющий вывести определённые дочерние открытые ключи. Это не пароль для расходования, однако он может позволить наблюдать семейство адресов. Отпечаток корня — короткий идентификатор для сопоставления записей. Он не гарантирует идентичность и не исключает коллизий.

Дескриптор описывает построение скриптов и адресов через тип скрипта, ключи, происхождение и деривации. Дескриптор watch-only с открытыми ключами обеспечивает наблюдение, но не подписание. Само название «дескриптор» не гарантирует открытости содержимого: некоторые форматы допускают закрытые ключи. Никогда не загружайте реальный дескриптор в курс.

Для восстановления мультиподписи обычно нужна вся политика, а не только слова одного подписанта. Храните порог, состав участников, xpub, пути, сеть, тип скрипта и сведения для поиска адресов. Контрольная сумма дескриптора помогает обнаружить ошибки переписывания, но не удостоверяет участников.

Практика

1. Прочитайте вымышленный путь и объясните назначение, монету, счёт и ветвь. Не вводите реальные ключи.
2. Различайте адрес получения, xpub участника и полный дескриптор.
3. Подготовьте личную карточку восстановления с названиями незаполненных полей и отдельным указанием места хранения документации.

Проверьте себя на практике

Объясните, почему пустой восстановленный кошелёк не доказывает утрату: нужно проверить сеть, дополнительную фразу, скрипт, счёт, путь и поиск адресов.

Частый вопрос

Можно ли без последствий публиковать xpub? Сам по себе он обычно не даёт возможности тратить, но раскрывает приватную информацию и может увеличивать другие риски в отдельных криптографических сочетаниях.

Где сделать паузу

Сохраните в курсе только карточку без чувствительных значений.

Каких данных может не хватить при попытке восстановить кошелёк с мультиподписью только по одной сид-фразе?

1. Цвета устройства.
2. Политики и открытых ключей остальных участников.
3. Пароля от социальной сети.

> **Показать ответ: Политики и открытых ключей остальных участников.**
> Для восстановления скриптов, помимо порогового числа закрытых ключей, нужна полная политика.

Выбор кошелька и модели хранения

Цель

Сравнивайте инструменты по функциям, необходимому доверию и восстановлению.

Разберитесь в теме

Кошелёк — набор инструментов для описания, наблюдения и, когда это предусмотрено, авторизации расходов. Горячий кошелёк хранит возможность подписания в подключённой среде. Изолированное подписывающее устройство отделяет секреты от компьютера, обращающегося к сети. Кошелёк watch-only располагает открытыми данными для наблюдения и подготовки, но для подписи ему нужна другая система.

При хранении у третьей стороны счёт может отражать требование к компании. При самостоятельном хранении техническая возможность расходовать находится у вас единолично или совместно с другими. Восстановление по почте и возможность заблокировать вывод обычно указывают на первую модель. Оценивайте варианты с учётом разного распределения ответственности.

Сравните поддержку сетей и скриптов, экранную проверку, копии, обновление, совместимость, обслуживание, обращения к поставщикам и понятность ошибок. Списка монет или качества корпуса недостаточно. Подписывающее устройство не помешает вам принять неверный адрес, если вы его не проверите.

В Cuvex секреты защищаются криптограммами, а организация и запросы вынесены в Desk. Для этой модели нужно сохранять криптограмму и средства разблокировки. Защита от потери устройства не означает возможности восстановления при утрате всех копий или паролей. Изучите процедуру целиком до перевода имущества.

Практика

1. Сравните в таблице Cuvex, горячий кошелёк и биржу: кто подписывает, кто видит запросы, кто восстанавливает доступ и что произойдёт после закрытия компании.
2. Выберите два критерия, которые нужно подтвердить свидетельствами, а не рекламой.
3. Проверьте, что учебная среда не использует ключи ваших реальных накоплений.

Проверьте себя на практике

Обоснуйте выбор для конкретного случая, не объявляя инструмент неуязвимым.

Частый вопрос

Делает ли аппаратный кошелёк все транзакции конфиденциальными? Нет. В первую очередь он защищает возможность подписания и часть проверки. Цепочка, запросы и контрагенты по-прежнему создают сведения.

Где сделать паузу

Сохраните таблицу критериев без названий счетов.

Что может правильно настроенный кошелёк только для наблюдения с открытыми ключами?

1. Наблюдать и готовить операции без возможности самостоятельно их подписывать.
2. Заменить потерянную сид-фразу.
3. Гарантировать анонимность.

> **Показать ответ: Наблюдать и готовить операции без возможности самостоятельно их подписывать.**
> Возможности наблюдения и авторизации можно разделить.

Резервные копии, из которых можно восстановиться

Цель

Спроектируйте полную копию и проверьте восстановление до того, как придётся на неё полагаться.

Разберитесь в теме

Полезная копия восстанавливает возможность действовать, не просто файл. Для одиночной подписи могут потребоваться мнемоническая и дополнительная фразы, данные деривации. Для мультиподписи нужны также политика и достаточно подписантов. Для Desk может понадобиться зашифрованная копия и пароль. Восстановление идентичности чата не равнозначно возврату истории сообщений.

Избыточность защищает от случайной утраты, а разделение — от совместной компрометации. Две копии на разных носителях и в разных местах могут снизить риск связанных отказов. Каждая дополнительная копия требует контроля доступа, учёта и проверки. Имена файлов и метки не должны выдавать имущество или облегчать поиск всех компонентов.

Испытание должно подтвердить ранее проверенный адрес и, в учебной среде, возможность подписать контролируемую операцию. Открытие файла не доказывает принадлежности нужному кошельку. Не проверяйте копию вводом рабочей сид-фразы в произвольный компьютер.

Задокументируйте охват и исключения каждой копии. Смена текущего пароля не обновляет старые копии автоматически. Резервные копии с раскрытым старым паролем всё ещё уязвимы. Удаление файла с современного носителя не гарантирует удаления всех его копий и версий.

Практика

1. Заполните личную таблицу: объект, содержимое, соответствующий пароль, независимое место, дата проверки и ответственный.
2. Восстановите учебную копию в отдельной среде. Проверьте сеть, первый адрес и деривацию.
3. Смоделируйте потерю компьютера, затем потерю устройства. Определите, какая процедура меняется.

Проверьте себя на практике

Восстановите тестовый сценарий без импровизированной помощи и объясните, каких сведений всё ещё не хватило бы в другом случае.

Частый вопрос

Входит ли в общую копию Desk абсолютно всё? Так считать нельзя. В рассмотренной версии история и сеансы чата не включены. Политика мультиподписи и закрытые ключи выполняют разные функции.

Где сделать паузу

Запишите дату и результат испытания, но никогда не содержимое копии.

Что произойдёт с прежней копией после смены пароля Desk?

1. Она обновится сама.
2. Она автоматически лишится шифрования.
3. Она сохранит защиту и пароль, с которыми была создана.

> **Показать ответ: Она сохранит защиту и пароль, с которыми была создана.**
> Прежние копии — самостоятельные объекты.

M04

Знакомство с Original и BIT

Цель

Выберите правильную процедуру для модели и версии устройства.

Разберитесь в теме

Original переносит криптограммы и поддерживаемые операции на картах NFC, а для обновления использует Bluetooth. USB-C документированной модели служит для питания. BIT обменивается файлами по USB-C и поддерживает биометрию в требующих её криптограммах. Не переносите инструкции Original по NFC или Bluetooth на BIT.

Кроме настроек, на устройстве есть шифрование, расшифрование, создание кошельков и подписание. Original клонирует карты, BIT работает с файлами на USB-носителе. Надписи, языки и способы входа зависят от версии. Новый пункт «Проверка политик» на BIT ведёт к поддерживаемой процедуре, не меняя того, кто авторизует операции.

Рассмотренные в издании версии источников: Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 и Mirror beta.12.12. Подпись, распространение и физическую приёмку каждого сочетания нужно подтвердить с командой. Не заменяйте свою прошивку неподписанным бинарным файлом из инженерной сборки.

До использования проверьте происхождение, пломбы, внешний вид и версию. Прослеживаемость и подпись обновления помогают против отдельных угроз, но не заменяют остальных проверок. При следах вмешательства или неожиданной версии остановите настройку и обратитесь в поддержку по проверенному каналу.

Практика

1. Определите модель и запишите отображаемую версию, не фотографируя секреты.
2. Найдите шифрование, расшифрование, создание кошелька, PSBT и настройки. Для знакомства с меню не запускайте удаление или обновление.
3. Выберите в курсе ветвь Original или BIT и сохраняйте этот выбор во время упражнения.

Проверьте себя на практике

Объясните, как операция поступает на вашу модель и возвращается с неё и какой носитель следует защищать от перезаписи.

Частый вопрос

Всегда ли BIT безопаснее для любого человека? Модели предлагают разные способы работы. Ответ зависит от угроз, восстановления и правильного использования.

Где сделать паузу

Сохраните модель и версию в локальном блокноте. Курсу нужна только выбранная модель.

У вас BIT, а руководство требует записать NFC-карту с помощью самого устройства. Как вы поступите?

1. Проверю соответствие руководства своей модели и воспользуюсь поддерживаемой процедурой USB.
2. Принудительно установлю обновление для Original.
3. Отправлю сид-фразу на телефон.

> **Показать ответ: Проверю соответствие руководства своей модели и воспользуюсь поддерживаемой процедурой USB.**
> Инструкции должны соответствовать фактическому способу обмена данными конкретной модели.

M04

Генерация сид-фразы с помощью физической энтропии

Цель

Разберитесь в генерации и отработайте процедуру, не превращая учебные данные в собственные ключи.

Разберитесь в теме

Энтропия означает непредсказуемость. Подходящие кубики дают энтропию, если порядок установлен до броска, а алгоритм преобразования корректен. Отклонённые результаты повторяйте строго по процедуре. Подмена максимальным числом или выбор другого слова искажает распределение.

Рассмотренная процедура Cuvex использует монету и четыре кубика. Функция преобразования умножает результат монеты на 1 296 и прибавляет шестеричное число, цифры которого равны выпавшим значениям кубиков минус один. Допускаются индексы от 0 до 2 047. Если результат вне словаря, заново бросают и монету, и все четыре кубика. Повторный бросок только кубиков при прежнем результате монеты вносит смещение. Так устроен рассмотренный исходный код. Экраны и полную процедуру проверяют в каждой распространяемой прошивке.

Это отличается от выбора любимых слов. Не используйте публичную демонстрацию для хранения средств. Любая сид-фраза в учебном материале считается известной другим. Последнее слово и проверка должны формироваться полным алгоритмом устройства. Не дополняйте мнемоническую фразу вручную.

Подготовьте место без камер, активных голосовых помощников, записи экрана и наблюдателей. При вводе и проверке секрета преподаватель должен остановиться. Он может объяснить процедуру заранее и после неё задать вопросы о процессе, не слыша результатов бросков и слов.

После генерации проверьте резервную копию, зашифруйте её согласно модели и испытайте восстановление пустого кошелька. Контрольный адрес помогает подтвердить согласованность, не раскрывая сид компьютеру. Если принимаются противоречащие инструкции значения или появляются неожиданные слова, прекратите использование и запишите только версию, экран и ошибку.

Практика

1. На тренировке следуйте шагам устройства с данными без средств. Заранее зафиксируйте порядок кубиков и не меняйте результаты.
2. Повторяйте отклонённый ввод по указанию экрана, не подгоняя значения.
3. Проверьте содержимое без посторонних, создайте копию и убедитесь, что можете восстановить тот же учебный кошелёк.

Проверьте себя на практике

Объясните, почему физическая энтропия, правильное преобразование и секретность результата — три разных требования.

Частый вопрос

Можно ли продиктовать броски ИИ для проверки алгоритма? Для сид-фразы, которую собираетесь использовать, нельзя. В обучении применяются другие синтетические примеры.

Где сделать паузу

Завершите работу в безопасном состоянии устройства. Не оставляйте сид-фразу на экране на время перерыва.

Прошивка отклонила введённый результат броска. Какое действие соответствует процедуре?

1. Выбрать слово вручную.
2. Повторить бросок по указанию устройства, не искажая распределение.
3. Уменьшать число, пока оно не будет принято.

> **Показать ответ: Повторить бросок по указанию устройства, не искажая распределение.**
> Отбрасывание результатов является частью преобразования энтропии. Нельзя произвольно подменять их.

M04

Шифрование и расшифрование секрета с помощью Cuvex

Цель

Создайте учебную криптограмму и проверьте её восстановление.

Разберитесь в теме

Выберите правильный доступный тип содержимого: BIP39, SLIP39, Monero или текст. Это разные форматы. Шифрование текста SLIP39 не делает Cuvex подписывающим устройством для любой сети, использующей такой текст. Хранение секретов и реализация протоколов подписания имеют разный охват.

Чтобы исключить попадание секрета на подключённое оборудование, вводите содержимое прямо на устройстве. Импорт с телефона или компьютера уже мог раскрыть исходный секрет до последующего шифрования. На экране предварительной проверки ищите ошибки слов, порядка, регистра и полей.

Пароль криптограммы должен быть длинным, уникальным и восстанавливаемым по вашему плану. Рассмотренная клавиатура создания вмещает 40 символов. Проверка требует не менее 12, прописную и строчную буквы ASCII, цифру и распознаваемый символ. Не переносите диапазон Desk от 12 до 1 024 символов на клавиатуру Cuvex. У Desk иная политика. Для других полей восстановления пределы могут отличаться. Проверьте процедуру и версию.

На Original пишите на подходящую пустую карту и удерживайте её до подтверждения. На BIT сохраните файлы процедуры USB, включая необходимые биометрические компоненты. Не переименовывайте и не объединяйте их по догадке. После этого проверьте чтение и расшифрование на устройстве, не сообщая секрет преподавателю.

Практика

1. Зашифруйте учебный текст, созданный для упражнения, без данных доступа и экономической ценности.
2. Определите носитель и полученный объект. Приватно запишите псевдоним и назначение.
3. Снова начните расшифрование, проверьте текст на доверенном экране и закройте отображение по завершении.

Проверьте себя на практике

Различайте правильное содержимое, успешную запись и успешное восстановление. Сообщение «Файл скопирован» не доказывает все три.

Частый вопрос

Является ли псевдоним карты паролем? Нет. Это организационная информация. Не указывайте остатки и описания, по которым легко определить ваше имущество.

Где сделать паузу

Не оставляйте расшифрованное содержимое на виду. Отметьте только успех или неудачу испытания.

Как лучше всего убедиться, что из тестовой криптограммы можно восстановить содержимое?

1. У неё красивое имя.
2. Файл существует в двух папках.
3. Прочитать и расшифровать её по правильной процедуре и проверить содержимое без посторонних.

> **Показать ответ: Прочитать и расшифровать её по правильной процедуре и проверить содержимое без посторонних.**
> Одно лишь наличие копии не доказывает её пригодности или соответствия нужному содержимому.

Пороги доступа к зашифрованным данным и биометрия

Цель

Отличайте совместную защиту секрета от мультиподписи Bitcoin.

Разберитесь в теме

Криптограмма с несколькими паролями регулирует, кто может её расшифровать. Кошелёк Bitcoin с мультиподписью определяет, какие ключи должны авторизовать расходование в сети. Совместно зашифрованный секрет может относиться к кошельку с одной подписью, а у каждого подписанта мультиподписи может быть индивидуальная криптограмма.

Если несколько человек вместе открывают одну сид-фразу, а она позволяет тратить самостоятельно, порог в цепочке по-прежнему равен одному ключу. После раскрытия кто-то может сохранить её. Не описывайте схему так, будто для каждого платежа обязательно согласовывать несколько подписей.

Биометрия BIT добавляет условие доступа в использующих её форматах. Палец не является сид-фразой или универсальной заменой пароля. Учитывайте травмы, изменения отпечатка, поломку, доступность устройства и наследование. Сохраните и испытайте документированное восстановление конкретной криптограммы до того, как будете на него полагаться.

Экспорт для восстановления может раскрыть секрет на компьютере именно ради аварийного доступа. Наличие функции не делает компьютер эквивалентом изолированного устройства. Сохраняйте изоляцию при обычной работе. Подходите к локальному восстановлению осознанно и планируйте последующий перенос при раскрытии.

Практика

1. Изобразите две политики: «два пароля для открытия одной сид-фразы» и «два ключа из трёх для расходования».
2. В испытании без средств определите, какие файлы нужны для биометрической копии и где проверяется возможность её восстановления.
3. Смоделируйте недоступность одного человека и определите, позволяет ли порог продолжить.

Проверьте себя на практике

Объясните, кто может узнать секрет и кто сможет авторизовать трату после расшифрования.

Частый вопрос

Можно ли исключить участника сменой метки? Нет. Отличайте организационное изменение, новую защиту секрета и новую политику расходования.

Где сделать паузу

Сохраните схему без реальных имён и биометрических данных.

Три человека открывают двумя паролями криптограмму с одной сид-фразой кошелька с одной подписью. Сколько ключей требует Bitcoin для расходования?

1. Один, если такова политика кошелька.
2. Два, потому что для файла нужны два пароля.
3. Три, по числу людей.

> **Показать ответ: Один, если такова политика кошелька.**
> Порог для расшифрования не изменяет скрипт, управляющий средствами.

M04

Клонирование, хранение и проверка копий

Цель

Создайте резервирование, не уничтожив единственную действительную копию.

Разберитесь в теме

Клонирование копирует зашифрованные данные. Оно не создаёт нового остатка или сида и не делает копию независимой от раскрытого пароля. Одинаковые копии помогают при утрате носителя, а не при компрометации исходного секрета. Поэтому восстановление и перенос на новые ключи решают разные задачи.

На Original различайте карту криптограммы и транспортную карту PSBT. Операционный носитель можно использовать повторно по процедуре, но карта с резервной копией не должна становиться таким носителем. Если карта с криптограммой отклонена, не обходите защиту и не удаляйте заголовок вручную.

На BIT копия должна сохранять необходимый комплект и связи между файлами. Файловый менеджер может показать завершение передачи без гарантии проверки содержимого или завершения операции устройством. Дождитесь указанных состояний и проверьте копию контролируемым восстановлением.

Ведите личную опись с нейтральными идентификаторами, версией формата, датой и результатом последнего испытания. Разделите не менее двух копий с учётом выявленных угроз. Не загружайте резервные копии в поддержку для диагностики. Предоставляйте очищенные метаданные и коды ошибок.

Практика

1. Создайте на другом носителе копию учебной криптограммы по правильной процедуре.
2. Отключите исходный носитель и восстановите тестовый текст из копии.
3. Раздельно задокументируйте действия при потере, повреждении файла и раскрытии пароля. Это разные процедуры.

Проверьте себя на практике

Укажите испытанную копию и объясните, почему исходная не была перезаписана.

Частый вопрос

Можно ли удалить оригинал, увидев второй файл? Сначала проверьте восстановление и охват. Удаление должно следовать плану, а не зависеть просто от количества копий.

Где сделать паузу

Уберите носители до закрытия сеанса и не смешивайте карты с используемыми в учебных платежах.

Если кто-то знает пароль и получил копию криптограммы, что даст создание ещё трёх клонов?

1. Отзовёт копию злоумышленника.
2. Добавит резервные копии, но не отзовёт уже полученный доступ.
3. Автоматически изменит сид-фразу Bitcoin.

> **Показать ответ: Добавит резервные копии, но не отзовёт уже полученный доступ.**
> Дублирование не устраняет уже произошедшую компрометацию.

M05

Установка и защита Cuvex Desk

Цель

Откройте установку проверенного происхождения и защитите локальное хранилище.

Разберитесь в теме

Выберите пакет системы и архитектуры: macOS Intel или Apple Silicon, Windows x64 или ARM64, Linux x64 или ARM64 согласно доступному выпуску. Архив исходников, пакет для Manager и клиентский установщик — разные поставки. Курс не должен направлять учащегося к закрытому пакету подписания.

Проверьте происхождение и проверки системы. Инженерная подпись Windows сама по себе не обеспечивает публичного доверия к издателю. На Mac подпись приложения, нотаризация и проверка при открытии — отдельные средства. Не отключайте общую защиту по звонку якобы из поддержки. При неожиданном предупреждении сохраните текст и используйте официальный канал.

Desk создаёт локальное хранилище, зашифрованное паролем. В рассмотренной версии длина нового пароля от 12 до 1 024 символов, а при наличии поля подтверждения значения должны совпадать. Эти пределы не определяют стойкость. Выберите уникальную фразу и не используйте её повторно. Доступная биометрия компьютера упрощает вход и настраивается отдельно.

Настройте блокировку при бездействии и, если применимо, при переходе в фон. Задержка после ошибок и необязательное удаление рассматриваются в руководстве. Не включайте автоудаление на демонстрации. Приложение может работать без обычной учётной записи, однако запросы, чат и загрузки имеют собственные требования и сетевой обмен.

Практика

1. Проверьте платформу, отображаемую версию и происхождение пакета без передачи преподавателю приватных идентификаторов.
2. Создайте учебное хранилище и проверьте блокировку и повторное открытие. Вводите пароль без посторонних.
3. Запланируйте зашифрованную копию и сохраните пароль согласно плану. Не испытывайте повторные блокировки в рабочей среде.

Проверьте себя на практике

Различайте локальный пароль, коммерческую учётную запись и данные доступа подключаемых сервисов.

Частый вопрос

Изменятся ли пароли карт при смене пароля Desk? Нет. Это независимые механизмы защиты. Старые копии также не меняются сами.

Где сделать паузу

Заблокируйте Desk и сохраните номер урока без данных доступа.

Установщик не соответствует архитектуре вашего компьютера. Каков первый шаг?

1. Отключить защиту и принудительно запустить его.
2. Получить подходящий официальный пакет и проверить его требования.
3. Импортировать сид-фразу на сайт, чтобы продолжить.

> **Показать ответ: Получить подходящий официальный пакет и проверить его требования.**
> Совместимость и происхождение проверяют до использования материалов хранения.

M05

Привязка криптограмм и организация счетов WOW

Цель

Привяжите зашифрованную копию и отличайте её от счёта для наблюдения.

Разберитесь в теме

Desk организует криптограммы, привязанные по NFC, USB или из совместимого файла копии. Оформление и псевдоним помогают их узнавать, но не служат криптографическим доказательством идентичности. Карточка показывает источник и распознанные приложением свойства: формат, размер и особенности доступа.

Привязка импортирует или организует совместимый объект. Она не означает расшифрования на компьютере или проверки секрета. WOW — кошелёк наблюдения, привязанный через совместимые открытые данные. Из одного набора секретов возможны разные счета и ветви. Связь должна соответствовать нужному кошельку.

Активируйте или импортируйте счёт с дескриптором или открытыми данными, экспортированными устройством. Проверьте сеть, тип скрипта, отпечаток, путь и контрольный адрес. Название служит организации. Полученный из имени идентификатор не является надёжной анонимизацией, поскольку предсказуемое имя можно угадать.

Рассмотренный Desk хранит ожидающие привязки счета и поддерживает экспорт копий, клонирование и удаление локальных записей. Удаление карты из интерфейса не уничтожает внешние копии и не перемещает средства. «Нет резервной копии» означает, что приложение не подтверждает её по своим критериям, а не что копии нигде не существует.

Практика

1. Привяжите учебную криптограмму выбранным способом и проверьте карточку.
2. Импортируйте совместимый учебный счёт и проверьте его сеть и контрольный адрес без показа ключей преподавателю.
3. Различайте запись криптограммы, счёт WOW и физический носитель. Определите, что исчезнет после локального удаления.

Проверьте себя на практике

Объясните, какие данные нужны Desk для наблюдения и какие при обычном использовании должны оставаться вне компьютера.

Частый вопрос

Гарантирует ли привязка файла .bin, что это моя сид-фраза? Нет. Проверьте происхождение и восстановление. Расширение файла не удостоверяет содержимого.

Где сделать паузу

Сохраните только отметку «тестовая привязка проверена».

Перемещает ли локальное удаление счёта WOW его bitcoin?

1. Нет. Процедура удаляет локальные данные, но не расходует UTXO.
2. Да, оно отправляет их производителю.
3. Оно отменяет любые подписи, сохранённые другим человеком.

> **Показать ответ: Нет. Процедура удаляет локальные данные, но не расходует UTXO.**
> Локальное состояние и состояние цепочки различаются.

M05

Сопряжение Mirror и Desk

Цель

Установите и завершите авторизованное локальное соединение, не путая его коды.

Разберитесь в теме

Mirror выполняет локальные операции с Desk через показанную приложениями процедуру сопряжения с PIN-кодом и QR-кодом. Шестизначный PIN относится к этому сеансу. Это не пароль Desk, не пароль криптограммы и не слово восстановления. Проверьте, какой экран создаёт код и куда его вводить. Не используйте код, присланный незнакомцем.

Начинайте в правильном контексте Desk: привязка, считывание QR, перенос PSBT и работа с прошивкой имеют разные цели. Окно сообщает о поиске, соединении, обнаружении, PIN, QR и действии с картой или файлом. Обнаружение устройства не доказывает завершения всей операции.

Предоставьте нужные системе разрешения: камеру для оптического считывания, Bluetooth или NFC при необходимости. Установка ПО не добавляет телефону отсутствующую аппаратную возможность. В iOS есть различия адаптеров и проверки. Возможность собрать проект не доказывает его распространения и испытания на всех iPhone.

При сбое определите этап: устройство не видно, видно без соединения, PIN отклонён, QR нечитаем, карта не прочитана или ответ не получен. Завершите прежние сеансы, проверьте совместимые версии и разрешения и контролируемо повторите. Ошибочный PIN не оправдывает смену прошивки или ввод сид-фразы в другом месте.

Практика

1. Начните тестовое чтение в Desk и подключите Mirror через локальные экраны.
2. Проверьте назначение до предъявления QR-кода или учебной карты.
3. Отмените сеанс и проверьте, что позднее чтение из прежнего контекста не применяется. Откройте новый сеанс.

Проверьте себя на практике

Опишите этап сбоя и задействованные устройства без передачи активных кодов или чувствительного содержимого.

Частый вопрос

Должен ли Mirror быть подключён постоянно? Это зависит от операции. Не считайте его постоянным сервисом и не предполагайте сохранения авторизации после закрытия или перехода в фон.

Где сделать паузу

Завершите сеанс сопряжения и заблокируйте неиспользуемые приложения.

Что должен сделать преподаватель, если сопряжение прервалось до появления PIN-кода?

1. Попросить сид-фразу.
2. До следующего шага проверить обнаружение устройств, разрешения, сеанс и версии.
3. Считать соединение установленным.

> **Показать ответ: До следующего шага проверить обнаружение устройств, разрешения, сеанс и версии.**
> Диагностика должна учитывать фактически достигнутый этап. Нельзя объявлять подключение успешным без подтверждения.

NFC через Mirror, USB-C и чтение QR-кодов

Цель

Используйте каждый способ передачи данных в соответствии с его назначением и выполняйте предусмотренные проверки.

Разберитесь в теме

Для операций NFC в Cuvex Desktop нужен Cuvex Mirror на совместимом смартфоне, сопряжённом с компьютером по Bluetooth. Cuvex Desktop не поддерживает внешние USB-считыватели NFC. Карта, её формат и ёмкость также должны быть совместимы. Небольшая карта, достаточная для криптограммы, может не вместить PSBT с предыдущими транзакциями. Фактический предел зависит от всего содержимого, а не только от числа получателей. Не используйте резервную карту как транспортную.

При использовании Original приложение Mirror может записать запрос на карту для операций. Устройство обрабатывает запрос и записывает ответ, который Mirror возвращает в Desk. Подтверждение записи не означает получения ответа в Desk. Держите карту неподвижно, пока устройство не покажет результат. Если система отказывает в операции для защиты распознанной криптограммы, соблюдайте отказ.

BIT использует для обмена USB-том или папку. Во время операции том может отключиться и появиться вновь. Desk должен выбрать правильный носитель, проверить ответ и выполнить предусмотренное подтверждение получения. Копирование файла в одноимённую папку на компьютере не означает его доставки на устройство.

Причиной ошибки чтения QR-кода могут быть фокус, блики, размер, движение или плотность кода. Увеличьте изображение, подберите свет и расстояние. Не заменяйте длинный идентификатор его первыми буквами и не принимайте неполную запись. Успешное считывание — лишь начало проверки смысла прочитанных данных.

Практика

1. На учебной схеме покажите запрос, носитель и ответ для Original и BIT.
2. Попробуйте отменить чтение QR-кода без сохранения запоздавших значений. Повторите упражнение с другой целью.
3. Смоделируйте слишком большой файл. Объясните, почему нужно упростить операцию или выбрать совместимый носитель, сохранив все проверки.

Проверьте себя на практике

Укажите, какое устройство подтвердило каждый этап: чтение, запись, проверку, получение или подтверждение получения.

Частый вопрос

Доказывают ли хеш или подтверждение успешного копирования, что получатель bitcoin указан верно? Нет. Проверьте транзакцию и её выходы на подписывающем устройстве.

Где сделать паузу

Уберите резервные карты на хранение и явно обозначьте носитель для передачи данных.

Original сообщает, что ответ записан на карту. Чего ещё не хватает, чтобы считать ответ полученным в Desk?

1. Перекрасить карту.
2. Создать новую сид-фразу.
3. Считать ответ и проверить его в Desk по предусмотренной процедуре.

> **Показать ответ: Считать ответ и проверить его в Desk по предусмотренной процедуре.**
> Успешная запись и успешное получение — разные события.

Публичные поставщики данных и собственный узел

Цель

Выберите источник запросов и разберитесь, какие данные он может раскрывать и какими ограничениями обладает.

Разберитесь в теме

Desk может обращаться к совместимым публичным поставщикам или к настроенному пользователем Bitcoin Core. Поставщик видит получаемые запросы, их последовательность и данные соединения. Отказ от передачи полного xpub уменьшает конкретный вид раскрытия, но скрипты и их хеши также могут связываться друг с другом.

В Desk 9.21 помимо REST и собственного узла можно явно выбрать Blockstream Electrum по TLS. TLS защищает канал от некоторых сетевых наблюдателей, но поставщик всё равно получает запросы. Скрытой ротации, гарантирующей анонимность, нет. Выбор предполагает понимание обмена части конфиденциальности на удобство.

Для Core настройте конечную точку, аутентификацию и кошелёк наблюдения по соответствующему руководству. Не публикуйте порт RPC и не выставляйте его в интернет ради того, чтобы приложение «увидело» узел. Ограничьте доступ доверенной средой и используйте защищённый транспорт. Пароль RPC преподавателю не сообщают.

Первичная синхронизация и повторное сканирование могут занимать время. Ход работы не означает досрочного успеха. Desk сохраняет фоновую задачу, закрытие представления не останавливает узел. Документированный минимальный исторический диапазон не гарантирует нахождения более ранней активности. Для старого кошелька проверьте дату импорта и фактический охват сканирования.

Поиск адресов основан на истории, а не на положительном остатке. Адрес, с которого всё потрачено, остаётся использованным. В рассмотренной мультиподписи для каждой ветви и участника применяется промежуток в 20 последовательных адресов без истории, а также ограничения на выдачу адресов. Не переносите этот лимит на все кошельки.

Практика

1. Выберите учебный источник и объясните, какую информацию он может видеть.
2. Проверьте дату последней синхронизации, сеть и ход работы. При HTTP 429 выдержите паузу и не меняйте поставщика без осознанного решения.
3. Смоделируйте кошелёк с нулевым остатком и старой историей. Проверьте, чем «ноль» отличается от «не использовался».

Проверьте себя на практике

Определите, удовлетворяет ли источник требованиям проверки и конфиденциальности, и распознавайте неполный результат.

Частый вопрос

Делает ли собственный узел меня анонимным? Нет. Он уменьшает зависимость от чужих запросных сервисов, но нужно учитывать соединение, контрагентов, публикацию и другие метаданные.

Где сделать паузу

Запишите только тип поставщика и необходимость завершения сканирования.

На адресе нулевой остаток, но раньше на него приходили и с него тратились средства. Как учитывать его при поиске кошелька?

1. Как адрес с историей.
2. Как ни разу не использованный адрес.
3. Как недействительный адрес.

> **Показать ответ: Как адрес с историей.**
> Об использовании адреса судят по истории операций, а не по текущему остатку.

Получение bitcoin и проверка адреса

Цель

Создайте запрос на получение и проверьте его до передачи.

Разберитесь в теме

Откройте нужный счёт WOW, проверьте сеть и политику. Создайте или восстановите запрос получения. Для учёта можно указать назначение, наблюдателя и ожидаемую сумму. Это локальные поля, и ожидаемая сумма не мешает отправителю перевести иную.

Проверьте адрес доступным на устройстве способом и в контексте кошелька. Если эта процедура не проверена физически для вашего сочетания оборудования, остановитесь на симуляции и передайте вопрос на проверку до получения существенных средств. Два экрана с одним источником не дают независимой проверки.

Когда процедура позволяет, используйте новый адрес для новых отношений по получению платежа. В рассмотренной мультиподписи показанные адреса не переназначаются и не истекают: плательщик может воспользоваться ими позднее. Достигнув предела последовательных новых адресов без истории, восстановите подходящий прежний запрос и разберитесь в причине лимита. Не отматывайте индексы.

После передачи запроса наблюдайте за поступлением по своему источнику проверки. Письмо, квитанция биржи или снимок плательщика не доказывают расчёт. Проверьте сеть, txid, выход, сумму и подтверждения с учётом риска. Если ваш план предполагает приватность таких запросов, не вводите адрес в публичный обозреватель ради удобства.

Практика

1. Создайте запрос в лаборатории, проверьте счёт и сеть и объясните проверку адреса.
2. Задайте вымышленную метку и после закрытия представления снова найдите тот же запрос.
3. Смоделируйте поступление другой суммы и решите, как сверить его без изменения истории.

Проверьте себя на практике

Различайте созданный адрес, проверенный адрес, переданный запрос и подтверждённое поступление.

Частый вопрос

Перестаёт ли старый адрес работать при создании нового? Обычно нет. Сохранение поиска адресов и журнала запросов помогает не упустить запоздалые платежи.

Где сделать паузу

Сохраните состояние учебного запроса, не передавая преподавателю его содержимое.

Плательщик прислал снимок экрана с надписью «Вывод завершён». Что вы проверите перед признанием платежа?

1. Только качество снимка.
2. Соответствующий выход и необходимые подтверждения по надёжному сетевому источнику.
3. Пароль плательщика.

> **Показать ответ: Соответствующий выход и необходимые подтверждения по надёжному сетевому источнику.**
> Коммерческая квитанция или снимок экрана не заменяют проверку платежа.

M06

Метки, заморозка и выбор UTXO

Цель

Готовьте входы, избегая случайного объединения разных источников.

Разберитесь в теме

Метки сохраняют отсутствующий в цепочке контекст: источник, контрагента, цель и ограничения использования. В Desk у метки UTXO и заметки к адресу могут различаться длина и назначение. «Клиент А» полезно, а полное имя или номер документа создают излишне чувствительную запись.

Заморозка UTXO в Desk исключает его из некоторых локальных вариантов выбора. Она не блокирует расходование в Bitcoin, не меняет скрипт и не мешает другому приложению с ключами потратить выход. Общий и доступный остатки могут различаться. Проверьте, заморожен ли выход, зарезервирован ли черновиком или уже потрачен.

Автовыбор оптимизирует по алгоритму и его контексту, но не обязательно знает ваши приватные связи. Для конкретного платежа подумайте, можно ли выбрать выход из того же контекста вместо объединения накоплений, зарплаты и бизнеса. Разделение требует последовательности в дальнейшем, а не только удобных меток.

Экспорт меток BIP329 облегчает хранение и перенос. Сам формат не шифрует. Desk предлагает для экспорта зашифрованную оболочку; отличайте защищённый файл от совместимого открытого текста. Перед перезаписью при импорте проверьте соответствие кошельку и обработку состояний заморозки.

Практика

1. Пометьте три синтетических UTXO как накопления, деятельность и пожертвование.
2. Заморозьте один выход и проверьте разницу между наблюдаемым остатком и доступным для выбора.
3. Экспортируйте учебные метки с паролем, импортируйте в копию и проверьте результат без реальных приватных данных.

Проверьте себя на практике

Обоснуйте выбор входов издержками и раскрытием связей. Учитывайте локальный характер заморозки.

Частый вопрос

Передаётся ли метка получателю при платеже? Локальная метка сама по себе не передаётся. Она может раскрыться при экспорте, обмене файлами, использовании другого сервиса или добавлении в сообщение.

Где сделать паузу

Сохраните учебные метки и состояние заморозки.

Что происходит при заморозке UTXO в Desk?

1. В сети создаётся блокировка на уровне консенсуса.
2. UTXO переводится на специальный счёт.
3. Приложение применяет локальное ограничение на выбор UTXO.

> **Показать ответ: Приложение применяет локальное ограничение на выбор UTXO.**
> Возможность расходования с помощью других копий ключей сохраняется.

M06

Подготовка и проверка платежа

Цель

Составьте понятную PSBT и определите все издержки и выходы.

Разберитесь в теме

Выберите счёт, доступные входы, получателей и суммы. Проверьте источник запроса. После вставки или сканирования сверьте полный адрес и сеть: буфер обмена или изображение можно подменить. При возможности полной проверки не полагайтесь лишь на первые и последние символы.

Выберите ставку и проверьте абсолютную комиссию, оценочный размер, общую сумму и сдачу. При отправке всего остатка Desk вычитает комиссию из доступного. Если в чате чистая сумма ниже запрошенной, частичную оплату выбирают осознанно. Исходный запрос не меняют для сокрытия разницы.

Проверьте, мала ли сдача или её выхода нет. Принадлежность выхода, помеченного собственным, сверяют с политикой, а не с названием от координатора. При нецелесообразной сдаче пересмотрите перевод всего остатка или добавьте совместимый вход. Не допускайте незаметного превращения сдачи в несоразмерную комиссию.

PSBT — формат передачи сведений и подписей. Он сам по себе не гарантирует конфиденциальности или подлинности происхождения. В нём могут быть предыдущие транзакции, открытые ключи, пути и метаданные. В рассмотренных прошивках Final профиль мультиподписи использует PSBT v0/BIP174. «Транзакция версии 2» не означает «PSBT версии 2».

Практика

1. В симуляторе подготовьте платёж со входом 120 000, получателем на 70 000 и комиссией 1 000 sat.
2. Перечислите все выходы и объясните сдачу 49 000 sat. Повторите для перевода всего остатка.
3. Отмените черновик и объясните, что отменено локально. Не используйте симулятор для подписания или публикации.

Проверьте себя на практике

Перед экспортом объясните, что входит и выходит, кто получатель, каковы издержки и какой авторизации не хватает.

Частый вопрос

Можно ли отправить весь показанный остаток? Только если приложение рассчитает допустимую чистую сумму отправки с учётом комиссий. В остаток могут входить недоступные для расходования средства.

Где сделать паузу

Сохраните или отмените учебный черновик. Никогда не помещайте реальную PSBT на портал курса.

На экране указано «transaction version 2». Доказывает ли это, что файл имеет формат PSBT v2?

1. Нет. Это разные поля версии.
2. Да, всегда.
3. Это доказывает использование Taproot.

> **Показать ответ: Нет. Это разные поля версии.**
> BIP370 различает версию контейнера и версию транзакции.

Подписание с помощью Original и BIT

Цель

Пройдите ветвь подписания для каждой модели и получите ответ, связанный с нужной операцией.

Разберитесь в теме

Для Original передайте PSBT с помощью Cuvex Mirror и транспортной карты, предусмотренной совместимой процедурой. На устройстве считайте запрос, предоставьте криптограмму и разблокируйте её без посторонних. Проверьте все выходы, суммы, сдачу и комиссию. Ответ записывается на карту, после чего его считывают и проверяют в Desk. Успешная запись на карту не заменяет этот обратный этап.

Для BIT выберите нужный том и передайте запрос по USB-C. Пока вы работаете с устройством, локальная служба Desk обслуживает обмен. Предоставьте криптограмму по указаниям на экране и проверьте операцию на BIT. Команда «Получить с BIT» импортирует ответ. Desk проверяет и сохраняет его до подтверждения получения. Если связь оборвалась, восстановите именно эту операцию, не выбирая другую по внешнему сходству.

В прошивках Final при мультиподписи проверяют сводку и обязательные выходы, применимые предупреждения и три завершающих подтверждения действия «Подписать PSBT». Необязательный расширенный просмотр позволяет изучить дополнительные параметры. Выбор «Нет» не отменяет обязательные проверки. Независимая проверка политики представляет собой отдельную процедуру, и её выводы ограничены предметом этой проверки.

Для подписания нужна совместимая криптограмма с проверяемой подлинностью. Возможность восстановить секрет из архивной копии сама по себе не делает её пригодной для подписания. Если устройство предупредило о старой копии с неподтверждённой подлинностью, восстановите и проверьте секрет и создайте новую копию до подписания. Не редактируйте заголовки и не обходите отказ.

Если не совпадает адрес, неожиданна комиссия, не хватает данных, указана другая сеть или устройство отклоняет политику, отмените операцию. Не подтверждайте её под давлением из-за окончания звонка. ИИ не нажимает кнопки, не выполняет окончательное подтверждение и не объявляет подписанным то, что вы не проверили.

Практика

1. Пройдите процедуру для своей модели с пустым кошельком или в лаборатории, прошедшей физические приёмочные испытания.
2. Смоделируйте остановку перед последними подтверждениями и объясните, почему она не равна авторизации.
3. Проверьте возврат ответа, его связь с черновиком, а для BIT также состояние получения и подтверждения получения.

Проверьте себя на практике

Опишите процедуру без раскрытия учётных данных и различайте подтверждение на устройстве, импорт ответа и передачу транзакции в сеть.

Частый вопрос

Знает ли автономное устройство, что мои входы ещё не израсходованы? Самостоятельно проверить текущее состояние цепочки оно не может. Приложение должно сверить итоговую транзакцию со своим сетевым источником.

Где сделать паузу

Если вы прерываете подписание, отмените операцию или оставьте её в явно обозначенном состоянии ожидания согласно процедуре. Секретные данные не должны оставаться на виду.

BIT выполнил подписание, но Desk не подтвердил получение. Из какого состояния следует исходить?

1. Платёж окончательно передан в сеть.
2. Ответ ожидает получения или проверки. Восстановите ту же операцию.
3. Кошелёк потерян.

> **Показать ответ: Ответ ожидает получения или проверки. Восстановите ту же операцию.**
> Подписание, получение и передача в сеть — отдельные этапы.

Завершение и передача транзакции в сеть, устранение сбоев

Цель

Завершите платёж без дублирования и определяйте сбои по этапу.

Разберитесь в теме

Импортировав подпись, Desk должен проверить её соответствие черновику и намерению. При мультиподписи порог ещё может не быть достигнут. При одиночной подписи импорт тоже не отменяет проверку. Если все условия выполнены, завершение создаёт транзакцию, готовую к передаче в сеть.

Передавайте в сеть только после последней проверки. Ответ сервера или txid отражает результат запроса; дальнейшее наблюдение должно подтвердить принятие и состояние цепочки. Если приложение не получило ответ, проверьте перед повтором. Не создавайте новый платёж для устранения проблемы отображения.

Для ожидающего платежа проверьте ставку, действительность, конфликты и реальную возможность RBF. Если изменились политика или получатель, новому предложению необходимы новые надлежащие подписи. Локальная отмена не уничтожает сохранённые другим человеком подпись или транзакцию и не отменяет подтверждённое.

Разделяйте этапы: подготовка, транспорт, разблокировка, проверка, подпись, возврат, валидация, завершение, распространение и подтверждение. Запишите систему, версию, модель, этап, примерное время и код ошибки. Диагностика приложения рассчитана на исключение чувствительных данных, но проверьте её перед отправкой. Не прикладывайте копии, QR, ключ чата (Clave Chat) или данные доступа.

Практика

1. Расположите состояния вымышленного платежа по порядку и укажите место безопасной остановки.
2. Разберите три сбоя: недостаток средств, неполученный ответ USB и разрыв соединения при передаче в сеть.
3. Составьте обращение с синтетическими данными и проверяемым ожидаемым результатом.

Проверьте себя на практике

Определите, чьё действие ещё требуется: учащегося, устройства, координатора или сети. Избегайте лишнего второго платежа.

Частый вопрос

Исправляется ли FIRMWARE_CAPABILITY_REQUIRED сменой прошивки наугад? Нет. В документированном случае для распознавания сборки Final потребовалось исправление каталога Desk. Проверьте версию и профиль до изменений устройств.

Где сделать паузу

Сохраните состояние и следующее действие. Если вне лаборатории вы передали реальную транзакцию, ведите её учёт в личных документах.

Какое из этих действий само по себе может отменить уже подтверждённую транзакцию?

1. Удалить локальный черновик.
2. Закрыть Mirror.
3. Ни одно из этих действий.

> **Показать ответ: Ни одно из этих действий.**
> Локальное удаление не переписывает цепочку и не отзывает уже распространяющиеся авторизации.

Какие сведения видны в Bitcoin

Цель

Различайте публичные данные, выводы наблюдателей и сведения, добавленные вне цепочки.

Разберитесь в теме

Базовая цепочка Bitcoin публична: можно анализировать скрипты и представимые адреса, значения, отношения входов и выходов, положение в блоках. Ваше имя не обязательно указано, однако идентифицированная покупка, опубликованный счёт или переданный адрес могут связать вас с историей.

Псевдонимность означает работу с идентификаторами, которые сами по себе не выражают гражданскую личность. Анонимность требует множества и условий неразличимости, не возникающих от установки приложения. Конфиденциальность контекстна: магазин знает ваш платёж, биржа может знать вывод, сервер видит запросы, а человек — ваши устройства.

Разделяйте факты и выводы. «Этот выход потрачен в той транзакции» проверяется по цепочке. «Все входы принадлежат одному человеку» — эвристика, способная ошибиться. Внесетевое установление личности может усилить гипотезу, не превращая каждое толкование в достоверный факт.

Повторное использование адреса облегчает объединение активности. Совместное расходование UTXO разных контекстов может их связать. Раскрытие xpub даёт более широкий обзор, чем показ одного адреса. Передача txid может показать и другие выходы и связи, которые не требовались получателю.

Практика

1. Отметьте в вымышленной транзакции публичные данные и собственные метки.
2. Добавьте счёт с именем и опишите возникшую связь.
3. Составьте обращение для устранения ошибки без адреса, дескриптора или остатка.

Проверьте себя на практике

Различайте «это наблюдается» и «это выводится», объясняя, какого свидетельства не хватает.

Частый вопрос

Становлюсь ли я анонимным, никогда не повторяя адреса? Нет. По-прежнему важны выбор входов, сдача, запросы, контрагенты и другие метаданные.

Где сделать паузу

Сохраните схему наблюдателей без реальных имён и транзакций.

Какие данные обычно позволяют наблюдать семейство адресов счёта?

1. Цвет значка.
2. Его xpub и достаточный контекст деривации.
3. Марка кабеля.

> **Показать ответ: Его xpub и достаточный контекст деривации.**
> Расширенные открытые данные чувствительны для конфиденциальности, хотя сами по себе не авторизуют расходование.

Разделение контекстов и управление сдачей

Цель

Принимайте решения о расходовании с учётом происхождения UTXO.

Разберитесь в теме

Разделение контекстов начинается до платежа. Определите, относится ли поступление к накоплениям, работе, повседневным расходам или конкретным отношениям. Сохраните это в приватных метках, чтобы последующий выбор не стёр различие по незнанию.

Метка не разделяет выходы криптографически. Трата двух UTXO из разных контекстов в одной транзакции публикует их связь. Консолидация уменьшает число входов будущих платежей, но усиливает связь объединённых выходов. При низких комиссиях она может быть экономичной и одновременно противоречить цели конфиденциальности.

Сдача — новый выход под контролем той же политики, а не «невидимые деньги». Его последующее использование может продолжить прежние связи. Не определяйте сдачу по необычной сумме: в реальной проверке устройство должно установить принадлежность кошельку.

Не сводите конфиденциальность к механическим шаблонам сумм, времени или повторных переводов. Такие шаблоны тоже распознаются и создают дополнительные комиссии. Оцените известное каждой стороне и новые сведения, публикуемые предлагаемой операцией. Никакая последовательность не стирает уже опубликованную историю.

Практика

1. Создайте пять вымышленных UTXO из трёх контекстов и подготовьте платёж с минимально необходимым числом контекстов.
2. Определите полученную сдачу и выберите её метку.
3. Сравните издержки и раскрытие связей при объединении всех выходов и раздельном хранении.

Проверьте себя на практике

Обоснуйте консолидацию или отказ от неё конкретным обстоятельством, не применяя абсолютного правила ко всем случаям.

Частый вопрос

Разрывает ли историю перевод всего на другой собственный адрес? Нет. Он публикует дополнительную связь и может добавить издержки, не устранив угрозу.

Где сделать паузу

Сохраните обоснование из лаборатории и выбранную политику выбора входов.

К чему может привести объединение зарплаты и пожертвований в одной транзакции?

1. Сделать видимой связь между этими входами.
2. Удалить общедоступную историю их происхождения.
3. Превратить их в гарантированно анонимную наличность.

> **Показать ответ: Сделать видимой связь между этими входами.**
> Сокращение числа UTXO может увеличить число наблюдаемых связей.

Конфиденциальность в сети, Tor и VPN

Цель

Отличайте конфиденциальность соединения от конфиденциальности в цепочке.

Разберитесь в теме

Сервер запросов может связать обращения с соединением. Интернет-провайдер в зависимости от транспорта видит адресатов или шаблоны трафика. VPN переносит часть доверия на своего оператора, не устраняет публичные сведения Bitcoin и не мешает учётной записи с идентификацией узнавать вас.

Tor маршрутизирует трафик через сеть, уменьшая некоторые связи между источником и адресатом. Он не делает адрес Bitcoin приватным и не защищает приложение, трафик которого не проходит через Tor. Запуск Tor Browser не настраивает автоматически Desk, Bitcoin Core и остальные службы компьютера.

Прежде чем считать соединение защищённым, проверьте маршрут и настройки. В рассмотренной версии встроенный переключатель Tor в Desk не предполагается. Вариант с узлом или прокси требует инженерного руководства и проверки реального трафика. Не приписывайте интерфейсу поле только потому, что оно есть в другом кошельке.

Возможны утечки через DNS, синхронизацию счетов, ссылки на обозреватели и ценовые сервисы. Схема может защищать запросы остатка и всё же раскрывать активность при открытии публичного обозревателя. Определите охват каждой меры и поведение при сбое соединения. Избегайте незаметного перехода к менее приватному поставщику.

Практика

1. Нарисуйте маршрут через компьютер, поставщика связи, прокси при наличии, узел или сервис и сеть Bitcoin.
2. Укажите, кто получает запросы и кто видит вашу коммерческую идентичность.
3. Смоделируйте недоступность частного узла. Выберите паузу или явную смену источника с пониманием раскрытия.

Проверьте себя на практике

Объясните, какую угрозу уменьшает конфигурация и какая сохраняется.

Частый вопрос

Гарантирует ли Tor, что никто не свяжет платёж со мной? Нет. Контрагенты, коммерческая идентификация, шаблоны и ошибки использования могут сохранять связь.

Где сделать паузу

Запишите охват решения без приватных адресов подключения и паролей.

Заставляет ли запуск Tor Browser приложение Desk отправлять запросы через Tor?

1. Да, поскольку они работают на одном компьютере.
2. Да, если виден значок.
3. Нет. Для каждого приложения маршрут нужно настроить и проверить отдельно.

> **Показать ответ: Нет. Для каждого приложения маршрут нужно настроить и проверить отдельно.**
> Защита одного приложения не распространяется автоматически на остальные.

CoinJoin, Payjoin и их нынешние ограничения

Цель

Разберитесь в совместных инструментах без приписывания им отсутствующих анонимности или совместимости.

Разберитесь в теме

CoinJoin объединяет вклады нескольких людей в одной транзакции, чтобы затруднить отдельные выводы о входах и выходах. Это не передача монет кастодиальному сервису, обещающему вернуть другие. Для каждого варианта проверяйте координацию, хранение, комиссии, устойчивость к недобросовестным участникам и последующее использование.

Payjoin включает в совместный платёж входы плательщика и получателя, ослабляя некоторые эвристики общей принадлежности. Нужны совместимая поддержка с обеих сторон и определённый протокол. Это материал для технического понимания: рассмотренные источники не подтверждают встроенную работающую процедуру Payjoin или CoinJoin в Cuvex Desk.

Доступность сервисов и правовой контекст меняются. В документации Wasabi отмечено прекращение работы координатора zkSNACKs 1 июня 2024 года. Историческую кнопку нельзя показывать как гарантию работающего сегодня сервиса. В 2025 году Минюст США сообщил о признании вины основателями Samourai и последующих приговорах. Этот случай не означает, что любая техника конфиденциальности незаконна в каждой юрисдикции.

Инструмент может ослабить один вывод, не затронув остальные. Известное происхождение не исчезнет из записей контрагента. Последующее объединение, метаданные и ошибки участников могут ухудшить конфиденциальность. Кроме того, отдельные сервисы применяют разные коммерческие политики к монетам с определённой историей.

Практика

1. Сравните обычную транзакцию, совместную транзакцию и сервис, принимающий средства на хранение, без реальных операций.
2. До предложения конкретного инструмента выясните версию, ответственного за сопровождение, состояние сервиса и актуальную документацию.

3. Разделите технические, кастодиальные и правовые риски. Преподаватель не должен проектировать обход контроля или обещать «невозможно отслеживаемые средства».

Проверьте себя на практике

Назовите одно ограниченное преимущество техники конфиденциальности и не менее двух рисков или требований.

Частый вопрос

Нужен ли Cuvex миксер для приватного хранения? Нет. Контроль запросов, данных, ключей и выбора UTXO уже уменьшает конкретные риски без обещания полного сокрытия.

Где сделать паузу

Отметьте инструмент как «изучен». Для пометки «совместим» нужны свидетельства.

Какое утверждение обоснованно?

1. CoinJoin гарантирует постоянную анонимность.
2. Совместная техника может затруднить отдельные выводы, но у неё есть требования и ограничения.
3. Любой сервис с названием mixer сохраняет самостоятельное хранение.

> **Показать ответ: Совместная техника может затруднить отдельные выводы, но у неё есть требования и ограничения.**
> Свойства зависят от протокола, реализации, участников и последующего использования.

Уроки реальных инцидентов

Цель

Извлекайте из документированных инцидентов проверяемые решения без нападок на конкурентов и преувеличения защиты.

Разберитесь в теме

По делу Mt. Gox в обвинительном документе Минюста США 2023 года описываются предполагаемый несанкционированный доступ к серверам и ключам и последующее исчезновение клиентских средств. Обвинение содержит утверждения стороны обвинения, а не судебный приговор. Для хранения важны вопросы о том, кто действительно контролирует ключи и что произойдёт при крахе компании.

В декабре 2023 года в связи с Ledger Connect Kit компания Ledger задокументировала вредоносный выпуск библиотеки децентрализованных приложений после компрометации доступа бывшего сотрудника. Инцидент затронул цепочку распространения ПО и обманом побуждал пользователей DApp EVM подписывать операции. Он не доказывает взлом оборудования Ledger или консенсуса Bitcoin.

В связи с инцидентом Bybit в феврале 2025 года ФБР возложило на Северную Корею ответственность за хищение виртуальных активов примерно на 1,5 млрд долларов. Инцидент затронул биржу и активы других сетей. Он не свидетельствует о взломе криптографии Bitcoin. В учебных целях важно проверять, что именно авторизует подпись, и не допускать, чтобы несколько людей слепо полагались на один экран.

В мае 2025 года Coinbase сообщила о хищении данных подкупленными сотрудниками поддержки для содействия социальной инженерии. По заявлению компании, пароли и закрытые ключи не раскрылись. Важно понимать: знание подлинных сведений не перестаёт делать мошенника мошенником.

Bitcoin Core также публикует сведения об ошибках. В уведомлении CVE-2024-35202 описана возможность удалённого аварийного завершения версий до 25.0. Проверка правил не отменяет сопровождения ПО. Из этого уведомления не следует хищение ключей.

В январе 2026 года The Register сообщил о раскрытии через Global-e сведений о заказах и контактах покупателей Ledger. Издание сослалось на подтверждения обеих компаний. По их заявлениям, ключи восстановления не пострадали. Покупка может раскрыть факт владения устройством даже без взлома оборудования.

В апреле 2026 года The Record сообщил об атаке на Drift и объявленной платформой приостановке ввода и вывода. Drift — протокол децентрализованных финансов на Solana. Это не взлом Bitcoin. Первоначальные оценки потерь не следует выдавать за окончательную сумму, а последующие попытки восстановления — за гарантированный возврат.

Практика

1. Классифицируйте инциденты по хранению, интерфейсу или распространению, персональным данным, протоколам других сетей и доступности.
2. Для каждого предложите меру предупреждения и одно её ограничение.
3. Отработайте мошеннический звонок: «Я знаю о вашей покупке, переведите средства на этот безопасный адрес». Завершите звонок и проверьте через канал, в котором вы сами инициировали контакт.

Проверьте себя на практике

Объясните, почему ни один инцидент не доказывает неуязвимости другой марки. Свидетельства применимы к конкретному предмету.

Частый вопрос

Это исчерпывающий перечень последних взломов? Нет. Это проверенная подборка для редакции от 17 ноября 2026 года, а не полный реестр или наблюдение в реальном времени.

Где сделать паузу

Запишите, какую привычку вы измените и как проверите соблюдение.

Собеседник знает о вашей покупке и просит перевести средства в «спасательный кошелёк». Что доказывает знание о покупке?

1. Сведения могли утечь. Их знание не удостоверяет личность собеседника или адрес.
2. Что это обязательно настоящий сотрудник поддержки.
3. Что нужно передать сид-фразу.

> **Показать ответ: Сведения могли утечь. Их знание не удостоверяет личность собеседника или адрес.**
> Достоверные сведения могут использоваться для убедительного обмана.

Создание идентичности и проверка контактов в чате

Цель

Активируйте идентичность чата без раскрытия её ключа и проверьте собеседника.

Разберитесь в теме

В Desk чат связывается с криптограммой ключом чата (Clave Chat), созданным на Cuvex. Его представление может походить на xpub, но это секрет, а не открытый ключ счёта WOW. Преподавателю никогда не требуется читать его или видеть QR.

Процедура различает новый псевдоним и перенос или восстановление существующего. В рассмотренной реализации выбирают соответствующий мобильный профиль iOS или Android. Исторически выведенные идентичности нельзя считать взаимозаменяемыми по догадке. DEV и Production — отдельные среды. Их переключение автоматически не переносит переписку и псевдонимы.

Добавление псевдонима не подтверждает личность. Сверьте отпечаток по независимому аутентифицированному каналу. Для вопросов узнавания используйте непубличные сведения и избегайте ответов, раскрывающих пароли. Знакомый голос можно имитировать. При риске сочетайте заранее согласованные способы.

При смене идентичности контакта приостановите платежи и координацию до выяснения. Это может быть правомерное восстановление или злонамеренная подмена. Сквозное шифрование защищает канал в соответствии с протоколом и реализацией, но не доказывает, кто пользуется устройством собеседника.

Практика

1. В тестовой среде опишите создание или восстановление, не передавая ключ чата (Clave Chat).
2. Добавьте лабораторный контакт и договоритесь по другому каналу о сверке отпечатка.
3. Смоделируйте смену идентичности. Определите, как проверите изменение до платежа.

Проверьте себя на практике

Различайте псевдоним, открытый отпечаток, секретный ключ чата (Clave Chat) и личное доверие человеку.

Частый вопрос

Гарантирует ли прежний псевдоним, что это тот же человек? Нет. Непрерывность идентичности и изменения ключей проверяются по процедуре.

Где сделать паузу

Запишите только «тестовый контакт проверен» и метод. Не включайте ключи и приватные вопросы.

Строка называется ключом чата (Clave Chat) и похожа на xpub. Как с ней обращаются в Desk?

1. Как с данными для размещения на форуме.
2. Как с секретом для восстановления идентичности.
3. Как с адресом получения bitcoin.

> **Показать ответ: Как с секретом для восстановления идентичности.**
> Внешний вид данных не определяет их конфиденциальность или назначение.

Запрос и оплата в сатоши через чат

Цель

Переходите от переписки к платежу, сохраняя контекст и проверку.

Разберитесь в теме

Чат позволяет запросить адрес, ответить адресом получения, запросить платёж и начать подготовку из счёта WOW. Сохранение контекста снижает ошибки копирования между приложениями, но не превращает каждое сообщение в аутентифицированное распоряжение о расходовании.

Перед ответом или оплатой проверьте проверенный контакт, сеть, сумму и исходный запрос. Общая форма сохраняет выбор UTXO и комиссии. При запросе определённой суммы и выборе отправки всего остатка чистая сумма после комиссий может оказаться меньше. Тогда платёж нужно обозначить как частичный.

Авторизация остаётся на Cuvex. Чат передаёт намерение и координирует действия, но не имеет права автоматически подписывать. В отправленном контакту подтверждении различайте получение сообщения и наличие подтверждённой транзакции. Получатель проверяет по своему счёту или источнику.

Внешние ссылки, вложенные QR-коды и адреса остаются недоверенными до проверки. «Посмотреть в Mempool» может открыть сторонний сервис и раскрыть запросы. При политике собственного узла выбирайте совместимую проверку в WOW и оценивайте любой переход к внешнему публичному сервису.

Практика

1. Разыграйте две роли. Получатель запрашивает 50 000 sat, а плательщик готовит операцию, не передавая её в сеть.
2. Смоделируйте доступный чистый остаток 48 000 sat. Объясните, какого согласия и сверки не хватает для частичного платежа.
3. Намеренно измените сеть в тестовом сообщении и остановите процедуру.

Проверьте себя на практике

Проследите связь запроса, адреса, черновика, подписи и подтверждения, не сводя её к «в чате написано OK».

Частый вопрос

Означает ли отправка sats из чата использование Lightning? Нет. Документированная процедура WOW готовит платежи в базовой цепочке Bitcoin. Sats обозначает единицу, а не сеть передачи.

Где сделать паузу

Отмените учебный черновик или запишите его состояние. Не передавайте транзакцию в сеть ради демонстрации интерфейса.

В чате пришло подтверждение. Какая проверка решает, получен ли платёж?

1. Зелёный цвет значка сообщения.
2. Слова собеседника «подтверждено».
3. Проверка транзакции и её выходов в сети с помощью подходящего источника.

> **Показать ответ: Проверка транзакции и её выходов в сети с помощью подходящего источника.**
> Статус сообщения и состояние транзакции не равнозначны.

Осознанная передача криптограмм

Цель

Разберитесь, что означает передача зашифрованной копии другому человеку.

Разберитесь в теме

Передача криптограммы отправляет копию зашифрованного объекта. Она не обязательно переводит bitcoin и сама по себе не добавляет подписанта. Если получатель получит и достаточные средства разблокировки, он сможет открыть содержимое согласно схеме. Поэтому заранее определите передаваемую возможность.

Сквозное шифрование чата и шифрование файла защищают разные уровни. После загрузки получатель может хранить объект вне чата. Удаление сообщения или локальной записи не гарантирует изъятия всех копий. Пароль, переданный тем же каналом, может сосредоточить компоненты в одном месте передачи.

До отправки проверьте идентичность, формат и цель. Возможность привязать полученную криптограмму лишь организует копию и не доказывает безопасности расшифрования произвольного файла. Не используйте вложения, требующие ввести сид-фразу или пароль на сторонней странице.

Для восстановления нужна договорённость: кто хранит компоненты, кто может открыть, как обнаружить раскрытие и изменить хранение при прекращении отношений. Для обычного платежа обычно достаточно проверенного адреса. Передавать свою криптограмму не требуется.

Практика

1. Спланируйте передачу зашифрованного учебного текста лабораторному контакту.
2. Перечислите, что знает и может сделать получатель до и после получения пароля.
3. Смоделируйте прекращение отношений. Объясните, почему удаление сообщения не отзывает копию и ключи.

Проверьте себя на практике

Различайте «я передал данные», «я передал доступ к секрету» и «я подписал расходование».

Частый вопрос

Можно ли без последствий распространять зашифрованный файл? Он может раскрыть метаданные, облегчить попытки подбора пароля и храниться неопределённо долго. Оцените необходимость передачи.

Где сделать паузу

Не оставляйте материалы хранения во вложениях курса. Запишите только вывод упражнения.

Равнозначна ли передача криптограммы по чату отправке bitcoin?

1. Нет. Передаётся объект, у содержимого и доступа к которому другое назначение.
2. Да, если имя заканчивается на .bin.
3. Это автоматически активирует новую мультиподпись.

> **Показать ответ: Нет. Передаётся объект, у содержимого и доступа к которому другое назначение.**
> Передача секретов и перемещение UTXO — разные операции.

Восстановление чата и понимание его метаданных

Цель

Спланируйте смену устройства и разделяйте восстановление идентичности и сообщений.

Разберитесь в теме

Desk указывает, что история и сеансы зашифрованы локально и не входят в общую копию. Ключ чата (Clave Chat) восстанавливает идентичность, но не гарантирует возврата всей старой переписки. В приложении есть состояния и действия для незавершённой активации, обслуживания ключей и локального восстановления при наличии совместимых материалов.

Согласно рассмотренному руководству каждый псевдоним используется только на одном устройстве за раз. Не активируйте его на двух устройствах для «проверки синхронизации», если сценарий не поддерживается. При переносе следуйте процедуре и проверяйте непрерывность идентичности с контактами.

«Ожидается», «принято сервером», «получено» и «не удалось расшифровать» — разные этапы. Не отправляйте неподтверждённое сообщение повторно вслепую, сначала выясните, дошло ли оно. При отсутствии сеансового ключа или смене идентичности сохранённое ожидающее сообщение не равно прочитанному.

Шифрование содержимого не обязательно скрывает от всех вовлечённых систем время, размер, связи доставки, псевдонимы и данные соединения. Аналогично транспортное шифрование голоса не делает обычный звонок подходящим каналом для секретов. Используйте минимум сведений, необходимых для обучения и решения проблем.

Практика

1. Смоделируйте потерю компьютера и объясните, что восстанавливает каждый доступный материал.
2. Классифицируйте статусы сообщений и определите, когда нельзя повторно посылать запрос платежа.
3. Подготовьте уведомление о смене устройства, проверяемое контактами по независимому каналу.

Проверьте себя на практике

Объясните, какая переписка может быть утрачена и какую идентичность можно восстановить, не обещая не предусмотренного копией восстановления.

Частый вопрос

Удаляет ли локальное удаление чата сообщения у собеседника? Не делайте такого предположения. Получатель может независимо хранить сообщения и файлы.

Где сделать паузу

Сохраните план переноса с названиями пустых полей, без ключа чата (Clave Chat).

Что сам по себе обеспечивает ключ чата (Clave Chat) согласно рассмотренному руководству?

1. Всю прежнюю переписку на любом компьютере.
2. Возможность восстановить идентичность по совместимой процедуре, но не все старые сообщения.
3. Автоматический доступ к ключам Bitcoin контактов.

> **Показать ответ: Возможность восстановить идентичность по совместимой процедуре, но не все старые сообщения.**
> Восстановление идентичности и восстановление архива — разные возможности.

Повседневные настройки и проверка разрешений

Цель

Управляйте параметрами Desk, различая удобство и защиту.

Разберитесь в теме

Desk предлагает темы «Ночь», «День» или «Системная», автоматическую синхронизацию с периодами 3 или 5 минут, звуки транзакций, фон чата, язык и справочную валюту. Эти предпочтения меняют представление или частоту запросов. Они не изменяют подпись Bitcoin и не добавляют анонимности.

Рассмотренные настройки безопасности допускают блокировку при бездействии и переходе в фон, максимальную задержку после неудачных попыток и необязательное удаление. Схема бездействия допускает от 30 до 86 400 секунд, интерфейс может предлагать более узкий выбор. Значения по умолчанию проверяйте в используемой версии, а не предполагайте по видеозаписи урока.

Интеграция ссылок bitcoin: открывает запрос для разблокировки, выбора счёта и проверки. Она не авторизует автоматическую оплату. В Linux руководство различает интегрированную установку и AppImage при регистрации ссылок. Для счёта Lightning нужна отдельная совместимая процедура. Назначения Desk приложением по умолчанию недостаточно.

Котировка, график и информационные ссылки могут обращаться к внешним сервисам. Они служат для справки, а не дают сигнал покупки. До пересчёта сумм проверьте дату и источник. Тёмная тема или небольшое окно не должны скрывать завершающие кнопки, адрес или комиссию. Если это случилось, сделайте паузу и сообщите о проблеме компоновки.

Практика

1. Настройте оформление и блокировку учебного хранилища. Проверьте повторный вход.
2. Проверьте, какие автоматические функции вы включаете. Синхронизация, звуки и проверка прошивки — разные функции.
3. Откройте вымышленный запрос по ссылке bitcoin: и отмените до подготовки реальной операции.

Проверьте себя на практике

Объясните эффект каждой настройки и найдите те, что связаны с запросами или чувствительными действиями.

Частый вопрос

Заменяет ли биометрия компьютера резервную копию? Нет. Она может зависеть от оборудования и защищённого хранилища ОС. Сохраняйте независимую возможность восстановления.

Где сделать паузу

Заблокируйте Desk и запишите только изменённые предпочтения.

Что изменится при выборе синхронизации раз в три минуты?

1. Предусмотренная частота запросов во время работы функции.
2. Политика подписей в цепочке.
3. Сид-фраза устройства.

> **Показать ответ: Предусмотренная частота запросов во время работы функции.**
> Это рабочая настройка. Она не меняет порядок хранения средств.

Проектирование кошелька с мультиподписью

Цель

Выберите порог, устойчивый к разумно предполагаемым потерям и компрометации.

Разберитесь в теме

В политике M из N число N обозначает участников с разными ключами, а M — требуемое число подписей. Политика 2 из 3 выдерживает недоступность одного ключа, однако два скомпрометированных ключа позволяют авторизовать расходование. Если все три сид-фразы находятся в одном месте или могли раскрыться при одном событии, их независимость снижается.

Рассмотренный профиль мультиподписи Cuvex использует нативный P2WSH с sortedmulti и деривацией BIP48. Структурный предел Original — шесть ключей политики, а BIT — пятнадцать. При совместном использовании нужно учитывать возможности участника с меньшим пределом и фактический объём носителя. Структурные максимумы не гарантируют, что политика с множеством ключей и входов поместится.

Приложение допускает пороги, соответствующие условиям политики. Но при пороге 1 из N для расходования не требуется сотрудничество. Прошивка содержит специальные предупреждения об этом риске. Увеличение чисел не улучшает всё сразу. Растут потребность в координации, затраты, объём материалов для восстановления и риск блокировки.

MuSig2 — отдельная схема агрегации подписей Шнорра. Сама по себе она требует N из N, а не произвольные 3 из 5. В изученных прошивках Final не реализованы подписание входов Taproot, MuSig2 и Miniscript. Поддержка получателя P2TR не доказывает возможности подписывать из кошелька Taproot.

Практика

1. Спроектируйте вымышленную схему 2 из 3 с независимыми рисками каждого участника.
2. Смоделируйте утрату одного ключа и компрометацию одного ключа. Объясните, что возможно и что невозможно.
3. Проверьте пределы каждой модели до выбора более крупной политики.

Проверьте себя на практике

Укажите переносимую потерю, порог для атаки и общие зависимости вашего проекта.

Частый вопрос

Требует ли мультиподпись знания сид-фраз других участников? Нет. Цель — сохранение каждым собственной закрытой возможности и обмен открытыми данными, необходимыми для построения и восстановления политики.

Где сделать паузу

Сохраните проект с вымышленными участниками и их обязанностями.

Сколько закрытых ключей достаточно для авторизации действительного расходования при политике 2 из 3 с независимыми ключами?

1. Один.
2. Два.
3. Всегда все три.

> **Показать ответ: Два.**
> Для порога нужны две подписи. Остальные условия и проверки также должны выполняться.

M09

Создание приглашений и предоставление ключей

Цель

Постройте политику с проверенными участниками без обмена сид-фразами.

Разберитесь в теме

Создатель выбирает название, сеть, M, N, контакты, собственные открытые сведения и рабочие условия приглашения. Рассмотренная схема поддерживает mainnet и regtest, от 2 до 15 участников до применения пределов устройства и рабочий срок от 1 до 720 часов. Эти пределы не дают права обходить проверку возможностей.

Каждый участник проверяет приглашение, принимает или отклоняет его и предоставляет по совместимой процедуре свой расширенный открытый ключ с отпечатком и путём BIP48. Не предоставляются сид-фраза, закрытый ключ, отдельный адрес или полный дескриптор другого кошелька. Неправильный контекст ключа может создать другую политику, даже если он выглядит действительным xpub.

Создатель координирует, не заменяя проверку каждого подписанта. До получения средств все должны уметь восстановить и проверить одинаковые параметры и контрольный адрес. Принятие контакта в чате не означает автоматического одобрения любой присланной им политики.

Истечение приглашения — правило координации приложения. Оно само по себе не меняет скрипт с полученными средствами, не удаляет сохранённые другими подписи и не является временной блокировкой консенсуса. Отмена предложения и вывод средств из существующей политики — разные действия.

Практика

1. В подготовленной лаборатории regtest создайте предложение 2 из 3 с тестовыми контактами.
2. Разыграйте принятие, отказ и предоставление данных неверной сети. Проверьте, что последнее останавливается.
3. Перечислите данные для хранения всеми до финансирования: сеть, порог, открытые ключи, происхождение, скрипт и проверенный адрес.

Проверьте себя на практике

Распознайте неполное приглашение и объясните, какого одобрения не хватает, не предполагая его по наличию чата.

Частый вопрос

Делает ли дата истечения невозможным позднейшее расходование? Не в качестве поля приглашения. Временное ограничение Bitcoin требует определённых условий скрипта или транзакции и реальной поддержки.

Где сделать паузу

Сохраните учебный идентификатор предложения и ожидающее одобрение.

Что по документированной процедуре требуется от вас для участия в мультиподписи?

1. Сид-фразы всех участников.
2. Любой адрес для получения платежа.
3. Ваш расширенный открытый ключ с совместимыми отпечатком и данными происхождения по BIP48.

> **Показать ответ: Ваш расширенный открытый ключ с совместимыми отпечатком и данными происхождения по BIP48.**
> Правильные открытые данные позволяют построить политику без раскрытия закрытых ключей.

Проверка политик в Mirror в произвольном порядке

Цель

Сравнивайте поля целиком и точно понимайте, что подтверждает результат.

Разберитесь в теме

Независимая проверка показывает порог, сеть, профиль, SIGHASH, ID политики, первый адрес, позицию пользователя и данные каждого участника. Это контроль намерения и согласованности. Не предполагается постоянная регистрация политики устройством. Документированные выводы относятся к «этой проверке».

В Mirror 12.12 можно сначала считать QR-код Cuvex или Desk и выбрать любой элемент. Начинать с шага 1, сканировать всё или соблюдать порядок не обязательно. Если вы сверили текст вручную, пропуск сканирования не помечает его как проверенный в Mirror.

Средство сравнения показывает весь буквальный текст. Пробелы, переносы строк, регистр и различия Unicode имеют значение. «Совпадает» означает равенство двух значений в паре. Оно не удостоверяет происхождение, не доказывает принадлежность одной политике и не активирует кошелёк. Итоговое подтверждение и связанный ответ проходят через Cuvex и Desk.

Нынешние QR-коды Desk содержат только значение, без порядкового номера и сеанса. Mirror не всегда может определить шаг. Команда «Указать шаг Desk» добавляет ручной контекст, который должен обозначаться как ручной. Для N участников документированная карта включает 7 + 4N полей. При k от нуля 8+4k — отпечаток, 9+4k — путь, 10+4k — xpub, 11+4k — ID ключа. При N=2 шаг 15 содержит ID второго ключа и может проверяться первым.

Практика

1. Используйте синтетические данные. Сначала сравните ID с пометкой шага 15, затем сеть и порог.
2. Внесите расхождение в один символ. Проверьте «Не совпадает» и начните новую пару без переноса результата.
3. Сравните «2 / 3» и объясните, почему по тексту не всегда можно определить, порог это или позиция пользователя.

Проверьте себя на практике

Назовите проверенное поле, способ определения контекста и то, что ещё нужно одобрить. Не превращайте частичные совпадения в общее одобрение.

Частый вопрос

Обязательно ли сканировать все QR, чтобы продолжать обучение? Нет. Сравнение выполняется свободно. Обязательные проверки и авторизации подписанта сохраняют свою процедуру.

Где сделать паузу

Закройте средство сравнения. По рассмотренному проекту значения должны очищаться при выходе или переходе в фон.

Mirror сравнивает два QR-кода шага 15 и показывает «Совпадает». Что это подтверждает?

1. Точное равенство этой пары в определённом или вручную указанном контексте.
2. Одобрение всей политики.
3. Подлинность происхождения обоих QR-кодов.

> **Показать ответ: Точное равенство этой пары в определённом или вручную указанном контексте.**
> Сравнение не заменяет установления подлинности, полной проверки или ответа аппаратного устройства.

Координация подписей и передача транзакции с мультиподписью в сеть

Цель

Доведите предложение до порога подписей, сохраняя намерение и контроль.

Разберитесь в теме

Операция с мультиподписью задаёт входы, получателей, суммы, ставку, замену и рабочие примечания. Создатель может запросить подписи совместимых участников. Каждый подписант до авторизации на устройстве самостоятельно проверяет сеть, политику, входы, все выходы и комиссию.

Частичная подпись не перемещает средства при недостигнутом пороге. После достижения координатор может объединить подписи и завершить операцию по процедуре. Сообщения других участников или координатора — координационная информация, а не выполненная вами локальная проверка. Приложение должно различать эти источники.

Рассмотренная версия предлагает повтор, получение подписи, подтверждение получения, отказ и передачу координации. Передача не меняет ключи или порог в цепочке. Сохранённый ответ должен соответствовать запросу и фактически использованному профилю. Нельзя выбирать другую политику по сходству или первому месту в каталоге.

При изменении получателей или существенных условий проверяют новое предложение и получают соответствующие подписи. Не «исправляйте» PSBT вручную удалением защитных данных ради размещения на NFC. Прошивки требуют совместимых профиля и проверок с ограничениями входов, выходов и размера.

До передачи в сеть убедитесь в соответствии договорённой операции и отсутствии уже распространённой версии. Затем отслеживайте подтверждения через выбранный источник. Отказ в своём приложении автоматически не отзывает сохранённые другими подписи и не исключает всех действий при достижимом оставшимися ключами пороге.

Практика

1. Разыграйте схему 2 из 3 с тремя вымышленными участниками. Один подписывает, второй отказывается, третий просит разъяснение.
2. Измените адрес тестового платежа и объясните, почему прежнее устное одобрение не используется повторно.
3. Смоделируйте сбой подтверждения получения после сохранения подписи. Возобновите то же задание без дублирования платежа или изменения профиля.

Проверьте себя на практике

Укажите, кто координирует, подписывает и завершает и какое свидетельство есть для каждого этапа.

Частый вопрос

Равны ли два OK в чате двум подписям? Нет. Для порога требуются действительные криптографические авторизации по политике, а не сообщения.

Где сделать паузу

Запишите состояние, ожидающие подписи и следующего ответственного без приватного содержимого.

В операции 2 из 3 одна действительная подпись и два сообщения «согласен». Достигнут ли порог?

1. Да, поскольку участников трое.
2. Нет, нужна ещё одна действительная криптографическая подпись.
3. Да, если об этом объявил координатор.

> **Показать ответ: Нет, нужна ещё одна действительная криптографическая подпись.**
> Согласие в разговоре и действительная подпись — разные свидетельства.

Восстановление и изменение кошелька с мультиподписью

Цель

Восстановите политику и спланируйте потерю или замену участников.

Разберитесь в теме

Для восстановления нужны две категории: данные для построения политики и достаточные закрытые возможности расходования. Копия политики с xpub может раскрывать историю без сид-фраз. Шифрование защищает файл, но требует сохранить пароль. Расширение .cuvexms само по себе не доказывает шифрования. Проверьте формат и конкретную процедуру экспорта.

В Desk 9.21 восстановление запрашивает экспортированный с устройства расширенный открытый ключ участника с отпечатком и путём BIP48. Совместимая процедура поддерживает чтение веб-камерой или Mirror. Не подменяйте эти данные адресом получения и не отправляйте сид-фразу поддержке.

При утрате одного ключа в схеме 2 из 3 два других могут сохранить возможность расходования. Старая политика остаётся той же. Для фактического исключения участника и установки других ключей обычно создают новую политику и переводят средства с необходимыми авторизациями. Смена псевдонима или удаление кошелька из Desk не изменяет существующие UTXO.

Копии должны позволять восстановить обе ветви и найти историю. Храните индексы, выданные запросы и нужный контекст, чтобы не повторять адреса и не считать кошелёк пустым из-за неполного сканирования. При восстановлении и возобновлении ожидающей операции соблюдайте профиль, сохранённый при её создании.

Практика

1. Экспортируйте и восстановите лабораторную политику документированной функцией. Проверьте сеть и известный адрес.
2. Смоделируйте утрату участника и составьте план ротации без реального перевода.
3. Смоделируйте потерю, оставляющую меньше порога. Учитывайте, что поддержка и ИИ не могут создать недостающие подписи.

Проверьте себя на практике

Восстановите тестовый сценарий и различайте возврат информации и изменение контроля над средствами.

Частый вопрос

Отключает ли удаление мультиподписи в Desk кошелёк для всех? Нет. По процедуре удаляется локальное состояние. У других людей и в копиях могут сохраняться предусмотренные политикой возможности.

Где сделать паузу

Сохраните проверенную копию и личный план. В курсе отметьте только результат.

Вы хотите исключить человека из политики, на которую уже получены средства. Достаточно ли удалить его имя из Desk?

1. Да.
2. Да, если удалить и чат.
3. Нет. При необходимости нужно спланировать новую политику и авторизованный перевод средств.

> **Показать ответ: Нет. При необходимости нужно спланировать новую политику и авторизованный перевод средств.**
> Редактирование локальных записей не меняет скрипты существующих UTXO.

M10

Обновление прошивки по проверенной процедуре

Цель

Подготовьте совместимое обновление и проверьте результат на устройстве.

Разберитесь в теме

Обновление меняет доверенное ПО. Проверьте модель, аппаратную ревизию, версию, происхождение и механизм проверки подлинности производителя. Завершённая загрузка или совпадение хеша с указанным на странице не заменяют проверки подписи и совместимости. Никогда не устанавливайте неподписанное инженерное приложение прошивки как клиентский выпуск.

По документированной процедуре Original обновляется через Bluetooth. BIT использует USB-C. Mirror поддерживает соответствующие процедуры подготовки и передачи. Работа конкретного сочетания компьютера, телефона и устройства не обещается до его физических приёмочных испытаний. Известная проблема обновления Original в Windows требует отдельной диагностики. Нельзя объявлять успех при 99 %.

До начала проверьте восстанавливаемые копии, стабильное питание и отсутствие других операций. Подготовьте официальный файл или предварительно проверенную копию согласно приложению. Различайте передачу, проверку, установку, перезапуск и сверку версии. Индикатор хода не является итоговым подтверждением.

По завершении проверьте версию на экране устройства и запишите дату и результат. Каталог совместимости Desk не измеряет прошивку удалённо: firmwareAttestation остаётся false. Выбор профиля Final не подтверждает фактически установленные байты. При сбое следуйте документированному восстановлению, сохраните этап и ошибку, не разрывайте соединение наугад на критическом этапе.

Практика

1. Проверьте список подготовки, не запуская на тренировке реальное обновление.
2. Расположите состояния по порядку и объясните различие «передано» и «установлено».
3. Составьте вымышленный отчёт о сбое на 99 % с моделью, версией, системой, этапом и итоговым сообщением.

Проверьте себя на практике

Определите подходящий файл, способ передачи и итоговый критерий успеха.

Частый вопрос

Обновлять ли прошивку только ради устранения ошибки Desk? Сначала определите источник. Несовместимость каталога может требовать исправления Desk с сохранением проверенной прошивки.

Где сделать паузу

Реальное обновление приостанавливают только в явно безопасном по процедуре состоянии, а не по окончании звонка.

Что сам по себе подтверждает явно заданный каталог Desk?

1. Заявленные варианты совместимости без удалённого измерения установленной прошивки.
2. Физическую аттестацию всех подключённых устройств.
3. Отсутствие уязвимостей.

> **Показать ответ: Заявленные варианты совместимости без удалённого измерения установленной прошивки.**
> Совместимость, подпись, измерение и физическая приёмка — разные виды свидетельств.

Потеря, поломка и экстренное восстановление

Цель

Выберите соразмерное инциденту восстановление и сохраните полезные свидетельства.

Разберитесь в теме

Сначала определите, что потеряно или раскрыто: компьютер, устройство, карта, файл, пароль, сид-фраза, дополнительная фраза или политика. «Не могу войти» не обязательно значит «меня обокрали». При подозрении на компрометацию прекратите ввод секретов на подозрительном устройстве.

Потерю устройства можно компенсировать совместимыми носителями и данными восстановления. При потере компьютера может потребоваться восстановить хранилище Desk и заново настроить наблюдение. Потеря всех средств разблокировки или ключей с остатком ниже порога может не иметь технического решения. ИИ не может гарантировать спасение несуществующих ключей.

Desk включает локальное восстановление поддерживаемых форматов и экспорт соответствующих материалов. Расшифрование на компьютере может раскрыть секрет операционной системе или вредоносному ПО. Это исключительное решение. Нужны подготовленная среда, совместимые материалы и план переноса на новые ключи при возможном раскрытии. Не приравнивайте это к обычной изоляции Cuvex.

Если сид-фраза раскрыта, смена пароля Desk её не отзывает. Оцените авторизованный перенос на новый кошелёк и защитите его с доверенного устройства. Не публикуйте подробности, помогающие злоумышленнику. Не платите сервисам, обещающим восстановление в обмен на другую сид-фразу или мошенническую предоплату.

Практика

1. Разберите четыре вымышленных случая: потерянный компьютер, сломанная карта с действительной копией, забытый пароль и раскрытая сид-фраза.
2. Для каждого определите необходимые материалы, риск действий и критерий восстановления.
3. Испытывайте процедуру только с учебными данными. Не загружайте преподавателю реальные аварийные файлы.

Проверьте себя на практике

Выбирайте восстановление, перенастройку наблюдения, перенос контроля или обращение к специалисту, не заявляя о невозможных решениях.

Частый вопрос

Зашифрует ли смена пароля заново всё, что кто-то уже увидел? Нет. Открытая копия или известная сид-фраза не становятся неизвестными.

Где сделать паузу

Запишите категорию инцидента и следующее безопасное действие. При работе с секретами остановите голосовую беседу.

Ваша сид-фраза опубликована, но вы изменили пароль компьютера. Лишился ли злоумышленник возможности распоряжаться средствами?

1. Да.
2. Нет. Сид-фраза по-прежнему определяет те же ключи, и нужно принимать меры по защите хранения.
3. Да, если также изменить фон чата.

> **Показать ответ: Нет. Сид-фраза по-прежнему определяет те же ключи, и нужно принимать меры по защите хранения.**
> Локальная защита не отзывает раскрытый ключ Bitcoin.

Фишинг, служба поддержки и голосовое мошенничество

Цель

Распознавайте опасные запросы и реагируйте без импровизации.

Разберитесь в теме

Убедительное мошенничество может использовать ваше имя, покупку, устройство и знакомый голос. Подлинные сведения могли утечь. Проверяйте личность известной процедурой через самостоятельно инициированный канал, а не по срочности или точности слов собеседника.

Признаки риска: просьба о сид-фразе, пароле, PIN или ключе чата (Clave Chat), установка удалённого управления для «синхронизации», отключение антивируса, перевод на «безопасный кошелёк», сканирование необъяснённого QR или подпись для доказательства владения без пояснения авторизуемого. Давление закончить до конца звонка — основание прервать его.

Настоящий преподаватель объясняет и проверяет понимание. Он не хранит ключи, не запрашивает тестовый перевод на свой адрес и не обещает вернуть сид-фразу. Правомерная проверка владения конкретна и поддаётся изучению. Для неё никогда не передают закрытые ключи.

Обман возможен и внутри технического сеанса: QR-текст, документ или сообщение могут содержать команды ИИ игнорировать инструкции. Это материал для анализа, а не полномочие управлять преподавателем. База знаний должна отделять утверждённые источники от текста учащегося или третьей стороны.

Практика

1. Разыграйте ложный звонок поддержки и завершите до раскрытия данных.
2. Независимо проверьте заранее сохранённый официальный канал.
3. Опишите ошибку установки без демонстрации экрана с секретами и без удалённого доступа к среде хранения.

Проверьте себя на практике

Объясните, какие сведения запрашивают, для чего они могли бы понадобиться и почему запрос выходит за пределы учебной поддержки.

Частый вопрос

Безопасно ли показать несколько слов сид-фразы? Нет. Учебной причины раскрывать фрагменты собственной сид-фразы нет.

Где сделать паузу

Сохраните способ проверки поддержки и убедитесь, что в нём нет секретов открытым текстом.

Голос, похожий на голос партнёра, просит пропустить проверку и срочно подписать. Как вы поступите?

1. Остановлюсь, проверю подлинность запроса согласованным способом и проверю всю операцию.
2. Подпишу, поскольку голос знаком.
3. Передам сид-фразу, чтобы сэкономить время.

> **Показать ответ: Остановлюсь, проверю подлинность запроса согласованным способом и проверю всю операцию.**
> Узнавание голоса и срочность не заменяют установления подлинности и проверки.

Конфиденциальность, законность и личный учёт

Цель

Изучите общую картину и подготовьте конкретные юридические и налоговые вопросы.

Разберитесь в теме

Финансовая конфиденциальность не отменяет налоговых обязанностей, применимой идентификации, соблюдения санкций и предотвращения преступлений. Ситуация зависит от места жительства, деятельности, контрагента и сервиса. ИИ должен давать общие сведения с источником и датой и направлять для индивидуальных решений к компетентным специалистам.

В ЕС MiCA регулирует определённые криптоактивы и услуги. Общее применение началось 30 декабря 2024 года, а указанный регламентом максимальный переходный период, с учётом национальных решений, заканчивался 1 июля 2026 года. Проверяйте разрешение и его охват в действующих официальных реестрах. Старого упоминания о регистрации недостаточно. Разрешение не гарантирует цену, платёжеспособность или полное возмещение.

Регламент 2023/1113 устанавливает сведения, сопровождающие переводы с участием обязанных поставщиков. Для переводов свыше 1 000 евро с адресами самостоятельного хранения предусмотрены меры оценки владения или контроля. Порог не создаёт общего освобождения от идентификации ниже него. Переводы между лицами без поставщика исключены из сферы этого регламента, но другие обязанности сохраняются.

Храните достаточные для своего случая документы о покупках, продажах, комиссиях и происхождении, защищая их от лишнего доступа. Для частного учёта не нужно публиковать всю историю. В курсе также не обучают дроблению операций для обхода контроля, искажению данных или сокрытию доходов.

Если записывают или расшифровывают речь и можно определить учащегося по прогрессу, сервис должен определить цель, правовое основание, хранение, доступ, обработчиков и применимые права. Коммерческую конфигурацию конфиденциальности проверяют до продажи, а не определяют наугад во время звонка.

Практика

1. Подготовьте для консультанта вымышленный случай с местом жительства, деятельностью и операциями, без ключей.
2. Найдите, где проверить разрешение поставщика и дату сведений.
3. Разработайте частный журнал операций и политику минимизации данных учащегося.

Проверьте себя на практике

Различайте правовую норму, политику биржи и техническую возможность Bitcoin.

Частый вопрос

Запрещено ли в ЕС любое самостоятельное хранение? Из приведённых норм это не следует. Избегайте категоричных заголовков и проверяйте конкретное положение и его охват.

Где сделать паузу

Сохраните открытые вопросы для консультанта без передачи преподавателю личных документов.

Отменяет ли упомянутый для некоторых мер проверки адреса порог в 1 000 евро все обязанности ниже этой суммы?

1. Да.
2. Только если разбить операцию.
3. Нет. Это не общее освобождение от идентификации или других обязанностей.

> **Показать ответ: Нет. Это не общее освобождение от идентификации или других обязанностей.**
> Норму нужно толковать применительно к конкретной мере и её сфере действия. Порог не является универсальным освобождением.

Наследование, преемственность и ежегодная тренировка

Цель

Создайте план, позволяющий уполномоченным людям действовать без преждевременного раскрытия всего.

Разберитесь в теме

Наследование сочетает юридические полномочия, поиск материалов и техническую возможность. Человек может быть наследником и не уметь восстановить кошелёк. Другой может иметь ключ без права им пользоваться. С надлежащей консультацией план должен решить обе задачи.

Отделите общие инструкции от доступа к секретам. Опись описывает, что существует, к кому обратиться и что проверить, без помещения всех ключей и паролей в широко доступный документ. Не публикуйте сид-фразы в завещаниях или делах, которые могут обращаться за пределами вашего контроля.

Для мультиподписи определите, кто хранит политику и копии, какой порог достижим после потери и что произойдёт при смерти ключевого участника. Один хранитель с достаточным набором компонентов может стать единственной точкой злоупотребления. Чрезмерно сложное распределение способно сделать имущество невосстановимым.

Включите восстановление паролей криптограммы и дополнительной фразы при наличии, сведения деривации, совместимость устройств и процедуру прекращения работы производителя. Не предполагайте возможности использовать проприетарный файл или биометрический отпечаток без подготовки. Испытывайте совместимость на тестовых данных в документированных форматах.

Пересматривайте план после перемен в семье, месте жительства, политике, ПО или составе участников и проводите периодическую тренировку. Она должна проверить понимание инструкций доверенным человеком без раскрытия имущества и ненужного перевода денег.

Практика

1. Заполните личный шаблон с ответственными, компонентами, разрешённым доступом и заместителями.

2. Передайте другому человеку лабораторные инструкции без устного пояснения и наблюдайте, где возникнут трудности.
3. Устраните неоднозначности и запишите дату пересмотра. Курс не создаёт напоминаний автоматически.

Проверьте себя на практике

Объясните, что произойдёт при вашей недоступности и какие сведения нужны каждой роли на каждом этапе.

Частый вопрос

Заменяет ли схема 2 из 3 план наследования? Нет. Это технический инструмент. Наследникам по-прежнему нужны контекст, материалы, координация и законные полномочия.

Где сделать паузу

Храните план вне курса и отметьте только «тренировка проверена».

Какой критерий полезен при оценке плана наследования?

1. Уполномоченный человек может пройти документированную тренировку без импровизации и преждевременного получения секретов.
2. В нём много страниц.
3. Он зависит исключительно от запоминания одного пароля.

> **Показать ответ: Уполномоченный человек может пройти документированную тренировку без импровизации и преждевременного получения секретов.**
> Восстановимость и контроль доступа нужно проверять на практике.

Цена, накопления и фундаментальный анализ

Цель

Анализируйте инвестиционные доводы, отличая их от проверяемых технических свойств.

Разберитесь в теме

Цена складывается из сделок на конкретных рынках и может различаться по площадкам. На достижимый результат влияют ликвидность, валюта котировки, глубина рынка, часы банковских сервисов и спрос. Экранная котировка не является гарантированным предложением для вашего объёма.

Фундаментальный анализ изучает принятие, спрос, конкуренцию, экономическую безопасность, регулирование и предложение. Известный график выпуска сам по себе не определяет будущую цену. Оценки денежной полезности или «внутренней стоимости» зависят от допущений. ИИ не может представить объективное число как универсальную истину.

Периодические покупки распределяют время входа, но не гарантируют прибыль и не исключают продолжительных потерь. Долгосрочные накопления тоже требуют ликвидности для обязательств, переносимости волатильности и плана хранения. Курс не предписывает долю имущества и не решает за вас.

Разделите три вопроса: понимаю ли я актив, могу ли хранить и восстановить его, могу ли принять экономический риск? Умение обращаться с ключами не отвечает автоматически на третий вопрос. Обучение не превращает прогноз цены или исторический график в персональную рекомендацию.

Практика

1. Запишите вымышленный инвестиционный тезис, его допущения и факты, которые его опровергнут.
2. Смоделируйте падение на 50 % и одновременную потребность в ликвидности без ввода реальных активов.
3. Отметьте проверяемые данные довода и ожидания.

Проверьте себя на практике

Обсуждайте инвестиции без обещания доходности и без подмены свидетельств убеждённостью.

Частый вопрос

Гарантирует ли дефицит рост цены? Нет. Спрос и другие условия по-прежнему определяют рыночную цену.

Где сделать паузу

Сохраните учебные допущения без автоматической инструкции на покупку.

Что гарантируют периодические покупки?

1. Прибыль в долгосрочной перспективе.
2. Доходность не гарантируется. Покупки лишь распределяются по времени согласно выбранному правилу.
3. Защиту от потери ключей.

> **Показать ответ: Доходность не гарантируется. Покупки лишь распределяются по времени согласно выбранному правилу.**
> Распределение покупок по времени не устраняет экономических или операционных рисков.

Выбор места для приобретения bitcoin

Цель

Оцените поставщика по разрешениям, стоимости, выводу, конфиденциальности и кастодиальному риску.

Разберитесь в теме

Сравнивайте поставщиков по проверяемым критериям: юрлицо и юрисдикция, разрешённые услуги, сеть вывода, комиссии, спред, лимиты, поддержка, аутентификация и обработка данных. Торговое имя и спонсорство не доказывают разрешения на конкретную услугу.

В полную стоимость могут войти пополнение, конвертация, спред, торговая комиссия, вывод и банковские расходы. У торговли «без комиссии» может быть более широкий спред. Проверьте чистые суммы и справочную валюту. При цели самостоятельного хранения включите вывод в бюджет.

Пока остаток хранит кастодиан, вы зависите от поставщика. Доказательство резервов само по себе не подтверждает все обязательства, принадлежность средств или будущую платёжеспособность. Проверьте ограничения и до зависимости от новой процедуры сделайте небольшой посильный тестовый вывод.

Коммерческая идентификация может связать вашу личность с выводом средств. Последующая защита данных не стирает известное поставщику. Не искажайте сведения и не используйте курс для обхода обязанностей. Покупка учебного кода также создаёт коммерческую запись отдельно от кошелька.

Практика

1. Заполните вымышленную таблицу двух поставщиков с полной стоимостью, сетью, минимумом вывода, разрешением и требуемыми сведениями.
2. Рассчитайте чистую сумму учебной операции с учётом всех перечисленных расходов.
3. Спроектируйте пробный вывод на заранее проверенный адрес без выполнения с этого учебного сайта.

Проверьте себя на практике

Обоснуйте выбор для своего случая и определите устаревшие или непроверенные сведения.

Частый вопрос

Рекомендует ли курс одну лучшую биржу для всех? Нет. Разрешения, тарифы, обслуживаемые страны и условия меняются. Сравнение требует указания даты и сценария.

Где сделать паузу

Сохраните таблицу без данных доступа и удостоверяющих документов.

Что полезнее сравнить, чем одну лишь торговую комиссию?

1. Полную стоимость до получения BTC в нужной сети на нужный адрес.
2. Число подписчиков поставщика.
3. Цвет приложения.

> **Показать ответ: Полную стоимость до получения BTC в нужной сети на нужный адрес.**
> Итоговая цена включает статьи расходов, которые могут не входить в заявленную комиссию.

Счета, ордера и издержки исполнения

Цель

Разберитесь в основных ордерах и защите счёта, не превращая курс в торговый терминал.

Разберитесь в теме

Рыночный ордер отдаёт приоритет доступному исполнению с риском проскальзывания. Лимитный задаёт максимальную цену покупки или минимальную продажи, но может не исполниться или исполниться частично. Стоп-ордер запускает другое действие по правилам площадки. Сам по себе он не гарантирует итоговую цену.

Книга ордеров показывает доступные предложения, не обещая сохранения всех объёмов. При падении или низкой ликвидности результат может отличаться от последней котировки. У stop-market и stop-limit разные риски: исполнение по худшей цене либо возможное неисполнение.

Защитите вход уникальным паролем, устойчивой к фишингу аутентификацией при поддержке, проверкой сеансов и надлежащими ограничениями вывода. Храните восстановление второго фактора независимо. Ключ API автоматизации может давать гораздо более опасные разрешения, чем нужны для чтения. Не вводите его в чат с преподавателем или на учебном сайте.

До вывода проверьте актив и сеть Bitcoin, адрес кошелька и чистые суммы. Площадка может использовать одинаковый символ для разных продуктов. Затем сохраните подходящие документы о покупке, исполнении, комиссиях и выводе. Вывод на собственный кошелёк не равен новой покупке.

Практика

1. Смоделируйте книгу ордеров с 1 единицей по цене 100 и ещё одной по цене 102. Объясните, почему покупка двух единиц рыночным ордером не гарантирует средней цены 100.
2. Спроектируйте лимитный ордер и опишите ситуацию, в которой он не исполнится.
3. Проверьте разрешения вымышленного API и исключите вывод средств, если нужны только запросы.

Проверьте себя на практике

Опишите для каждого ордера приоритет, цену и риск того, что он не исполнится.

Частый вопрос

Всегда ли stop-loss точно ограничивает убыток? Нет. Могут помешать ценовые разрывы, ликвидность, проскальзывание и правила площадки.

Где сделать паузу

Сохраните результат упражнения без реальных ордеров и ключей API.

Какой риск сохраняет лимитный ордер на покупку по цене 100?

1. Ордер может не исполниться или исполниться частично.
2. Он обязательно исполнится по любой цене.
3. Он автоматически создаст резервную копию.

> **Показать ответ: Ордер может не исполниться или исполниться частично.**
> Если установить предельную цену, ордер может остаться неисполненным.

M11

Свечи, индикаторы и искажения технического анализа

Цель

Читайте графики как исторические данные и оценивайте стратегию, не принимая шаблоны за предсказание.

Разберитесь в теме

Свеча сводит цены открытия, максимума, минимума и закрытия периода. Объём зависит от источника. Площадка, валюта, часовой пояс или интервал могут изменить изображение. Свеча не показывает полного порядка движений внутри интервала.

Скользящая средняя сглаживает прошлые цены. Индикатор момента преобразует наблюдаемые данные по формуле. Ни один не знает будущего. Два показателя из одного ряда могут давать тесно связанную информацию, несмотря на разные имена и цвета.

До просмотра результата задайте вход, выход, условие недействительности, издержки, размер и данные. Избегайте выбора одних победителей, подгонки параметров и использования будущих данных для прежнего решения. Разделяйте обучающие данные и временную проверку.

Тест на исторических данных учитывает спред, комиссии, проскальзывание, наличие данных и достижимость исполнения. Валовая доходность, доля успехов, максимальный убыток и распределение потерь отвечают на разные вопросы. Система с множеством удач может терять деньги при больших неудачах. Сигнал покупки или продажи не преподносится как достоверность.

Практика

1. Прочитайте вымышленную свечу и объясните, какой информации о порядке событий она не содержит.
2. Запишите правило до оценки десяти синтетических результатов, учитывая издержки и критерий неудачи.
3. Сравните 9 выигрышей по 1 с убытком 15. Валовой результат −6, несмотря на 90 % удачных сделок.

Проверьте себя на практике

Оцените привлекательный результат с позиций отбора, издержек или риска без реальных сделок.

Частый вопрос

Гарантирует ли сочетание множества индикаторов лучший сигнал? Нет. Оно может усилить переобучение и сложность, не добавляя независимой информации.

Где сделать паузу

Сохраните правило и результаты лаборатории, не создавая рыночный ордер.

Девять сделок приносят по 1 единице, а одна теряет 15. Каков результат до издержек?

1. +90 %.
2. +6.
3. −6.

> **Показать ответ: −6.**
> Девять единиц прибыли минус пятнадцать убытка дают шесть единиц убытка.

Маржинальные операции, фьючерсы и автоматизация

Цель

До рассмотрения сложных продуктов разберитесь в размере позиции, ликвидации и сбоях автоматизации.

Разберитесь в теме

Плечо увеличивает размер позиции относительно вложенного капитала. В упрощённом примере при марже 100 и позиции 1 000 неблагоприятное движение базового актива на 5 % означает потерю 50 до издержек — половину начальной маржи. Реальные требования поддержания, ликвидации, обеспечения и комиссий могут ухудшить результат и сработать раньше ожидаемого.

Фьючерсы и бессрочные контракты могут включать срок исполнения, расчёт разницы, ставки финансирования и справочные цены, отличные от последней сделки. Они не равны выводу нативного bitcoin на Cuvex. Хранение сид-фразы не защищает позицию от ликвидации или несостоятельности контрагента.

Бот автоматизирует правила вместе с их ошибками. Нужны ограничения позиции, минимальные разрешения, идемпотентность ордеров, сверка, контроль убытков, аварийная остановка и наблюдение. Повтор запроса после тайм-аута при неизвестном первом результате может удвоить позицию.

ИИ может объяснить понятия и выявить несогласованность в вымышленном случае. Он не должен получать ключи API, включать торговлю или обещать прибыльную стратегию. Для основной цели курса знание рисков позволяет отказаться от непонятных продуктов.

Практика

1. Решите пример позиции и маржи, не предполагая ликвидацию ровно при 10 %.
2. Смоделируйте API, исполнивший ордер с потерей ответа. Объясните необходимость сверки перед повтором.
3. Не подключаясь к брокеру, спроектируйте остановку, запрещающую новые ордера и проверяющую уже открытые.

Проверьте себя на практике

Назовите по риску, сохраняющемуся после стоп-ордера, при работе бота и при самостоятельном хранении внешних средств.

Частый вопрос

Убирает ли автоматизация эмоции и гарантирует ли результат? Нет. Она может уменьшить импульсивные вмешательства и одновременно умножить ошибки проектирования или исполнения.

Где сделать паузу

Отметьте дополнительную тему как понятую без включения сложных продуктов.

При позиции 1 000 и марже 100 убыток в 5 % от позиции до издержек равен чему?

1. Убытку 5.
2. Убытку 50, то есть 50 % маржи.
3. Нулю, если используется бот.

> **Показать ответ: Убытку 50, то есть 50 % маржи.**
> Из-за кредитного плеча и издержек результат относительно маржи отличается от изменения цены актива.

Lightning и другие уровни

Цель

Разберитесь в платежах по каналам и определите функции, отсутствующие в рассмотренной процедуре Cuvex.

Разберитесь в теме

Lightning использует каналы и механизмы обновления для платежей без записи каждого отдельного обмена в базовую цепочку. Открытие, закрытие каналов и отдельные сценарии восстановления могут требовать транзакций в цепочке. Доступность, входящая и исходящая ликвидность и наблюдение зависят от устройства кошелька и используемых сервисов.

Счёт может содержать сумму, описание и срок действия. Единицу в зависимости от контекста выражают в сатоши или миллисатоши. Миллисатоши не означают наличия выходов меньше сатоши в базовой цепочке. Нужны совместимость и доступный маршрут. QR-код не гарантирует оплату любым приложением.

Кастодиальные и некастодиальные сервисы используют очень разные модели. Обычная быстрота не доказывает отсутствия рисков. Не представляйте Lightning как полную анонимность: остаются наблюдатели, маршруты, контрагенты и существенные метаданные.

Чат Cuvex может координировать запросы sat, оплачиваемые со счёта WOW в базовой цепочке. В этой редакции Desk не приписывают узел Lightning, управление каналами или подписание счетов Lightning. Если запрос содержит несколько способов, проверьте, какой понимаете вы и какой выполнит приложение.

Практика

1. Классифицируйте учебные адрес базовой цепочки, URI bitcoin: и счёт Lightning.
2. Сравните платёж по цепочке и по каналу по подтверждению, ликвидности, хранению и восстановлению.
3. Объясните, почему истёкший счёт нужно уточнить с получателем, а не переосмысливать как адрес.

Проверьте себя на практике

Отклоните несовместимый способ без раскрытия ключей и необоснованного приписывания сбоя Cuvex.

Частый вопрос

Все платежи в sats идут через Lightning? Нет. Сатоши выражают стоимость, а способ зависит от протокола.

Где сделать паузу

Сохраните способ оплаты из упражнения без реальных счетов.

Каких данных достаточно, чтобы определить оплату запроса через Lightning?

1. Присутствия слова sats.
2. Того, что запрос пришёл через чат.
3. Совместимых формата и способа оплаты, а не только единицы измерения или канала сообщения.

> **Показать ответ: Совместимых формата и способа оплаты, а не только единицы измерения или канала сообщения.**
> Расчётная единица и платёжная сеть — разные характеристики.

Taproot, MuSig2 и постквантовая перспектива

Цель

Различайте стандарты, предложения и реализованные возможности.

Разберитесь в теме

Taproot допускает условия расходования по ключевому и скриптовому путям. Подписи Шнорра и агрегация могут улучшать отдельные конструкции, однако конфиденциальность зависит от настройки и способа расходования. Адрес bc1p не доказывает отсутствия других участников и не раскрывает всех скрытых условий.

MuSig2 позволяет группе подписантов в ходе взаимодействия агрегировать ключи и получить совместимую подпись Шнорра. Базовый стандарт — N из N. Для произвольного порога M из N нужна другая конструкция или дополнительный протокол. Управление одноразовыми значениями nonce и сеансами критично и не реализуется неформальным обменом сообщениями.

PSBT v2 меняет организацию информации относительно v0. Это не автоматическое обновление любого файла с транзакцией версии 2. Прошивки Final этой редакции сохраняют PSBT v0, P2WSH/sortedmulti и SIGHASH_ALL для профиля мультиподписи. Будущим возможностям нужны собственные протокольные условия и проверка.

В 2024 году NIST опубликовал первые окончательные постквантовые стандарты. Само по себе это не меняет подписей Bitcoin. Постквантовый алгоритм проверки подлинности прошивки защищал бы этот уровень, не превращая автоматически ECDSA или Schnorr конкретной UTXO в постквантовые подписи. Преподаватель не может с уверенностью назвать и дату будущей атаки.

Практика

1. Распределите пять утверждений по категориям: стандарт, проверенная реализация, предложение или реклама.
2. Объясните, почему «поддерживает получателя Taproot» не доказывает «подписывает вход Taproot».
3. Изобразите отдельные уровни: подпись прошивки, шифрование секрета, чат и подпись расходования Bitcoin.

Проверьте себя на практике

Запрашивайте свидетельство для конкретного уровня и не переносите гарантии между протоколами.

Частый вопрос

Переносить ли средства из-за заголовка о квантовых вычислениях? Реальное решение требует актуальных технических свидетельств, проверяемой поддержки, оценки рисков и плана безопасного переноса. Курс не предписывает движение средств по заголовкам.

Где сделать паузу

Запишите технические вопросы без создания автоматического плана расходования.

Если постквантовая подпись загрузчика реализована и проверена, меняет ли она условия подписания уже существующей UTXO?

1. Нет. Это разные уровни.
2. Да, она переводит всю сеть на другой алгоритм.
3. Она устраняет потребность в резервных копиях.

> **Показать ответ: Нет. Это разные уровни.**
> Проверка подлинности обновления не переписывает условия расходования в Bitcoin.

Совместимость и выход из экосистемы производителя

Цель

Спланируйте продолжение работы при изменении ПО, устройства или поставщика.

Разберитесь в теме

Совместимость не проверяется перечнем сокращений. Должны сохраняться сеть, скрипт, деривация, ключи, политика, формат транзакции и смысл подписей. Оба приложения могут понимать BIP174 и всё же не поддерживать одинаковые поля, размеры или типы входов.

Чтобы выйти из зависимости от интерфейса, храните документированные сведения восстановления и тренируйтесь с учебными кошельками. Стандартная мнемоника может позволить вывод ключей, но при мультиподписи нужна полная политика. Метки BIP329 добавляют контекст конфиденциальности, а история чата имеет другую область применения.

Не раскрывайте реальную сид-фразу ради проверки совместимости. Сначала испытайте экспорт открытых дескрипторов и восстановление watch-only. Если в аварийном случае необходимо воссоздать ключи, используйте предназначенную среду и рассмотрите последующий перенос. Нулевой остаток несовместимого кошелька сам по себе не доказывает потерю средств.

Храните проверяемые копии документации, версии курса и нужных инструментов. На установку влияют подписи приложений, истекшие сертификаты и изменения систем. Наличие открытого исходного кода не гарантирует, что любой человек соберёт его через годы без сохранения зависимостей и знаний.

Практика

1. Спланируйте проверку выхода с пустым счётом: одинаковые сеть, политика и контрольный адрес в двух совместимых реализациях.
2. Перечислите стандартные части и те, для которых нужны преобразователь или документация формата Cuvex.
3. Определите результат, подтверждающий совместимость, и то, что ещё требует оборудования или реальной подписи.

Проверьте себя на практике

Опишите восстановление без зависимости от того, будет ли компания продолжать тот же сервис.

Частый вопрос

Означает ли открытый код, что производитель уже не важен? Нет. Распространение, обслуживание, физические компоненты и практический опыт по-прежнему важны. Открытость позволяет проверку и потенциальную преемственность, но не гарантирует их автоматически.

Где сделать паузу

Сохраните результаты лаборатории с версиями и наблюдавшимися пределами.

Какое свидетельство совместимости убедительнее?

1. В обоих приложениях есть слово «Bitcoin».
2. В лаборатории на установленных версиях восстановлены и проверены те же политика и адрес.
3. Значки приложений похожи.

> **Показать ответ: В лаборатории на установленных версиях восстановлены и проверены те же политика и адрес.**
> Испытание должно сохранять существенные условия и давать проверяемый результат.

Техническая лаборатория с regtest

Цель

Разберитесь в воспроизводимой лаборатории, не смешивая синтетические испытания и физическое использование.

Разберитесь в теме

Regtest позволяет создать контролируемую локальную цепочку для генерации блоков и испытания транзакций без экономической ценности. Используйте отдельные каталоги и данные доступа, не импортируйте реальные материалы. Результаты сами по себе не подтверждают работу USB, NFC, Bluetooth или камеры физического устройства.

Полная лаборатория фиксирует версии, конфигурацию сети, политику, тестовые входы, PSBT, подписи, итоговую транзакцию и результат принятия. Можно проверить равенство сумм, отказ изменённой подписи и включение действительного платежа в локальный блок. Испытание должно включать отказы, а не только удачное прохождение.

В материалах проверки Desk 9.21 указаны испытания с Bitcoin Core 31 regtest и автоматические проверки движка и моделируемого интерфейса. Редакция использует их как документальные свидетельства и не заявляет о повторении испытаний или операциях с устройствами. Проверка пакета также не доказывает установку на всех системах.

До технического занятия инженер предоставляет готовую лабораторию и процедуру, совместимую с версией учащегося. Не открывайте RPC в интернет, чтобы им управлял преподаватель. ИИ может помочь истолковать синтетические результаты, но не должен получать данные доступа или административные разрешения.

Практика

1. В подготовленной лаборатории наблюдайте действительную транзакцию и транзакцию с изменённой подписью. Запишите принятие или отказ.
2. Проверьте пример неверной сдачи и пример несовместимой сети.
3. Разделите в отчёте «проверка движка», «смоделированный интерфейс» и «физическое оборудование».

Проверьте себя на практике

Точно укажите испытанное и оставшееся, не представляя симуляцию как сертификацию.

Частый вопрос

Если regtest работает, можно ли продавать курс как проверенный на всех устройствах? Нет. Ещё требуются проверки физических процедур, установки, доступности, восстановления и коммерческого сервиса.

Где сделать паузу

Остановите и сохраните лабораторию по её инструкциям, оставив только синтетические данные.

Доказывает ли проверка движка в regtest фактическое чтение NFC конкретным телефоном?

1. Да, поскольку оба используют Bitcoin.
2. Да, если PSBT невелик.
3. Нет. Для этого нужно отдельное физическое испытание.

> **Показать ответ: Нет. Для этого нужно отдельное физическое испытание.**
> Разные среды проверки имеют разные пределы применимости.

Итоговый проект и план преемственности

Цель

Продемонстрируйте самостоятельность от подготовки до восстановления и конфиденциальности.

Разберитесь в теме

Итог курса — умение объяснить намерение, проверить результат и остановить непонятную операцию, а не запомнить меню. Оценка сочетает понятия, практику под руководством и самостоятельный случай. Она никогда не требует раскрывать проверяющему сид-фразы, имущество или личные адреса.

Случай A: настройте учебную среду, определите модели и версии, защитите Desk, привяжите учебную криптограмму и восстановите счёт watch-only. Объясните необходимые копии и сведения, наблюдаемые вашим поставщиком.

Случай B: спроектируйте платёж с вымышленными UTXO разных контекстов, обоснуйте выбор, проверьте получателя, сдачу и комиссию и опишите ветвь подписания своего устройства. Разберите разрывы при возврате ответа и при публикации без дублирования платежа. При отсутствии физически принятого оборудования часть фиксируется как смоделированная и остаётся открытой для физической проверки.

Случай C: спроектируйте схему 2 из 3, разыграйте приглашение и проверку, сравните в Mirror выбранное поле в произвольном порядке и объясните охват отметки OK. Восстановите учебную политику, смоделируйте потерю участника и подготовьте преемственность и наследование.

Предлагаемое условие успешного завершения — не менее 80 % по знаниям и правильное выполнение всех критических проверок: не раскрывать секреты, проверять сеть и выходы, различать этапы и сохранять восстановление. Критическая ошибка требует разбора и новой практики и не компенсируется правильными ответами о рынке. Если выдаётся коммерческий сертификат, в нём указывают оценивавшееся и наличие физического наблюдения или только симуляции.

Практика

1. Завершите три случая с синтетическими данными и собственным объяснением.

2. Пройдите итоговую проверку в приложении к курсу и разберите каждый ошибочный ответ.
3. Передайте только лист результатов без секретов с подтверждением охвата и перечнем оставшегося.

Проверьте себя на практике

Умейте самостоятельно остановиться при недостатке свидетельств для операции и определить, что нужно для продолжения.

Частый вопрос

Означает ли прочтение всех страниц готовность хранить любую сумму? Нет. Навыки следует испытать, риск оценить для своей ситуации. Чтение и тренировки не гарантируют будущих результатов.

Где сделать паузу

Сохраните план пересмотра и незавершённые упражнения. Возвращайтесь к нужной главе без повтора всего курса.

Какое условие существенно для завершения практического обучения?

1. Открыть все страницы.
2. Продемонстрировать восстановление и проверку операций в документированных пределах без раскрытия секретов.
3. Предсказать цену в следующем месяце.

> **Показать ответ: Продемонстрировать восстановление и проверку операций в документированных пределах без раскрытия секретов.**
> Усвоение материала подтверждается проверенными навыками и пониманием их пределов, а не переходами по страницам или прогнозами.

Руководство учащегося

Практическое руководство Cuvex

Руководство дополняет уроки. Для каждой процедуры описаны последовательность действий из рассмотренных источников, проверки и точка остановки. Это кандидат для пилотного использования. Он не подтверждает собственных физических испытаний Original, BIT, телефонов или каждой настольной платформы. До обучения на реальных средствах команда должна заполнить матрицу приёмки и исправить расхождения в надписях или изображениях экранов.

Справочные версии: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 и Mirror 1.0.0-beta.12.12. Выбор профиля в Desk отражает заявленную совместимость и не является удалённым измерением прошивки. Приведённые снимки экрана Mirror получены из эмулятора Android для пакета 12.12. Фотографии продукции — корпоративные материалы, которые не подтверждают версию на имеющемся устройстве.

P01 | Проверка происхождения и версии | Cuvex | L16,L21 | C01,C02

Подготовка: подготовьте сведения о покупке и официальный канал, который вы можете проверить независимо. Пока не вводите секреты.

1. Осмотрите упаковку и пломбы. При признаках вмешательства остановите ввод в эксплуатацию и сохраните свидетельства без чувствительных данных.
2. Пройдите проверку целостности и пломб в приложении, совместимом с вашей поставкой. Вводите коды только там, никогда не сообщайте их преподавателю.
3. Определите модель Original или BIT и доступную ревизию. Проверьте версии, отображаемые устройством и приложениями.
4. Сверьте с опубликованной командой матрицей. Каталог или хеш не заменяют подтверждения подлинности прошивки и физической приёмки.

Результат: модель, версии и происхождение проверены без раскрытия секретов. Если коды недействительны или интерфейс отличается, не пытайтесь принудительно продолжить по старому руководству.

Пауза: остановитесь перед загрузкой материалов хранения. Прослеживаемость продажи сама по себе не гарантирует отсутствия сложного вмешательства.

P02 | Обновление Original по Bluetooth | Original | L46 | C01,C02,C03

Подготовка: нужны проверенные резервные копии, стабильное питание, официальный совместимый пакет и принятая для вашей системы процедура. Курс не подтверждает физическую доступность всех шагов на каждой платформе.

1. В разделе устройств или прошивки приложения выберите Original и соответствующую официальную загрузку либо подлинный локальный файл.
2. Включите режим обновления в меню устройства и установите соединение по процедуре приложения. Держите устройства рядом и избегайте конкурирующих сеансов.
3. Введите код с экрана Original в указанное поле. Не путайте его с паролем криптограммы.
4. Проследите этапы передачи, проверки, установки и перезапуска. Показание процентов не доказывает успешной установки.
5. Проверьте итоговую версию на Original и запишите её в приложении, если предусмотрено соответствующее поле.

Результат: версия проверена на экране после перезапуска, завершение процедуры подтверждено. Если сбой возник до PIN-кода, во время передачи пакетов или в конце, запишите этап и код ошибки. Не отключайте устройство и не меняйте ПО наугад, пытаясь «пройти 99 %».

P03 | Обновление BIT по USB | BIT | L46 | C01,C02,C03

Подготовка: определите фактический носитель BIT, питание и совместимый официальный пакет. Сохраните резервные копии до изменения ПО.

1. В совместимой процедуре обновления прошивки Desk или Mirror выберите BIT.
2. Подключите устройство подходящими кабелем и адаптером для передачи данных. Когда приложение запросит, разрешите доступ к тому или папке.
3. Выберите подлинную прошивку для модели. До передачи проверьте версию и сведения о совместимости.
4. Дождитесь этапов передачи и проверки устройством. В соответствии с протоколом том может исчезнуть и смонтироваться вновь.
5. После перезапуска проверьте версию на BIT и итоговый результат в приложении.

Результат: установка проверена на устройстве. Если том не появился, проверьте режим устройства, кабель данных, разрешения, монтирование и другие активные сеансы. Не подменяйте том одноимённой папкой на компьютере. Для восстановления после неудачного обновления нужна официальная процедура именно этого оборудования.

P04 | Генерация кошелька с помощью монеты и кубиков | Cuvex | L17 | C01

Подготовка: уединённое место, подходящие кубики и монета. Микрофон преподавателя и камеры должны быть выключены. Используйте учебный кошелёк.

1. Откройте создание кошелька и процедуру получения энтропии в прошивке. Заранее установите порядок четырёх кубиков.
2. Введите результат монеты и каждого кубика как указано на экране. Не меняйте результаты по своему предпочтению.
3. В рассмотренном исходном коде индекс = монета × 1 296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Принимаются только индексы от 0 до 2 047 включительно.
4. Если результат отклонён, снова бросьте монету и все кубики. Предупреждение сохраняет предыдущие слова и просит повторить весь набор бросков.
5. Завершите алгоритм на устройстве, включая итоговую проверку. Защитите мнемоническую фразу и проверьте восстановление без посторонних.

Результат: кошелёк создан полной процедурой, без ручного выбора слов. Если экран расходится с источником, остановитесь. Не используйте публичный пример бросков, сид-фразы или ключа как собственный материал.

P05 | Шифрование секрета | Cuvex | L18,L19 | C01

Подготовка: выберите модель, формат содержимого и защиту. Ввод на компьютере или телефоне раскрывает исходные данные в этой среде, даже если у получателя они зашифрованы.

1. Выберите шифрование и поддерживаемый тип BIP39, SLIP39, Monero или текст. Не подменяйте один словарь другим. Рассмотренная клавиатура для обычного текста допускает до 500 символов. Хранение другого формата не означает поддержки подписания для его сети.
2. Для сохранения изоляции вводите содержимое прямо на устройстве. Проверьте порядок, символы и дополнительные поля на его экране.

3. Выберите индивидуальную или совместную защиту согласно процедуре, а на BIT при необходимости биометрию. Отличайте этот порог от порога подписей Bitcoin.
4. Введите и подтвердите пароли без посторонних по правилам проверки прошивки. Не применяйте автоматически правила Desk.
5. Для Original запишите данные на пустую совместимую карту. Для BIT сохраните объекты, экспортируемые процедурой USB. Дождитесь подтверждения.
6. Выполните пробное восстановление для проверки содержимого и закройте секрет по завершении.

Результат: восстановление криптограммы проверено. При сбое записи или чтения защитите оригинал и повторите операцию по подсказке устройства. Не удаляйте заголовки и не принуждайте систему к перезаписи.

P06 | Расшифрование на устройстве | Cuvex | L18 | C01,C02

Подготовка: обеспечьте уединение и наличие достаточных компонентов разблокировки. Рядом с отображаемым секретом отключите микрофон и захват экрана.

1. Запустите расшифрование на нужной модели и передайте криптограмму в Original по NFC или в BIT по процедуре USB.
2. До ввода данных доступа проверьте псевдоним и идентификатор объекта.
3. Предоставьте необходимые пароли и биометрические данные, если этого требует формат. При ошибках не повторяйте попытки автоматически: действуют ограничения доступа и блокировка.
4. Проверяйте содержимое только на предусмотренном экране. QR-код с секретом так же чувствителен, как текст секрета.
5. Закройте или завершите процедуру согласно указаниям устройства. Храните носитель и данные доступа раздельно в соответствии с вашим планом.

Результат: содержимое восстановлено без посторонних, сеанс завершён. Если формат не распознан, подлинность не подтверждается или содержимое неожиданно, не «исправляйте» его неизвестным приложением. Сообщите поддержке версию, формат и ошибку без передачи секрета.

P07 | Подготовка к восстановлению биометрической криптограммы | BIT | L19,L47 | C01,C02

Подготовка: учебная криптограмма и документация её формата. Наличие одной копии .bin не доказывает возможность восстановления.

1. В карточке Desk проверьте наличие биометрических компонентов и доступные варианты экспорта для восстановления.
2. Сохраните связанный процедурой комплект файлов и независимую копию, используя нейтральные идентификаторы.
3. Испытайте обычную разблокировку на BIT и задокументируйте, какие пароли и условия требуются.
4. Изучите исключительный способ локального восстановления и поддерживаемые форматы. Убедитесь в наличии необходимых материалов до того, как они понадобятся.
5. На данных без средств отработайте сценарий неисправного устройства или недоступного отпечатка.

Результат: проверенный план для конкретного формата с известными ограничениями. Это не означает, что любую биометрию можно обойти или что отпечаток заменяет копии. После восстановления секрета на компьютере оцените его раскрытие и необходимость последующего переноса контроля.

P08 | Создание и проверка копии криптограммы | Cuvex и Desk | L20 | C01,C02

Подготовка: определите исходную копию и совместимый носитель назначения без данных, требующих сохранения.

1. Для Original используйте клонирование на устройстве или совместимую функцию Desk и предоставьте исходный и целевой носители в указанном порядке.
2. Держите карты неподвижно и соблюдайте отказ в записи на носитель, уже содержащий криптограммы.
3. Для BIT или файла экспортируйте весь комплект компонентов процедуры и сохраните требуемые имена или связи между файлами.
4. Изолируйте оригинал и выполните пробные чтение и восстановление с новой копии.
5. Запишите дату, формат и результат в личный журнал. Храните копии раздельно с учётом независимости физических рисков.

Результат: вторая проверенная копия. Она не создаёт иного кошелька, не отзывает пароли и не защищает уже раскрытую сид-фразу. При неудаче на целевом носителе сохраните оригинал и не пытайтесь «починить» его ради совпадения двух копий.

P09 | Создание пароля Desk, разблокировка и смена пароля | Desk | L21,L40 | C02

Подготовка: проверенный установщик, подходящая архитектура и план резервного копирования хранилища.

1. Создайте хранилище с уникальным паролем длиной от 12 до 1 024 символов и введите тот же пароль для подтверждения.
2. Заблокируйте и вновь откройте хранилище, чтобы проверить доступ. Вводите пароль только в Desk.
3. В разделе безопасности откройте настройки доступа и блокировки и проверьте поведение при бездействии и переходе в фон. Во время демонстрации не включайте необязательное удаление данных.
4. Для смены пароля введите текущий и подтвердите новый по предусмотренной процедуре.
5. Если использовалась биометрия компьютера, настройте её заново по подсказке. Создайте актуальную копию и сохраните сведения о связи с предыдущими.

Результат: доступ проверен. Прежние копии сохраняют исходные пароли и шифрование. Биометрия компьютера и биометрия BIT — разные механизмы. При неудаче прекратите повторные попытки и проверьте способы восстановления. Не просите преподавателя хранить данные доступа.

P10 | Привязка и проверка криптограммы в Desk | Desk | L22 | C02

Подготовка: тестовая криптограмма известного происхождения и доступный способ передачи.

1. Откройте криптограммы или карты и выберите привязку через NFC, USB или совместимую копию.
2. Выберите оформление и источник. Для NFC используйте Cuvex Mirror, сопряжённый с компьютером по Bluetooth. При обмене через USB-C выберите том подключённого Cuvex BIT. Внешние USB-считыватели NFC в Cuvex Desktop не поддерживаются.
3. В карточке проверьте псевдоним, источник, размер, формат и распознанные условия. Это метаданные, а не расшифрованное содержимое.
4. Проверьте сохранённые счета, ожидающие привязки, и свяжите только проверенный счёт.

5. Если резервных копий недостаточно, экспортируйте копию и отдельно проверьте восстановление.

Результат: объект организован локально. Статус «Привязан» не удостоверяет сид-фразу или остаток. Для нераспознанного объекта проверьте формат и версию. Не меняйте расширение и не удаляйте данные, чтобы заставить приложение принять объект.

P11 | Активация счёта WOW только для наблюдения | Desk и Cuvex | L13,L22 | C01,C02

Подготовка: открытая информация, полученная в процедуре устройства, и самостоятельная приватная проверка её происхождения.

1. В карточке нужной криптограммы откройте активацию WOW или добавление счёта.
2. В зависимости от функции импортируйте дескриптор или поддерживаемые открытые данные из файла, с веб-камеры либо через Mirror.
3. Проверьте сеть, скрипт, происхождение, отпечаток, путь и контрольную сумму, когда они применимы. Не вводите сид-фразу или xprv.
4. Назовите счёт и осознанно выберите источник запросов, дав согласие на его использование.
5. Прежде чем делать вывод об остатке, проверьте контрольный адрес и охват поиска адресов.

Результат: кошелёк для наблюдения привязан. При нулевом остатке проверьте сеть, исходную дополнительную парольную фразу, деривацию, счёт, поставщика и сканирование, прежде чем считать средства исчезнувшими. Общий интерфейс может поддерживать сети, недоступные конкретному профилю мультиподписи. Учитывайте контекст.

P12 | Настройка узла и синхронизации | Desk | L25,L33 | C02

Подготовка: определите требования к конфиденциальности. При использовании Core нужен доступ к защищённому синхронизированному узлу.

1. В разделе безопасности откройте настройки конфиденциальности и узлов, выберите счёт WOW и проверьте его поставщика.
2. Явно выберите совместимый публичный сервис или Core. Для Core вводите адрес конечной точки, кошелёк и данные доступа только в приложении.
3. Дайте согласие на запрос, выяснив, какие данные получает каждый сервис. TLS не скрывает запрос от поставщика.

4. Синхронизируйте и проверьте дату, вершину цепочки, ход и завершённость. При повторном сканировании проверьте глубину охваченной истории и непрерывность выполнения.
5. При ответе 429 выдержите паузу. При сбое не считайте, что подключился другой узел. Конфигурация не переключает узлы без уведомления.

Результат: источник и состояние известны. Не открывайте RPC в интернет, не передавайте пароль и не ограничивайте поиск адресами с положительным остатком. Пустая история может быть частичным результатом.

P13 | Создание и восстановление запроса на получение | Desk и Cuvex | L26 | C01,C02

Подготовка: проверьте счёт, сеть и политику.

1. Откройте получение и создайте или восстановите подходящий запрос.
2. Добавляйте наблюдателя, назначение и ожидаемую сумму только при необходимости в этих локальных метаданных.
3. До получения существенной суммы проверьте адрес совместимым способом на устройстве. Если физических приёмочных испытаний не было, ограничьте упражнение симуляцией.
4. Передавайте только необходимые данные через аутентифицированный канал получателя.
5. Проверьте поступление, сумму и подтверждения по вашему сетевому источнику.

Результат: получение сверено, а не просто выпущен запрос. В мультиподписи показанные адреса сохраняют для запоздалых платежей и не назначают повторно. Достигнув лимита новых адресов без истории, восстановите прежние запросы. Не выставляйте индексы вручную в обход ограничения.

P14 | Метки, заморозка и BIP329 | Desk | L27 | C02,B13

Подготовка: лабораторный счёт с UTXO и пароль для защищённого экспорта.

1. Пометьте вход с учётом его контекста, без лишних персональных данных.
2. Осознанно заморозьте или разморозьте выход и проверьте доступный для расходования остаток. Ограничение локальное.
3. Экспортируйте метки защищённой функцией. Отличайте формат меток BIP329 от шифрования файла.
4. Импортируйте в совместимую копию и проверьте соответствие ссылок, меток и состояний заморозки.

5. Сохраните актуальную резервную копию метаданных и относящийся к ней пароль согласно вашему плану.

Результат: контекст сохранён, выбор выходов понятен. Не используйте импорт для автоматической разморозки без проверки. Не отправляйте преподавателю файл меток. Даже без ключей расходования он может раскрывать контрагентов и связи.

P15 | Подготовка платежа и отправка всего остатка | Desk | L28 | C02

Подготовка: проверенный запрос и счёт с достаточными доступными для расходования входами.

1. Откройте оплату из WOW, списка UTXO или чата и подтвердите счёт и сеть.
2. Выберите входы, получателей и суммы. Проверьте, какие контексты при этом связываются.
3. Выберите ставку и проверьте абсолютную комиссию, сдачу и предупреждения. При возникновении пыли рассмотрите альтернативы, не соглашаясь на скрытую комиссию.
4. При отправке всего остатка проверьте чистую сумму после комиссии. В чате явно подтвердите частичную оплату, если она не покрывает запрос.
5. Подготовьте черновик и проверьте все данные до экспорта на подписание.

Результат: назначение понятно, для операции подготовлена PSBT. Общая форма может допускать больше входов или получателей, чем оборудование. Соблюдайте фактические пределы подписывающего устройства и носителя. Изменение выходов или условий требует новой проверки.

P16 | Подписание PSBT на Original и возврат ответа | Original и Mirror | L29 | C01,C02,C03

Подготовка: правильный черновик, совместимые транспортная карта и проверенная подлинная криптограмма, а также средства для приватной разблокировки. Архивная копия без проверки подлинности может потребовать проверенного восстановления и создания новой копии до подписания. Редактирование заголовка не решает проблему.

1. Экспортируйте запрос из Desk/Mirror по поддерживаемой процедуре NFC.
2. Перенесите запрос на Original. По запросу предоставьте криптограмму и разблокируйте её, не произнося вслух данные доступа.
3. Проверьте сеть, сводку, полные данные всех выходов, комиссию, сдачу и обязательные предупреждения.
4. В процедуре мультиподписи Final выберите, просматривать ли расширенные параметры. Выполняйте три последних подтверждения только при полном совпадении данных.

5. Дождитесь записи ответа на карту и повторного чтения с неё.
6. Считайте ответ с помощью Cuvex Mirror и проверьте его в соответствующей операции Desk.

Результат: подпись получена и связана с черновиком, что ещё не означает передачи в сеть. При сбое записи сохраните состояние и действуйте по процедуре повтора. Никогда не используйте резервную карту как расходный носитель для платежей.

P17 | Подписание, получение ответа и подтверждение получения с BIT | BIT и Desk | L29 | C01,C02

Подготовка: правильный черновик, совместимая криптограмма с подтверждённой подлинностью и выбранный реальный том BIT. Если архивная копия отклонена для подписания, пройдите указанное восстановление и обновление копии, не пытаясь навязать формат.

1. Передайте запрос по USB-C через службу Desk и следуйте указаниям экрана устройства для предоставления криптограммы.
2. Разблокируйте без посторонних и проверьте сводку, все выходы, комиссию и предупреждения.
3. В мультиподписи Final при желании просмотрите расширенные сведения и авторизуйте операцию с обязательными завершающими подтверждениями.
4. В Desk воспользуйтесь командой «Получить с BIT» для импорта и проверки ответа именно на это задание.
5. Проверьте сохранение и подтверждение получения. Если подтверждение не удалось после получения, повторите ту же операцию, а не выбирайте новую по модели устройства.

Результат: подпись проверена, состояние обмена согласовано. При отключении до получения или после сохранения сохраните профиль запроса. Не переключайтесь на другую прошивку каталога, чтобы подогнать ожидающий ответ.

P18 | Завершение, передача в сеть и отслеживание операции | Desk | L30,L44 | C02

Подготовка: проверенные подписи и достигнутый порог, если он применяется.

1. Ещё раз проверьте намерение, входы, выходы, комиссию и сеть.
2. Завершите операцию соответствующей командой и проверьте, что все подписи и условия на месте.
3. Авторизуйте передачу в сеть и сохраните локальный результат. Если сетевой ответ потерян, проверьте состояние перед повтором.

4. Отслеживайте мемпул и подтверждения у выбранного поставщика, учитывая дату синхронизации.
5. При рассмотрении RBF проверьте заменяющую транзакцию и получите нужные подписи. Не предполагайте наличие встроенной функции CPFP.

Результат: состояние в цепочке проверено по известному источнику. Отмена черновика не отзывает уже экспортированные подписи и не переписывает подтверждённые платежи. Сообщение чата или снимок экрана не заменяют отслеживания.

P19 | Сравнение двух QR-кодов политики в произвольном порядке | Mirror | L43 | C03,C02

Подготовка: поле отображается в Desk и на Cuvex. В упражнении используйте только синтетические образцы курса.

1. Откройте сравнение политик и сначала считайте данные с любой стороны.
2. Выберите проверяемое значение. Можно начать с шага 15 и пропустить другие, сверенные вручную.
3. Считайте соответствующее значение другой стороны и просмотрите оба текста полностью. При неоднозначности используйте «Указать шаг Desk», помня, что контекст введён вручную.
4. Относите «Совпадает» и «Не совпадает» только к посимвольному сравнению этой пары. Значение имеют пробелы, регистр и кодировка.
5. Начните сравнение следующей пары в любом порядке. Для завершения выйдите или переведите приложение в фон с учётом рассмотренного поведения очистки.

Результат: выполнено локальное сравнение отдельной пары. Оно не удостоверяет происхождение, сеанс, общее одобрение или активацию. Выясняйте причину различий по источникам, не нормализуя текст ради отметки OK.

P20 | Активация, восстановление и перенос чата | Desk и Cuvex | L36,L39 | C02

Подготовка: выберите среду DEV или Production. Псевдоним и ключ чата (Clave Chat) должны находиться на устройстве. Никогда не вводите их в учебной среде.

1. Откройте активацию или восстановление чата из контекста криптограммы.
2. Выберите новый псевдоним или перенос существующего и совместимый мобильный профиль, указанный приложением.
3. Введите или считайте ключ чата (Clave Chat) только в приватной процедуре. Не используйте сид-фразу, PIN-код или ключ WOW.
4. Проверьте активацию через сервис. Если она ещё ожидается, используйте действие завершения или проверки и не считайте её успешной заранее.

5. После переноса проверьте сохранность связи с контактами и избегайте одновременного использования одного псевдонима на нескольких устройствах.

Результат: идентичность активирована или восстановлена в нужной среде. Ключ чата (Clave Chat) и общая копия Desk автоматически не восстанавливают прежние сеансы и историю. Учитывайте пределы имеющихся материалов.

P21 | Проверка личности контакта | Desk | L36,L48 | C02

Подготовка: независимый канал, заранее согласованный с человеком.

1. Добавьте псевдоним и запросите открытые данные идентичности в приложении.
2. Сверьте отпечаток по аутентифицированному каналу, не ограничиваясь только что созданной беседой.
3. Если используете проверку узнавания, избегайте общедоступных сведений и секретов, повторно используемых в других сервисах.
4. Подтверждайте только после устранения расхождений. При изменении идентичности приостановите платежи и координацию до проверки.
5. Задокументируйте метод проверки без сохранения чувствительных ответов в курсе.

Результат: установлено доверие к контакту в данном контексте, а не гарантия всех дальнейших запросов. Голос можно имитировать, подлинное устройство может быть скомпрометировано. Каждая операция подлежит собственной проверке.

P22 | Запрос адреса, запрос платежа и оплата через чат | Desk и Cuvex | L37 | C02,C01

Подготовка: проверенный контакт и совместимый счёт WOW.

1. Согласно цели выберите запрос адреса, ответ адресом или запрос платежа.
2. Перед отправкой проверьте исходный запрос, сеть, сумму и примечание.
3. Для оплаты откройте подготовку из нужного счёта, выберите UTXO и ставку комиссии, затем проверьте чистую сумму.
4. Авторизуйте операцию на Cuvex по процедуре модели. Чат не подписывает автоматически.
5. Отслеживайте передачу в сеть и подтверждение по своему источнику. Сверяйте явно обозначенные частичные платежи с исходным запросом.

Результат: координация выполнена с сохранением проверки хранения. Статус сообщения не равен состоянию транзакции. Переход по ссылке на обозреватель может передать информацию третьей стороне. Оцените это до открытия.

P23 | Передача и привязка полученной криптограммы | Desk | L38 | C02

Подготовка: определите конкретную необходимость передачи, проверьте контакт и установите, какие средства доступа он получит.

1. В действиях чата выберите передачу криптограммы и проверьте объект.
2. Не добавляйте в комментарий пароль, сид-фразу или ключ чата (Clave Chat).
3. Получатель проверяет происхождение и привязывает совместимый объект через действие получения.
4. Оцените, какими возможностями получатель располагает сейчас и какие получит при достаточных данных для разблокировки.
5. Поддерживайте реалистичный план отзыва доступа. Удаление сообщений не отзывает внешние копии или уже известные ключи.

Результат: выполнена осознанная передача зашифрованного объекта. Это не платёж и само по себе не добавляет ключ в мультиподпись. Если вложение отправляет вас на незнакомый сайт для расшифрования, остановитесь.

P24 | Общая резервная копия и восстановление Desk | Desk | L15,L21 | C02

Подготовка: учебное хранилище и подконтрольное вам место для копии.

1. Откройте резервное копирование хранилища и задайте требуемый пароль. Сохраните сведения о его связи с этой конкретной копией.
2. Храните копию вне единственного рабочего устройства. По предусмотренной процедуре проверьте её происхождение и целостность.
3. Восстановите копию в отдельной тестовой среде и проверьте счета, конфигурацию и охваченные данные.
4. Проверьте исключения. Нельзя предполагать, что чат, его сеансы и история вошли в копию. Политика мультиподписи и закрытые ключи не взаимозаменяемы.
5. Повторяйте процедуру после существенных изменений и храните инструкции по восстановлению.

Результат: резервная копия с известными охватом и паролем. Старые копии сохраняют прежние пароли. При изменении доступа или раскрытии данных оцените и эти копии. Одного изменения действующего хранилища недостаточно.

P25 | Создание кошелька с мультиподписью и принятие приглашения | Desk и Cuvex | L41,L42 | C01,C02

Подготовка: независимые участники, проверенные контакты, согласованные сеть и фактические ограничения.

1. Создатель выбирает название, M/N, сеть, участников и рабочий срок действия.
2. Предоставьте правильный расширенный открытый ключ с отпечатком и путём BIP48 по совместимой процедуре.
3. Каждый участник проверяет предложение, принимает или отклоняет его и предоставляет открытые данные. Сид-фразой никто не делится.
4. Соберите полную политику и подготовьте её проверку на каждом устройстве.
5. До внесения средств сохраните копии политики, проверьте контрольный адрес и возможность восстановления.

Результат: полное и проверяемое предложение. Принятие приглашения не заменяет проверку на аппаратном устройстве. При участии Original учитывайте максимум в шесть ключей и ёмкость NFC. Возможности BIT не расширяют возможности других участников.

P26 | Проверка политики и получение подтверждения | Desk и Cuvex | L43 | C01,C02,C03

Подготовка: одна и та же полная политика для всех, правильный профиль прошивки и устройство без конкурирующих операций.

1. Начните проверку политик в совместимом контексте. Для Original нужно явно выбрать установленный профиль. BIT согласует возможности по своему протоколу.
2. Передайте запрос по NFC/Mirror или USB-C в зависимости от модели.
3. Проверьте поля политики на устройстве. При желании используйте Mirror для сравнения выбранных пар без обязательного порядка.
4. Завершите подтверждение на устройстве и верните ответ соответствующим способом передачи.
5. В Desk проверьте ответ, связанный с запросом. Визуальная отметка OK в средстве сравнения не заменяет этот шаг.

Результат: проверка сопоставлена с запросом и ограничена своим предметом. Каталог не удостоверяет прошивку удалённо, а устройство не заявлено как постоянное хранилище политик. При FIRMWARE_CAPABILITY_REQUIRED сначала проверьте версию Desk и сочетание модели и сборки.

P27 | Запрос и получение подписей, передача координации | Desk и Cuvex | L44 | C01,C02

Подготовка: проверенная политика, однозначно определённая операция и согласованные получатели.

1. Подготовьте входы, выходы, комиссию и примечания. Запросите подписи у совместимых участников.
2. Каждый участник проверяет и подписывает операцию на своём устройстве через подходящий для него канал передачи.
3. Получите, проверьте и сохраните каждую подпись. Обработайте ожидающие подтверждения получения без изменения сохранённого профиля.
4. При передаче координации получатель принимает её и проверяет состояние. Это не меняет M/N или принадлежность ключей.
5. По достижении порога проверьте и завершите транзакцию перед передачей в сеть. Затем отслеживайте её в сети.

Результат: координация выполнена с различением свидетельств по этапам. Отчёт координатора не является вашей локальной проверкой. Отмена или отказ в одном приложении не обязательно уничтожают подписи, которые сохранили третьи лица.

P28 | Экспорт, восстановление и удаление локальной записи мультиподписи | Desk | L45 | C02

Подготовка: известная политика и зашифрованная копия с уникальным паролем.

1. Экспортируйте материалы восстановления командой Desk. В текущей процедуре для этого экспорта используется аутентифицированный контейнер CVXMSBK1.
2. Храните копию и пароль с независимыми рисками. Не делайте вывод о шифровании архивного файла только по расширению.
3. Для восстановления предоставьте копию, пароль и открытый ключ участника с правильными данными происхождения, при необходимости через веб-камеру или Mirror.
4. Перед работой проверьте политику, сеть, адрес и результат поиска адресов.
5. Перед локальным удалением прочитайте его область действия и подтверждение. Если хотите сохранить возможность восстановления, сохраните копию. Последующее восстановление выполняется явно.

Результат: политика подлежит восстановлению либо осознанно удалена локально. Удаление не перемещает средства, не удаляет ключи других подписантов и само по себе не отменяет сохранённые другими людьми операции.

P29 | Исключительная процедура восстановления на компьютере | Desk | L47 | C02

Подготовка: материал поддерживаемого формата, подготовленная чистая среда и резервная копия. Эта операция может раскрыть секрет компьютеру. В курсе используйте учебные данные.

1. Запустите локальное восстановление в правильном контексте и ознакомьтесь с ограничениями формата и предупреждениями.
2. Осознанно примите риск и отключите сеть, как требует процедура. Перед разрешением продолжить окно проверяет состояние соединения.
3. Вводите только необходимые данные доступа в приватном окне. Не диктуйте их, не вставляйте в курс и не передавайте поддержке.
4. Включайте отображение только в месте без камер и слушающих помощников. Соблюдайте таймер и порядок закрытия.
5. Завершите процедуру, оцените возможное раскрытие и при необходимости спланируйте переход на новые ключи.

Результат: исключительное восстановление, без гарантии криминалистического уничтожения следов или эквивалентности изолированному оборудованию. Если отсутствуют проверка подлинности, подходящий формат или материалы доступа, не испытывайте инструменты из интернета на реальной копии.

P30 | Проверка предпочтений, биометрии и блокировки | Desk | L40 | C02

Подготовка: перед изменением безопасности убедитесь, что пароль известен, а восстановление из копии проверено.

1. В разделе доступа и блокировки проверьте пароль, доступную биометрию, бездействие и блокировку при переходе в фон.
2. Перед изменением выясните задержку после неудачных попыток и установленный предел.
3. Держите необязательное удаление выключенным, пока не разберётесь в условиях, пороге и восстановлении. Не испытывайте его в рабочей среде.
4. В предпочтениях настройте язык, тему, валюту, синхронизацию каждые 3 или 5 минут и звуки.

5. При регистрации ссылок bitcoin: проверьте, что открытие запроса сохраняет этапы разблокировки, выбора и проверки. Само открытие платежа не выполняет.

Результат: конфигурация понятна. Биометрия операционной системы зависит от устройства и не заменяет пароль или резервную копию. Визуальные настройки не меняют политику Bitcoin.

P31 | Удаление записей с учётом области действия | Desk | L22,L45 | C02

Подготовка: определите, что вы удаляете — локальную криптограмму, счёт, WOW, чат или мультиподпись — и какую копию оставите.

1. Проверьте выбранный объект и предупреждение. По запросу приложения подтвердите точный псевдоним или явно указанное условие.
2. Если позднее понадобится восстановить это состояние, экспортируйте и проверьте копию.
3. Удалите только намеченный объект и проверьте, какие связи процедура сохранила или убрала.
4. Проверьте оставшиеся операции и внешних участников. Не считайте, что на других устройствах исчезли сообщения, подписи или файлы.
5. Запишите изменение в личной описи, не вводя чувствительные данные в курс.

Результат: локальное состояние изменено осознанно. Ни одно из этих действий само по себе не меняет скрипты UTXO со средствами, не уничтожает известную третьему лицу сид-фразу и не отменяет подтверждённые транзакции.

P32 | Диагностика без раскрытия секретов | Desk и Mirror | L23,L30,L48 | C02,C03

Подготовка: запишите примерное время, систему, архитектуру, версию и этап. Не повторяйте чувствительную операцию, если её состояние неизвестно.

1. Определите этап сбоя: поиск, сопряжение, чтение, запись, проверка, подписание, возврат ответа, сеть или отображение.
2. Скопируйте код и текст ошибки без QR-кодов и приватных данных. При необходимости используйте диагностику приложения.
3. Перед передачей просмотрите файл. Не прикладывайте копию хранилища, криптограмму, сид-фразу, ключ чата (Clave Chat), дескриптор или данные доступа RPC.
4. При проблеме интерфейса зафиксируйте размер окна, масштаб и скрытые элементы управления на синтетическом примере.

5. Отправьте ожидаемый результат и воспроизводимые шаги через официальный канал. Курс не отправляет сообщения в поддержку автоматически.

Результат: отчёт, позволяющий провести расследование с минимумом данных. При отсутствии свидетельства этап отмечается как ожидающий, а не завершённый. Голосовой поддержке не нужен удалённый доступ к вашему устройству хранения.

Словарь Bitcoin и самостоятельного хранения

Bitcoin

Сеть и набор правил для передачи стоимости и проверки истории операций без единого администратора реестра.

BTC

Денежная единица Bitcoin. Один BTC равен ста миллионам сатоши.

Сатоши

Единица базовой цепочки, равная одной стомиллионной BTC.

Блокчейн

История связанных друг с другом блоков, проверенных по установленным правилам. Термин сам по себе не описывает все свойства сети.

Блок

Набор данных, включающий транзакции и проверяемый заголовок блока.

Полный узел

Программа, проверяющая соблюдение правил для блоков и транзакций, которые она принимает.

Майнинг

Создание блоков посредством доказательства работы по правилам сети.

Доказательство работы

Механизм, требующий выполнить проверяемую вычислительную работу, чтобы предложить блок.

Консенсус

Согласованность участников относительно принимаемых ими правил и действительной истории.

Политика мемпула

Локальные правила приёма и ретрансляции транзакций, которые могут отличаться от правил консенсуса.

Мемпул

Локальный набор неподтверждённых транзакций, хранимых узлом.

Подтверждение

Включение транзакции в блок принятой цепочки и последующая глубина этого блока.

Реорганизация

Замена участка принятой цепочки, которая может изменить подтверждения транзакций.

UTXO

Неизрасходованный выход транзакции, который можно потратить при выполнении его условий.

Вход

Ссылка на предыдущий выход и данные, необходимые для авторизации его расходования.

Выход

Сумма и условие расходования, созданные транзакцией.

Сдача

Выход, возвращающий под контроль плательщика часть входных средств, оставшуюся после платежа и комиссии.

Комиссия

Разность суммарных значений входов и выходов транзакции.

vbyte

Единица виртуального размера, используемая для выражения относительной стоимости транзакции.

sat на vbyte

Ставка комиссии в сатоши на единицу виртуального размера.

Пыль (dust)

Малый выход с учётом правил обработки и затрат на его расходование. Порог зависит от контекста и скрипта.

RBF

Замена неподтверждённой транзакции при совместимых политиках узлов. Отмена не гарантирована.

CPFP

Использование дочерней транзакции для повышения стимула включить её и родительскую транзакцию в блок вместе.

Хеш

Отпечаток данных, полезный для проверки целостности. Он сам по себе не шифрует данные и не устанавливает их автора.

Закрытый ключ

Криптографическое средство создания авторизаций по соответствующей схеме.

Открытый ключ

Данные для проверки подписей и построения определённых условий без раскрытия закрытого ключа.

Цифровая подпись

Криптографическое подтверждение авторизации конкретного сообщения. Его содержимое при этом не скрывается.

Шифрование

Защита конфиденциальности с использованием ключа и алгоритма.

Аутентифицированное шифрование

Шифрование с предусмотренной схемой проверкой изменений данных.

AES GCM

Семейство схем аутентифицированного шифрования для форматов экосистемы. Свойства зависят от реализации и обращения с ключами.

Мнемоническая фраза

Словесное представление исходных и проверочных данных по заданному формату.

Сид

Данные, из которых выводятся ключи. В разговорной речи так называют и набор слов, поэтому значение следует уточнять по контексту.

Энтропия

Непредсказуемость исходных данных для генерации. Выбор запоминающихся слов её не обеспечивает.

Контрольная сумма

Проверочное значение для обнаружения определённых ошибок. Оно не удостоверяет автора.

BIP39

Спецификация мнемонических фраз и получения сида с возможностью использовать дополнительную парольную фразу.

Дополнительная парольная фраза BIP39

Дополнительное входное значение для вывода ключей. Другая фраза может дать иной, действительный, но пустой кошелёк.

BIP32

Спецификация иерархического вывода ключей.

Путь деривации

Последовательность ветвей для получения ключей из корня.

Усиленная деривация

Шаг деривации, обычно обозначаемый апострофом или буквой h. Его свойства отличаются от обычного вывода открытых ключей.

xpub

Расширенный открытый ключ с контекстом для вывода дочерних ключей. Чувствителен с точки зрения конфиденциальности.

xprv

Расширенный закрытый ключ. Его нельзя передавать другим или импортировать в учебную среду.

Отпечаток корня

Короткий идентификатор корня. Удобен для сопоставления, но недостаточен для доказательства идентичности.

Дескриптор

Выражение для построения скриптов из ключей и данных деривации. Может быть открытым или содержать секретные данные.

Только для наблюдения (watch-only)

Кошелёк для наблюдения, которому не хватает закрытых ключей для самостоятельного подписания.

WOW

Название счетов для наблюдения и управления кошельками в экосистеме Cuvex.

Горячий кошелёк

Средство подписания, работающее в подключённой к сети среде.

Самостоятельное хранение

Модель, в которой пользователь сохраняет техническую возможность расходовать средства самостоятельно или совместно согласно своей политике.

Кастодиан

Организация, которая контролирует расходование средств от имени клиента и устанавливает условия доступа.

Криптограмма Cuvex

Зашифрованный объект, защищающий секрет. Сама криптограмма не является транзакцией или остатком средств.

Пароль Desk

Защищает доступ к локальному хранилищу. Это не сид-фраза и не пароль криптограммы.

Ключ чата (Clave Chat)

Секрет восстановления идентичности в чате. Он может выглядеть как открытые данные, но остаётся секретным.

PIN-код сопряжения

Временный код сеанса подключения. Он не служит паролем хранения средств.

Изоляция сред (air gap)

Операционное разделение сред. Переносимые между ними данные по-прежнему требуют проверки.

NFC

Технология связи ближнего поля, применяемая с совместимыми картами и считывателями.

USB Mass Storage

Интерфейс файлового обмена модели BIT. Он требует собственного протокола, проверок и подтверждений получения.

PSBT

Контейнер с данными и подписями для координации построения и авторизации транзакции.

PSBT v0

Версия формата, определённая в BIP174 и используемая в рассмотренном профиле мультиподписи Final.

PSBT v2

Версия, описанная в BIP370. Из версии 2 самой транзакции не следует, что PSBT имеет версию v2.

SIGHASH ALL

Используемый в рассмотренном профиле режим, определяющий, какие данные охватывает подпись. Проверка этой области входит в проверку операции.

P2WPKH

Условие расходования SegWit с одним ключом, обычно связанное со счетами BIP84.

P2WSH

Условие SegWit с криптографической привязкой к скрипту. Применяется в рассмотренном профиле мультиподписи Final.

P2TR

Тип выхода Taproot. Поддержка такого получателя не означает возможность подписывать расходование с такого выхода.

sortedmulti

Конструкция мультиподписи, которая упорядочивает ключи детерминированным образом при построении скрипта.

Порог M из N

Число M обязательных авторизаций среди N участников согласно конкретной политике.

MuSig2

Протокол агрегации подписей Шнорра, базовая схема которого требует N из N. Он отличается от схемы с произвольным порогом.

Taproot

Набор механизмов расходования и криптографических обязательств Bitcoin с путями по ключу и по скрипту.

Miniscript

Язык описания и анализа определённых скриптовых политик. В рассмотренном профиле Final не реализован.

Regtest

Локальная лабораторная сеть без экономической ценности, управляемая создателем среды.

Signet

Тестовая сеть со своими особенностями. По умолчанию не взаимозаменяема с regtest.

Mainnet

Сеть Bitcoin, используемая для операций с реальной экономической ценностью.

Предел промежутка адресов (gap limit)

Критерий для поиска по последовательности адресов без истории. Область его применения зависит от кошелька.

Выбор монет (coin control)

Осознанный выбор UTXO для расходования.

Консолидация

Объединение выходов для уменьшения дробления средств. Влияет на затраты и конфиденциальность.

Псевдонимность

Использование идентификаторов вместо прямого указания гражданского имени. Само по себе не обеспечивает анонимности.

Анонимность

Зависящая от контекста неразличимость для определённых наблюдателей. Приложение не может гарантировать её одним заявлением.

Метаданные

Сведения о коммуникации или активности, например время, размеры и связи, отличные от самого содержания.

CoinJoin

Совместное построение транзакций, затрудняющее определённые выводы, но не гарантирующее постоянной анонимности.

Payjoin

Совместный платёж, в котором плательщик и получатель предоставляют входы по совместимому протоколу.

Tor

Сеть и инструменты для защиты соединения. Использование необходимо настроить и проверить для каждого приложения.

VPN

Канал, переносящий часть доверия к соединению на его оператора. Он не скрывает данные блокчейна.

Lightning

Система платежей по каналам с требованиями и рисками, отличными от перевода в основной цепочке.

Платёжный запрос (invoice)

Структурированный запрос платежа, для которого нужно определить формат и способ оплаты.

RPC

Интерфейс вызовов для сервиса, например Bitcoin Core. Он требует аутентификации и защиты.

TLS

Защищает передачу данных от определённых угроз. Принимающий сервер всё равно видит запросы.

SRTP

Защищает аудио на отдельных участках VoIP. Это не означает автоматической конфиденциальности от оператора.

Идемпотентность

Свойство, предотвращающее повторный эффект при повторении идентифицированного запроса.

Webhook

Событие, передаваемое между серверами. Необходимо проверять его подлинность и повторное получение.

RAG

Поиск фрагментов знаний для обоснования ответа с учётом контекста и версии материала.

Объяснение своими словами (teach-back)

Проверка усвоения материала, при которой учащегося просят объяснить понятое своими словами.

Фишинг

Обман с подменой личности и убедительным контекстом для получения доступа или побуждения человека к действию.

Социальная инженерия

Манипулирование решениями людей, в том числе с помощью достоверных данных и чувства срочности.

Нотаризация Apple

Контроль распространения со стороны Apple. Он отличается от аудита продукта и испытания всех сценариев на физических устройствах.

Аттестация

Свидетельство о состоянии, полученное конкретным механизмом. Каталог совместимости Desk не является удалённым измерением.

MiCA

Европейская нормативная база для определённых криптоактивов и услуг. Не гарантирует доходности или полного возмещения.

Travel Rule

Требования к передаче сведений при переводах, подпадающих под действие правила. Самостоятельное хранение не освобождает от них.

Точка продолжения (checkpoint)

Точка возобновления обучения с минимальными данными, без сведений о кошельке.

Проверьте, чему вы научились

Выполняйте задания без реальных средств. Проверка знаний открыта для всех и не требует учётной записи.

Кто авторизует расходование средств при обычной работе с Cuvex?

1. Устройство после проверки пользователем
2. Голосовой преподаватель
3. Сервер курса

> **Показать ответ: Устройство после проверки пользователем**
> Авторизация по-прежнему выполняется на устройстве Cuvex.

Сколько сатоши в 0,001 BTC?

1. 1 000
2. 100 000
3. 1 000 000

> **Показать ответ: 100 000**
> В одном BTC 100 000 000 sat.

Сумма входов 120 000 sat, сумма выходов 119 000 sat. Какова комиссия?

1. 1 000 sat
2. 119 000 sat
3. 1 sat/vB без дополнительных данных

> **Показать ответ: 1 000 sat**
> Разность сумм равна абсолютному размеру комиссии.

Каково состояние подписанной транзакции, которую ещё не передали в сеть?

1. Подтверждена
2. Необратима, поскольку подписана
3. Авторизована, но ещё могла не попасть в сеть

> **Показать ответ: Авторизована, но ещё могла не попасть в сеть**
> Подписание и передача в сеть — разные этапы.

Какова комиссия за транзакцию размером 200 vB при ставке 6 sat/vB?

1. 206 sat
2. 1 200 sat
3. 6 % от суммы перевода

> **Показать ответ: 1 200 sat**
> Виртуальный размер умножают на ставку комиссии.

Что следует проверить перед выводом средств с биржи?

1. Только самую низкую комиссию
2. Совместимость актива, сети и адреса, а также итоговую сумму к получению
3. Сид-фразу другой стороны

> **Показать ответ: Совместимость актива, сети и адреса, а также итоговую сумму к получению**
> Не каждая сеть с обозначением BTC проводит операции в основной цепочке Bitcoin.

Что сама по себе обеспечивает цифровая подпись?

1. Скрывает всё сообщение
2. Подтверждает авторизацию сообщения, проверяемую по соответствующей схеме
3. Удаляет опубликованные данные

> **Показать ответ: Подтверждает авторизацию сообщения, проверяемую по соответствующей схеме**
> Для конфиденциальности нужен другой механизм.

К чему может привести изменение дополнительной парольной фразы BIP39?

1. К появлению другого действительного, на вид пустого кошелька
2. К возможности всегда сбрасывать её по электронной почте
3. К изменению общедоступной истории предыдущих платежей

> **Показать ответ: К появлению другого действительного, на вид пустого кошелька**
> Дополнительная парольная фраза участвует в выводе ключей.

Как следует обращаться с xpub счёта?

1. Как с данными, раскрытие которых не имеет последствий
2. Как с точной копией секретной сид-фразы
3. Как с данными, чувствительными с точки зрения конфиденциальности

> **Показать ответ: Как с данными, чувствительными с точки зрения конфиденциальности**
> Этот ключ может расширить возможности наблюдения за операциями.

Почему одной сид-фразы может оказаться недостаточно для кошелька с мультиподписью?

1. Не хватает политики и авторизаций для достижения порога
2. Bitcoin вообще не позволяет ничего восстановить
3. Нужно знать первоначальный цвет приложения

> **Показать ответ: Не хватает политики и авторизаций для достижения порога**
> Сохранить политику и сохранить доступ к закрытым ключам для подписания — разные задачи.

Что нужно сделать, если рассмотренный алгоритм версии Final отклонил результат броска?

1. Перебрасывать только монету до принятия результата
2. Снова бросить и монету, и все четыре кубика
3. Выбрать знакомое слово

> **Показать ответ: Снова бросить и монету, и все четыре кубика**
> Повторение лишь части бросков может исказить распределение при сопоставлении результатов.

Что означает требование двух паролей для доступа к сид-фразе кошелька с одной подписью?

1. В цепочке обязательно нужны два ключа
2. Используется мультиподпись Taproot
3. Порог доступа к секрету отделён от порога подписей Bitcoin

> **Показать ответ: Порог доступа к секрету отделён от порога подписей Bitcoin**
> Шифрование не изменяет скрипт.

Что следует учитывать при оценке общей резервной копии Desk?

1. Она обязательно содержит всю переписку
2. У неё есть определённый охват и исключения. Нельзя считать, что переписка обязательно включена
3. Она обновляет все прежние копии

> **Показать ответ: У неё есть определённый охват и исключения. Нельзя считать, что переписка обязательно включена**
> Восстановление идентичности и восстановление сообщений — разные задачи.

Что даёт правильно настроенный собственный узел?

1. Устраняет все утечки данных
2. Уменьшает зависимость от запросов к третьим сторонам и позволяет самостоятельно проверять данные
3. Восстанавливает потерянные ключи

> **Показать ответ: Уменьшает зависимость от запросов к третьим сторонам и позволяет самостоятельно проверять данные**
> Он не гарантирует анонимность и не восстанавливает секретные данные.

Что означает заморозка UTXO в Desk?

1. Это локальное ограничение, действующее в приложении
2. Изменяется условие консенсуса
3. Другие копии сид-фразы отзываются

> **Показать ответ: Это локальное ограничение, действующее в приложении**
> Это не глобальный запрет на расходование.

Что делать, если связь оборвалась непосредственно при передаче транзакции в сеть?

1. Сразу заплатить повторно
2. Удалить кошелёк
3. Сначала проверить, успела ли транзакция распространиться по сети

> **Показать ответ: Сначала проверить, успела ли транзакция распространиться по сети**
> Истечение времени ожидания не доказывает, что операция не была выполнена.

К чему может привести повторное использование адресов или объединение UTXO из разных контекстов?

1. Упростить выявление связей между операциями
2. Стереть историю
3. Гарантировать анонимность

> **Показать ответ: Упростить выявление связей между операциями**
> Конфиденциальность зависит от контекста и дальнейшего использования средств.

Настраивается ли Desk автоматически при запуске Tor Browser?

1. Да
2. Нет
3. Только при тёмной теме

> **Показать ответ: Нет**
> Маршрут сетевого трафика каждого приложения нужно проверять отдельно.

Чем является ключ чата (Clave Chat), внешне похожий на xpub?

1. Данные для публикации
2. Адрес для получения средств
3. Секретные данные идентичности

> **Показать ответ: Секретные данные идентичности**
> Чувствительность данных определяется их назначением.

Что означает сообщение в чате со статусом «оплачено»?

1. Оно заменяет подтверждения
2. Платёж нужно независимо проверить в сети
3. Оно меняет сеть в запросе

> **Показать ответ: Платёж нужно независимо проверить в сети**
> Статус сообщения и состояние платежа различаются.

Что использует рассмотренный профиль мультиподписи версии Final?

1. MuSig2 и PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Любой скрипт Bitcoin

> **Показать ответ: P2WSH sortedmulti BIP48 PSBT v0**
> Пожелания или торговые названия не расширяют фактическую поддержку.

С чего можно начать сравнение в Mirror 12.12?

1. Только с шага 1
2. С любого выбранного элемента, в том числе с 15-го
3. Только с последнего элемента после всех остальных

> **Показать ответ: С любого выбранного элемента, в том числе с 15-го**
> Пары данных можно сравнивать независимо друг от друга и в любом порядке.

Что подтверждает результат «Совпадает» в Mirror?

1. Полное одобрение
2. Подлинность происхождения обоих QR-кодов
3. Точное совпадение двух значений в паре

> **Показать ответ: Точное совпадение двух значений в паре**
> Остальные проверки и ответ по-прежнему необходимы.

Что даёт смена пароля Desk после раскрытия сид-фразы?

1. Лишает злоумышленника доступа
2. Не отзывает ключи, производные от этой сид-фразы
3. Удаляет все копии

> **Показать ответ: Не отзывает ключи, производные от этой сид-фразы**
> Необходимо оценить безопасный перенос контроля над средствами.

Что следует указать при завершении практического обучения?

1. Что было изучено чтением, что смоделировано, что проверено на физических устройствах и что ещё предстоит сделать
2. Только количество проданных часов
3. Обещание абсолютно неуязвимого хранения

> **Показать ответ: Что было изучено чтением, что смоделировано, что проверено на физических устройствах и что ещё предстоит сделать**
> Разные виды свидетельств подтверждают разные аспекты.