CUVEX

CUVEX ACADEMY · 0.1

Ucz się. Zrozum. Przejmij kontrolę.

Bitcoin i samodzielna piecza nad środkami krok po kroku. Kurs, podręcznik, słownik i ćwiczenia są bezpłatne, bez rejestracji. Ty wybierasz, od czego zacząć.

Bezpłatnie · bez rejestracji

Wszystkie sekcje

1. Przygotuj miejsce do nauki
2. Pieniądz cyfrowy i problem zaufania
3. Historia i ograniczenia Bitcoina
4. Satoshi i bezbłędne obliczenia
5. Twój model zagrożeń
6. Węzły, wydobycie i konsensus
7. UTXO i reszta transakcji
8. Mempool, potwierdzenia i reorganizacje
9. Opłaty, rozmiar wirtualny i zastępowanie transakcji
10. Sieci, adresy i żądania płatności
11. Skróty, podpisy i szyfrowanie
12. Fraza seed, hasło dodatkowe i hasło dostępu
13. Wyprowadzanie kluczy, xpub i deskryptory
14. Wybór portfela i modelu przechowywania
15. Kopie zapasowe, które można odtworzyć
16. Poznaj Original i BIT
17. Generowanie frazy seed z entropii fizycznej
18. Szyfrowanie i odszyfrowywanie sekretu w Cuvex
19. Progi szyfrowania i biometria
20. Klonowanie, przechowywanie i weryfikacja kopii
21. Instalowanie i zabezpieczanie Cuvex Desk
22. Łączenie kryptogramów i zarządzanie WOW
23. Parowanie Mirror z Desk
24. NFC przez Mirror, USB-C i odczytywanie kodów QR
25. Publiczni dostawcy i własny węzeł
26. Odbieranie bitcoinów i weryfikacja adresu
27. Etykietowanie, zamrażanie i wybieranie UTXO
28. Przygotowanie i sprawdzenie płatności
29. Podpisywanie za pomocą Original i BIT
30. Finalizowanie, publikacja i rozwiązywanie problemów
31. Co można zaobserwować w Bitcoinie
32. Rozdzielanie kontekstów i zarządzanie resztą
33. Prywatność sieciowa, Tor i VPN
34. CoinJoin, Payjoin i ich obecne ograniczenia
35. Wnioski z rzeczywistych incydentów

36. Tworzenie tożsamości i sprawdzanie kontaktów na czacie
37. Żądanie i płacenie satoshi z czatu
38. Świadome udostępnianie kryptogramów
39. Odzyskiwanie czatu i rozumienie jego metadanych
40. Codzienne ustawienia i przegląd uprawnień
41. Projektowanie portfela wielopodpisowego
42. Tworzenie zaproszeń i dodawanie kluczy
43. Sprawdzanie polityk w Mirror w dowolnej kolejności
44. Koordynacja podpisów i publikacja transakcji wielopodpisowej
45. Odtwarzanie i zmiana wielopodpisu
46. Planowa aktualizacja oprogramowania układowego
47. Utrata, awaria i odzyskiwanie awaryjne
48. Phishing, wsparcie i oszustwa głosowe
49. Prywatność, prawo i własna dokumentacja
50. Dziedziczenie, ciągłość i coroczna próba
51. Cena, oszczędzanie i analiza fundamentalna
52. Wybór miejsca zakupu bitcoinów
53. Konta, zlecenia i koszty realizacji
54. Świece, wskaźniki i błędy poznawcze w analizie technicznej
55. Depozyt zabezpieczający, kontrakty terminowe i automatyzacja
56. Lightning i inne warstwy
57. Taproot, MuSig2 i przyszłość postkwantowa
58. Interoperacyjność i uniezależnienie się od producenta
59. Laboratorium techniczne z regtest
60. Projekt końcowy i plan ciągłości
61. Podręcznik uczestnika
62. Słownik Bitcoina i samodzielnego przechowywania
63. Sprawdź, co już potrafisz

M01

Przygotuj miejsce do nauki

Cel

Przygotuj się do kursu, naucz się odróżniać trzy urządzenia i ustal, których informacji nigdy nie przekazuje się tutorowi.

Zrozumienie tematu

Nauczysz się samodzielnie odbierać, przechowywać, wydawać i odzyskiwać bitcoiny. Ostateczny cel to umieć wyjaśnić decyzję, zanim ją zatwierdzisz. Kurs możesz czytać samodzielnie. Pomoc głosowa dostarcza wyjaśnień, pytań i wskazówek. Nie potrzebuje wglądu w twój majątek ani kontroli nad twoimi urządzeniami.

Cuvex chroni sekrety i pozwala zatwierdzać operacje na własnym ekranie. Desk zarządza na komputerze kryptogramami, portfelami obserwacyjnymi i płatnościami oraz koordynuje działania. Mirror służy jako lokalny most dla obsługiwanych operacji i do porównywania danych. Nie podpisuje ani nie działa jako samodzielny portfel. Dostępna ścieżka zależy od wersji i modelu.

Przeznacz jeden ekran na kurs, drugi na Desk. Miej telefon i Cuvex pod ręką. Jeśli masz jeden ekran, przełączaj się między widokami. Nie udostępniaj ekranu w rozmowie wideo podczas wpisywania sekretów. Rozmowa może się skończyć przed ukończeniem ćwiczenia. Przerwa nie oznacza porażki. Zapisz tylko identyfikator lekcji, osiągnięty krok i napotkaną trudność.

Ani człowiek prowadzący zajęcia, ani AI nie mogą otrzymać fraz seed, dodatkowych haseł BIP39, haseł, klucza czatu, PIN-u, prywatnych plików ani pełnych kodów zakupu. Nie potrzebują też twojego xpub, rzeczywistego deskryptora ani adresu. Choć te dane nie pozwalają wydawać środków, ujawniają aktywność. Opisuj komunikaty o błędach i korzystaj z fikcyjnych danych ćwiczeniowych.

Ćwiczenie

1. Rozpoznaj na miejscu komputer, telefon i model Cuvex. Zapisz ich wersje w prywatnym notatniku.
2. Oddziel środowisko szkoleniowe bez środków od rzeczywistego portfela. Nie importuj do ćwiczeń używanej frazy seed.
3. Otwórz tę lekcję i znajdź pauzę, pomoc oraz słownik. Jeśli ktoś poprosi o sekret, przerwij kontakt.

Sprawdź swoje umiejętności

Wyjaśnij, kto podpisuje, kto odpytuje sieć i kto przenosi dane. Możesz przejść dalej, gdy samodzielnie odróżnisz te role.

Częste pytanie

Czy muszę codziennie rozmawiać z tutorem? Nie. Możesz uczyć się samodzielnie, powtarzać sesje i prosić o pomoc tylko przy wybranej procedurze. Dostęp do kursu i saldo usługi głosowej to odrębne uprawnienia.

Miejsce na przerwę

Lekcja L01 ukończona, urządzenia rozpoznane, żadnego sekretu nie zapisano w kursie.

Tutor prosi o frazę seed, żeby sprawdzić, czy zapis jest poprawny. Co robisz?

1. Powoli ją dyktuję.
2. Odmawiam i sprawdzam frazę tylko we własnym bezpiecznym środowisku.
3. Wysyłam tylko pierwsze słowa.

> **Pokaż odpowiedź: Odmawiam i sprawdzam frazę tylko we własnym bezpiecznym środowisku.**
> Żaden fragment sekretu nie należy do materiału udostępnianego podczas nauki.

M01

Pieniądz cyfrowy i problem zaufania

Cel

Zrozum, jaki problem próbuje rozwiązać Bitcoin, zanim otworzysz portfel.

Zrozumienie tematu

Saldo bankowe to zapis prowadzony przez instytucję. Uwierzytelnia ona klienta, decyduje, które przelewy wykonać, i prowadzi księgowość. Zwykły plik cyfrowy łatwo skopiować. Po wysłaniu zdjęcia można zachować jego egzemplarz. Aby cyfrowa jednostka mogła być pieniądzem, trzeba zapobiec jej dwukrotnemu wydaniu.

Bitcoin łączy reguły weryfikacji, podpisy i wspólną historię transakcji. Zamiast powierzać cały rejestr jednej instytucji, pozwala niezależnym uczestnikom sprawdzić, czy transakcja przestrzega reguł. Ograniczona podaż zależy od dalszego sprawdzania i akceptowania tych reguł. Nie wynika z obrazka monety ani z kursu ogłoszonego przez giełdę.

Samodzielne przechowywanie zmienia zakres odpowiedzialności. Możesz zachować zdolność wydawania bez zgody powiernika, ale możesz ją utracić przez zniszczenie wszystkich kopii lub podpisanie błędnej płatności. Samodzielność nie usuwa potrzeby zabezpieczeń, koordynacji, połączenia potrzebnego do publikacji ani obowiązku przestrzegania właściwych przepisów.

Odróżniaj Bitcoin, czyli sieć i protokół, od BTC, czyli jednostki pieniężnej. Inne sieci mogą używać słowa blockchain i mieć odmienne właściwości. Obietnica firmy określana jako „bitcoin” to również co innego niż dysponowanie wyjściem Bitcoin pod kontrolą własnych kluczy.

Ćwiczenie

1. Porównaj saldo w banku, saldo na giełdzie i UTXO kontrolowane własnymi kluczami.
2. Dla każdego wskaż, kto może zablokować przesunięcie środków, a kto pomóc, gdy zapomnisz danych dostępu.
3. Opisz skutki skopiowania zdjęcia i skutki próby wydania tego samego wyjścia dwa razy.

Sprawdź swoje umiejętności

Wyjaśnij własnymi słowami różnicę między saldem a możliwością złożenia podpisu. Nie trzeba zapamiętywać terminów technicznych.

Częste pytanie

Czy samodzielne przechowywanie oznacza zniknięcie wszystkich pośredników? Możesz wybierać usługi zakupu, wyszukiwania informacji lub komunikacji. Liczy się to, jakie uprawnienia zachowują i jakie dane otrzymują.

Miejsce na przerwę

Zachowaj porównanie odpowiedzialności bez nazw rzeczywistych kont.

Którego problemu pieniądza nie rozwiązuje sam podpis cyfrowy?

1. Zapobiegania próbom dwukrotnego wydania tego samego wyjścia.
2. Wykazania autoryzacji za pomocą klucza.
3. Wykrycia zmiany podpisanej wiadomości.

> **Pokaż odpowiedź: Zapobiegania próbom dwukrotnego wydania tego samego wyjścia.**
> Podpisy upoważniają do wydania. Reguły i konsensus ustalają kolejność sprzecznych wydatków.

M01

Historia i ograniczenia Bitcoina

Cel

Poznaj początki Bitcoina i odróżniaj fakty historyczne od opowieści marketingowych.

Zrozumienie tematu

Dokument Satoshiego Nakamoto opublikowano w 2008 roku, a sieć ruszyła w 2009. Proponował elektroniczną gotówkę między równorzędnymi uczestnikami, wykorzystując wcześniejsze pomysły z kryptografii, dowodu pracy i pieniądza cyfrowego. Weryfikacja programu lub transakcji nie wymaga znajomości rzeczywistej tożsamości Satoshiego.

Rozwój nie polegał na jednostronnym zastępowaniu reguł przez jedną firmę. Programiści proponują i oceniają zmiany, operatorzy wybierają oprogramowanie, górnicy budują bloki, a użytkownicy i usługodawcy decydują, co zaakceptują. Podział ten może prowadzić do sporów. Rozwidlenie sieci i aktualizacja aplikacji to różne pojęcia.

Węzeł może odrzucić blok łamiący jego reguły mimo ogromu wykonanej pracy. Konsensus nie jest zwykłym głosowaniem według liczby komputerów. Uruchomienie tysięcy kopii węzła nie daje automatycznie większej siły decyzyjnej. Podobnie większość górników nie zyskuje przez sam ten fakt klucza prywatnego użytkownika.

Bitcoin przyjmuje świadome ograniczenia i kompromisy dotyczące pojemności bloków, kosztów weryfikacji, zmiennych czasów potwierdzenia i publicznego rejestru. Nie przewiduje administracyjnego cofania płatności ani domyślnej pełnej poufności. Dodatkowe warstwy i aplikacje obsługują konkretne zastosowania kosztem nowych zależności.

Ćwiczenie

1. Umieść na osi czasu pierwotny dokument, start sieci, wprowadzenie SegWit i aktywację Taproot. Przed publikacją dat sprawdź je w źródłach.
2. Sklasyfikuj „firma gwarantuje cenę”, „węzeł weryfikuje” i „górnik proponuje blok” jako obietnicę handlową lub funkcję techniczną.
3. Podaj jedną zaletę i jeden koszt braku administratora, który cofa płatności.

Sprawdź swoje umiejętności

Odróżniaj regułę konsensusu, lokalną politykę i decyzję firmy. Używana aplikacja to jedynie część sieci.

Częste pytanie

Czy nowsze oprogramowanie zawsze zmienia reguły pieniężne? Nie. Nowe wersje usuwają również usterki, poprawiają wydajność lub zmieniają lokalną politykę. Czytaj informacje o wydaniu i zgodności.

Miejsce na przerwę

Zapisz jedną właściwość, którą można sprawdzić, i jedno twierdzenie wymagające dodatkowych dowodów.

Blok zawiera wydatek bez prawidłowego upoważnienia. Czy większość górników może uczynić go ważnym?

1. Tak, jeśli przekracza 51%.
2. Tylko jeśli giełda to ogłosi.
3. Nie dla węzła, który stosuje reguły odrzucające taki blok.

> **Pokaż odpowiedź: Nie dla węzła, który stosuje reguły odrzucające taki blok.**
> Skumulowaną pracę porównuje się między historiami ważnymi według reguł węzła.

M01

Satoshi i bezbłędne obliczenia

Cel

Przeliczaj BTC i satoshi oraz sprawdzaj kwoty niezależnie od kursu.

Zrozumienie tematu

Jeden BTC to 100 000 000 satoshi. „sat” oznacza jednostkę tej samej waluty. W łańcuchu bazowym kwoty zapisuje się jako całkowitą liczbę satoshi. 0,001 BTC to 100 000 sat, a 0,00001000 BTC to 1 000 sat. Separator dziesiętny zależy od języka interfejsu. Nie dopisuj zer na oko.

Notowanie przelicza BTC w danym momencie na walutę, np. EUR lub USD. Nie zmienia liczby kontrolowanych satoshi. Gdy masz 100 000 sat i zmienia się kurs, nadal masz tyle samo satoshi. Desk podaje kurs orientacyjny ze źródłem i datą. Nieaktualny kurs może prowadzić do błędnej decyzji ekonomicznej mimo poprawnego salda BTC.

Przy płatności odróżniaj kwotę odbiorcy, opłatę sieciową i łączny wydatek. Gdy wysyłasz 50 000 sat z opłatą 600 sat, z portfela ubywa 50 600 sat, z zastrzeżeniem innych własnych wyjść. „Wyślij wszystko” zazwyczaj wylicza kwotę netto dla odbiorcy niższą niż dostępne saldo, ponieważ trzeba pokryć opłatę.

Przykłady w kursie służą do nauki arytmetyki, nie podają cen rynkowych ani zalecanych stawek. Przed podpisaniem sprawdź jednostkę, sieć, odbiorcę i łączny koszt na odpowiednim ekranie. Głos może powiedzieć „pięćdziesiąt tysięcy satoshi” i jednocześnie wyświetlić „50 000 sat”. Nie wolno ustalać kwoty na podstawie niepewnej transkrypcji.

Ćwiczenie

1. Przelicz 250 000 sat na BTC: 0,0025 BTC. Przelicz 0,00025000 BTC: 25 000 sat.
2. Oblicz wydatek dla płatności 75 000 sat z opłatą 900 sat. Łącznie to 75 900 sat.
3. W symulatorze użyj 120 000 sat, wyślij 70 000 przy opłacie 1 000 i sprawdź resztę 49 000 sat.

Sprawdź swoje umiejętności

Odczytaj kwotę w BTC i w sat. Wyjaśnij, która wartość uwzględnia opłatę. W razie wątpliwości wstrzymaj operację.

Częste pytanie

Czy muszę kupić całego bitcoina? Nie. Możesz kupić część, z uwzględnieniem minimalnych kwot i kosztów dostawcy.

Miejsce na przerwę

Zachowaj tylko wyniki ćwiczenia.

Masz 80 000 sat i chcesz wysłać całość z opłatą 1 200 sat. Ile otrzyma odbiorca?

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

> **Pokaż odpowiedź: 78 800 sat.**
> Przy braku innych wyjść odbiorca dostaje dostępne saldo pomniejszone o opłatę.

M01

Twój model zagrożeń

Cel

Dobierz proporcjonalne środki przeciw utracie, kradzieży, oszustwu i ujawnieniu danych.

Zrozumienie tematu

Bezpieczeństwo oznacza możliwość działania zgodnie z zamiarem. Prywatność to kontrola nad tym, kto zna twoje dane i powiązania. Dostępność oznacza dostęp wtedy, gdy go potrzebujesz. Sejf niedostępny dla wszystkich może być niedostępny również dla ciebie. Bardzo wygodna kopia może ujawniać zbyt wiele.

Określ chronione zasoby, przeciwników i wypadki. Zasoby obejmują klucze, kopie zapasowe, historię, miejsca przechowywania i tożsamość kontaktów. Zagrożenia obejmują złośliwe oprogramowanie, phishing, pożar, zapomnienie, przymus, awarię, śmierć i własne błędy. Różne ryzyka wymagają różnych narzędzi.

Przygotuj prostą tabelę z przybliżonym prawdopodobieństwem, skutkiem i konkretnym działaniem. Długie hasło utrudnia zgadywanie, ale nie poprawi adresu oszusta, który samodzielnie zatwierdzisz. Dwie kopie w tej samej torbie nie pomogą po jej zgubieniu. Przy wielopodpisie jedna osoba kontrolująca wszystkie urządzenia i kopie może pozostać wspólnym punktem awarii.

Kurs i tutor także należą do modelu. Zakupy, rozmowy, czas połączeń i postępy mogą tworzyć metadane. Strona kursu nie powinna prosić o adresy ani salda w celu dopasowania zajęć. Brak tradycyjnej rejestracji w Desk lub Mirror nie oznacza, że sklep, dostawca głosu czy strona trzecia obsługująca zapytanie nie widzą twojej aktywności.

Ćwiczenie

1. Wypisz trzy najważniejsze zagrożenia bez kwot majątku i dokładnych lokalizacji.
2. Dla każdego dobierz zapobieganie, wykrywanie i odzyskiwanie. Przykład utraty karty: dwie oddzielne kopie, spis i test odtworzenia.
3. Odróżnij osoby lub systemy mogące obserwować zakup, rozmowę, odczyt salda i publiczną transakcję.

Sprawdź swoje umiejętności

Uzasadnij, na jakie konkretne ryzyko odpowiada następny środek. Unikaj komplikacji, których nie zdołasz utrzymać ani wyjaśnić spadkobiercom.

Częste pytanie

Czy więcej urządzeń zawsze zwiększa bezpieczeństwo? Tylko jeśli ograniczają wspólne zależności i potrafisz przetestować odzyskiwanie. Więcej sprzętu to także więcej obsługi i możliwości pomyłki.

Miejsce na przerwę

Plan zachowaj we własnej dokumentacji. W kursie zapisz tylko „sprawdzono model zagrożeń”.

Co najlepiej ogranicza ryzyko utraty wszystkich kopii w jednym pożarze?

1. Zmiana koloru karty.
2. Umieszczenie dwóch kopii w tej samej szufladzie.
3. Przechowywanie sprawdzonych kopii w miejscach narażonych na niezależne zagrożenia.

> **Pokaż odpowiedź: Przechowywanie sprawdzonych kopii w miejscach narażonych na niezależne zagrożenia.**
> Nadmiarowe kopie muszą przetrwać zdarzenie, które zagraża oryginałowi.

M02

Węzły, wydobycie i konsensus

Cel

Wyjaśnij, co sprawdzają węzły i jaką rolę odgrywa wydobycie.

Zrozumienie tematu

Pełny węzeł odbiera bloki i transakcje, sprawdza reguły i utrzymuje własny obraz łańcucha. Nie musi ufać saldu wyświetlanemu przez stronę. Wydobycie polega na proponowaniu bloków za pomocą dowodu pracy. Górnicy wybierają prawidłowe transakcje i rywalizują o znalezienie dopuszczalnego bloku.

Dowód pracy sprawia, że zmiana historii jest kosztowna. Gdy istnieje kilka poprawnych historii, liczy się skumulowana praca, a nie sama liczba bloków bez uwzględnienia trudności. Odstępy między blokami są zmienne. Dziesięć minut to docelowa średnia, a nie termin kolejnej płatności.

Wynagrodzenie górników składa się z dotacji blokowej i opłat. Dotacja maleje zgodnie z harmonogramem zależnym od wysokości bloku. Opłaty wynikają z dołączonych transakcji. Wyższa opłata nie naprawi błędnego podpisu. Bezpieczeństwo ekonomiczne i koszt ataku nie dają matematycznej nieodwracalności niedawnej płatności.

Własny węzeł ogranicza potrzebę ujawniania zapytań innym dostawcom i pozwala samodzielnie weryfikować dane. Nadal trzeba chronić jego system operacyjny, dostęp i połączenie. Niezsynchronizowany węzeł lub aplikacja odpytująca inny serwer mimo działania twojego węzła nie zapewnią automatycznie tych korzyści.

Ćwiczenie

1. Przypisz zadania: sprawdzenie podpisu, wybór transakcji do bloku, przechowywanie frazy seed i decyzja o przyjęciu płatności.
2. Wyjaśnij, dlaczego stwierdzenie „górnik przechowuje moje bitcoiny” jest błędne.
3. W sieci ćwiczeniowej obserwuj wysokość i synchronizację. Nie publikuj danych uwierzytelniających RPC.

Sprawdź swoje umiejętności

Odróżnij weryfikację od proponowania. Możesz użyć analogii, ale zakończ poprawnym objaśnieniem funkcji technicznej.

Częste pytanie

Czy muszę kopać, by używać Bitcoina? Nie. Na początek nie potrzebujesz również własnego węzła, musisz jednak wiedzieć, w jakim stopniu ufasz dostawcy.

Miejsce na przerwę

Zapisz typ dostawcy w laboratorium bez prywatnego adresu URL.

Co daje użytkownikowi prawidłowo skonfigurowany pełny węzeł?

1. Sprawdza reguły łańcucha, który użytkownik akceptuje.
2. Odzyskuje każdy utracony klucz.
3. Gwarantuje wzrost ceny.

> **Pokaż odpowiedź: Sprawdza reguły łańcucha, który użytkownik akceptuje.**
> Weryfikacja i przechowywanie to odrębne funkcje.

M02

UTXO i reszta transakcji

Cel

Odczytuj transakcję jako zużywanie i tworzenie wyjść.

Zrozumienie tematu

UTXO to niewydane wyjście wcześniejszej transakcji. Portfel wylicza saldo, rozpoznając wyjścia, które może kontrolować. Nie ma uniwersalnego konta obciążanego jak w księdze bankowej. Wejście wskazuje wcześniejsze wyjście za pomocą identyfikatora transakcji i pozycji.

Wydanie UTXO zużywa je w całości. Jeśli płacisz mniej, niż wynosi jego wartość, zwykle powstają wyjście dla odbiorcy i kontrolowane przez ciebie wyjście reszty. Przy wejściu 120 000 sat, kwocie 70 000 dla odbiorcy i opłacie 1 000 reszta to 49 000. Suma wejść równa się sumie wyjść i opłaty.

Adres nie jest UTXO. Może przyjąć wiele wyjść i nie musi oznaczać osoby. Identyfikator transakcji może być publiczny, lecz powiązanie go z twoją tożsamością lub opisanie właściciela każdego wyjścia ujawnia informacje, których sam łańcuch nie podaje.

Ma to znaczenie dla prywatności. Łączenie wejść może sugerować wspólną kontrolę, a reszta może powiązać przyszłe płatności. Transakcje współtworzone przez wiele stron pokazują, że taki wniosek nie zawsze jest dowodem. Coin control oznacza świadomy wybór wydawanych wyjść z uwzględnieniem skutków ich połączenia.

Ćwiczenie

1. Narysuj trzy fikcyjne wejścia: 40 000, 60 000 i 200 000 sat. Zapłać 70 000 z opłatą 1 000, używając tylko dwóch pierwszych.
2. Sprawdź, czy reszta to 29 000 sat, a trzecie wejście nie uczestniczy w transakcji.
3. Powtórz tylko z 200 000 sat. Reszta wyniosłaby 129 000. Porównaj możliwe koszty i powiązania bez zakładania jednakowych rozmiarów.

Sprawdź swoje umiejętności

Wskaż na rysunku kursowym wejście, odbiorcę, resztę i opłatę. Jeśli nie potrafisz rozpoznać któregoś wyjścia, nie podpisuj rzeczywistej operacji.

Częste pytanie

Czy wszystko, co wraca do mojego portfela, jest resztą? Nie. Może to być przelew na inny własny adres. Do klasyfikacji potrzebna jest znajomość polityki i ścieżki wyprowadzania. Nie zgaduj na podstawie kwoty.

Miejsce na przerwę

Zachowaj fikcyjny schemat. Nigdy nie zapisuj zrzutu ekranu swojego majątku.

Wejście 100 000 sat tworzy wyjścia 30 000 i 69 200. Jaka jest opłata?

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

> **Pokaż odpowiedź: 800 sat.**
> 100 000 minus 99 200 daje 800 sat.

M02

Mempool, potwierdzenia i reorganizacje

Cel

Odróżnij transakcję przygotowaną, opublikowaną i potwierdzoną.

Zrozumienie tematu

Mempool to lokalny zbiór niepotwierdzonych transakcji, które węzeł przechowuje według własnej polityki. Nie ma jednej identycznej kolejki na całym świecie. Widoczność płatności w eksploratorze oznacza, że ten serwis o niej wie. Nie gwarantuje to przyjęcia przez wszystkie węzły ani potwierdzenia w określonym czasie.

Przygotowanie PSBT niczego nie publikuje. Podpis oznacza autoryzację. Finalizacja buduje transakcję gotową do rozesłania. Publikacja jest próbą jej nadania. Potwierdzenie oznacza włączenie do bloku łańcucha akceptowanego przez twoje źródło weryfikacji. Drugie potwierdzenie to następny blok nad pierwszym, a nie drugi podpis odbiorcy.

Reorganizacja zmienia fragment łańcucha. Transakcja może utracić potwierdzenia lub ponownie oczekiwać. Przy płatnościach o większym ryzyku strony zwykle wymagają więcej potwierdzeń. Żadna liczba nie usuwa wszystkich zagrożeń dla każdej kwoty i sytuacji.

Gdy Desk pokazuje zapisany stan, sprawdź datę synchronizacji. „Potwierdzona” na starej migawce nie musi opisywać obecnego stanu. Jeśli przelewu nie widać, zachowaj lokalny identyfikator i sprawdź publikację oraz historię przed przygotowaniem go ponownie. Niecierpliwość może spowodować drugą ważną płatność.

Ćwiczenie

1. Uporządkuj karty: szkic, PSBT, podpis, finalna transakcja, rozesłanie, włączenie do bloku.
2. Zasymuluj zerwanie połączenia po publikacji. Ustal, co sprawdzić przed ponowną zapłatą.
3. Wyjaśnij sprzedawcy, dlaczego wiadomość „zapłacono” na czacie nie zastępuje weryfikacji w sieci.

Sprawdź swoje umiejętności

Opisz stan operacji, źródło i datę tej informacji bez traktowania jej jak gwarancji.

Częste pytanie

Czy zamknięcie Desk anuluje opublikowaną transakcję? Nie. Inne węzły i uczestnicy mogą ją zachować. Usunięcie lokalnego szkicu ma inny zakres.

Miejsce na przerwę

Zapisz stan symulacji. Nie podawaj tutorowi rzeczywistych identyfikatorów.

Komputer traci połączenie tuż po kliknięciu publikacji. Co robisz najpierw?

1. Przygotowuję tę samą płatność od zera.
2. Usuwam portfel.
3. Przywracam połączenie i sprawdzam transakcję oraz jej wejścia.

> **Pokaż odpowiedź: Przywracam połączenie i sprawdzam transakcję oraz jej wejścia.**
> Brak odpowiedzi nie dowodzi niepowodzenia rozesłania.

M02

Opłaty, rozmiar wirtualny i zastępowanie transakcji

Cel

Szacuj koszty, interpretuj sat za wirtualny bajt i poznaj RBF oraz CPFP.

Zrozumienie tematu

Opłata sieciowa jest różnicą sum wejść i wyjść. Jej konkurencyjność określa się zwykle w sat/vB, czyli satoshi za wirtualny bajt. Nie zależy bezpośrednio od wartości przelewu. Wiele wejść może zwiększyć koszt małej płatności, a duża płatność z kilkoma wejściami może zajmować mniej miejsca.

Przy 200 vB i stawce 5 sat/vB opłata wynosi 1 000 sat. Przed podpisaniem masz tylko szacunek, ponieważ rozmiar końcowy może zależeć od podpisów i struktury. Desk pokazuje orientacyjne prędkości i pozwala ręcznie ustawić stawkę. Etykieta „szybko” nie gwarantuje terminu potwierdzenia.

RBF to polityka zastępowania niepotwierdzonych transakcji na określonych warunkach. Pozwala zaproponować sprzeczną transakcję z wyższą opłatą. Polityki węzłów ewoluowały, więc sygnał zakazujący zastąpienia nie gwarantuje otrzymania zapłaty. Zastąpienie wymaga nowej kontroli i odpowiednich podpisów.

W CPFP wydajesz wyjście oczekującej transakcji, aby transakcje rodzica i dziecka łącznie stały się atrakcyjne. Musisz kontrolować dostępne wyjście, spełnić wymagania polityki i zapłacić koszt. To mechanizm Bitcoina. Nie zakładaj, że twoja wersja Cuvex ma przycisk CPFP.

„Dust” to wyjście zbyt małe według właściwych polityk i szacowanego kosztu wydania. Nie ma uniwersalnego progu dla wszystkich skryptów. Nie przedstawiaj jednej liczby jako reguły konsensusu. Gdy utworzenie reszty jest niepraktyczne, sprawdź kwotę, wejścia, możliwość wysłania całości i rzeczywistą opłatę.

Ćwiczenie

1. Oblicz koszt 180 vB przy 8 sat/vB: 1 440 sat. Sprawdź, czy przekracza budżet ćwiczenia.
2. Porównaj jedno wejście z dziesięcioma. Wyjaśnij, dlaczego kwota wysyłki nie wystarcza do oszacowania kosztu.
3. Zasymuluj oczekującą transakcję. Wybierz czekanie, RBF lub rozważenie CPFP bez zakładania zgodności.

Sprawdź swoje umiejętności

Uzasadnij stawkę, bezwzględną opłatę i jej koszt w stosunku do kwoty. Odrzuć opłatę, której nie rozumiesz.

Częste pytanie

Czy RBF z pewnością anuluje poprzednią płatność? Nie. Wersje konkurują do potwierdzenia i znaczenie ma rozchodzenie się ich w sieci. Nie wydawaj towaru na podstawie obietnicy anulowania.

Miejsce na przerwę

Zachowaj decyzję z ćwiczenia i jej uzasadnienie.

Jaka jest opłata za 250 vB przy 4 sat/vB?

1. 1 000 sat.
2. 254 sat.
3. 4% wysyłanej kwoty.

> **Pokaż odpowiedź: 1 000 sat.**
> Rozmiar wirtualny pomnożony przez stawkę daje szacowaną opłatę.

M02

Sieci, adresy i żądania płatności

Cel

Rozpoznawaj sieć, format adresu i instrukcje płatności przed kopiowaniem lub skanowaniem.

Zrozumienie tematu

W mainnecie przesyła się bitcoiny o wartości ekonomicznej. Sieci testowe służą do programowania i nauki, ale nie są wzajemnie zamienne. Regtest to sieć lokalna kontrolowana przez organizatora laboratorium. Signet i testnet mają własne reguły i ekosystemy. Obsługa pojedynczego podpisu w signet nie oznacza, że sieć tę obsługuje profil wielopodpisu Cuvex.

Adresy kodują warunki odbioru. W mainnecie spotkasz formaty z początkiem 1, 3, bc1q lub bc1p. Prefiks pomaga rozpoznać rodzinę, ale nie uwierzytelnia odbiorcy, nie gwarantuje zgodności urządzenia podpisującego i nie zastępuje pełnej weryfikacji formatu.

Kod QR to wizualny nośnik. Może zawierać adres, żądanie płatności, deskryptor lub szkodliwy tekst. Skan nie uwierzytelnia twórcy. Odnośnik bitcoin: może dodawać kwotę i wiadomość. Współczesny standard BIP321 zastępuje BIP21. Sprawdzona implementacja Desk zachowuje terminologię i zgodność BIP21. Ulepszenie standardu samo nie rozszerza obsługi przez aplikację.

Faktura Lightning nie jest adresem on-chain. Może zawierać termin ważności i inne pola. Nie wklejaj jej do wysyłki w łańcuchu bez obsługi odpowiedniej procedury. Token o nazwie BTC w innej sieci również nie jest automatycznie natywnym bitcoinem.

Ćwiczenie

1. Sklasyfikuj opisane przykłady kursowe bez używania adresów do rzeczywistych środków: adres, URI bitcoin:, faktura Lightning i deskryptor.
2. Wskaż sieć wybraną w laboratorium. Sprawdzony profil wielopodpisu Cuvex obsługuje mainnet i regtest.
3. Przed rzeczywistą operacją porównaj pełny tekst podany przez odbiorcę za pomocą uwierzytelnionego kanału.

Sprawdź swoje umiejętności

Potrafisz odmówić spełnienia żądania, którego sieci lub metody nie znasz, i wyjaśnić, co trzeba sprawdzić.

Częste pytanie

Czy mogę wysyłać BTC przez dowolną sieć pokazaną przez giełdę? Nie. Sieć wypłaty musi odpowiadać faktycznej metodzie odbioru. Nie wybieraj wyłącznie według najniższej opłaty.

Miejsce na przerwę

Zapisz jedynie typ sieci ćwiczeniowej.

Adres odbiorczy bc1 sam nie upoważnia do wypłaty BTC przez inną sieć tokenów. Czego brakuje?

1. Zmiany aliasu odbiorcy.
2. Potwierdzenia, że wypłata następuje on-chain w sieci Bitcoin i wszystkie dane są zgodne.
3. Wprowadzenia frazy seed na giełdzie.

> **Pokaż odpowiedź: Potwierdzenia, że wypłata następuje on-chain w sieci Bitcoin i wszystkie dane są zgodne.**
> Zasób, sieć i metoda odbioru muszą być zgodne.

M03

Skróty, podpisy i szyfrowanie

Cel

Odróżniaj integralność, autoryzację i poufność.

Zrozumienie tematu

Funkcja skrótu przekształca dane w odcisk o stałej długości. Porównanie ze znanym odciskiem pomaga wykryć zmiany. Nie szyfruje pliku i samo nie ustala tożsamości wydawcy. Jeśli plik i skrót pobierasz z tej samej przejętej strony, napastnik mógł podmienić oba.

Klucz prywatny umożliwia składanie podpisów, a odpowiadający mu klucz publiczny ich weryfikację. Podpis wiąże upoważnienie z konkretną wiadomością według algorytmu i jego reguł. Nie ukrywa podpisanej treści. W Bitcoinie prawidłowy podpis to część warunków koniecznych do wydania wyjścia.

Szyfrowanie ma udostępniać treść tylko posiadaczowi odpowiedniego środka dostępu. Szyfrowanie uwierzytelnione dodatkowo wykrywa modyfikacje. W środowisku Cuvex kryptogramy chronią sekrety, podpisane transakcje upoważniają do wydania, a szyfrowane kanały przenoszą wiadomości. Choć wszystkie używają kryptografii, są różnymi obiektami.

Hasło człowieka zwykle przechodzi przez funkcję wyprowadzania przed użyciem go jako klucza kryptograficznego. „AES-256” opisuje algorytm i długość klucza, ale nie wzmacnia przewidywalnego hasła. Całość bezpieczeństwa obejmuje generowanie, implementację, przechowywanie, ekran i odzyskiwanie.

Złożony wygląd kodu QR również nie świadczy o bezpieczeństwie. Trzeba znać zawartość, twórcę i działanie aplikacji po odczycie. Przed zatwierdzeniem poproś tutora o wyjaśnienie celu bez ujawniania prywatnych danych.

Ćwiczenie

1. Dopasuj „wykrycie zmiany pliku”, „ukrycie frazy seed” i „autoryzację płatności” do skrótu, szyfrowania i podpisu.
2. Zmień jedną literę fikcyjnego tekstu i zobacz, że zmienia się skrót. Nie używaj sekretów w demonstracji.
3. Wyjaśnij, jak transakcja może być jednocześnie publiczna i podpisana.

Sprawdź swoje umiejętności

Opisz oczekiwaną gwarancję i zapewniający ją mechanizm. Nie używaj słowa „zaszyfrowane” jako określenia wszystkiego, co bezpieczne.

Częste pytanie

Czy skrót oprogramowania układowego poświadcza brak błędów? Nie. Identyfikuje bajty, o ile wzorzec jest wiarygodny. Audyt, podpis producenta i test fizyczny odpowiadają na różne pytania.

Miejsce na przerwę

Zachowaj trzy pary z ćwiczenia.

Który mechanizm ukrywa treść sekretu?

1. Opublikowanie nazwy jego pliku.
2. Podpisanie go bez szyfrowania.
3. Prawidłowe zaszyfrowanie go chronionym kluczem.

> **Pokaż odpowiedź: Prawidłowe zaszyfrowanie go chronionym kluczem.**
> Sam podpis ani odcisk nie zapewnia poufności.

M03

Fraza seed, hasło dodatkowe i hasło dostępu

Cel

Unikaj mylenia różnych danych uwierzytelniających w systemie.

Zrozumienie tematu

Mnemonik BIP39 przedstawia entropię i sumę kontrolną za pomocą słów ze słownika. Standardowe długości to 12, 15, 18, 21 lub 24 słowa. Łatwe do zapamiętania zdanie, tekst piosenki czy słowa wybrane przez człowieka na chybił trafił nie zastępują bezpiecznego generowania. Suma kontrolna wykrywa część błędów, ale nie dowodzi, kto utworzył frazę ani że nikt inny jej nie zna.

Dodatkowe hasło BIP39 (passphrase) uczestniczy w wyprowadzaniu binarnego ziarna. Inne hasło może otworzyć zupełnie odmienny, pozornie pusty portfel. Komunikat „nieprawidłowe hasło dodatkowe” nie musi się pojawić. Hasło nie musi należeć do słownika i nie jest dosłownie dwudziestym piątym słowem.

Hasło kryptogramu Cuvex chroni przechowywany sekret. Hasło Desk zabezpiecza lokalny magazyn komputera. PIN parowania upoważnia do sesji komunikacyjnej. Klucz czatu odtwarza tożsamość komunikatora. Żadne z nich nie jest frazą seed. Znajomość jednego nie oznacza możliwości odtworzenia pozostałych.

Fraza seed i hasło dodatkowe w jednym kryptogramie mogą ułatwić odzyskanie, ale osoba, która go odszyfruje, otrzyma oba. Oddzielenie stawia większe wymagania tobie i spadkobiercom. Decyzję należy udokumentować i przetestować. Nie podejmuj jej dlatego, że tutor uważa wariant za „bardziej zaawansowany”.

Ćwiczenie

1. Przygotuj pięć papierowych kart bez tajnych wartości: fraza seed, hasło dodatkowe, hasło Cuvex, hasło Desk i klucz czatu.
2. Zapisz, co odtwarza każdy element i co utracisz, gdy go zapomnisz.
3. Zaprojektuj test na pustym portfelu. Słowa i hasło dodatkowe wprowadź prywatnie. Tutorowi przekaż tylko wynik.

Sprawdź swoje umiejętności

Wyjaśnij, dlaczego kurs nie może prosić o hasło w celu „sprawdzenia” nauki. Wskaż sekret wymagany przez twoją procedurę odzyskiwania.

Częste pytanie

Czy mogę zresetować hasło dodatkowe przez e-mail? BIP39 nie przewiduje takiego mechanizmu. Powiernik może oferować odzyskiwanie konta, ale to inny model.

Miejsce na przerwę

Zapisz „rozróżniono dane uwierzytelniające”, bez ich wartości.

Zmieniasz literę hasła dodatkowego BIP39 i widzisz zerowe saldo. Która interpretacja jest poprawna?

1. Może to być inny prawidłowy portfel wyprowadzony z innego hasła.
2. Sieć skasowała twoje środki.
3. Desk powinien odgadnąć pierwotne hasło.

> **Pokaż odpowiedź: Może to być inny prawidłowy portfel wyprowadzony z innego hasła.**
> Odmienne hasło dodatkowe może utworzyć inny portfel bez zgłaszania błędu.

Wyprowadzanie kluczy, xpub i deskryptory

Cel

Zrozum, jak opisać portfel bez przekazywania możliwości wydawania środków.

Zrozumienie tematu

Portfel hierarchiczny wyprowadza wiele kluczy z jednego korzenia. Ścieżka określa gałąź. W mainnecie BIP84 zwykle używa m/84'/0'/0' dla pierwszego konta SegWit z jednym podpisem, a BIP48 P2WSH stosuje m/48'/0'/0'/2' dla pierwszego konta wielopodpisowego. Apostrof oznacza wyprowadzanie utwardzone. Zmiana konta, sieci lub skryptu może dać inne adresy z tego samego mnemonika.

Xpub to rozszerzony klucz publiczny pozwalający wyprowadzić określone potomne klucze publiczne. Nie jest hasłem do wydawania, ale może pozwolić obserwować rodzinę adresów. Odcisk klucza głównego to krótki identyfikator ułatwiający kojarzenie wpisów. Sam nie gwarantuje tożsamości ani nie wyklucza kolizji.

Deskryptor opisuje budowę skryptów i adresów za pomocą typu skryptu, kluczy, ich pochodzenia i ścieżek. Deskryptor obserwacyjny z kluczami publicznymi pozwala obserwować, nie podpisywać. Sama nazwa „deskryptor” nie gwarantuje wyłącznie publicznej zawartości. Niektóre formaty mogą zawierać klucze prywatne. Nigdy nie przesyłaj rzeczywistego deskryptora do kursu.

Odzyskanie wielopodpisu zwykle wymaga pełnej polityki, a nie tylko słów jednego podpisującego. Zachowaj próg, uczestników, xpub, ścieżki, sieć, typ skryptu i dane do odkrywania adresów. Suma kontrolna deskryptora pomaga wykryć błędy przepisania, ale nie uwierzytelnia uczestników.

Ćwiczenie

1. Odczytaj fikcyjną ścieżkę i wyjaśnij jej cel, walutę, konto i gałąź. Nie wprowadzaj prawdziwych kluczy.
2. Odróżnij adres odbiorczy, xpub uczestnika i pełny deskryptor.
3. Przygotuj prywatną kartę odzyskiwania z podpisanymi pustymi polami i oddzielnym miejscem przechowywania dokumentacji.

Sprawdź swoje umiejętności

Wyjaśnij, dlaczego pusty portfel po odtworzeniu nie dowodzi utraty. Sprawdź sieć, dodatkowe hasło, skrypt, konto, ścieżkę i odkrywanie adresów.

Częste pytanie

Czy xpub można publikować bez konsekwencji? Sam zwykle nie daje możliwości wydawania, ale naraża prywatność, a w szczególnych kombinacjach kryptograficznych może zwiększyć inne ryzyka.

Miejsce na przerwę

W kursie zachowaj wyłącznie kartę bez wrażliwych wartości.

Czego może brakować przy próbie odzyskania wielopodpisu tylko z jedną frazą seed?

1. Koloru urządzenia.
2. Polityki i kluczy publicznych pozostałych uczestników.
3. Hasła do serwisu społecznościowego.

> **Pokaż odpowiedź: Polityki i kluczy publicznych pozostałych uczestników.**
> Odtworzenie skryptów wymaga pełnej polityki oraz progowej liczby kluczy prywatnych.

M03

Wybór portfela i modelu przechowywania

Cel

Porównaj narzędzia pod względem funkcji, zaufania i możliwości odzyskania.

Zrozumienie tematu

Portfel to narzędzia do opisu, obserwowania i, w odpowiednich przypadkach, autoryzowania wydatków. Gorący portfel może podpisywać w środowisku podłączonym do sieci. Odizolowane urządzenie podpisujące oddziela sekrety od sprzętu odpytującego sieć. Portfel obserwacyjny ma publiczne dane wystarczające do obserwacji i przygotowania transakcji. Do podpisu potrzebuje innego systemu.

W modelu powierniczym konto może oznaczać roszczenie wobec firmy. Przy samodzielnym przechowywaniu zachowujesz techniczną możliwość wydawania, samodzielnie lub wspólnie. Odzyskiwanie dostępu przez e-mail i uprawnienie do blokowania wypłat zwykle wskazują pierwszy model. Oceniając oba, uwzględnij różny podział odpowiedzialności.

Porównaj obsługę sieci i skryptów, weryfikację na ekranie, kopie, aktualizacje, interoperacyjność, utrzymanie, zapytania do dostawców i czytelność błędów. Lista walut i wykończenie obudowy nie wystarczą. Urządzenie podpisujące nie uchroni przed zatwierdzeniem niesprawdzonego błędnego adresu.

Cuvex oddziela sekrety chronione w kryptogramach od organizacji danych i zapytań w Desk. Trzeba zachować kryptogram i środki jego odblokowania. Ochrona przed utratą urządzenia nie zapewni odzyskania, gdy znikną także wszystkie kopie lub hasła. Poznaj całą procedurę przed przeniesieniem majątku.

Ćwiczenie

1. Porównaj w tabeli Cuvex, gorący portfel i giełdę. Kto podpisuje, kto widzi zapytania, kto może odzyskać dostęp i co się stanie po zamknięciu firmy?
2. Wybierz dwa kryteria wymagające dowodów innych niż reklama.
3. Sprawdź, czy środowisko ćwiczeń nie dzieli kluczy z twoimi oszczędnościami.

Sprawdź swoje umiejętności

Uzasadnij wybór dla konkretnego przypadku, nie ogłaszając żadnego narzędzia niezniszczalnym.

Częste pytanie

Czy portfel sprzętowy zapewnia prywatność wszystkich transakcji? Nie. Chroni głównie możliwość podpisu i część weryfikacji. Łańcuch, zapytania i kontrahenci nadal ujawniają informacje.

Miejsce na przerwę

Zachowaj tabelę kryteriów bez nazw kont.

Co może zrobić prawidłowo skonfigurowany portfel obserwacyjny z kluczami publicznymi?

1. Obserwować i przygotowywać operacje bez możliwości samodzielnego podpisu.
2. Zmienić utraconą frazę seed.
3. Zagwarantować anonimowość.

> **Pokaż odpowiedź: Obserwować i przygotowywać operacje bez możliwości samodzielnego podpisu.**
> Obserwowanie i autoryzowanie to rozdzielne możliwości.

Kopie zapasowe, które można odtworzyć

Cel

Zaprojektuj pełną kopię i sprawdź odzyskanie, zanim zaczniesz na niej polegać.

Zrozumienie tematu

Przydatna kopia przywraca możliwość działania, nie tylko plik. Przy jednym podpisie może wymagać mnemonika, dodatkowego hasła i danych wyprowadzania. Przy wielopodpisie potrzeba również polityki i wystarczającej liczby podpisujących. Desk może wymagać zaszyfrowanej kopii i jej hasła. Odzyskanie tożsamości czatu nie oznacza odzyskania dawnych wiadomości.

Nadmiarowe kopie chronią przed przypadkową utratą, a ich rozdzielenie przed wspólnym naruszeniem. Dwa nośniki w różnych miejscach mogą ograniczyć powiązane awarie. Każda kolejna kopia wymaga kontroli dostępu, spisu i przeglądu. Nazwy plików i etykiety nie powinny ujawniać majątku ani ułatwiać odnalezienia wszystkich składników.

Test powinien potwierdzić wcześniej sprawdzony adres, a w środowisku nauki również zdolność podpisania kontrolowanej operacji. Otwarcie pliku nie dowodzi, że należy on do właściwego portfela. Nie sprawdzaj kopii przez wpisywanie rzeczywistej frazy seed na przypadkowym komputerze.

Udokumentuj, co każda kopia obejmuje i pomija. Zmiana bieżącego hasła nie aktualizuje starych kopii. Ujawnienie dawnego hasła nadal wpływa na chronione nim egzemplarze. Skasowanie pliku z nowoczesnego nośnika nie gwarantuje usunięcia wszystkich kopii i wersji.

Ćwiczenie

1. Wypełnij prywatną tabelę: obiekt, zawartość, powiązane hasło, odrębna lokalizacja, data próby i osoba odpowiedzialna.
2. Odtwórz kopię ćwiczeniową w osobnym środowisku. Sprawdź sieć, pierwszy adres i wyprowadzanie.
3. Zasymuluj najpierw utratę komputera, potem urządzenia. Wskaż, która procedura się zmieni.

Sprawdź swoje umiejętności

Odtwórz scenariusz testowy bez improwizowanej pomocy i wyjaśnij, jakich informacji nadal brakowałoby w innym scenariuszu.

Częste pytanie

Czy pełna kopia Desk obejmuje wszystko? Nie zakładaj tego. W sprawdzonej wersji nie obejmuje historii ani sesji czatu. Polityka wielopodpisowa i klucze prywatne pełnią odmienne funkcje.

Miejsce na przerwę

Zapisz datę i wynik próby, nigdy zawartość kopii.

Zmieniasz hasło Desk. Co dzieje się z wcześniejszą kopią?

1. Aktualizuje się sama.
2. Automatycznie traci szyfrowanie.
3. Zachowuje zabezpieczenie i hasło użyte przy jej tworzeniu.

> **Pokaż odpowiedź: Zachowuje zabezpieczenie i hasło użyte przy jej tworzeniu.**
> Wcześniejsze kopie to niezależne obiekty.

M04

Poznaj Original i BIT

Cel

Wybierz właściwą procedurę dla swojego urządzenia i jego wersji.

Zrozumienie tematu

Original przenosi kryptogramy i obsługiwane operacje na kartach NFC. Bluetooth uczestniczy w aktualizacji, a USB-C w opisanym modelu służy do zasilania. BIT wymienia pliki przez USB-C i dodaje biometrię dla kryptogramów, które jej wymagają. Nie stosuj instrukcji NFC ani Bluetooth dla Original do BIT.

Poza ustawieniami urządzenie oferuje szyfrowanie, odszyfrowywanie, tworzenie portfeli i podpisywanie. Original klonuje karty, a BIT pracuje na plikach nośnika USB. Nazwy, języki i sposób dostępu mogą zależeć od wersji. Nowa pozycja „Sprawdź polityki” w BIT otwiera obsługiwaną procedurę, nie zmieniając tego, kto autoryzuje.

Sprawdzone odniesienia redakcyjne to Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 i Mirror beta.12.12. Są to wersje źródłowe. Podpis, dystrybucję i fizyczny odbiór każdej kombinacji trzeba sprawdzić z zespołem. Nie zastępuj oprogramowania układowego niepodpisanym plikiem binarnym z pakietu inżynierskiego.

Przed użyciem sprawdź pochodzenie, plomby, wygląd i wersję. Identyfikowalność i podpis aktualizacji pomagają wobec konkretnych zagrożeń, lecz nie zastępują wszystkich kontroli. Przy śladach ingerencji lub nieoczekiwanej wersji wstrzymaj inicjalizację i skontaktuj się ze wsparciem niezależnie sprawdzonym kanałem.

Ćwiczenie

1. Rozpoznaj model i zapisz widoczną wersję bez fotografowania sekretów.
2. Znajdź szyfrowanie, odszyfrowywanie, tworzenie portfela, PSBT i ustawienia. Nie uruchamiaj kasowania ani aktualizacji dla samego poznania menu.
3. Wybierz w kursie ścieżkę Original lub BIT i zachowaj wybór na czas ćwiczenia.

Sprawdź swoje umiejętności

Wyjaśnij, jak operacja dociera do twojego modelu i wraca z niego oraz który nośnik trzeba chronić przed nadpisaniem.

Częste pytanie

Czy BIT jest automatycznie bezpieczniejszy dla każdego? Modele oferują różne rozwiązania operacyjne. Odpowiedź zależy od zagrożeń, odzyskiwania i prawidłowego użycia.

Miejsce na przerwę

Zapisz model i wersję w prywatnym notatniku. Kurs potrzebuje tylko wybranego modelu.

Masz BIT, a instrukcja każe zapisać kartę NFC samym urządzeniem. Co robisz?

1. Sprawdzam, czy instrukcja dotyczy mojego modelu, i korzystam z obsługiwanej ścieżki USB.
2. Wymuszam aktualizację Original.
3. Wysyłam frazę seed na telefon.

> **Pokaż odpowiedź: Sprawdzam, czy instrukcja dotyczy mojego modelu, i korzystam z obsługiwanej ścieżki USB.**
> Instrukcje muszą odpowiadać rzeczywistemu sposobowi przesyłania danych w modelu.

Generowanie frazy seed z entropii fizycznej

Cel

Poznaj generowanie i przećwicz procedurę bez używania danych kursowych jako własnych kluczy.

Zrozumienie tematu

Entropia to nieprzewidywalność. Odpowiednie kości mogą jej dostarczyć, jeśli kolejność wyznaczysz przed rzutem, a algorytm konwersji jest prawidłowy. Odrzucone wyniki powtarzaj dokładnie według instrukcji. Zastąpienie ich maksymalną liczbą lub wybranym słowem zniekształca rozkład.

Sprawdzony proces Cuvex używa monety i czterech kości. Funkcja liczy wynik monety × 1 296 plus liczbę w systemie szóstkowym, której cyfry to wyniki kolejnych kości pomniejszone o jeden. Dopuszcza indeksy od 0 do 2 047. Jeśli wynik wypada poza słownik, powtórz monetę i wszystkie cztery kości. Zachowanie monety i powtórzenie samych kości zniekształca rozkład. Tak działa sprawdzony kod. Ekran i pełną ścieżkę trzeba zweryfikować dla każdego wydawanego oprogramowania układowego.

To nie to samo co wybór ulubionych słów. Nie używaj publicznej demonstracji do zabezpieczania pieniędzy. Każdą frazę seed widoczną w materiałach uznaje się za znaną. Ostatnie słowo i jego sprawdzenie musi wyznaczyć pełny algorytm urządzenia. Nie uzupełniaj mnemonika ręcznie.

Przygotuj miejsce bez kamer, ekranowego nagrywania, obserwatorów i włączonych w pobliżu asystentów głosowych. Tutor powinien przerwać pracę na czas wpisywania i sprawdzania sekretu. Może objaśnić procedurę przed ćwiczeniem i ocenić ją później pytaniami, nie słysząc wyników rzutów ani słów.

Po wygenerowaniu sprawdź kopię, zaszyfruj ją odpowiednio do modelu i przetestuj odzyskanie pustego portfela. Adres weryfikacyjny pomaga potwierdzić zgodność bez ujawniania frazy komputerowi. Jeśli procedura przyjmuje wartości sprzeczne z instrukcją lub pokazuje nieoczekiwane słowa, przerwij i zapisz tylko wersję, ekran i błąd.

Ćwiczenie

1. Podczas próby wykonuj kroki urządzenia z materiałem bez środków. Ustal kolejność kości i nie zmieniaj wyników.

2. Powtarzaj odrzucone wejścia zgodnie z ekranem, nie poprawiając ich pod oczekiwany zakres.
3. Prywatnie sprawdź zawartość, utwórz kopię i potwierdź możliwość odtworzenia tego samego portfela ćwiczeniowego.

Sprawdź swoje umiejętności

Wyjaśnij, dlaczego fizyczna entropia, prawidłowe przekształcenie i tajność wyniku są odrębnymi wymaganiami.

Częste pytanie

Czy mogę podać rzuty AI, by sprawdziła algorytm? Nie dla frazy seed, której zamierzasz używać. Pomoc pracuje na innych, sztucznych przykładach.

Miejsce na przerwę

Zakończ w bezpiecznym stanie urządzenia. Podczas przerwy nie zostawiaj widocznej frazy.

Oprogramowanie układowe odrzuca wynik rzutu kośćmi. Które działanie jest poprawne?

1. Ręcznie wybrać słowo.
2. Powtórzyć według wskazania urządzenia, nie zniekształcając wyniku.
3. Zmniejszać liczbę aż do zaakceptowania.

> **Pokaż odpowiedź: Powtórzyć według wskazania urządzenia, nie zniekształcając wyniku.**
> Odrzucenia stanowią część przekształcania entropii. Nie wolno ich dowolnie zastępować.

Szyfrowanie i odszyfrowywanie sekretu w Cuvex

Cel

Utwórz kryptogram ćwiczeniowy i sprawdź odzyskanie jego treści.

Zrozumienie tematu

Wybierz właściwy typ treści: BIP39, SLIP39, Monero lub tekst, jeśli jest dostępny. To różne formaty. Zaszyfrowanie tekstu SLIP39 nie czyni z Cuvex urządzenia podpisującego dla wszystkich sieci, które mogą go używać. Przechowywanie sekretów i realizacja protokołów podpisu mają różny zakres.

Aby utrzymać treść poza połączonymi urządzeniami, wpisuj ją bezpośrednio na urządzeniu. Import z telefonu lub komputera mógł już ujawnić sekret u źródła mimo późniejszego zaszyfrowania. Na ekranie przed zatwierdzeniem sprawdź słowa, kolejność, wielkość liter i pola.

Hasło kryptogramu powinno być długie, unikalne i możliwe do odzyskania zgodnie z planem. Sprawdzona klawiatura tworzenia przyjmuje 40 znaków. Walidator wymaga co najmniej 12, dużej i małej litery ASCII, cyfry i rozpoznawanego symbolu. Zakres Desk od 12 do 1 024 znaków nie przenosi się automatycznie na klawiaturę Cuvex. Inne pola odzyskiwania mogą mieć odrębne limity. Sprawdź procedurę i wersję.

W Original zapisz na odpowiedniej pustej karcie i utrzymaj ją w miejscu do potwierdzenia. W BIT zachowaj wszystkie pliki utworzone w procedurze USB, w tym wymagane składniki biometryczne, jeśli występują. Nie zmieniaj nazw ani nie łącz plików intuicyjnie. Potem próbnie odczytaj i odszyfruj treść na urządzeniu, nie przekazując sekretu tutorowi.

Ćwiczenie

1. Zaszyfruj tekst dydaktyczny utworzony na potrzeby tego ćwiczenia, bez danych dostępu i wartości ekonomicznej.
2. Rozpoznaj nośnik i powstały obiekt. Prywatnie zapisz alias i funkcję.
3. Uruchom ponownie proces odszyfrowania, sprawdź tekst na zaufanym ekranie i po zakończeniu zamknij widok.

Sprawdź swoje umiejętności

Odróżnij właściwą treść, poprawny zapis i skuteczne odzyskanie. Komunikat „plik skopiowany” nie dowodzi wszystkich trzech.

Częste pytanie

Czy alias karty jest hasłem? Nie. Służy organizacji. Unikaj sald i opisów ułatwiających rozpoznanie majątku.

Miejsce na przerwę

Nie zostawiaj odszyfrowanej treści na widoku. Zapisz tylko powodzenie lub niepowodzenie próby.

Co najlepiej dowodzi, że można odzyskać zawartość testowego kryptogramu?

1. Ma ładną nazwę.
2. Plik znajduje się w dwóch folderach.
3. Odczytanie i odszyfrowanie go właściwą procedurą oraz prywatne sprawdzenie treści.

> **Pokaż odpowiedź: Odczytanie i odszyfrowanie go właściwą procedurą oraz prywatne sprawdzenie treści.**
> Istnienie kopii nie dowodzi jej użyteczności ani zgodności z oryginałem.

M04

Progi szyfrowania i biometria

Cel

Odróżnij wspólną ochronę sekretu od wielopodpisu Bitcoin.

Zrozumienie tematu

Kryptogram chroniony wieloma hasłami określa, kto może odszyfrować treść. Portfel wielopodpisowy Bitcoin określa, które klucze muszą zatwierdzić wydatek w sieci. Wspólnie zaszyfrowany sekret może należeć do portfela z jednym podpisem. Każdy podpisujący w wielopodpisie może też mieć osobny, indywidualny kryptogram.

Gdy kilka osób razem odblokowuje jedną frazę, która pozwala samodzielnie wydać środki, próg w łańcuchu pozostaje równy jednemu kluczowi. Po ujawnieniu ktoś może zachować frazę. Nie opisuj tego jako wymogu koordynowania kilku podpisów przy każdym wydatku.

Biometria BIT dodaje warunek dostępu w formatach, które jej używają. Palec nie jest frazą seed ani uniwersalnym zastępstwem hasła. Uwzględnij urazy, zmiany odcisku, awarie, dostępność sprzętu i dziedziczenie. Zachowaj i przetestuj udokumentowaną metodę odzyskania danego kryptogramu, zanim stanie się potrzebna.

Eksport odzyskiwania może ujawnić sekret na komputerze właśnie po to, by poradzić sobie z sytuacją awaryjną. Istnienie funkcji nie czyni komputera środowiskiem równoważnym urządzeniu. W zwykłym użyciu zachowaj izolację. Lokalną procedurę odzyskiwania przeanalizuj świadomie i przygotuj późniejszą migrację w razie ujawnienia.

Ćwiczenie

1. Narysuj dwie polityki: „dwa hasła do otwarcia frazy seed” i „dwa klucze z trzech do wydania”.
2. W próbie bez środków ustal, których plików wymaga kopia biometryczna i gdzie sprawdza się jej odtworzenie.
3. Zasymuluj niedostępność jednej osoby. Określ, czy próg twojego schematu pozwala kontynuować.

Sprawdź swoje umiejętności

Wyjaśnij, kto może poznać sekret i kto po odszyfrowaniu może zatwierdzić wydatek.

Częste pytanie

Czy można usunąć uczestnika zmianą etykiety? Nie. Odróżniaj zmiany organizacyjne od nowego zabezpieczenia sekretu i nowej polityki wydawania.

Miejsce na przerwę

Zachowaj schemat bez rzeczywistych nazwisk i danych biometrycznych.

Trzy osoby dwoma hasłami otwierają kryptogram z jedną frazą seed portfela z pojedynczym podpisem. Ilu kluczy wymaga Bitcoin do wydania?

1. Jednego, jeśli taka jest polityka portfela.
2. Dwóch, ponieważ plik wymagał dwóch haseł.
3. Trzech ze względu na liczbę osób.

> **Pokaż odpowiedź: Jednego, jeśli taka jest polityka portfela.**
> Próg szyfrowania nie zmienia skryptu kontrolującego środki.

Klonowanie, przechowywanie i weryfikacja kopii

Cel

Utwórz nadmiarowe kopie, nie niszcząc jedynego ważnego egzemplarza.

Zrozumienie tematu

Klonowanie kryptogramu kopiuje zaszyfrowane dane. Nie tworzy salda, nowej frazy ani niezależności od ujawnionego hasła. Identyczne kopie pomagają po utracie nośnika, nie po naruszeniu sekretu źródłowego. Odtworzenie i migracja na nowe klucze odpowiadają więc na inne zdarzenia.

W Original odróżniaj kartę kryptogramu od karty transportowej PSBT. Nośnik operacyjny można ponownie wykorzystać zgodnie z procedurą. Karta z kopią zapasową nie powinna przejmować tej roli. Jeśli operacja odrzuca kartę zawierającą kryptogram, nie omijaj ochrony ani nie kasuj ręcznie nagłówka.

Kopia w BIT musi zachować komplet wymaganych plików i ich powiązania. Menedżer plików może wskazać zakończenie transferu bez gwarancji, że urządzenie zatwierdziło treść lub zakończyło operację. Poczekaj na wymagane stany i sprawdź kopię przez kontrolowane odzyskanie.

Prowadź prywatny spis z dyskretnymi identyfikatorami, wersją formatu, datą i wynikiem ostatniej próby. Rozdziel co najmniej dwie kopie względem określonych zagrożeń. Nie wgrywaj kopii do kanału wsparcia dla diagnozy. Przekaż oczyszczone metadane i kody błędów.

Ćwiczenie

1. Skopiuj ćwiczeniowy kryptogram na inny nośnik właściwą procedurą.
2. Odłącz pierwotny nośnik i odtwórz próbny tekst z kopii.
3. Opisz postępowanie po utracie, uszkodzeniu pliku i ujawnieniu hasła. To odrębne procedury.

Sprawdź swoje umiejętności

Wskaż sprawdzoną kopię i wyjaśnij, dlaczego oryginał nie został nadpisany.

Częste pytanie

Czy mogę skasować oryginał po zobaczeniu drugiego pliku? Najpierw sprawdź odzyskanie i zakres kopii. Usunięcie powinno wynikać z planu, a nie samej liczby kopii.

Miejsce na przerwę

Schowaj nośniki przed końcem sesji i nie mieszaj kart kopii z kartami prób płatności.

Ktoś zna hasło i uzyskuje kopię kryptogramu. Co daje utworzenie trzech dalszych klonów?

1. Unieważnia kopię napastnika.
2. Zapewnia nadmiarowe kopie, ale nie unieważnia jego dostępu.
3. Automatycznie zmienia frazę seed Bitcoina.

> **Pokaż odpowiedź: Zapewnia nadmiarowe kopie, ale nie unieważnia jego dostępu.**
> Duplikowanie nie usuwa skutków istniejącego naruszenia.

M05

Instalowanie i zabezpieczanie Cuvex Desk

Cel

Uruchom instalację ze sprawdzonego źródła i zabezpiecz jej lokalny magazyn.

Zrozumienie tematu

Wybierz dostępny pakiet dla systemu i architektury: macOS Intel lub Apple Silicon, Windows x64 lub ARM64, Linux x64 lub ARM64. ZIP z kodem źródłowym, pakiet menedżera i instalator klienta to różne wydania. Kurs nie powinien kierować uczestnika do prywatnego pakietu do podpisywania.

Sprawdź pochodzenie i kontrole systemowe. Inżynierski podpis Windows sam nie nadaje wydawcy publicznego zaufania. Na Macu podpis aplikacji, notaryzacja i ocena przy otwarciu to różne kontrole. Nie wyłączaj ogólnych zabezpieczeń na polecenie rzekomego wsparcia. Przy nieoczekiwanym ostrzeżeniu zachowaj treść i użyj oficjalnego kanału.

Desk tworzy lokalny magazyn zaszyfrowany hasłem. W sprawdzonej wersji nowe hasła mają od 12 do 1 024 znaków. Przy potwierdzeniu pola muszą być zgodne. Sama długość nie określa jakości. Użyj unikalnej frazy i nie stosuj jej ponownie. Biometria komputera, o ile dostępna, ułatwia dostęp i wymaga osobnej konfiguracji.

Ustaw blokadę przy bezczynności i, jeśli dotyczy, przy przejściu w tło. Podręcznik omawia opóźnienia po błędach i opcjonalne usuwanie. Nie włączaj automatycznego kasowania podczas demonstracji. Aplikacja może działać bez tradycyjnego konta użytkownika, ale usługi zapytań, czatu i pobierania mają własne wymagania i połączenia.

Ćwiczenie

1. Sprawdź platformę, widoczną wersję i pochodzenie pakietu bez podawania tutorowi prywatnych identyfikatorów.
2. Utwórz magazyn ćwiczeniowy i sprawdź blokadę oraz ponowne otwarcie. Wpisuj hasło prywatnie.
3. Zaplanuj zaszyfrowaną kopię i zachowaj hasło zgodnie z planem. Nie testuj kolejnych blokad w rzeczywistym środowisku.

Sprawdź swoje umiejętności

Odróżnij lokalne hasło, konto handlowe i dane dostępu do dodawanych usług.

Częste pytanie

Czy zmiana hasła Desk zmienia hasła kart? Nie. To niezależne zabezpieczenia. Stare kopie również nie zmieniają się same.

Miejsce na przerwę

Zablokuj Desk i zachowaj identyfikator lekcji bez danych uwierzytelniających.

Instalator nie pasuje do architektury twojego systemu. Jaki jest pierwszy krok?

1. Wyłączyć zabezpieczenia i wymusić uruchomienie.
2. Pobrać odpowiedni oficjalny pakiet i sprawdzić jego wymagania.
3. Zaimportować frazę seed na stronie internetowej, aby kontynuować.

> **Pokaż odpowiedź: Pobrać odpowiedni oficjalny pakiet i sprawdzić jego wymagania.**
> Zgodność i pochodzenie ustala się przed użyciem materiału do przechowywania środków.

M05

Łączenie kryptogramów i zarządzanie WOW

Cel

Powiąż zaszyfrowaną kopię i odróżnij ją od konta obserwacyjnego.

Zrozumienie tematu

Desk organizuje kryptogramy powiązane przez NFC, USB lub zgodny plik kopii. Wzór i alias pomagają je rozpoznać, ale nie są kryptograficznym dowodem tożsamości. W szczegółach można odczytać pochodzenie i właściwości zinterpretowane przez aplikację, m.in. format, rozmiar i cechy dostępu.

Powiązanie importuje lub porządkuje zgodny obiekt. Nie oznacza odszyfrowania na komputerze ani sprawdzenia sekretu. WOW jest portfelem obserwacyjnym powiązanym odpowiednimi danymi publicznymi. Ten sam zestaw sekretów może odpowiadać różnym kontom i ścieżkom. Powiązanie musi dotyczyć portfela, którym chcesz zarządzać.

Aktywuj lub importuj konto za pomocą deskryptora lub danych publicznych wyeksportowanych przez urządzenie. Sprawdź sieć, typ skryptu, odcisk, ścieżkę i adres kontrolny. Nazwa konta służy organizacji. Identyfikator wyprowadzony z przewidywalnej nazwy nie zapewnia silnej anonimizacji, gdyż nazwę można odgadnąć.

Sprawdzona wersja Desk zachowuje konta oczekujące na powiązanie i pozwala eksportować kopie, klonować lub usuwać lokalne wpisy. Usunięcie karty z interfejsu nie niszczy zewnętrznych kopii i nie przesuwa środków. „Brak kopii” oznacza, że aplikacja nie potwierdziła jej według własnych kryteriów, a nie że nigdzie nie istnieje.

Ćwiczenie

1. Powiąż kryptogram ćwiczeniowy wybranym sposobem i sprawdź szczegóły.
2. Zaimportuj zgodne konto ćwiczeniowe, sprawdź sieć i adres kontrolny bez pokazywania tutorowi kluczy.
3. Odróżnij wpis kryptogramu, konto WOW i fizyczny nośnik. Wskaż, co zniknie po usunięciu lokalnym.

Sprawdź swoje umiejętności

Wyjaśnij, jakich danych Desk potrzebuje do obserwowania i które przy zwykłym użyciu powinny pozostać poza komputerem.

Częste pytanie

Czy powiązanie pliku .bin gwarantuje, że zawiera moją frazę seed? Nie. Sprawdź pochodzenie i odzyskanie. Rozszerzenie nie poświadcza treści.

Miejsce na przerwę

Zachowaj tylko stan „sprawdzono powiązanie testowe”.

Czy lokalne usunięcie konta WOW przenosi jego bitcoiny?

1. Nie. Zgodnie z procedurą usuwa lokalne informacje, nie wydaje UTXO.
2. Tak. Wysyła je producentowi.
3. Anuluje każdy podpis przechowywany przez inną osobę.

> **Pokaż odpowiedź: Nie. Zgodnie z procedurą usuwa lokalne informacje, nie wydaje UTXO.**
> Stan lokalny i stan łańcucha są odrębne.

M05

Parowanie Mirror z Desk

Cel

Nawiąż i zakończ autoryzowane połączenie lokalne, odróżniając używane kody.

Zrozumienie tematu

Mirror umożliwia lokalną współpracę z Desk przez parowanie, PIN i QR pokazywane w aplikacjach. Sześciocyfrowy PIN należy do danej sesji. Nie jest hasłem Desk, hasłem kryptogramu ani słowem odzyskiwania. Sprawdź, kto go generuje i gdzie trzeba go wpisać. Nie używaj kodu przysłanego przez nieznajomą osobę.

Rozpocznij we właściwym kontekście Desk. Powiązanie, odczyt QR, transport PSBT i oprogramowanie układowe służą innym celom. Okno pokazuje wyszukiwanie, połączenie, wykrycie, PIN, QR oraz działanie na karcie lub pliku. Widoczność urządzenia w wyszukiwaniu nie dowodzi zakończenia całej operacji.

Przyznaj uprawnienia potrzebne w danym systemie: kamera do odczytu optycznego, Bluetooth lub NFC, jeśli wymaga ich procedura. Instalacja aplikacji nie zapewni telefonowi brakującego sprzętu. W iOS występują różnice adaptera i weryfikacji. Możliwość zbudowania projektu nie dowodzi udostępnienia i przetestowania go na wszystkich iPhone’ach.

Przy błędzie ustal dokładny etap: brak urządzenia, wykryte bez połączenia, odrzucony PIN, nieczytelny QR, nieodczytana karta lub brak odpowiedzi. Zamknij stare sesje, sprawdź wersje oraz uprawnienia i ponów w kontrolowany sposób. Błędny PIN nie uzasadnia zmiany firmware ani wpisywania fraz w innym miejscu.

Ćwiczenie

1. Zacznij próbny odczyt z Desk i połącz Mirror przez lokalne ekrany.
2. Sprawdź cel przed pokazaniem ćwiczeniowego kodu QR lub karty.
3. Anuluj sesję i sprawdź, czy później nie zostanie użyty wynik z wcześniejszego kontekstu. Otwórz nową sesję.

Sprawdź swoje umiejętności

Opisz nieudany etap i zaangażowane urządzenia bez ujawniania aktywnych kodów lub wrażliwych treści.

Częste pytanie

Czy Mirror musi być stale połączony? Zależy od operacji. Nie traktuj go jak usługi stałej i nie zakładaj, że sesja nadal ma upoważnienie po zamknięciu lub przejściu w tło.

Miejsce na przerwę

Zamknij sesję parowania i zablokuj aplikacje, których nie używasz.

Co powinien zrobić tutor, jeśli parowanie nie udaje się przed wyświetleniem PIN-u?

1. Poprosić o frazę seed.
2. Sprawdzić wykrywanie urządzeń, uprawnienia, sesję i wersje przed przejściem dalej.
3. Uznać połączenie za zakończone powodzeniem.

> **Pokaż odpowiedź: Sprawdzić wykrywanie urządzeń, uprawnienia, sesję i wersje przed przejściem dalej.**
> Diagnoza musi odpowiadać zaobserwowanemu etapowi i nie może zakładać udanego połączenia.

NFC przez Mirror, USB-C i odczytywanie kodów QR

Cel

Stosuj każdy nośnik zgodnie z przeznaczeniem i właściwymi dla niego kontrolami.

Zrozumienie tematu

Obsługa NFC w Cuvex Desktop wymaga Cuvex Mirror na zgodnym smartfonie połączonym z komputerem przez Bluetooth. Cuvex Desktop nie obsługuje zewnętrznych czytników NFC na USB. Zgodne muszą być również karta, jej format i pojemność. Mała karta mieszcząca kryptogram może nie pomieścić PSBT z wcześniejszymi transakcjami. Rzeczywisty limit zależy od całej zawartości, a nie tylko liczby odbiorców. Nie używaj karty z kopią zapasową jako karty transportowej.

W Original Mirror może zapisać żądanie na karcie operacyjnej. Urządzenie je przetwarza i zapisuje odpowiedź, którą Mirror zwraca do Desk. Potwierdzenie zapisu nie oznacza odbioru w Desk. Trzymaj kartę nieruchomo do komunikatu o wyniku. Jeśli system chroni rozpoznany kryptogram, uszanuj odrzucenie.

BIT używa woluminu lub folderu wymiany USB. Procedura może odmontować i ponownie udostępnić wolumin. Desk musi wybrać prawidłowy nośnik, zweryfikować odpowiedź i wystawić przewidziane potwierdzenie. Skopiowanie pliku do folderu o tej samej nazwie na komputerze nie dostarcza go urządzeniu.

Skan QR może się nie udać przez ostrość, odbicie, rozmiar, ruch lub gęstość kodu. Powiększ widok, popraw oświetlenie i odległość. Nie skracaj identyfikatora do pierwszych liter ani nie przyjmuj częściowego zapisu. Po udanym odczycie dopiero zaczyna się weryfikacja treści.

Ćwiczenie

1. Na diagramie z materiałami szkoleniowymi wskaż żądanie, nośnik i odpowiedź dla Original i BIT.
2. Anuluj próbny odczyt QR bez zapisywania spóźnionych wyników. Powtórz dla innego celu.
3. Zasymuluj za duży plik i wyjaśnij potrzebę uproszczenia operacji lub użycia zgodnego nośnika bez pomijania weryfikacji.

Sprawdź swoje umiejętności

Wskaż, które urządzenie potwierdziło odczyt, zapis, walidację, odbiór lub pokwitowanie.

Częste pytanie

Czy skrót lub komunikat o skopiowaniu dowodzi właściwego odbiorcy Bitcoin? Nie. Sprawdź operację i wyjścia na urządzeniu podpisującym.

Miejsce na przerwę

Wyjmij i schowaj karty kopii zapasowych. Oznacz nośnik transportowy.

Original zgłasza zapis odpowiedzi na karcie. Co jeszcze trzeba zrobić przed stwierdzeniem, że odebrał ją Desk?

1. Pomalować kartę innym kolorem.
2. Utworzyć nową frazę seed.
3. Wczytać i zweryfikować odpowiedź w Desk odpowiednią procedurą.

> **Pokaż odpowiedź: Wczytać i zweryfikować odpowiedź w Desk odpowiednią procedurą.**
> Udany zapis i udany odbiór są odrębnymi zdarzeniami.

Publiczni dostawcy i własny węzeł

Cel

Wybierz źródło zapytań, poznaj zakres ujawnianych danych i ograniczenia.

Zrozumienie tematu

Desk może odpytywać zgodnych publicznych dostawców lub Bitcoin Core skonfigurowany przez użytkownika. Dostawca może widzieć zapytania, ich kolejność i dane połączenia. Nieprzekazywanie całego xpub ogranicza jeden rodzaj ujawnienia. Skrypty lub ich skróty również można ze sobą powiązać.

Desk 9.21 udostępnia jawny wybór Blockstream Electrum przez TLS obok wariantów REST i własnego węzła. TLS chroni kanał przed niektórymi obserwatorami sieci, ale dostawca nadal otrzymuje zapytania. Nie ma cichej rotacji gwarantującej anonimowość. Weź pod uwagę cenę wygody dla prywatności.

Dla Core skonfiguruj punkt końcowy, uwierzytelnianie i portfel obserwacyjny według instrukcji. Nie publikuj portu RPC ani nie wystawiaj go do internetu, aby aplikacja go „widziała”. Ogranicz dostęp do zaufanych środowisk i zastosuj odpowiednio chroniony transport. Nie dyktuj tutorowi hasła RPC.

Początkowa synchronizacja i ponowne skanowanie mogą potrwać. Postęp wskazuje trwającą pracę, nie jej przyszły sukces. Desk kontynuuje pracę w tle, a zamknięcie widoku nie zatrzymuje węzła. Udokumentowane minimalne okno historii nie gwarantuje znalezienia wcześniejszej aktywności. Przy starszym portfelu sprawdź datę importu i rzeczywisty zakres skanu.

Odkrywanie opiera się na historii, nie dodatnim saldzie. Adres opróżniony do zera nadal jest używany. Sprawdzony wielopodpis stosuje lukę 20 kolejnych adresów bez historii dla każdej gałęzi i uczestnika oraz limity wydawania nowych adresów. Nie przenoś jednego globalnego limitu na wszystkie portfele.

Ćwiczenie

1. Wybierz źródło do ćwiczeń i wyjaśnij, jakie informacje może zobaczyć.
2. Sprawdź datę ostatniej synchronizacji, sieć i postęp. Przy HTTP 429 respektuj przerwę i zmieniaj dostawcę tylko świadomie.
3. Zasymuluj portfel z zerowym saldem i dawną historią. Wyjaśnij różnicę między „zero” a „nieużywany”.

Sprawdź swoje umiejętności

Oceń, czy źródło spełnia potrzeby weryfikacji i prywatności, i rozpoznaj niepełny stan.

Częste pytanie

Czy własny węzeł zapewnia anonimowość? Nie. Zmniejsza zależność zapytań od dostawców. Nadal uwzględniaj połączenie, kontrahentów, publikację i inne metadane.

Miejsce na przerwę

Zapisz tylko typ dostawcy i potrzebę dokończenia skanowania.

Adres ma zerowe saldo, ale wcześniej odebrał i wydał środki. Jak go traktować przy wykrywaniu portfela?

1. Jako adres z historią.
2. Jako adres nigdy nieużywany.
3. Jako adres nieprawidłowy.

> **Pokaż odpowiedź: Jako adres z historią.**
> O użyciu świadczy historia, a nie bieżące saldo.

Odbieranie bitcoinów i weryfikacja adresu

Cel

Przygotuj żądanie płatności i zweryfikuj je przed przekazaniem.

Zrozumienie tematu

Otwórz właściwe konto WOW i potwierdź sieć oraz politykę. Utwórz lub odszukaj żądanie płatności. Dla własnej organizacji możesz dodać cel, obserwatora i oczekiwaną kwotę. To pola lokalne. Oczekiwana kwota nie uniemożliwia wysłania innej.

Sprawdź adres dostępną na urządzeniu ścieżką w kontekście portfela. Jeśli dana kombinacja nie została potwierdzona fizycznie, pozostań przy symulacji i zgłoś potrzebę sprawdzenia przed odbiorem znacznych środków. Dwa ekrany z tym samym źródłem nie stają się niezależne.

Dla nowej relacji płatniczej używaj nowego adresu, gdy procedura na to pozwala. W sprawdzonym wielopodpisie pokazane adresy nie są przydzielane ponownie ani nie wygasają, gdyż płatnik może użyć ich później. Po osiągnięciu limitu kolejnych nowych adresów bez historii odszukaj wcześniejsze właściwe żądanie i ustal przyczynę limitu. Nie cofaj indeksów.

Po przekazaniu żądania obserwuj wpływ w źródle weryfikacji. E-mail, pokwitowanie giełdy ani zrzut płatnika nie dowodzą rozliczenia. Sprawdź sieć, txid, wyjście, kwotę i potwierdzenia stosownie do ryzyka. Nie otwieraj dla wygody publicznego eksploratora z własnym adresem, jeśli plan wymaga prywatnych zapytań.

Ćwiczenie

1. Utwórz żądanie w laboratorium, sprawdź konto i sieć oraz wyjaśnij, jak zweryfikujesz adres.
2. Nadaj fikcyjną etykietę i odszukaj to samo żądanie po zamknięciu widoku.
3. Zasymuluj wpływ innej kwoty i ustal, jak go uzgodnić bez zmiany historii.

Sprawdź swoje umiejętności

Odróżnij adres wygenerowany i zweryfikowany, przekazane żądanie oraz potwierdzoną płatność.

Częste pytanie

Czy stary adres przestaje działać po utworzeniu następnego? Zwykle nie. Zachowanie mechanizmu odkrywania i rejestru żądań pozwala dostrzec spóźnione płatności.

Miejsce na przerwę

Zachowaj stan żądania laboratoryjnego. Nie zapisuj jego treści u tutora.

Płatnik wysyła zrzut z napisem „wypłata zakończona”. Co sprawdzasz przed uznaniem płatności?

1. Tylko jakość zrzutu.
2. Właściwe wyjście w wiarygodnym źródle sieciowym i wymaganą liczbę potwierdzeń.
3. Hasło płatnika.

> **Pokaż odpowiedź: Właściwe wyjście w wiarygodnym źródle sieciowym i wymaganą liczbę potwierdzeń.**
> Dokument handlowy ani zrzut nie zastępują sprawdzenia płatności.

Etykietowanie, zamrażanie i wybieranie UTXO

Cel

Przygotuj wejścia bez przypadkowego łączenia różnych źródeł.

Zrozumienie tematu

Etykiety zachowują kontekst nieobecny w łańcuchu, np. pochodzenie, kontrahenta, cel i ograniczenia użycia. W Desk etykieta UTXO i notatka adresu mogą mieć odmienne limity długości i funkcje. „Klient A” może wystarczyć. Numer dokumentu lub pełne nazwisko niepotrzebnie zwiększają wrażliwość wpisu.

Zamrożenie UTXO w Desk wyklucza je z niektórych lokalnych wyborów. Nie blokuje wydania w Bitcoinie, nie zmienia skryptu i nie powstrzymuje innej aplikacji z kluczami. Saldo całkowite może się różnić od dostępnego. Sprawdź, czy moneta jest zamrożona, zarezerwowana przez szkic czy rzeczywiście wydana.

Automatyczny wybór optymalizuje według algorytmu i kontekstu, bez koniecznej wiedzy o twoich prywatnych relacjach. Przy danej płatności oceń, czy można użyć wyjścia z tego samego kontekstu zamiast łączyć oszczędności, wynagrodzenie i działalność. Rozdzielenie wymaga dalszej konsekwencji, nie tylko ładnych etykiet.

Eksport etykiet w BIP329 ułatwia przechowywanie lub migrację. Format sam nie szyfruje. Desk oferuje zaszyfrowane opakowanie eksportu. Odróżnij zabezpieczony plik od zgodnego tekstu jawnego. Przed nadpisaniem danych przy imporcie sprawdź zgodność z portfelem i sposób traktowania zamrożeń.

Ćwiczenie

1. Oznacz trzy syntetyczne UTXO jako oszczędności, działalność i darowiznę.
2. Zamroź jedno i porównaj saldo obserwowane z dostępnym do wyboru.
3. Wyeksportuj etykiety laboratoryjne z hasłem, zaimportuj do kopii i sprawdź wyniki bez prawdziwych danych prywatnych.

Sprawdź swoje umiejętności

Uzasadnij wybór wejść kosztem i ujawnianymi powiązaniami. Rozpoznaj zamrożenie jako lokalną preferencję.

Częste pytanie

Czy etykieta dociera do odbiorcy płatności? Nie przez sam fakt, że istnieje lokalnie. Może wyciec przy eksporcie, udostępnianiu plików, użyciu innej usługi lub dodaniu do wiadomości.

Miejsce na przerwę

Zachowaj etykiety ćwiczeniowe i stan zamrożenia.

Jaki skutek ma zamrożenie UTXO w Desk?

1. Tworzy blokadę na poziomie konsensusu sieci.
2. Przenosi je na specjalne konto.
3. Nakłada lokalne ograniczenie wyboru według reguł aplikacji.

> **Pokaż odpowiedź: Nakłada lokalne ograniczenie wyboru według reguł aplikacji.**
> Nie odbiera uprawnień innym kopiom kluczy.

Przygotowanie i sprawdzenie płatności

Cel

Zbuduj czytelną PSBT i rozpoznaj wszystkie wyjścia oraz koszty.

Zrozumienie tematu

Wybierz konto, dostępne wejścia, odbiorców i kwoty. Sprawdź źródło żądania. Po wklejeniu lub skanie zweryfikuj cały adres i sieć. Schowek lub obraz mogą zostać podmienione. Nie polegaj tylko na początkowych i końcowych znakach, gdy można porównać całość.

Wybierz stawkę i sprawdź bezwzględną opłatę, szacunkowy rozmiar, sumę i resztę. Przy „Wyślij wszystko” Desk odlicza opłatę od dostępnej kwoty. Gdy operacja pochodzi z czatu, a kwota netto nie pokrywa żądania, świadomie zdecyduj o częściowej płatności. Pierwotnego żądania nie zmienia się, by ukryć różnicę.

Sprawdź małą resztę lub brak wyjścia reszty. Wyjście oznaczone jako własne zweryfikuj z polityką, nie z nazwą nadaną przez koordynatora. Jeśli reszta jest niepraktyczna, sprawdź wysłanie całości lub dodaj zgodne wejście. Nie pozwalaj na cichą zamianę reszty w nieproporcjonalną opłatę.

PSBT jest formatem przenoszenia informacji i podpisów. Nie zapewnia samoistnie prywatności ani autentyczności źródła. Może obejmować wcześniejsze transakcje, klucze publiczne, ścieżki i metadane. W sprawdzonych wersjach Final profil wielopodpisowy używa PSBT v0/BIP174. „Transakcja w wersji 2” nie oznacza „PSBT w wersji 2”.

Ćwiczenie

1. Zbuduj w symulatorze płatność z wejściem 120 000 sat, kwotą odbiorcy 70 000 sat i opłatą 1 000 sat.
2. Wymień wszystkie wyjścia i wyjaśnij resztę 49 000 sat. Powtórz z wysłaniem całości.
3. Anuluj szkic i wyjaśnij, co anulowano lokalnie. Nie używaj symulatora do podpisywania ani publikowania.

Sprawdź swoje umiejętności

Przed eksportem wyjaśnij wejścia, wyjścia, odbiorców, koszt i brakujące upoważnienie.

Częste pytanie

Czy można wysłać całe wyświetlone saldo? Tylko jeśli aplikacja wyliczy wykonalną kwotę netto, a opłaty są pokryte. Saldo może obejmować niedostępne monety.

Miejsce na przerwę

Zachowaj szkic ćwiczeniowy lub go anuluj. Nigdy nie zapisuj prawdziwej PSBT w portalu kursu.

Ekran pokazuje „transaction version 2”. Czy to dowodzi, że plik ma format PSBT v2?

1. Nie. To odrębne pola wersji.
2. Tak, zawsze.
3. Dowodzi to użycia Taproot.

> **Pokaż odpowiedź: Nie. To odrębne pola wersji.**
> BIP370 rozróżnia wersję kontenera i wersję transakcji.

Podpisywanie za pomocą Original i BIT

Cel

Przejdź obie ścieżki podpisu i odbierz odpowiedź powiązaną z właściwą operacją.

Zrozumienie tematu

Original: Przekaż PSBT przez kartę transportową w obsługiwanym procesie za pomocą Cuvex Mirror. Odczytaj żądanie na urządzeniu, podaj kryptogram i odblokuj go prywatnie. Sprawdź wszystkie wyjścia, kwoty, resztę i opłatę. Odpowiedź zostaje zapisana na karcie, a następnie odczytana i zweryfikowana w Desk. Udany zapis nie zastępuje tego przekazania zwrotnego.

BIT: Wybierz właściwy wolumin i przekaż żądanie przez USB-C. Lokalna usługa Desk obsługuje wymianę, podczas gdy ty korzystasz z urządzenia. Podaj kryptogram zgodnie z ekranem i przeprowadź kontrolę w BIT. „Odbierz z BIT” importuje odpowiedź. Desk sprawdza i zapisuje ją przed pokwitowaniem. Po rozłączeniu wznów tę samą operację, nie podobną do niej.

Przy wielopodpisie w wersjach firmware Final sprawdza się obowiązkowe podsumowanie i wyjścia, odpowiednie ostrzeżenia i trzy końcowe potwierdzenia „Podpisz PSBT”. Opcjonalny rozszerzony przegląd umożliwia odczyt dodatkowych parametrów. Wybór „Nie” nie usuwa wymaganych kontroli. Niezależna weryfikacja polityki stanowi osobną ścieżkę o właściwym jej zakresie.

Podpis wymaga zgodnego kryptogramu o sprawdzalnej autentyczności. Stara kopia nadal umożliwiająca odzyskanie sekretu nie uzyskuje przez to prawa do podpisywania. Jeśli urządzenie ostrzega o starej kopii bez potwierdzonej autentyczności, odtwórz i sprawdź sekret właściwą procedurą, a przed podpisem utwórz nową kopię. Nie zmieniaj nagłówków ani nie omijaj odrzucenia.

Anuluj przy niezgodnym adresie, nieoczekiwanej opłacie, brakujących danych, innej sieci lub odrzuconej polityce. Presja zakończenia rozmowy nie jest powodem do zgody. AI nie naciska przycisków, nie potwierdza ostatecznie ani nie uznaje za podpisane tego, czego nie sprawdzono.

Ćwiczenie

1. Przejdź ścieżkę swojego modelu z pustym portfelem lub w laboratorium po fizycznym odbiorze.

2. Zasymuluj zatrzymanie przed końcowymi potwierdzeniami i wyjaśnij, dlaczego nie oznacza autoryzacji.
3. Sprawdź powrót odpowiedzi, związek ze szkicem i, w BIT, stan odbioru i pokwitowania.

Sprawdź swoje umiejętności

Opisz ścieżkę bez poufnych danych. Odróżnij zgodę na urządzeniu, importowaną odpowiedź i opublikowaną transakcję.

Częste pytanie

Czy urządzenie offline wie, że wejścia nadal są niewydane? Samo nie sprawdzi aktualnego łańcucha. Aplikacja musi zweryfikować finalną transakcję w swoim źródle sieciowym.

Miejsce na przerwę

Jeśli przerwiesz podpisywanie, anuluj operację lub pozostaw oznaczony stan oczekiwania zgodnie z procedurą, bez widocznych sekretów.

BIT podpisuje, lecz Desk nie potwierdza odbioru. Jaki stan zakładasz?

1. Płatność została definitywnie opublikowana.
2. Odpowiedź czeka na odbiór lub weryfikację. Wznów tę samą operację.
3. Portfel został utracony.

> **Pokaż odpowiedź: Odpowiedź czeka na odbiór lub weryfikację. Wznów tę samą operację.**
> Podpisanie, odebranie i publikacja to odrębne etapy.

Finalizowanie, publikacja i rozwiązywanie problemów

Cel

Zamknij cykl płatności bez jej powielania i diagnozuj błędy na właściwym etapie.

Zrozumienie tematu

Po imporcie podpisu Desk musi sprawdzić zgodność ze szkicem i zachowanie intencji. Przy wielopodpisie może brakować progu. Przy pojedynczym podpisie import również nie zwalnia z kontroli. Gdy wszystkie warunki są spełnione, finalizacja daje transakcję gotową do rozesłania.

Publikuj dopiero po ostatecznej kontroli. Odpowiedź serwera lub txid wskazują wynik żądania, ale dalsza obserwacja musi potwierdzić przyjęcie i stan łańcucha. Przy braku odpowiedzi najpierw sprawdź stan. Nie twórz nowej płatności, aby rozwiązać problem wyświetlania.

Przy oczekującej płatności sprawdź stawkę, ważność, konflikty i rzeczywistą możliwość RBF. Zmiana polityki lub odbiorcy wymaga właściwych nowych podpisów. Lokalne anulowanie nie niszczy podpisu ani transakcji zachowanej przez inną osobę i nie cofa potwierdzenia.

Diagnozuj etapami: przygotowanie, transport, odblokowanie, przegląd, podpis, powrót, weryfikacja, finalizacja, rozesłanie i potwierdzenie. Zapisz system, wersję, model, etap, przybliżoną godzinę i kod błędu. Diagnostyka aplikacji ma pomijać dane wrażliwe, ale sprawdź ją przed udostępnieniem i nie dołączaj kopii, kodów QR, klucza czatu ani danych uwierzytelniających.

Ćwiczenie

1. Uporządkuj stany fikcyjnej płatności i wskaż miejsce na bezpieczną przerwę.
2. Rozwiąż trzy przypadki: niewystarczające saldo, brak odpowiedzi USB i zerwane połączenie podczas publikacji.
3. Napisz zgłoszenie na danych syntetycznych ze sprawdzalnym oczekiwanym wynikiem.

Sprawdź swoje umiejętności

Ustal, czy brakuje działania uczestnika, urządzenia, koordynatora czy sieci. Uniknij zbędnej drugiej płatności.

Częste pytanie

Czy FIRMWARE_CAPABILITY_REQUIRED naprawia się przez zmianę firmware w ciemno? Nie. W opisanym przypadku Desk rozpoznanie kompilacji Final wymagało poprawienia katalogu Desk. Przed modyfikacją urządzeń sprawdź wersję i profil.

Miejsce na przerwę

Zachowaj stan i następny krok. Dokumentację rzeczywistej operacji opublikowanej poza laboratorium przechowuj prywatnie.

Które działanie samo może odwołać już potwierdzoną transakcję?

1. Usunięcie lokalnego szkicu.
2. Zamknięcie Mirror.
3. Żadne z tych działań.

> **Pokaż odpowiedź: Żadne z tych działań.**
> Lokalne usunięcie nie przepisuje łańcucha ani nie wycofuje krążących już autoryzacji.

Co można zaobserwować w Bitcoinie

Cel

Rozpoznawaj dane publiczne, wnioski i dane dodawane poza łańcuchem.

Zrozumienie tematu

Bitcoin on-chain jest publiczny. Można analizować skrypty i odpowiadające im adresy, wartości, związki wejść z wyjściami oraz pozycję w blokach. Twoje nazwisko nie musi być widoczne, lecz zidentyfikowany zakup, opublikowana faktura lub udostępniony adres mogą cię powiązać z tą historią.

Pseudonimowość oznacza używanie identyfikatorów, które same nie stanowią twojej tożsamości cywilnej. Anonimowość wymaga zbioru i warunków nierozróżnialności, których nie daje sama instalacja aplikacji. Prywatność zależy od kontekstu. Sprzedawca zna płatność, giełda może znać wypłatę, serwer widzi zapytania, ktoś może obserwować urządzenia.

Odróżniaj fakty od wniosków. „To wyjście wydano w tej transakcji” można sprawdzić w łańcuchu. „Wszystkie te wejścia należą do jednej osoby” jest zawodną heurystyką. Identyfikacja poza łańcuchem może wzmocnić hipotezę, nie zamieniając każdej interpretacji w pewnik.

Ponowne użycie adresu ułatwia łączenie aktywności. Łączenie UTXO z różnych kontekstów może ujawnić ich związek. Ujawnienie xpub daje szerszy wgląd niż pokazanie jednego adresu. Podanie txid może odsłonić również inne wyjścia i relacje niepotrzebne odbiorcy.

Ćwiczenie

1. Zaznacz w fikcyjnej transakcji dane publiczne i własne etykiety.
2. Dodaj fakturę z nazwiskiem i opisz nowe powiązanie.
3. Napisz zgłoszenie pozwalające rozwiązać błąd bez adresu, deskryptora i salda.

Sprawdź swoje umiejętności

Odróżnij „to widać” od „to wniosek” i wskaż brakujące dowody.

Częste pytanie

Czy nieużywanie adresów ponownie zapewnia anonimowość? Nie. Wybór wejść, reszta, zapytania, kontrahenci i inne metadane nadal mają znaczenie.

Miejsce na przerwę

Zachowaj mapę obserwatorów bez rzeczywistych tożsamości i transakcji.

Co zwykle pozwala obserwować rodzinę adresów konta?

1. Kolor ikony.
2. Xpub tego konta i wystarczający kontekst wyprowadzania.
3. Marka przewodu.

> **Pokaż odpowiedź: Xpub tego konta i wystarczający kontekst wyprowadzania.**
> Rozszerzone dane publiczne są istotne dla prywatności, nawet gdy same nie pozwalają wydawać środków.

M07

Rozdzielanie kontekstów i zarządzanie resztą

Cel

Podejmuj decyzje o wydawaniu zgodnie z pochodzeniem swoich UTXO.

Zrozumienie tematu

Rozdzielanie kontekstów zaczyna się przed płatnością. Ustal, czy wpływ dotyczy oszczędności, pracy, codziennych wydatków lub konkretnej relacji. Zachowaj to w prywatnych etykietach, aby przy przyszłym wyborze nie zatrzeć podziału z niewiedzy.

Etykieta nie rozdziela wyjść kryptograficznie. Wspólne wydanie dwóch UTXO z różnych kontekstów publikuje ich związek. Konsolidacja zmniejsza liczbę wejść przyszłych płatności, ale wzmacnia związek między konsolidowanymi wyjściami. Przy niskich opłatach może być efektywna, a zarazem sprzeczna z celem prywatności.

Reszta to nowe wyjście pod tą samą polityką, nie „niewidzialne pieniądze”. Późniejsze użycie może rozszerzyć wcześniejsze powiązania. Nie uznawaj adresu za resztę z powodu nietypowej kwoty. Przy rzeczywistej weryfikacji urządzenie powinno potwierdzić jego przynależność do portfela.

Unikaj mechanicznych wzorców kwot, czasu i powtarzanych transferów. One również mogą być rozpoznawalne i generować opłaty. Oceń, jakie dane zna każda strona i co nowego opublikuje proponowana transakcja. Żadna sekwencja nie kasuje opublikowanej historii.

Ćwiczenie

1. Utwórz pięć fikcyjnych UTXO z trzech kontekstów i przygotuj płatność używającą minimalnej koniecznej liczby kontekstów.
2. Rozpoznaj powstałą resztę i zdecyduj, jak ją oznaczyć.
3. Porównaj koszt i ujawnienia przy konsolidacji wszystkich wyjść oraz zachowaniu ich osobno.

Sprawdź swoje umiejętności

Uzasadnij konsolidację lub odmowę konkretnym powodem bez stosowania jednej bezwzględnej reguły.

Częste pytanie

Czy przesunięcie wszystkiego na inny własny adres odcina historię? Nie. Publikuje kolejne powiązanie i może zwiększyć koszt bez rozwiązania zagrożenia.

Miejsce na przerwę

Zachowaj rozumowanie z laboratorium i przyjętą politykę wyboru.

Co może spowodować skonsolidowanie pensji i darowizn w jednej transakcji?

1. Ujawnić związek między tymi wejściami.
2. Usunąć ich publiczne pochodzenie.
3. Zamienić je w gwarantowaną anonimową gotówkę.

> **Pokaż odpowiedź: Ujawnić związek między tymi wejściami.**
> Zmniejszenie liczby UTXO może zwiększyć liczbę widocznych powiązań.

M07

Prywatność sieciowa, Tor i VPN

Cel

Odróżniaj prywatność połączenia od prywatności w łańcuchu.

Zrozumienie tematu

Serwer zapytań może łączyć żądania z połączeniem. Dostawca internetu może widzieć cele lub wzorce zależnie od transportu. VPN przenosi część zaufania na operatora VPN. Nie usuwa publicznych danych Bitcoina ani nie powstrzymuje zidentyfikowanego konta przed rozpoznaniem użytkownika.

Tor kieruje ruch przez sieć, aby ograniczyć niektóre związki źródła z celem. Nie czyni adresu Bitcoin prywatnym i nie chroni aplikacji, której ruch omija Tor. Otwarcie Tor Browser nie konfiguruje automatycznie Desk, Bitcoin Core ani wszystkich usług komputera.

Przed stwierdzeniem ochrony sprawdź trasę i konfigurację. W tej wersji nie zakłada się wbudowanego przełącznika Tor w Desk. Wdrożenie z węzłem lub proxy wymaga instrukcji technicznej i sprawdzenia rzeczywistego ruchu. Obecność pola w innym portfelu nie dowodzi istnienia go w Desk.

Wycieki mogą dotyczyć także DNS, synchronizacji kont, linków do eksploratora i usług kursowych. Konfiguracja może chronić zapytania o saldo i jednocześnie ujawnić aktywność po otwarciu publicznego eksploratora. Określ zakres ochrony i zachowanie po awarii. Unikaj cichego przełączania na mniej prywatnego dostawcę.

Ćwiczenie

1. Narysuj trasę od komputera przez dostawcę łącza, ewentualne proxy i węzeł lub usługę do sieci Bitcoin.
2. Wskaż, kto otrzymuje zapytania, a kto zna twoją tożsamość z relacji handlowej.
3. Zasymuluj brak odpowiedzi prywatnego węzła. Wybierz pauzę lub wyraźną zmianę źródła ze świadomością ujawnienia danych.

Sprawdź swoje umiejętności

Wyjaśnij, które zagrożenie ogranicza konfiguracja i które nadal występuje.

Częste pytanie

Czy Tor gwarantuje, że nikt nie połączy ze mną płatności? Nie. Nadal mogą to umożliwić kontrahenci, identyfikacja handlowa, wzorce i błędy operacyjne.

Miejsce na przerwę

Zapisz zakres rozwiązania bez prywatnych punktów końcowych i haseł.

Czy otwarcie Tor Browser zmusza Desk do wysyłania zapytań przez Tor?

1. Tak, ponieważ działają na tym samym komputerze.
2. Tak, jeśli widoczna jest ikona.
3. Nie. Drogę połączenia każdej aplikacji trzeba skonfigurować i sprawdzić.

> **Pokaż odpowiedź: Nie. Drogę połączenia każdej aplikacji trzeba skonfigurować i sprawdzić.**
> Ochrona jednej aplikacji nie przechodzi automatycznie na pozostałe.

CoinJoin, Payjoin i ich obecne ograniczenia

Cel

Poznaj techniki współpracy bez przypisywania im anonimowości czy zgodności, których nie zapewniają.

Zrozumienie tematu

CoinJoin łączy wkłady kilku osób w jednej transakcji, utrudniając niektóre wnioski dotyczące wejść i wyjść. Nie jest to przekazanie monet powiernikowi obiecującemu zwrócić inne. Zależnie od konstrukcji oceń koordynację, pieczę, opłaty, odporność na złośliwych uczestników i dalsze postępowanie.

Payjoin włącza wejścia płatnika i odbiorcy do wspólnej płatności, osłabiając część heurystyk o wspólnej własności. Wymaga obsługi obu stron i określonego protokołu. Jest to wiedza techniczna. Sprawdzone źródła nie potwierdzają zintegrowanej i działającej ścieżki Payjoin lub CoinJoin w Cuvex Desk.

Dostępność i kontekst prawny się zmieniają. Dokumentacja Wasabi odnotowuje zamknięcie koordynatora zkSNACKs 1 czerwca 2024 roku. Dawny przycisk nie gwarantuje obecnej usługi. W 2025 roku amerykański Departament Sprawiedliwości poinformował o przyznaniu się do winy i późniejszych wyrokach wobec założycieli Samourai. Nie dowodzi to nielegalności każdej techniki prywatności w każdej jurysdykcji.

Narzędzie może osłabić jeden wniosek, pozostawiając inne. Zidentyfikowane pochodzenie nie znika z zapisków kontrahenta. Późniejsze łączenie wyjść, metadane i błędy grupy uczestników mogą pogorszyć prywatność. Niektóre usługi stosują odmienne zasady handlowe do monet o określonej historii.

Ćwiczenie

1. Porównaj zwykłą transakcję, transakcję wspólną i usługę przejmującą pieczę bez rzeczywistych operacji.
2. Przed zaproponowaniem narzędzia ustal wersję, opiekuna, stan usługi i aktualną dokumentację.
3. Oddziel zagrożenia techniczne, powiernicze i prawne. Tutor nie powinien projektować obchodzenia kontroli ani obiecywać „środków niemożliwych do wyśledzenia”.

Sprawdź swoje umiejętności

Wyjaśnij jedną ograniczoną zaletę i co najmniej dwa ryzyka lub wymagania techniki prywatności.

Częste pytanie

Czy Cuvex wymaga miksera do prywatnego przechowywania? Nie. Kontrola zapytań, danych, kluczy i wyboru UTXO ogranicza konkretne ryzyka bez obietnicy pełnego ukrycia.

Miejsce na przerwę

Bez dowodu zgodności oznacz narzędzie jako „przeanalizowane”, nie „obsługiwane”.

Które stwierdzenie jest uzasadnione?

1. CoinJoin gwarantuje trwałą anonimowość.
2. Technika współpracy może utrudnić wyciąganie niektórych wniosków, ale ma wymagania i ograniczenia.
3. Każda usługa nazywana mikserem zachowuje samodzielną kontrolę nad środkami.

> **Pokaż odpowiedź: Technika współpracy może utrudnić wyciąganie niektórych wniosków, ale ma wymagania i ograniczenia.**
> Właściwości zależą od protokołu, implementacji, uczestników i późniejszego użycia.

Wnioski z rzeczywistych incydentów

Cel

Przełóż udokumentowane incydenty na sprawdzalne decyzje bez atakowania konkurencji i wyolbrzymiania ochrony.

Zrozumienie tematu

Mt. Gox: akt oskarżenia amerykańskiego Departamentu Sprawiedliwości z 2023 roku opisuje nieuprawniony dostęp do serwerów i kluczy, a następnie zniknięcie środków klientów. Akt oskarżenia przedstawia zarzuty, nie wyrok. Przy przechowywaniu pytaj, kto faktycznie kontroluje klucze i co się stanie po upadku firmy.

Ledger Connect Kit, grudzień 2023: Ledger udokumentował złośliwe wydanie biblioteki używanej przez zdecentralizowane aplikacje po przejęciu dostępu byłego pracownika. Incydent dotknął łańcucha dystrybucji oprogramowania i podstępnie skłonił użytkowników aplikacji EVM do podpisania. Nie dowodzi złamania sprzętu Ledger ani konsensusu Bitcoina.

Bybit, luty 2025: FBI przypisało Korei Północnej kradzież aktywów wirtualnych o wartości około 1 500 mln dolarów. Zdarzenie dotyczyło giełdy i aktywów innych sieci. Nie przedstawia się go jako złamania kryptografii Bitcoina. Sprawdzaj intencję podpisu i unikaj sytuacji, w której wiele osób ślepo ufa temu samemu ekranowi.

Coinbase, maj 2025: firma poinformowała o kradzieży danych przez przekupionych pracowników wsparcia w celu ułatwienia socjotechniki. Według jej oświadczenia nie ujawniono haseł ani kluczy prywatnych. Oszust może znać prawdziwe informacje i nadal być oszustem.

Bitcoin Core również publikuje informacje o błędach. Komunikat CVE-2024-35202 opisał możliwość zdalnego zatrzymania programu w wersjach sprzed 25.0. Weryfikacja reguł nie usuwa potrzeby utrzymywania oprogramowania. Z komunikatu nie wynika kradzież kluczy.

W styczniu 2026 roku The Register opisał ujawnienie przez Global-e danych zamówień i danych kontaktowych klientów Ledger. Potwierdzenia przypisano obu firmom. Według tych oświadczeń klucze odzyskiwania nie zostały naruszone. Zakup może ujawnić posiadanie urządzenia mimo braku naruszenia sprzętu.

W kwietniu 2026 roku The Record poinformował o ataku na Drift i ogłoszonym przez platformę zawieszeniu wpłat i wypłat. To protokół zdecentralizowanych finansów na Solanie, nie złamanie Bitcoina. Początkowych szacunków strat i późniejszego odzyskiwania nie należy przedstawiać jako ostatecznej liczby ani gwarantowanego zwrotu.

Ćwiczenie

1. Sklasyfikuj przypadki według pieczy, interfejsu lub dystrybucji, danych osobowych, protokołów innych sieci i dostępności.
2. Dla każdego podaj jedną metodę zapobiegania i jej ograniczenie.
3. Przećwicz oszukańczy telefon: „Znam twój zakup, przenieś środki na ten bezpieczny adres”. Rozłącz się i sprawdź samodzielnie rozpoczętym kontaktem.

Sprawdź swoje umiejętności

Wyjaśnij, dlaczego żaden incydent nie dowodzi niezawodności innej marki. Dowody dotyczą określonego zakresu.

Częste pytanie

Czy to wszystkie najnowsze włamania? Nie. To wybrane przypadki zweryfikowane na potrzeby wydania z 17 listopada 2026 roku, nie wyczerpujący wykaz ani monitoring bieżący.

Miejsce na przerwę

Zapisz nawyk, który zmienisz, i sposób sprawdzania, czy go przestrzegasz.

Rozmówca zna twój zakup i prosi o przelew na „portfel ratunkowy”. Czego dowodzi znajomość zakupu?

1. Informacja mogła wyciec. Nie uwierzytelnia osoby ani adresu.
2. To z pewnością prawdziwe wsparcie.
3. Należy podać frazę seed.

> **Pokaż odpowiedź: Informacja mogła wyciec. Nie uwierzytelnia osoby ani adresu.**
> Prawdziwe dane można wykorzystać do zbudowania przekonującego oszustwa.

M08

Tworzenie tożsamości i sprawdzanie kontaktów na czacie

Cel

Aktywuj tożsamość czatu bez ujawniania jej klucza i sprawdź drugą stronę.

Zrozumienie tematu

W Desk czat łączy się z kryptogramem kluczem czatu generowanym w Cuvex. Może on wyglądać jak xpub, ale jest tajny. Nie traktuj go jak publicznego klucza konta WOW. Tutor nie potrzebuje go czytać ani widzieć w kodzie QR.

Procedura odróżnia nowy alias od przeniesienia lub odzyskania istniejącego. W sprawdzonej implementacji wybiera się właściwy profil mobilny iOS lub Android. Historycznie wyprowadzone tożsamości nie są dowolnie zamienne. DEV i środowisko produkcyjne są niezależne. Zmiana środowiska nie przenosi automatycznie rozmów ani aliasów.

Dodanie aliasu nie weryfikuje tożsamości. Sprawdź odcisk niezależnym uwierzytelnionym kanałem. Jeśli aplikacja oferuje pytania rozpoznawcze, użyj informacji niepublicznych i unikaj odpowiedzi ujawniających hasła. Znajomy głos można naśladować. W sytuacjach ryzyka łącz wcześniej uzgodnione metody.

Gdy tożsamość kontaktu się zmieni, wstrzymaj płatności i koordynację do wyjaśnienia. Może to być prawidłowe odzyskanie lub złośliwa podmiana. Szyfrowanie od końca do końca chroni kanał zgodnie z protokołem i implementacją, lecz nie dowodzi, kto używa urządzenia po drugiej stronie.

Ćwiczenie

1. W środowisku testowym objaśnij utworzenie lub odzyskanie bez ujawniania klucza czatu.
2. Dodaj kontakt laboratoryjny i ustal innym kanałem porównanie odcisków.
3. Zasymuluj zmianę tożsamości. Określ sposób jej potwierdzenia przed płatnością.

Sprawdź swoje umiejętności

Odróżnij alias, publiczny odcisk, tajny klucz czatu i osobiste zaufanie do człowieka.

Częste pytanie

Czy stary alias gwarantuje tę samą osobę? Nie. Ciągłość i zmiany kluczy trzeba zweryfikować właściwą procedurą.

Miejsce na przerwę

Zapisz jedynie „zweryfikowany kontakt testowy” i metodę, bez kluczy i prywatnych pytań.

Ciąg znaków nazywa się kluczem czatu i przypomina xpub. Jak traktować go w Desk?

1. Jako dane do publikowania na forach.
2. Jako sekret do odzyskania tożsamości.
3. Jako adres odbiorczy Bitcoin.

> **Pokaż odpowiedź: Jako sekret do odzyskania tożsamości.**
> Wygląd nie rozstrzyga o poufności ani przeznaczeniu danych.

M08

Żądanie i płacenie satoshi z czatu

Cel

Przejdź od rozmowy do płatności, zachowując weryfikację i kontekst.

Zrozumienie tematu

Czat pozwala poprosić o adres, odpowiedzieć adresem odbiorczym, zażądać płatności i otworzyć jej przygotowanie z konta WOW. Zachowanie kontekstu zmniejsza ryzyko błędu przy kopiowaniu między aplikacjami, ale nie zamienia każdej wiadomości w uwierzytelnione polecenie wydania.

Przed odpowiedzią lub zapłatą sprawdź zweryfikowany kontakt, sieć, kwotę i pierwotne żądanie. Wspólny formularz zachowuje wybór UTXO i opłatę. Po wybraniu „Wyślij wszystko” kwota netto po opłatach może być niższa od żądanej. Gdy ma to zastosowanie, wyraźnie oznacz płatność częściową.

Autoryzacja pozostaje w Cuvex. Czat przenosi intencję i ustalenia, bez możliwości automatycznego podpisu. Komunikat płatniczy wysłany kontaktowi musi odróżniać otrzymaną wiadomość od istnienia potwierdzonej transakcji. Odbiorca sprawdza to własnym kontem lub źródłem.

Linki zewnętrzne, załączone QR i adresy są niezaufane do czasu weryfikacji. „Pokaż w Mempool” może otworzyć zewnętrzną usługę i ujawnić zapytanie. Jeśli polityka wymaga własnego węzła, wybierz zgodną weryfikację w WOW i oceń każde przejście do publicznego serwisu.

Ćwiczenie

1. Odegraj dwie role: odbiorca prosi o 50 000 sat, płatnik przygotowuje przelew bez publikacji.
2. Zasymuluj dostępne saldo netto 48 000 sat. Wyjaśnij, jakich zgód i uzgodnień brakuje przy częściowej płatności.
3. Celowo zmień sieć w testowej wiadomości i zatrzymaj proces.

Sprawdź swoje umiejętności

Prześledź związek żądania, adresu, szkicu, podpisu i potwierdzenia bez sprowadzania go do „czat mówi OK”.

Częste pytanie

Czy wysyłanie satoshi z czatu oznacza użycie Lightning? Nie. Opisany proces WOW przygotowuje płatności Bitcoin w łańcuchu. Satoshi oznacza jednostkę, nie sieć transportową.

Miejsce na przerwę

Anuluj szkic laboratoryjny lub zapisz stan. Nie publikuj tylko dla demonstracji interfejsu.

Dostajesz potwierdzenie na czacie. Co rozstrzyga o otrzymaniu środków?

1. Zielony kolor ikony wiadomości.
2. Słowo „potwierdzono” od rozmówcy.
3. Sprawdzenie transakcji i jej wyjść w sieci za pomocą właściwego źródła.

> **Pokaż odpowiedź: Sprawdzenie transakcji i jej wyjść w sieci za pomocą właściwego źródła.**
> Stan wiadomości i stan transakcji nie są równoważne.

Świadome udostępnianie kryptogramów

Cel

Zrozum skutki przekazania zaszyfrowanej kopii innej osobie.

Zrozumienie tematu

Udostępnienie kryptogramu przekazuje kopię zaszyfrowanego obiektu. Nie musi wysyłać bitcoinów i samo nie dodaje podpisującego. Jeśli odbiorca otrzyma też wystarczające środki odblokowania, może uzyskać dostęp według schematu. Wcześniej ustal, jaką możliwość przekazujesz.

Szyfrowanie czatu od końca do końca i szyfrowanie pliku chronią inne warstwy. Po pobraniu odbiorca może zachować obiekt poza czatem. Usunięcie twojej wiadomości lub lokalnego wpisu nie gwarantuje wycofania wszystkich kopii. Podanie hasła tym samym kanałem może skupić składniki w jednej drodze.

Przed wysłaniem zweryfikuj tożsamość, format i cel. Powiązanie otrzymanego kryptogramu organizuje kopię, ale nie dowodzi bezpieczeństwa odszyfrowania dowolnego pliku. Nie używaj załączników wymagających wpisania frazy lub hasła na zewnętrznej stronie.

Odzyskanie wymaga ustaleń: kto zachowuje każdy składnik, kto może go otworzyć, jak wykryć ujawnienie i jak zmienić pieczę po ustaniu relacji. Do zwykłej płatności zazwyczaj wystarcza sprawdzony adres. Kryptogramu nie trzeba udostępniać.

Ćwiczenie

1. Zaprojektuj przekazanie zaszyfrowanego tekstu ćwiczeniowego kontaktowi laboratoryjnemu.
2. Wymień, co odbiorca wie i może zrobić przed poznaniem hasła i po nim.
3. Zasymuluj zakończenie relacji. Wyjaśnij, dlaczego usunięcie wiadomości nie unieważnia kopii ani kluczy.

Sprawdź swoje umiejętności

Odróżnij „udostępniono dane”, „udostępniono dostęp do sekretu” i „podpisano wydatek”.

Częste pytanie

Czy zaszyfrowany plik może krążyć bez konsekwencji? Może ujawniać metadane, umożliwiać próby odgadnięcia hasła i pozostać zachowany bezterminowo. Oceń konieczność udostępnienia.

Miejsce na przerwę

Nie zostawiaj załączników związanych z pieczą w kursie. Zapisz jedynie wniosek z ćwiczenia.

Czy wysłanie kryptogramu na czacie jest równoznaczne z wysłaniem bitcoinów?

1. Nie. Przekazuje obiekt, którego zawartość i dostęp mają inne znaczenie.
2. Tak, jeśli plik ma rozszerzenie .bin.
3. Automatycznie aktywuje nowy wielopodpis.

> **Pokaż odpowiedź: Nie. Przekazuje obiekt, którego zawartość i dostęp mają inne znaczenie.**
> Przenoszenie sekretów i wydawanie UTXO to inne operacje.

Odzyskiwanie czatu i rozumienie jego metadanych

Cel

Zaplanuj zmianę urządzenia i odróżnij odzyskanie tożsamości od odzyskania wiadomości.

Zrozumienie tematu

Desk podaje, że historia i sesje są lokalnie szyfrowane i nie należą do jego pełnej kopii. Klucz czatu pozwala odzyskać tożsamość, ale nie gwarantuje odzyskania dawnych rozmów. Aplikacja ma stany i działania dla oczekującej aktywacji, utrzymania kluczy i lokalnego odzyskiwania, kiedy istnieje zgodny materiał.

Według sprawdzonej instrukcji każdego aliasu należy używać na jednym urządzeniu jednocześnie. Nie aktywuj go naraz na dwóch dla „testu synchronizacji”, jeśli takie użycie nie jest obsługiwane. Przeniesienie wymaga właściwej procedury i potwierdzenia ciągłości z kontaktami.

„Oczekuje”, „przyjęto przez serwer”, „odebrano” i „nie udało się odszyfrować” opisują różne etapy. Nie ponawiaj w ciemno niepotwierdzonej wysyłki. Najpierw ustal, czy dotarła. Przy braku klucza sesji lub zmianie tożsamości zachowana oczekująca wiadomość nie jest jeszcze odczytana.

Zaszyfrowana treść nie musi ukrywać przed wszystkimi systemami czasu, rozmiaru, relacji doręczenia, aliasów ani danych połączenia. Podobnie szyfrowanie transportu nie sprawia, że zwykła rozmowa głosowa nadaje się do podawania sekretów. Do nauki i rozwiązywania problemów używaj minimalnych potrzebnych danych.

Ćwiczenie

1. Zasymuluj utratę komputera i wyjaśnij, co pozwala odtworzyć każdy dostępny materiał.
2. Sklasyfikuj stany wiadomości i zdecyduj, kiedy nie ponawiać żądania płatności.
3. Przygotuj zawiadomienie o zmianie urządzenia, które kontakty mogą sprawdzić niezależnym kanałem.

Sprawdź swoje umiejętności

Wyjaśnij, która rozmowa przepadnie, a jaką tożsamość można odtworzyć. Nie obiecuj odzyskania rzeczy nieobjętych kopią.

Częste pytanie

Czy usunięcie lokalnego czatu kasuje wiadomości po drugiej stronie? Nie zakładaj tego. Odbiorca może niezależnie zachować wiadomości i pliki.

Miejsce na przerwę

Zachowaj plan przeniesienia z nazwami pustych pól, bez klucza czatu.

Co sam klucz czatu gwarantuje według sprawdzonej instrukcji?

1. Wszystkie dawne rozmowy na dowolnym komputerze.
2. Odzyskanie tożsamości właściwą procedurą, ale nie wszystkich dawnych wiadomości.
3. Automatyczny dostęp do kluczy Bitcoin kontaktów.

> **Pokaż odpowiedź: Odzyskanie tożsamości właściwą procedurą, ale nie wszystkich dawnych wiadomości.**
> Tożsamość i archiwum historyczne to odrębne możliwości.

Codzienne ustawienia i przegląd uprawnień

Cel

Kontroluj parametry Desk, odróżniając wygodę od ochrony.

Zrozumienie tematu

Desk oferuje motyw nocny, dzienny lub systemowy, automatyczną synchronizację co 3 lub 5 minut, dźwięki transakcji, tło czatu, język i walutę odniesienia. Ustawienia zmieniają wygląd lub częstość zapytań. Nie zmieniają podpisu Bitcoin ani nie dodają anonimowości.

Sprawdzona konfiguracja bezpieczeństwa pozwala ustawić blokadę po bezczynności i przejściu w tło, maksymalne opóźnienie po błędach i opcjonalne kasowanie. Schemat bezczynności dopuszcza od 30 do 86 400 sekund. Interfejs może pokazywać węższy wybór. Odczytaj wartości domyślne w swojej wersji zamiast zakładać je na podstawie nagranej lekcji.

Obsługa odnośników bitcoin: otwiera żądanie odblokowania, wyboru konta i weryfikacji. Nie autoryzuje automatycznej płatności. W Linuksie instrukcja odróżnia rejestrację linków dla instalacji zintegrowanej i AppImage. Faktura Lightning wymaga osobnej zgodnej ścieżki. Ustanowienie Desk aplikacją domyślną nie wystarcza.

Notowanie, wykres i linki informacyjne mogą odpytywać zewnętrzne usługi. Informują, a nie wskazują momentu zakupu. Sprawdź datę i źródło przed przeliczeniem kwot. Ciemny motyw lub małe okno nie powinny zasłaniać końcowych przycisków, adresu ani opłaty. Jeśli tak jest, przerwij i zgłoś problem z układem.

Ćwiczenie

1. Dopasuj wygląd i blokadę w magazynie ćwiczeniowym. Sprawdź, czy możesz ponownie wejść.
2. Sprawdź włączane automatyzacje. Synchronizacja, dźwięki i kontrola firmware to różne funkcje.
3. Otwórz fikcyjne żądanie z odnośnika bitcoin: i anuluj przed przygotowaniem rzeczywistej operacji.

Sprawdź swoje umiejętności

Wyjaśnij skutki ustawień i wskaż te, które powodują zapytania lub działania wrażliwe.

Częste pytanie

Czy biometria komputera zastępuje kopię odzyskiwania? Nie. Może zależeć od sprzętu i bezpiecznego magazynu systemu. Zachowaj niezależną metodę odzyskania.

Miejsce na przerwę

Zablokuj Desk i zapisz tylko zmienione preferencje.

Co zmienia wybór synchronizacji co trzy minuty?

1. Planowaną częstość zapytań, gdy funkcja jest uruchomiona.
2. Politykę podpisów w łańcuchu.
3. Frazę seed urządzenia.

> **Pokaż odpowiedź: Planowaną częstość zapytań, gdy funkcja jest uruchomiona.**
> To ustawienie działania, nie zmiana sposobu pieczy nad środkami.

Projektowanie portfela wielopodpisowego

Cel

Dobierz próg odporny na prawdopodobne utraty i naruszenia kluczy.

Zrozumienie tematu

W polityce M z N liczba N oznacza uczestników z odrębnymi kluczami, a M wymaganą liczbę podpisów. Schemat 2 z 3 toleruje niedostępność jednego klucza. Przejęcie dwóch kluczy może jednak umożliwić wydatek. Jeśli trzy frazy znajdują się w jednym miejscu lub wynikają z tego samego ujawnienia, niezależność maleje.

Sprawdzony profil wielopodpisowy Cuvex używa natywnego P2WSH z sortedmulti i wyprowadzaniem BIP48. Struktura Original obsługuje do sześciu kluczy polityki, a BIT do piętnastu. Przy obu modelach obowiązują ograniczenia słabszego uczestnika i rzeczywisty rozmiar nośnika. Maksimum struktury nie gwarantuje zmieszczenia polityki z wieloma kluczami i wejściami.

Aplikacja obsługuje progi zgodne z zależnościami polityki, ale 1 z N nie wymaga współpracy przy wydaniu. Firmware zachowuje osobne ostrzeżenia o tym ryzyku. Większa liczba zwiększa także koordynację, koszty, ilość materiału odzyskiwania i możliwość blokady.

MuSig2 to odrębny schemat agregacji podpisów Schnorra, sam w sobie N z N, a nie dowolne 3 z 5. Badane wersje Final nie implementują podpisywania wejść Taproot, MuSig2 ani Miniscript. Obsługa odbiorcy P2TR nie dowodzi możliwości podpisywania z portfela Taproot.

Ćwiczenie

1. Zaprojektuj fikcyjną politykę 2 z 3 z niezależnymi zagrożeniami dla uczestników.
2. Zasymuluj utratę jednego klucza i przejęcie jednego klucza. Wyjaśnij, co można, a czego nie można zrobić.
3. Przed wyborem większej polityki sprawdź limity modeli.

Sprawdź swoje umiejętności

Określ tolerancję utraty, próg ataku i wspólne zależności projektu.

Częste pytanie

Czy wielopodpis wymaga wzajemnej znajomości fraz seed? Nie. Każdy zachowuje prywatną zdolność podpisu. Udostępnia się publiczne dane potrzebne do zbudowania i odzyskania polityki.

Miejsce na przerwę

Zachowaj projekt z fikcyjnymi uczestnikami i ich odpowiedzialnością.

W schemacie 2 z 3 z niezależnymi kluczami ile kluczy prywatnych wystarcza do autoryzacji prawidłowego wydatku według tej polityki?

1. Jeden.
2. Dwa.
3. Zawsze wszystkie trzy.

> **Pokaż odpowiedź: Dwa.**
> Próg wymaga dwóch. Trzeba też spełnić pozostałe warunki i przejść weryfikację.

Tworzenie zaproszeń i dodawanie kluczy

Cel

Zbuduj politykę ze sprawdzonymi uczestnikami bez udostępniania fraz seed.

Zrozumienie tematu

Twórca wybiera nazwę, sieć, M, N, kontakty, własne dane publiczne i operacyjne warunki zaproszenia. Sprawdzony schemat obsługuje mainnet i regtest, od 2 do 15 uczestników przed uwzględnieniem limitów urządzeń oraz ważność od 1 do 720 godzin. Zakresy nie uprawniają do pominięcia kontroli możliwości.

Każdy sprawdza zaproszenie, przyjmuje je lub odrzuca i przekazuje obsługiwaną ścieżką własny rozszerzony klucz publiczny z odciskiem i ścieżką BIP48. Nie przekazuje frazy seed, klucza prywatnego, pojedynczego adresu ani całego deskryptora innego portfela. Klucz w błędnym kontekście może dać inną politykę, nawet gdy wygląda jak prawidłowy xpub.

Twórca koordynuje, ale każdy podpisujący musi sam sprawdzić dane. Przed wpłatą wszyscy powinni umieć odtworzyć i zweryfikować te same parametry i adres kontrolny. Zaakceptowany kontakt na czacie nie oznacza automatycznej zgody na każdą przysłaną politykę.

Wygaśnięcie zaproszenia to reguła koordynacyjna aplikacji. Nie zmienia istniejącego skryptu ze środkami, nie kasuje podpisów zachowanych przez innych i nie działa jak blokada czasowa konsensusu. Anulowanie propozycji i wypłata środków z istniejącej polityki to inne działania.

Ćwiczenie

1. W przygotowanym laboratorium regtest utwórz propozycję 2 z 3 z testowymi kontaktami.
2. Odegraj akceptację, odmowę i wkład z niewłaściwą siecią. Sprawdź zatrzymanie ostatniego.
3. Wymień dane do zachowania przed wpłatą: sieć, próg, klucze publiczne, pochodzenie, skrypt i sprawdzony adres.

Sprawdź swoje umiejętności

Rozpoznaj niepełne zaproszenie i wyjaśnij, jakiej zgody brakuje. Sam czat jej nie poświadcza.

Częste pytanie

Czy data wygaśnięcia uniemożliwia późniejsze wydanie? Nie jako pole zaproszenia. Ograniczenie czasowe Bitcoina wymaga określonych warunków skryptu lub transakcji i rzeczywistej obsługi.

Miejsce na przerwę

Zachowaj szkoleniowy identyfikator propozycji i informację o oczekującym zatwierdzeniu.

Czego wymaga opisana procedura, aby wnieść swój udział do wielopodpisu?

1. Fraz seed wszystkich uczestników.
2. Dowolnego adresu odbiorczego.
3. Twojego rozszerzonego klucza publicznego ze zgodnym odciskiem i pochodzeniem BIP48.

> **Pokaż odpowiedź: Twojego rozszerzonego klucza publicznego ze zgodnym odciskiem i pochodzeniem BIP48.**
> Poprawny materiał publiczny pozwala zbudować politykę bez ujawniania kluczy prywatnych.

Sprawdzanie polityk w Mirror w dowolnej kolejności

Cel

Porównuj całe pola i określ dokładnie, co poświadcza wynik.

Zrozumienie tematu

Niezależna weryfikacja pokazuje próg, sieć, profil, SIGHASH, identyfikator polityki, pierwszy adres, pozycję użytkownika i dane każdego uczestnika. Sprawdza intencję i spójność. Nie zakłada trwałej rejestracji polityki w urządzeniu. Udokumentowany zakres dotyczy „tego sprawdzenia”.

W Mirror 12.12 można jako pierwszy odczytać QR z Cuvex lub z Desk i wybrać dowolne dane. Nie trzeba zaczynać od kroku 1, skanować wszystkich ani przestrzegać kolejności. Jeśli sprawdzisz tekst ręcznie, pominięcie skanu nie oznaczy go jako sprawdzonego przez Mirror.

Porównywarka pokazuje pełny dosłowny tekst. Liczą się spacje, nowe wiersze, wielkość liter i różnice Unicode. „Zgodne” oznacza tylko równość dwóch wartości z pary. Nie uwierzytelnia źródła, nie dowodzi przynależności do jednej polityki i nie aktywuje portfela. Końcowa zgoda i skojarzona odpowiedź nadal przechodzą przez Cuvex i Desk.

Obecne kody QR Desk zawierają tylko wartość, bez numeru i sesji. Mirror nie zawsze rozpozna krok. „Podaj krok Desk” dodaje ręcznie wprowadzony kontekst i musi to być widoczne. Dla N uczestników mapa ma 7 + 4N pól: 8+4k odcisk, 9+4k ścieżka, 10+4k xpub i 11+4k identyfikator klucza, gdzie k zaczyna się od zera. Dla N=2 krok 15 to identyfikator drugiego klucza i od niego można zacząć.

Ćwiczenie

1. Na syntetycznych danych porównaj najpierw identyfikator oznaczony jako krok 15, potem sieć i próg.
2. Wprowadź różnicę jednego znaku. Sprawdź „Niezgodne” i zacznij nową parę bez przenoszenia wyniku.
3. Porównaj „2 / 3” i wyjaśnij, dlaczego sam tekst nie zawsze rozróżnia próg i pozycję użytkownika.

Sprawdź swoje umiejętności

Opisz sprawdzone pole, sposób ustalenia kontekstu i pozostałe zgody. Częściowa zgodność nie stanowi akceptacji całości.

Częste pytanie

Czy muszę zeskanować wszystkie QR, aby uczyć się dalej? Nie. Porównywanie jest dowolne. Obowiązkowe kontrole i zatwierdzenia podpisującego mają osobny przebieg.

Miejsce na przerwę

Zamknij porównywarkę. Według sprawdzonego projektu wartości powinny się usuwać po wyjściu lub przejściu w tło.

Mirror porównuje dwa kody QR z kroku 15 i pokazuje „Zgodne”. Co to potwierdza?

1. Dosłowną zgodność tej pary w rozpoznanym lub podanym kontekście.
2. Zatwierdzenie całej polityki.
3. Uwierzytelnienie źródeł obu kodów QR.

> **Pokaż odpowiedź: Dosłowną zgodność tej pary w rozpoznanym lub podanym kontekście.**
> Porównanie nie zastępuje uwierzytelnienia, pełnego przeglądu ani odpowiedzi urządzenia.

Koordynacja podpisów i publikacja transakcji wielopodpisowej

Cel

Doprowadź propozycję do progu podpisów, zachowując intencję płatności i kontrolę.

Zrozumienie tematu

Operacja wielopodpisowa określa wejścia, odbiorców, kwoty, stawkę, zastępowanie i uwagi operacyjne. Twórca może poprosić zgodnych uczestników o podpisy. Każdy przed zatwierdzeniem na urządzeniu samodzielnie sprawdza sieć, politykę, wejścia, wszystkie wyjścia i opłatę.

Częściowy podpis sam nie przesuwa środków, gdy nie osiągnięto progu. Po osiągnięciu koordynator może połączyć podpisy i sfinalizować według procedury. Raporty innych uczestników lub koordynatora służą koordynacji i nie stanowią twojej lokalnej weryfikacji. Aplikacja musi rozróżniać ich pochodzenie.

Sprawdzona wersja obsługuje ponowienie, odbiór podpisu, potwierdzenie, odmowę i przekazanie koordynacji. Przekazanie nie zmienia kluczy ani progu w łańcuchu. Zapisana odpowiedź musi odpowiadać żądaniu i rzeczywiście użytemu profilowi. Nie wybieraj podobnej polityki ani pierwszej pozycji katalogu.

Jeśli ktoś zmieni odbiorców lub istotne warunki, sprawdź nową propozycję i uzyskaj odpowiednie podpisy. Nie „naprawiaj” PSBT, ręcznie usuwając dane bezpieczeństwa, aby zmieściła się na NFC. Firmware wymaga zgodnego profilu i weryfikacji z limitami wejść, wyjść i rozmiaru.

Przed publikacją sprawdź zgodność z ustaleniami i brak już rozesłanej wersji. Następnie obserwuj potwierdzenia wybranym źródłem. Odmowa w twojej aplikacji nie unieważnia automatycznie zapisanych przez innych podpisów i nie blokuje działań dopuszczalnych przy pozostałym progu.

Ćwiczenie

1. Odegraj 2 z 3 z trzema fikcyjnymi rolami. Jedna podpisuje, druga odmawia, trzecia prosi o wyjaśnienie.
2. Zmień adres płatności testowej i wyjaśnij, dlaczego wcześniejsza ustna zgoda nie wystarcza.

3. Zasymuluj błąd potwierdzenia po zapisaniu podpisu. Wznów tę samą pracę bez powielenia płatności i zmiany profilu.

Sprawdź swoje umiejętności

Wskaż koordynatora, podpisujących, osobę finalizującą i dowód każdego etapu.

Częste pytanie

Czy dwa „OK” na czacie to dwa podpisy? Nie. Próg spełniają ważne upoważnienia kryptograficzne zgodne z polityką, nie wiadomości.

Miejsce na przerwę

Zapisz stan, brakujące podpisy i następną osobę odpowiedzialną bez prywatnej treści.

Operacja 2 z 3 ma jeden ważny podpis i dwie wiadomości „zgadzam się”. Czy próg został osiągnięty?

1. Tak, ponieważ uczestniczą trzy osoby.
2. Nie. Brakuje jeszcze jednego ważnego podpisu kryptograficznego.
3. Tak, jeśli koordynator to ogłosi.

> **Pokaż odpowiedź: Nie. Brakuje jeszcze jednego ważnego podpisu kryptograficznego.**
> Zgoda w rozmowie i ważny podpis to różne dowody.

M09

Odtwarzanie i zmiana wielopodpisu

Cel

Odtwórz politykę i zaplanuj utratę lub wymianę uczestników.

Zrozumienie tematu

Odzyskanie wymaga danych odtwarzających politykę i wystarczających prywatnych możliwości wydania. Kopia polityki z xpub może ujawnić historię bez fraz seed. Zaszyfrowana kopia zabezpiecza plik, lecz wymaga zachowania hasła. Rozszerzenie .cuvexms samo nie dowodzi szyfrowania. Sprawdź format i konkretny eksport.

W Desk 9.21 odzyskiwanie wymaga rozszerzonego klucza publicznego uczestnika z odciskiem i ścieżką BIP48, wyeksportowanego z jego urządzenia. Obsługiwana procedura pozwala na odczyt kamerą internetową lub przez Mirror. Nie zastępuj wkładu adresem odbiorczym i nie przesyłaj frazy wsparciu.

Po utracie jednego klucza w 2 z 3 dwa pozostałe mogą nadal umożliwiać wydanie. Stara polityka pozostaje taka sama. Aby skutecznie usunąć uczestnika i ustanowić inne klucze, zwykle tworzy się nową politykę i przenosi środki z wymaganymi upoważnieniami. Zmiana aliasu lub skasowanie portfela z Desk nie zmienia istniejących UTXO.

Kopie powinny odtwarzać obie gałęzie i umożliwiać odkrycie historii. Zachowaj indeksy, wystawione żądania i niezbędny kontekst, by nie używać adresów ponownie ani nie wziąć niepełnego skanu za pusty portfel. Odtworzenie i wznowienie operacji musi uwzględniać profil zapisany przy jej tworzeniu.

Ćwiczenie

1. Wyeksportuj i odtwórz politykę laboratoryjną udokumentowaną funkcją. Sprawdź sieć i znany adres.
2. Zasymuluj utratę uczestnika i przygotuj plan wymiany bez rzeczywistych przelewów.
3. Zasymuluj utratę powodującą zejście poniżej progu. Wsparcie ani AI nie wytworzą brakujących podpisów.

Sprawdź swoje umiejętności

Odtwórz scenariusz testowy i odróżnij przywrócenie informacji od zmiany kontroli nad monetami.

Częste pytanie

Czy usunięcie wielopodpisu w Desk wyłącza portfel wszystkim? Nie. Usuwa stan lokalny zgodnie z procedurą. Inne osoby i kopie mogą nadal zachować możliwość działania według polityki.

Miejsce na przerwę

Zachowaj sprawdzoną kopię i prywatny plan. W kursie zapisz tylko wynik.

Chcesz usunąć osobę z polityki, która już kontroluje środki. Czy wystarczy usunąć jej nazwę w Desk?

1. Tak.
2. Tak, jeśli usuniesz również czat.
3. Nie. Trzeba zaplanować nową politykę i, w razie potrzeby, autoryzowane przeniesienie środków.

> **Pokaż odpowiedź: Nie. Trzeba zaplanować nową politykę i, w razie potrzeby, autoryzowane przeniesienie środków.**
> Skrypty istniejących UTXO nie zmieniają się od edycji lokalnych wpisów.

Planowa aktualizacja oprogramowania układowego

Cel

Przygotuj zgodną aktualizację i sprawdź rezultat na urządzeniu.

Zrozumienie tematu

Aktualizacja zmienia zaufane oprogramowanie. Sprawdź model, rewizję sprzętu, wersję, pochodzenie i mechanizm uwierzytelniania producenta. Pełne pobranie ani skrót zgodny ze stroną nie zastępują weryfikacji podpisu i zgodności. Nigdy nie instaluj niepodpisanej aplikacji firmware dla inżyniera jako wydania klienckiego.

Original aktualizuje się w opisanej procedurze przez Bluetooth, a BIT przez USB-C. Mirror ma zgodne ścieżki przygotowania i transportu. Konkretnego zestawu komputer, telefon i urządzenie nie uważa się za działający bez fizycznego odbioru. Historyczny problem aktualizacji Original w Windows wymaga odpowiedniej diagnozy. Stan 99% nie jest powodzeniem.

Przed startem sprawdź odtwarzalne kopie, stabilne zasilanie i brak innych operacji. Przygotuj oficjalny plik lub wcześniej sprawdzoną zgodnie z aplikacją kopię. Rozróżniaj przesyłanie, walidację, instalację, ponowne uruchomienie i sprawdzenie wersji. Pasek postępu nie jest dowodem końcowym.

Po zakończeniu sprawdź wersję na urządzeniu, zapisz datę i wynik. Katalog zgodności Desk nie mierzy zdalnie firmware: firmwareAttestation pozostaje false. Wybranie profilu Final nie potwierdza rzeczywiście zainstalowanych bajtów. Po błędzie zastosuj udokumentowane odzyskiwanie, zachowaj etap i błąd, nie odłączając w ciemno w krytycznym momencie.

Ćwiczenie

1. Sprawdź listę przygotowań bez rozpoczynania rzeczywistej aktualizacji w trakcie ćwiczenia.
2. Uporządkuj stany i wyjaśnij różnicę między „przesłano” i „zainstalowano”.
3. Napisz fikcyjny raport awarii przy 99% z modelem, wersją, systemem, etapem i końcowym komunikatem.

Sprawdź swoje umiejętności

Wskaż prawidłowy plik, drogę przesyłania i końcowe kryterium powodzenia.

Częste pytanie

Czy aktualizować tylko po to, by zniknął błąd Desk? Najpierw ustal przyczynę. Niezgodność katalogu może wymagać poprawienia Desk i zachowania sprawdzonego firmware.

Miejsce na przerwę

Rzeczywistą aktualizację wolno wstrzymać tylko w stanie wyraźnie określonym jako bezpieczny, nie z powodu końca rozmowy.

Co sam określony wprost katalog Desk weryfikuje?

1. Obsługiwane odniesienia do zgodności, bez zdalnego pomiaru zainstalowanego oprogramowania układowego.
2. Fizyczną atestację wszystkich podłączonych urządzeń.
3. Brak podatności.

> **Pokaż odpowiedź: Obsługiwane odniesienia do zgodności, bez zdalnego pomiaru zainstalowanego oprogramowania układowego.**
> Zgodność, podpis, pomiar i odbiór fizyczny to różne dowody.

Utrata, awaria i odzyskiwanie awaryjne

Cel

Dobierz sposób odzyskania do incydentu i zachowaj przydatne dowody.

Zrozumienie tematu

Przy incydencie najpierw sklasyfikuj utratę lub ujawnienie: komputer, urządzenie, karta, plik, hasło, fraza seed, dodatkowe hasło lub polityka. „Nie mogę wejść” nie oznacza automatycznie kradzieży. Przy podejrzeniu naruszenia nie wpisuj dalszych sekretów na podejrzanym sprzęcie.

Utratę urządzenia można czasem rozwiązać zgodnymi nośnikami i danymi odzyskiwania. Utrata komputera może wymagać odtworzenia magazynu Desk i obserwacji portfela. Utrata wszystkich środków odblokowania lub brak liczby kluczy wymaganej przez próg może nie mieć technicznego rozwiązania. Żadna AI nie zagwarantuje odzyskania nieistniejących kluczy.

Desk oferuje lokalne odzyskiwanie w obsługiwanych formatach i eksport odpowiedniego materiału. Odszyfrowanie na komputerze może ujawnić sekret systemowi lub złośliwemu programowi. To wyjątkowa decyzja. Użyj przygotowanego środowiska, zgodnego materiału i planu przeniesienia na nowe klucze przy możliwym ujawnieniu. Nie zrównuj tej operacji ze zwykłą izolacją Cuvex.

Jeśli fraza wyciekła, zmiana hasła Desk jej nie unieważnia. Oceń autoryzowane przeniesienie do nowego portfela i zabezpiecz go z zaufanego urządzenia. Nie publikuj szczegółów pomocnych napastnikowi i nie płać usługom obiecującym odzyskanie w zamian za inną frazę lub oszukańczą zaliczkę.

Ćwiczenie

1. Rozwiąż cztery fikcyjne przypadki: utracony komputer, uszkodzona karta z ważną kopią, zapomniane hasło i ujawniona fraza seed.
2. Dla każdego wskaż potrzebny materiał, ryzyko działania i kryterium odzyskania.
3. Ćwicz tylko na danych szkoleniowych. Nie przesyłaj tutorowi prawdziwych plików awaryjnych.

Sprawdź swoje umiejętności

Wybierz odtwarzanie, ponowną konfigurację obserwacji, przeniesienie kontroli lub zwrócenie się do specjalisty bez obiecywania niemożliwego.

Częste pytanie

Czy zmiana hasła ponownie szyfruje sekrety, które ktoś już widział? Nie. Jawna kopia lub znana fraza pozostaje znana.

Miejsce na przerwę

Zapisz kategorię incydentu i bezpieczny następny krok. Wyłącz rozmowę przed pracą z sekretami.

Twoja fraza seed została opublikowana, ale zmieniasz hasło komputera. Czy napastnik utracił możliwość wydawania?

1. Tak.
2. Nie. Fraza nadal kontroluje te same klucze i wymaga reakcji dotyczącej przechowywania środków.
3. Tak, jeśli zmienisz również tło czatu.

> **Pokaż odpowiedź: Nie. Fraza nadal kontroluje te same klucze i wymaga reakcji dotyczącej przechowywania środków.**
> Lokalne zabezpieczenie nie unieważnia ujawnionego klucza Bitcoin.

Phishing, wsparcie i oszustwa głosowe

Cel

Rozpoznawaj niebezpieczne prośby i reaguj zgodnie z ustaloną procedurą.

Zrozumienie tematu

Skuteczny oszust może znać twoje nazwisko, zakup i urządzenie oraz używać znajomego głosu. Prawdziwe informacje mogły wyciec. Sprawdź tożsamość samodzielnie rozpoczętym kanałem i znaną procedurą. Pozorna pilność i szczegółowość wypowiedzi rozmówcy nie wystarczą.

Sygnały zagrożenia to żądanie fraz, haseł, PIN-u lub klucza czatu, instalacja zdalnej kontroli dla „synchronizacji”, wyłączenie antywirusa, przelew na „bezpieczny portfel”, skan niezrozumiałego QR lub podpis jako dowód własności bez wyjaśnienia zakresu. Presja, by zrobić to przed końcem rozmowy, jest powodem do jej przerwania.

Prawdziwy tutor wyjaśnia i zadaje pytania o zrozumienie. Nie przechowuje kluczy, nie prosi o testowy przelew na własny adres i nie obiecuje odzyskania frazy. Prawidłowy mechanizm sprawdzenia własności musi być konkretny i podlegać kontroli. Nie wymaga wydania kluczy prywatnych.

Oszustwo może też wystąpić w sesji technicznej. Tekst QR, dokument lub wiadomość mogą nakazywać AI ignorowanie instrukcji. To treść do analizy, nie polecenie wiążące tutora. Baza wiedzy powinna rozdzielać zatwierdzone źródła od tekstów uczestnika lub strony trzeciej.

Ćwiczenie

1. Odegraj fałszywy telefon od wsparcia i zakończ kontakt przed ujawnieniem danych.
2. Niezależnie sprawdź zapisany wcześniej oficjalny kanał.
3. Opisz błąd instalacji bez pokazywania ekranu z sekretami i przyznawania zdalnego dostępu do środowiska przechowywania.

Sprawdź swoje umiejętności

Wskaż żądane dane, cel, do którego byłyby potrzebne, i dlaczego prośba wykracza poza pomoc szkoleniową.

Częste pytanie

Czy bezpiecznie pokazać tylko kilka słów frazy seed? Nie. Nie ma dydaktycznego powodu ujawniania fragmentów własnej frazy.

Miejsce na przerwę

Zachowaj procedurę weryfikacji wsparcia i sprawdź, czy nie zawiera jawnych sekretów.

Głos podobny do głosu wspólnika prosi o pominięcie weryfikacji i pilny podpis. Co robisz?

1. Wstrzymuję działanie, uwierzytelniam prośbę ustaloną metodą i sprawdzam całą operację.
2. Podpisuję, ponieważ zgadza się głos.
3. Podaję frazę seed, by oszczędzić czas.

> **Pokaż odpowiedź: Wstrzymuję działanie, uwierzytelniam prośbę ustaloną metodą i sprawdzam całą operację.**
> Rozpoznanie głosu i presja czasu nie zastępują uwierzytelnienia ani weryfikacji operacji.

Prywatność, prawo i własna dokumentacja

Cel

Poznaj ogólne ramy i przygotuj konkretne pytania prawne oraz podatkowe.

Zrozumienie tematu

Prywatność finansowa nie znosi obowiązków podatkowych, identyfikacyjnych, gdy mają zastosowanie, sankcyjnych ani związanych z zapobieganiem przestępczości. Znaczenie mają rezydencja, działalność, kontrahent i usługa. AI powinna podawać informacje ogólne ze źródłem i datą oraz kierować indywidualne decyzje do właściwych specjalistów.

W UE MiCA reguluje określone kryptoaktywa i usługi. Ogólne stosowanie rozpoczęło się 30 grudnia 2024 roku. Maksymalny okres przejściowy wskazany w rozporządzeniu sięgał 1 lipca 2026 roku, z zastrzeżeniem decyzji krajowych. Sprawdź zezwolenie i jego zakres w aktualnych oficjalnych rejestrach. Dawna wzmianka o rejestracji nie wystarcza. Zezwolenie nie gwarantuje ceny, wypłacalności ani pełnej rekompensaty.

Rozporządzenie 2023/1113 określa informacje towarzyszące transferom z udziałem zobowiązanych dostawców. Przy transferach powyżej 1 000 euro z adresami pozostającymi pod własną kontrolą przewiduje środki oceny własności lub kontroli. Poniżej progu nie powstaje ogólne zwolnienie z identyfikacji. Transfery między osobami bez dostawcy są wyłączone z zakresu tego rozporządzenia. Inne obowiązki nadal istnieją.

Zachowaj odpowiednią dla sytuacji dokumentację zakupów, sprzedaży, opłat i pochodzenia, chroniąc ją przed zbędnym dostępem. Prywatne rejestry nie wymagają publikowania całej historii. Kurs nie uczy dzielenia operacji w celu obchodzenia kontroli, podawania fałszywych informacji ani ukrywania dochodów.

Jeśli nagrywa się lub transkrybuje głos i przetwarza identyfikowalne postępy, usługa musi określić cel, podstawę prawną, okres przechowywania, dostęp, podmioty przetwarzające i właściwe prawa. Komercyjną konfigurację prywatności sprawdza się przed sprzedażą, nie improwizuje podczas rozmowy.

Ćwiczenie

1. Przygotuj dla doradcy fikcyjny przypadek z rezydencją, działalnością i operacjami, bez kluczy.
2. Sprawdź, gdzie zweryfikować zezwolenie dostawcy i datę informacji.

3. Zaprojektuj prywatny rejestr przepływów i minimalną politykę danych uczestnika.

Sprawdź swoje umiejętności

Odróżnij przepis prawa, politykę giełdy i techniczną możliwość Bitcoina.

Częste pytanie

Czy samodzielne przechowywanie jest w UE całkowicie zakazane? Nie wynika to z przywołanych regulacji. Unikaj kategorycznych nagłówków i sprawdzaj konkretny przepis oraz zakres.

Miejsce na przerwę

Zachowaj pytania do doradcy bez przesyłania tutorowi osobistych dokumentów.

Czy poniżej progu 1 000 euro podawanego dla określonych kontroli adresu znikają wszystkie obowiązki?

1. Tak.
2. Tylko jeśli podzielisz operację.
3. Nie. Nie jest to ogólne zwolnienie z identyfikacji ani innych obowiązków.

> **Pokaż odpowiedź: Nie. Nie jest to ogólne zwolnienie z identyfikacji ani innych obowiązków.**
> Przepis należy czytać z uwzględnieniem danego środka i zakresu. Próg nie stanowi powszechnego zwolnienia.

Dziedziczenie, ciągłość i coroczna próba

Cel

Ułóż plan umożliwiający działanie upoważnionym osobom bez przedwczesnego ujawniania wszystkiego.

Zrozumienie tematu

Dziedziczenie łączy uprawnienie prawne, odnalezienie materiałów i zdolność techniczną. Uprawniony spadkobierca może nie umieć odtworzyć portfela, a posiadacz klucza może nie mieć prawa go użyć. Plan powinien rozwiązać oba zagadnienia z odpowiednim doradztwem.

Oddziel ogólnodostępne instrukcje od dostępu do sekretów. Spis opisuje, co istnieje, z kim się skontaktować i co sprawdzić. Nie umieszczaj wszystkich kluczy i haseł w szeroko dostępnym dokumencie. Nie publikuj fraz w testamentach ani aktach, które mogą krążyć poza twoją kontrolą.

Dla wielopodpisu zaplanuj opiekunów polityki i kopii, próg dostępny po utracie oraz skutki śmierci kluczowej osoby. Jeden powiernik z wystarczającą liczbą elementów może stać się pojedynczym punktem nadużycia. Zbyt skomplikowany rozdział może uniemożliwić odzyskanie majątku.

Uwzględnij odzyskanie haseł kryptogramu i dodatkowego hasła, jeśli istnieje, dane wyprowadzania, zgodność urządzeń i postępowanie po zakończeniu działalności producenta. Nie zakładaj użyteczności własnościowego pliku lub odcisku biometrycznego bez przygotowania. Przećwicz interoperacyjność na danych testowych i udokumentowanych formatach.

Sprawdzaj plan po zmianach rodzinnych, miejsca zamieszkania, polityki, oprogramowania lub uczestników i wykonuj okresowe próby. Próba powinna wykazać zrozumienie instrukcji przez zaufaną osobę bez ujawniania majątku i niepotrzebnego przesuwania pieniędzy.

Ćwiczenie

1. Wypełnij prywatny szablon osobami odpowiedzialnymi, elementami, dozwolonym dostępem i zastępcami.
2. Daj drugiej osobie instrukcję laboratoryjną bez ustnych objaśnień i zobacz, gdzie się zatrzyma.

3. Popraw niejasności i zapisz termin przeglądu. Kurs nie tworzy przypomnień automatycznie.

Sprawdź swoje umiejętności

Wyjaśnij, co się stanie podczas twojej niedostępności i jakich informacji potrzebuje każda rola na każdym etapie.

Częste pytanie

Czy 2 z 3 zastępuje plan dziedziczenia? Nie. To narzędzie techniczne. Spadkobiercy nadal potrzebują kontekstu, materiałów, koordynacji i uprawnienia.

Miejsce na przerwę

Zachowaj plan poza kursem i zaznacz jedynie „sprawdzono próbę”.

Co jest przydatnym kryterium oceny planu spadkowego?

1. Upoważniona osoba może przeprowadzić udokumentowaną próbę bez improwizowania i bez przedwczesnego otrzymania sekretów.
2. Plan ma dużo stron.
3. Plan zależy wyłącznie od zapamiętania hasła.

> **Pokaż odpowiedź: Upoważniona osoba może przeprowadzić udokumentowaną próbę bez improwizowania i bez przedwczesnego otrzymania sekretów.**
> Możliwość odzyskania i kontrolę dostępu trzeba sprawdzić w praktyce.

M11

Cena, oszczędzanie i analiza fundamentalna

Cel

Analizuj argumenty inwestycyjne, odróżniając je od sprawdzalnych właściwości technicznych.

Zrozumienie tematu

Cena wynika z wymiany na konkretnych rynkach i może się różnić między platformami. Na możliwą do uzyskania cenę wpływają płynność, waluta notowania, głębokość rynku, godziny pracy dostawców bankowych i popyt. Kurs na ekranie nie jest gwarantowaną ofertą dla twojej ilości.

Analiza fundamentalna bada przyjęcie przez użytkowników, popyt, konkurencję, bezpieczeństwo ekonomiczne, regulacje i podaż. Znany harmonogram emisji sam nie określa przyszłej ceny. Oceny użyteczności pieniężnej lub „wartości wewnętrznej” zależą od założeń. AI nie może przedstawić jednej obiektywnej liczby jako powszechnego pewnika.

Regularne zakupy rozkładają moment wejścia, ale nie gwarantują zysku ani uniknięcia długotrwałych strat. Długoterminowe oszczędzanie wymaga płynności na zobowiązania, tolerancji wahań i planu przechowywania. Kurs nie wyznacza udziału w twoim majątku ani nie podejmuje decyzji za ciebie.

Oddziel trzy pytania: czy rozumiem aktywo, potrafię je przechować i odzyskać oraz czy mogę ponieść ryzyko ekonomiczne? Umiejętność zarządzania kluczami nie odpowiada automatycznie na trzecie. Nauka nie zamienia prognozy ceny lub wykresu historycznego w indywidualną rekomendację.

Ćwiczenie

1. Sformułuj fikcyjną tezę, jej założenia i fakty, które by ją obaliły.
2. Zasymuluj spadek o 50% i jednoczesną potrzebę płynności bez podawania prawdziwego majątku.
3. Wskaż sprawdzalne dane i oczekiwania zawarte w argumentacji.

Sprawdź swoje umiejętności

Omów inwestowanie bez obiecywania rentowności i mylenia przekonania z dowodem.

Częste pytanie

Czy ograniczona podaż gwarantuje wzrost ceny? Nie. Dla ceny rynkowej nadal kluczowy jest popyt i pozostałe warunki.

Miejsce na przerwę

Zachowaj założenia laboratoryjne, nie automatyczne polecenie zakupu.

Co gwarantują regularne zakupy?

1. Zysk w dłuższej perspektywie.
2. Żadnej stopy zwrotu. Rozkładają momenty zakupu według wybranej reguły.
3. Ochronę przed utratą kluczy.

> **Pokaż odpowiedź: Żadnej stopy zwrotu. Rozkładają momenty zakupu według wybranej reguły.**
> Rozłożenie zakupów nie usuwa ryzyka ekonomicznego ani operacyjnego.

Wybór miejsca zakupu bitcoinów

Cel

Oceń dostawcę pod względem zezwoleń, kosztów, wypłaty, prywatności i ryzyka powierniczego.

Zrozumienie tematu

Porównuj sprawdzalne kryteria: podmiot prawny, jurysdykcję, dozwolone usługi, sieć wypłaty, opłaty, spread, limity, wsparcie, uwierzytelnianie i przetwarzanie danych. Nazwa handlowa i sponsoring nie dowodzą zezwolenia na konkretną usługę.

Łączny koszt może obejmować wpłatę, przewalutowanie, spread, prowizję handlową, wypłatę i koszt bankowy. Handel „bez prowizji” może mieć większy spread. Sprawdź kwoty netto i walutę odniesienia. Uwzględnij koszt wypłaty do własnego portfela, jeśli to twój cel.

Dopóki środki są u powiernika, zależysz od dostawcy. Dowód rezerw sam nie ujawnia wszystkich zobowiązań, własności środków ani przyszłej wypłacalności. Sprawdź ograniczenia i wykonaj małą wypłatę, na którą możesz sobie pozwolić, zanim polegać będziesz na nowym procesie.

Identyfikacja handlowa może połączyć twoją tożsamość z wypłatą. Dalsza ochrona tych informacji nie usuwa wiedzy dostawcy. Nie fałszuj danych ani nie korzystaj z kursu do obchodzenia obowiązków. Zakup kodu szkoleniowego również tworzy zapis handlowy odrębny od portfela.

Ćwiczenie

1. Wypełnij fikcyjną tabelę dla dwóch dostawców: koszt całkowity, sieć, minimalna wypłata, zezwolenie i wymagane dane.
2. Oblicz kwotę netto dla operacji ćwiczeniowej po wszystkich wskazanych opłatach.
3. Zaplanuj próbną wypłatę na uprzednio sprawdzony adres, nie wykonując jej z tej strony kursowej.

Sprawdź swoje umiejętności

Uzasadnij wybór dla swojej sytuacji i rozpoznaj informacje przestarzałe lub niesprawdzone.

Częste pytanie

Czy kurs poleca jedną giełdę najlepszą dla wszystkich? Nie. Uprawnienia, opłaty, obsługiwane kraje i warunki się zmieniają. Porównanie wymaga daty i przypadku użycia.

Miejsce na przerwę

Zachowaj tabelę bez danych uwierzytelniających i dokumentów tożsamości.

Co warto porównać zamiast patrzeć tylko na prowizję od transakcji?

1. Całkowity koszt do momentu otrzymania BTC w wybranej sieci na wskazanym adresie.
2. Liczbę obserwujących dostawcę.
3. Kolor jego aplikacji.

> **Pokaż odpowiedź: Całkowity koszt do momentu otrzymania BTC w wybranej sieci na wskazanym adresie.**
> Cena końcowa obejmuje pozycje, które mogą nie wchodzić w skład reklamowanej prowizji.

Konta, zlecenia i koszty realizacji

Cel

Poznaj podstawowe zlecenia i chroń konto, nie traktując kursu jak terminala transakcyjnego.

Zrozumienie tematu

Zlecenie rynkowe uprzywilejowuje dostępną realizację przy ryzyku poślizgu ceny. Limit określa maksymalną cenę kupna lub minimalną sprzedaży, ale zlecenie może nie zostać wykonane albo zostać wykonane częściowo. Zlecenie stop uruchamia dalsze działanie zgodnie z zasadami dostawcy i samo nie gwarantuje ceny końcowej.

Arkusz zleceń pokazuje dostępne oferty, nie zobowiązanie, że wszystkie ilości pozostaną dostępne. Przy spadku lub niskiej płynności wynik może się różnić od ostatniego kursu. Stop-market niesie ryzyko gorszej ceny, stop-limit braku wykonania.

Chroń dostęp unikalnym hasłem, odpornym na phishing uwierzytelnianiem tam, gdzie jest obsługiwane, kontrolą sesji i odpowiednimi ograniczeniami wypłat. Zachowaj niezależną metodę odzyskania drugiego składnika. Klucz API do automatyzacji może mieć groźniejsze uprawnienia niż potrzebne do odczytu. Nie wpisuj go tutorowi ani na stronie kursu.

Przed wypłatą sprawdź aktywo i sieć Bitcoin, własny adres oraz kwoty netto. Platforma może używać identycznych symboli dla odmiennych produktów. Zachowaj właściwe dla sytuacji potwierdzenia zakupu, realizacji, opłat i wypłaty. Wypłata do swojego portfela nie jest nowym zakupem.

Ćwiczenie

1. Zasymuluj arkusz z 1 jednostką po 100 i drugą po 102. Wyjaśnij, dlaczego rynkowy zakup dwóch nie zapewnia średniej ceny 100.
2. Zaprojektuj zlecenie z limitem i opisz przypadek, w którym nie zostanie całkowicie wykonane.
3. Sprawdź uprawnienia fikcyjnego API i usuń możliwość wypłat, jeśli potrzebny jest tylko odczyt.

Sprawdź swoje umiejętności

Opisz priorytet, cenę i ryzyko niewykonania dla każdego typu zlecenia.

Częste pytanie

Czy stop-loss zawsze ogranicza stratę do dokładnej wartości? Nie. Luki cenowe, płynność, poślizg i zasady dostawcy mogą to uniemożliwić.

Miejsce na przerwę

Zachowaj wynik bez rzeczywistych zleceń i kluczy API.

Jakie ryzyko pozostaje przy zleceniu kupna z limitem 100?

1. Zlecenie może nie zostać wykonane lub być wykonane tylko częściowo.
2. Musi zostać wykonane po dowolnej cenie.
3. Automatycznie tworzy kopię zapasową.

> **Pokaż odpowiedź: Zlecenie może nie zostać wykonane lub być wykonane tylko częściowo.**
> Kontroli ceny towarzyszy ryzyko braku realizacji.

M11

Świece, wskaźniki i błędy poznawcze w analizie technicznej

Cel

Czytaj wykresy jako dane historyczne i oceniaj strategię bez mylenia wzorców z prognozą.

Zrozumienie tematu

Świeca przedstawia cenę otwarcia, maksimum, minimum i zamknięcia okresu. Wolumen zależy od źródła. Zmiana platformy, waluty, strefy czasowej lub interwału może zmienić obraz. Świeca nie pokazuje kolejności wszystkich ruchów w swoim przedziale.

Średnia krocząca wygładza historyczne ceny. Wskaźnik momentum przekształca obserwowane dane według wzoru. Żaden nie zna przyszłości. Dwa wskaźniki z tej samej serii mogą nieść silnie skorelowane informacje mimo innych kolorów i nazw.

Przed obejrzeniem wyniku określ wejście, wyjście, kryterium unieważnienia, koszty, rozmiar pozycji i dane. Unikaj wyboru wyłącznie zyskownych przykładów, dopasowywania parametrów do wyniku oraz korzystania z przyszłych danych w decyzji z przeszłości. Oddziel dane treningowe od późniejszej walidacji czasowej.

Test historyczny powinien uwzględniać spread, prowizje, poślizg, dostępność danych i możliwość realizacji. Zwrot brutto, trafność, maksymalna strata i rozkład strat odpowiadają na odmienne pytania. Liczne trafienia nie zapobiegają stracie, jeśli porażki są duże. Sygnał kupna lub sprzedaży nie jest nauczany jako pewnik.

Ćwiczenie

1. Odczytaj fikcyjną świecę i wyjaśnij, jakiej informacji o kolejności nie zawiera.
2. Zapisz regułę przed oceną dziesięciu syntetycznych wyników. Uwzględnij koszty i kryterium porażki.
3. Porównaj 9 zysków po 1 ze stratą 15. Wynik brutto to -6 mimo 90% trafności.

Sprawdź swoje umiejętności

Oceń atrakcyjny wynik pod kątem selekcji przykładów, kosztów i ryzyka bez wykonywania transakcji.

Częste pytanie

Czy połączenie wielu wskaźników gwarantuje lepszy sygnał? Nie. Może zwiększyć przeuczenie i złożoność bez niezależnych informacji.

Miejsce na przerwę

Zachowaj regułę i wyniki laboratoryjne, nie zlecenie rynkowe.

Dziewięć operacji przynosi po 1 zysku, jedna stratę 15. Jaki jest wynik przed kosztami?

1. +90%.
2. +6.
3. -6.

> **Pokaż odpowiedź: -6.**
> Dziewięć jednostek zysku minus piętnaście straty daje stratę sześciu jednostek.

Depozyt zabezpieczający, kontrakty terminowe i automatyzacja

Cel

Poznaj ekspozycję, likwidację i awarie automatyzacji przed rozważeniem złożonych produktów.

Zrozumienie tematu

Dźwignia zwiększa ekspozycję względem wniesionego kapitału. W uproszczeniu przy depozycie 100 i ekspozycji 1 000 niekorzystny ruch instrumentu bazowego o 5% oznacza przed kosztami stratę 50, czyli połowy początkowego depozytu. Rzeczywiste zasady utrzymania, likwidacji, zabezpieczenia i opłat mogą pogorszyć wynik i zadziałać wcześniej niż oczekujesz.

Kontrakty futures i bezterminowe mogą obejmować termin zapadalności, rozliczenie różnicowe, stawki finansowania i ceny referencyjne inne niż ostatnia transakcja. Nie odpowiadają wypłacie natywnego bitcoina do Cuvex. Przechowywanie frazy seed nie chroni pozycji przed likwidacją ani niewykonaniem zobowiązań przez kontrahenta.

Bot automatyzuje reguły wraz z błędami. Wymaga limitów pozycji, minimalnych uprawnień, idempotencji zleceń, uzgadniania stanu, kontroli strat, awaryjnego zatrzymania i nadzoru. Ponowienie żądania po przekroczeniu czasu może podwoić ekspozycję, jeśli wynik wcześniejszego jest nieznany.

AI może objaśniać pojęcia i wykrywać niespójności w fikcyjnym przypadku. Nie powinna otrzymywać kluczy API, uruchamiać handlu ani obiecywać rentownej strategii. Zrozumienie ryzyka pomaga zgodnie z celem kursu zrezygnować z niezrozumiałych produktów.

Ćwiczenie

1. Rozwiąż przykład ekspozycji i depozytu bez zakładania, że likwidacja nastąpi dokładnie przy 10%.
2. Zasymuluj API, które wykonuje zlecenie, lecz traci odpowiedź. Wyjaśnij konieczność uzgodnienia przed ponowieniem.
3. Zaprojektuj przycisk zatrzymujący nowe zlecenia i sprawdzający już otwarte, bez połączenia z brokerem.

Sprawdź swoje umiejętności

Opisz ryzyko pozostające mimo zlecenia stop, inne mimo użycia bota i kolejne mimo samodzielnego przechowywania środków poza platformą.

Częste pytanie

Czy automatyzacja usuwa emocje i gwarantuje wynik? Nie. Może ograniczyć impulsywne działania, jednocześnie powielając błędy projektu lub realizacji.

Miejsce na przerwę

Oznacz rozszerzenie jako zrozumiane bez włączania złożonych produktów.

Przy ekspozycji 1 000 i depozycie 100 strata 5% ekspozycji oznacza przed kosztami:

1. Stratę 5.
2. Stratę 50, czyli 50% depozytu.
3. Brak straty, jeśli działa bot.

> **Pokaż odpowiedź: Stratę 50, czyli 50% depozytu.**
> Dźwignia i koszty powodują, że wynik względem depozytu różni się od zmiany ceny aktywa.

M12

Lightning i inne warstwy

Cel

Poznaj płatności kanałowe i rozpoznaj funkcje niedostępne w sprawdzonym procesie Cuvex.

Zrozumienie tematu

Lightning wykorzystuje kanały i mechanizmy aktualizacji, aby płacić bez zapisywania każdej wymiany w łańcuchu bazowym. Otwarcie i zamknięcie kanału oraz niektóre przypadki odzyskiwania mogą wymagać transakcji on-chain. Dostępność, płynność przychodząca i wychodząca oraz monitorowanie zależą od konstrukcji portfela i używanych usług.

Faktura może zawierać kwotę, opis i termin wygaśnięcia. W zależności od kontekstu jednostką są satoshi lub milisatoshi. Te ostatnie nie oznaczają wyjść poniżej jednego satoshi w łańcuchu bazowym. Płatność wymaga zgodności i dostępnej trasy. QR nie gwarantuje obsługi przez każdą aplikację.

Usługi powiernicze i bezpowiernicze mają bardzo różne modele. Zwykła szybkość nie dowodzi braku ryzyka. Lightning nie należy też przedstawiać jako pełnej anonimowości. Znaczenie mają obserwatorzy, trasy, kontrahenci i metadane.

Czat Cuvex może koordynować żądania satoshi płacone w łańcuchu przez konto WOW. W tym wydaniu nie przypisuje się Desk węzła Lightning, zarządzania kanałami ani podpisywania faktur Lightning. Gdy żądanie ma kilka trybów, sprawdź, który rozumiesz i który wykona aplikacja.

Ćwiczenie

1. Sklasyfikuj szkoleniowy adres on-chain, URI bitcoin: i fakturę Lightning.
2. Porównaj płatność w łańcuchu i przez kanał według potwierdzenia, płynności, pieczy i odzyskiwania.
3. Wyjaśnij, dlaczego przedawnioną fakturę należy uzgodnić z odbiorcą, a nie potraktować jak adres.

Sprawdź swoje umiejętności

Odrzuć niezgodną metodę bez ujawniania kluczy i bez błędnego przypisywania awarii Cuvex.

Częste pytanie

Czy wszystkie płatności w satoshi używają Lightning? Nie. Satoshi wyrażają wartość, a metoda zależy od protokołu.

Miejsce na przerwę

Zachowaj tryb ćwiczenia bez prawdziwych faktur.

Co wystarcza do rozpoznania żądania opłacanego przez Lightning?

1. Użycie słowa „sats”.
2. Doręczenie na czacie.
3. Zgodny format i tryb płatności, nie tylko jednostka lub kanał wiadomości.

> **Pokaż odpowiedź: Zgodny format i tryb płatności, nie tylko jednostka lub kanał wiadomości.**
> Jednostka rozliczeniowa i sieć płatnicza to odrębne cechy.

Taproot, MuSig2 i przyszłość postkwantowa

Cel

Odróżniaj standardy, propozycje i wdrożone funkcje.

Zrozumienie tematu

Taproot pozwala określać warunki wydania ścieżką klucza lub skryptu. Podpisy Schnorra i agregacja mogą ulepszać niektóre konstrukcje. Prywatność zależy od konfiguracji i sposobu wydania. Adres bc1p nie dowodzi braku innych uczestników ani nie ujawnia wszystkich ukrytych warunków.

MuSig2 pozwala grupie agregować klucze i wspólnie tworzyć zgodny podpis Schnorra przez interakcję. Podstawowy schemat to N z N. Dowolny próg M z N wymaga innej konstrukcji lub dodatkowego protokołu. Zarządzanie wartościami nonce i sesjami jest krytyczne. Nie zastępuje go nieformalna wymiana wiadomości.

PSBT v2 inaczej organizuje informacje niż v0. Plik z transakcją w wersji 2 nie uzyskuje przez to automatycznie nowszej wersji formatu kontenera. Firmware Final tego wydania zachowuje w profilu wielopodpisowym PSBT v0, P2WSH/sortedmulti i SIGHASH_ALL. Przyszłe funkcje wymagają osobnych specyfikacji i weryfikacji.

W 2024 roku NIST opublikował pierwsze ukończone standardy postkwantowe. Samo to nie zmienia podpisów Bitcoina. Algorytm postkwantowy do uwierzytelniania firmware chroniłby tę warstwę, ale nie przekształcałby automatycznie ECDSA lub Schnorra dla UTXO w podpis postkwantowy. Tutor nie może też podać pewnej daty przyszłego ataku.

Ćwiczenie

1. Sklasyfikuj pięć twierdzeń jako standard, sprawdzoną implementację, propozycję lub reklamę.
2. Wyjaśnij, dlaczego „obsługuje odbiorcę Taproot” nie dowodzi „podpisuje wejście Taproot”.
3. Narysuj osobne warstwy podpisu firmware, szyfrowania sekretu, czatu i podpisu wydatku Bitcoin.

Sprawdź swoje umiejętności

Poproś o dowód właściwy dla warstwy i nie przenoś gwarancji między protokołami.

Częste pytanie

Czy migrować środki z powodu nagłówka o komputerach kwantowych? Rzeczywista decyzja wymaga bieżących dowodów technicznych, sprawdzalnej obsługi, oceny ryzyka i bezpiecznego planu migracji. Kurs nie zleca przelewów na podstawie nagłówków.

Miejsce na przerwę

Zapisz pytania techniczne bez tworzenia automatycznego planu wydania.

Czy wdrożony i zweryfikowany podpis postkwantowy w programie rozruchowym zmieniłby warunki podpisywania istniejącego UTXO?

1. Nie. To odrębne warstwy.
2. Tak. Przełącza całą sieć na inny algorytm.
3. Usuwa potrzebę tworzenia kopii.

> **Pokaż odpowiedź: Nie. To odrębne warstwy.**
> Uwierzytelnienie aktualizacji nie zmienia warunków wydawania Bitcoina.

Interoperacyjność i uniezależnienie się od producenta

Cel

Zaplanuj ciągłość po zmianie oprogramowania, urządzenia lub dostawcy.

Zrozumienie tematu

Interoperacyjności nie dowodzi lista skrótów. Trzeba zachować sieć, skrypt, wyprowadzanie, klucze, politykę, format transakcji i znaczenie podpisów. Dwie aplikacje mogą rozumieć BIP174, lecz nie obsługiwać tych samych pól, rozmiarów lub typów wejść.

Aby uniezależnić się od interfejsu, zachowaj udokumentowane dane odzyskiwania i przećwicz je z portfelami szkoleniowymi. Standardowy mnemonik może umożliwić wyprowadzenie kluczy, ale odtworzenie wielopodpisu wymaga pełnej polityki. Etykiety BIP329 dodają kontekst prywatności. Historia czatu ma inny zakres.

Test zgodności nie może prowadzić do ujawnienia prawdziwej frazy. Najpierw sprawdź publiczny eksport deskryptorów i odzyskanie portfela obserwacyjnego. Jeśli awaria wymaga odtworzenia kluczy, użyj przeznaczonego środowiska i rozważ późniejszą migrację. Zerowe saldo w niezgodnym portfelu samo nie dowodzi utraty środków.

Zachowaj sprawdzalną kopię dokumentacji, wersji kursu i potrzebnych narzędzi. Podpisy aplikacji, wygasłe certyfikaty i zmiany systemów mogą wpływać na instalację. Dostępny otwarty kod nie gwarantuje, że każdy zbuduje program po latach bez zachowania zależności i wiedzy.

Ćwiczenie

1. Zaprojektuj test wyjścia na pustym koncie: ta sama sieć, polityka i adres kontrolny w dwóch zgodnych implementacjach.
2. Wymień elementy standardowe i te wymagające konwertera lub dokumentacji formatu Cuvex.
3. Określ wynik potwierdzający zgodność oraz brakujące próby sprzętowe i rzeczywistego podpisu.

Sprawdź swoje umiejętności

Opisz sposób odzyskania niezależny od dalszego świadczenia tej samej usługi przez firmę.

Częste pytanie

Czy otwarty kod oznacza, że producent nie ma znaczenia? Nie. Dystrybucja, utrzymanie, fizyczne części i doświadczenie operacyjne nadal się liczą. Otwarty kod pozwala na inspekcję i potencjalną ciągłość, nie gwarantuje ich automatycznie.

Miejsce na przerwę

Zachowaj wyniki z wersjami i zaobserwowanymi ograniczeniami.

Co stanowi mocniejszy dowód interoperacyjności?

1. Obie aplikacje wyświetlają słowo „Bitcoin”.
2. Odtworzenie i sprawdzenie w laboratorium tej samej polityki i adresu z podaniem konkretnych wersji.
3. Podobieństwo ikon.

> **Pokaż odpowiedź: Odtworzenie i sprawdzenie w laboratorium tej samej polityki i adresu z podaniem konkretnych wersji.**
> Próba powinna zachować istotne warunki i dać sprawdzalny wynik.

M12

Laboratorium techniczne z regtest

Cel

Poznaj powtarzalne środowisko ćwiczeń i odróżnij testy syntetyczne od fizycznego użycia.

Zrozumienie tematu

Regtest umożliwia stworzenie kontrolowanego lokalnego łańcucha, generowanie bloków i próby transakcji bez wartości ekonomicznej. Używaj osobnych katalogów i danych dostępu bez importowania prawdziwego materiału. Wyniki same nie wykazują zgodności USB, NFC, Bluetooth ani kamery fizycznego urządzenia.

Pełne laboratorium zapisuje wersje, konfigurację sieci, politykę, wejścia testowe, PSBT, podpisy, finalną transakcję i wynik przyjęcia. Może sprawdzić zgodność sum, odrzucenie zmienionego podpisu i włączenie ważnej płatności do lokalnego bloku. Próby muszą obejmować również błędy.

Walidacja Desk 9.21 opisuje testy w Bitcoin Core 31 regtest i automatyczne testy silnika oraz symulowanego interfejsu. To wydanie korzysta z nich jako dokumentacji. Nie twierdzi, że powtórzono testy lub wykonano operacje z urządzeniami. Sprawdzenie pakietu nie dowodzi instalacji na wszystkich systemach.

Przed lekcją techniczną inżynier powinien dostarczyć skonfigurowane laboratorium i procedurę zgodną z wersją uczestnika. Nie udostępniaj RPC w internecie, aby tutor je kontrolował. AI może pomagać interpretować wyniki syntetyczne, lecz nie powinna otrzymywać danych dostępu ani praw administratora.

Ćwiczenie

1. W przygotowanym laboratorium obserwuj prawidłową transakcję i drugą ze zmienionym podpisem. Zapisz przyjęcie lub odrzucenie.
2. Sprawdź przypadek nieprawidłowej reszty i niezgodnej sieci.
3. Oddziel w raporcie „test silnika”, „symulowany interfejs” i „sprzęt fizyczny”.

Sprawdź swoje umiejętności

Określ dokładnie, co sprawdzono i co pozostaje otwarte, bez przedstawiania symulacji jako certyfikacji.

Częste pytanie

Czy po udanym regtest można sprzedawać kurs jako zweryfikowany dla każdego urządzenia? Nie. Pozostają testy przebiegów fizycznych, instalacji, dostępności, odzyskiwania i usługi komercyjnej.

Miejsce na przerwę

Zatrzymaj i zachowaj środowisko według instrukcji, pozostawiając tylko dane syntetyczne.

Czy test silnika w regtest dowodzi rzeczywistego odczytu NFC na konkretnym telefonie?

1. Tak, ponieważ oba używają Bitcoina.
2. Tak, jeśli PSBT jest mała.
3. Nie. Potrzebny jest osobny test fizyczny.

> **Pokaż odpowiedź: Nie. Potrzebny jest osobny test fizyczny.**
> Środowiska weryfikacji mają różny zakres.

Projekt końcowy i plan ciągłości

Cel

Wykaż samodzielność od przygotowania po odzyskiwanie środków i ochronę prywatności.

Zrozumienie tematu

Celem jest wyjaśnienie zamiaru, sprawdzenie wyniku i zatrzymanie niezrozumiałej operacji, nie zapamiętanie menu. Ocena łączy wiedzę, ćwiczenie prowadzone i samodzielny przypadek. Nigdy nie zależy od podania oceniającemu fraz, majątku ani osobistych adresów.

Przypadek A: przygotuj środowisko nauki, rozpoznaj modele i wersje, zabezpiecz Desk, powiąż kryptogram szkoleniowy i odtwórz konto obserwacyjne. Wyjaśnij potrzebne kopie i dane, które może widzieć dostawca.

Przypadek B: zaprojektuj płatność z fikcyjnymi UTXO z różnych kontekstów, uzasadnij wybór, sprawdź odbiorcę, resztę i opłatę oraz opisz ścieżkę podpisu dla swojego urządzenia. Rozwiąż przerwę przy powrocie i publikacji bez podwójnej płatności. Jeśli brak sprzętu po fizycznym odbiorze, oznacz część jako symulowaną i nadal oczekującą.

Przypadek C: zaprojektuj 2 z 3, odegraj zaproszenie i weryfikację, porównaj w Mirror dowolne pole w wybranej kolejności i wyjaśnij zakres „OK”. Odtwórz politykę ćwiczeniową, zasymuluj utratę uczestnika i przygotuj ciągłość oraz dziedziczenie.

Proponowane zaliczenie wymaga przynajmniej 80% z wiedzy i prawidłowych wszystkich krytycznych kontroli: zachowania sekretów, sprawdzenia sieci i wyjść, rozróżnienia etapów i zachowania możliwości odzyskania. Błąd krytyczny wymaga powtórki i nowego ćwiczenia. Nie wyrównają go poprawne odpowiedzi o rynku. Ewentualny certyfikat komercyjny powinien wskazywać, co oceniono i czy była to obserwacja fizyczna czy tylko symulacja.

Ćwiczenie

1. Wykonaj trzy przypadki na danych syntetycznych z własnym wyjaśnieniem.
2. Rozwiąż końcowy sprawdzian z załącznika i przejrzyj każdą błędną odpowiedź.
3. Oddaj wyłącznie kartę wyników bez sekretów, z dowodami zakresu i pozostałymi zadaniami.

Sprawdź swoje umiejętności

Samodzielnie zatrzymaj się, gdy brak wystarczających dowodów do wykonania operacji, i określ warunki kontynuacji.

Częste pytanie

Czy przeczytanie stron przygotowuje do przechowywania dowolnej kwoty? Nie. Umiejętności trzeba sprawdzić, a ryzyko ocenić według swojej sytuacji. Lektura i próby nie gwarantują przyszłych wyników.

Miejsce na przerwę

Zachowaj plan przeglądu i niedokończone ćwiczenia. Możesz wrócić do wybranego rozdziału bez powtarzania całego kursu.

Jaki jest kluczowy warunek ukończenia szkolenia praktycznego?

1. Otwarcie wszystkich stron.
2. Wykazanie odzyskiwania i sprawdzania operacji w udokumentowanym zakresie bez ujawniania sekretów.
3. Trafna prognoza ceny na przyszły miesiąc.

> **Pokaż odpowiedź: Wykazanie odzyskiwania i sprawdzania operacji w udokumentowanym zakresie bez ujawniania sekretów.**
> O nauce świadczą sprawdzone umiejętności i ich granice, a nie przeglądanie stron czy prognozowanie.

Podręcznik uczestnika

Podręcznik obsługi Cuvex

Podręcznik towarzyszy lekcjom. Każda procedura opisuje przebieg znaleziony w sprawdzonych źródłach, jego kontrole i punkt zatrzymania. To wersja przewidziana do pilotażu. Nie potwierdza własnych testów fizycznych z Original, BIT, telefonami ani każdą platformą komputerową. Przed nauką z prawdziwymi środkami zespół musi uzupełnić macierz odbioru i skorygować różniące się etykiety lub ekrany.

Wersje odniesienia to Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 i Mirror 1.0.0-beta.12.12. Wybór profilu w Desk określa deklarowaną zgodność i nie jest zdalnym pomiarem firmware. Zamieszczone rzeczywiste zrzuty Mirror pochodzą z emulatora Android pakietu 12.12. Zdjęcia produktów są materiałami firmy i nie potwierdzają wersji wyświetlanej na obecnym urządzeniu.

P01 | Sprawdzenie pochodzenia i wersji | Cuvex | L16,L21 | C01,C02

Przygotowanie: przygotuj dane zakupu i niezależnie sprawdzalny oficjalny kanał. Nie wpisuj jeszcze sekretów.

1. Obejrzyj opakowanie i plomby. Przy oznakach ingerencji zatrzymaj uruchomienie i zachowaj dowody bez danych wrażliwych.
2. Użyj w aplikacji zgodnej z dostawą procedury sprawdzania integralności i plomb. Kody wpisuj tylko tam, nigdy u tutora.
3. Rozpoznaj Original lub BIT i dostępną rewizję. Sprawdź widoczne wersje urządzenia i aplikacji.
4. Porównaj z macierzą opublikowaną przez zespół. Katalog ani skrót nie zastępują uwierzytelnienia firmware i fizycznego odbioru.

Wynik: model i wersje rozpoznane, pochodzenie sprawdzone bez ujawnienia sekretów. Przy nieważnych kodach lub innym interfejsie nie wymuszaj użycia według starej instrukcji.

Przerwij przed wczytaniem materiału do przechowywania. Sama identyfikowalność handlowa nie gwarantuje braku zaawansowanej ingerencji.

P02 | Aktualizacja Original przez Bluetooth | Original | L46 | C01,C02,C03

Przygotowanie: odtwarzalne kopie, stabilne zasilanie, zgodny oficjalny pakiet i ścieżka odebrana dla danego systemu. Kurs nie potwierdza pełnej dostępności fizycznej na każdej platformie.

1. W sekcji urządzeń lub firmware aplikacji wybierz Original i oficjalne pobranie albo odpowiadający mu autentyczny plik lokalny.
2. Włącz aktualizację w menu urządzenia i połącz je procedurą aplikacji. Zachowaj bliskość i unikaj konkurencyjnych sesji.
3. Wpisz kod z ekranu Original we wskazanym polu. Nie pomyl go z hasłem kryptogramu.
4. Obserwuj transfer, weryfikację, instalację i restart. Procent postępu nie jest dowodem instalacji.
5. Sprawdź końcową wersję na Original i zapisz ją w aplikacji, jeśli przewidziano takie pole.

Wynik: wersja sprawdzona na ekranie po restarcie, zakończenie procedury potwierdzone. Przy błędzie przed PIN-em, podczas pakietów lub na końcu zapisz fazę i kod. Nie odłączaj ani nie zmieniaj oprogramowania na chybił trafił, by „przejść 99%”.

P03 | Aktualizacja BIT przez USB | BIT | L46 | C01,C02,C03

Przygotowanie: rozpoznaj rzeczywisty nośnik BIT, zasilanie i zgodny oficjalny pakiet. Przed zmianą oprogramowania zachowaj kopie.

1. Wybierz BIT w zgodnej ścieżce firmware w Desk lub Mirror.
2. Podłącz urządzenie odpowiednim przewodem do danych i adapterem. Zezwól aplikacji na dostęp do woluminu lub folderu, gdy o to poprosi.
3. Wybierz autentyczne firmware właściwego modelu. Przed przesłaniem sprawdź wersję i dane zgodności.
4. Poczekaj na transfer i weryfikację w urządzeniu. Wolumin może zniknąć i ponownie zostać zamontowany zgodnie z protokołem.
5. Po restarcie sprawdź wersję na BIT i końcowy wynik aplikacji.

Wynik: instalacja potwierdzona na urządzeniu. Jeśli wolumin nie jest widoczny, sprawdź tryb urządzenia, przewód danych, uprawnienia, montowanie i inne aktywne sesje. Nie zastępuj go folderem o tej samej nazwie na komputerze. Odzyskanie po nieudanej aktualizacji wymaga oficjalnej procedury dla tego sprzętu.

P04 | Generowanie portfela monetą i kośćmi | Cuvex | L17 | C01

Przygotowanie: prywatne miejsce, odpowiednie kości i moneta, bez kamer i aktywnego mikrofonu tutora. Użyj portfela ćwiczeniowego.

1. Otwórz tworzenie portfela i ścieżkę entropii firmware. Wcześniej ustal kolejność czterech kości.
2. Wprowadź monetę i każdą kość zgodnie z ekranem. Nie zmieniaj wyników według upodobania.
3. Sprawdzony kod liczy indeks = moneta × 1 296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Dopuszczalne są tylko indeksy od 0 do 2 047.
4. Po odrzuceniu ponownie rzuć monetą i wszystkimi kośćmi. Komunikat zachowuje wcześniejsze słowa i prosi o powtórzenie całego zestawu.
5. Dokończ algorytm urządzenia wraz z końcową weryfikacją, zabezpiecz mnemonik i prywatnie sprawdź odzyskanie.

Wynik: portfel utworzony pełną procedurą, bez ręcznego wybierania słów. Jeśli ekran nie zgadza się ze źródłem, przerwij. Nie używaj publicznych przykładów rzutów, fraz ani kluczy jako własnego materiału.

P05 | Szyfrowanie sekretu | Cuvex | L18,L19 | C01

Przygotowanie: wybierz model, format treści i ochronę. Wpisanie na telefonie lub komputerze ujawnia treść u źródła mimo zaszyfrowania w miejscu docelowym.

1. Wybierz szyfrowanie i typ BIP39, SLIP39, Monero albo obsługiwany tekst. Nie zamieniaj słowników. Sprawdzona klawiatura tekstu jawnego przyjmuje do 500 znaków. Zapis innego formatu nie oznacza podpisywania w jego sieci.
2. Wpisz treść bezpośrednio na urządzeniu, by zachować izolację. Sprawdź na jego ekranie kolejność, znaki i pola pomocnicze.
3. Wybierz ochronę indywidualną lub wspólną zgodnie z procesem, a w BIT biometrię, jeśli dotyczy. Odróżnij ten próg od progu Bitcoin.
4. Wprowadź i potwierdź hasła prywatnie zgodnie z walidatorem firmware. Nie przenoś automatycznie reguł Desk.
5. W Original zapisz na zgodnej pustej karcie, a w BIT zachowaj obiekty eksportu procedury USB. Poczekaj na potwierdzenie.
6. Uruchom próbne odzyskanie, sprawdź treść i po zakończeniu zamknij widok sekretu.

Wynik: kryptogram o sprawdzonym odzyskiwaniu. Przy błędzie zapisu lub odczytu chroń oryginał i ponów według ekranu. Nie kasuj nagłówków ani nie wymuszaj nadpisania.

P06 | Odszyfrowywanie na urządzeniu | Cuvex | L18 | C01,C02

Przygotowanie: prywatność fizyczna i wystarczające składniki odblokowania. Wyłącz mikrofon i rejestrowanie ekranu w pobliżu sekretu.

1. Rozpocznij odszyfrowywanie we właściwym modelu i przekaż kryptogram przez NFC w Original lub procedurą USB w BIT.
2. Przed podaniem danych uwierzytelniających sprawdź alias i tożsamość obiektu.
3. Podaj wymagane hasła oraz biometrię, gdy wymaga jej format. Po błędach nie ponawiaj automatycznie. Działają kontrola dostępu i blokada.
4. Sprawdź treść tylko na przewidzianym ekranie. Kod QR sekretu jest tak samo wrażliwy jak tekst.
5. Zamknij lub zakończ proces zgodnie z urządzeniem i przechowuj nośnik oraz dane dostępu oddzielnie według planu.

Wynik: treść prywatnie odzyskana, sesja zakończona. Przy nierozpoznanym formacie, błędzie uwierzytelnienia lub nieoczekiwanej treści nie „poprawiaj” jej nieznaną aplikacją. Podaj wsparciu wersję, format i błąd bez dołączania sekretu.

P07 | Przygotowanie odzyskania kryptogramu biometrycznego | BIT | L19,L47 | C01,C02

Przygotowanie: kryptogram szkoleniowy i dokumentacja jego formatu. Samo posiadanie kopii .bin nie dowodzi możliwości odzyskania.

1. W szczegółach Desk ustal, czy występują elementy biometryczne i jaki eksport odzyskiwania jest dostępny.
2. Zachowaj powiązany zestaw plików oraz niezależną kopię z dyskretnymi identyfikatorami.
3. Sprawdź zwykłe odblokowanie na BIT i udokumentuj wymagane hasła oraz warunki.
4. Przeanalizuj wyjątkowe odzyskiwanie lokalne i obsługiwane formaty. Sprawdź, czy masz potrzebne materiały, zanim staną się niezbędne.
5. Przećwicz z danymi bez środków awarię urządzenia lub niedostępność odcisku palca.

Wynik: sprawdzony plan z granicami dla konkretnego formatu. Nie każdą biometrię można pominąć i odcisk nie zastępuje kopii. Po odzyskaniu sekretu na komputerze oceń ujawnienie i potrzebę późniejszego przeniesienia kontroli.

P08 | Tworzenie i sprawdzanie kopii kryptogramu | Cuvex i Desk | L20 | C01,C02

Przygotowanie: rozpoznany oryginalny egzemplarz i zgodne miejsce docelowe bez danych do zachowania.

1. W Original użyj klonowania na urządzeniu lub obsługiwanej funkcji Desk. Przedstaw źródło i cel we wskazanej kolejności.
2. Trzymaj karty nieruchomo i uszanuj odrzucenie nośnika zawierającego już kryptogramy.
3. W BIT lub przy pliku wyeksportuj komplet elementów procedury i zachowaj potrzebne nazwy albo powiązania.
4. Odizoluj pierwotną kopię i przetestuj odczyt oraz odzyskanie z nowej.
5. Prywatnie zapisz datę, format i wynik. Przechowuj kopie w miejscach o niezależnych zagrożeniach fizycznych.

Wynik: druga sprawdzona kopia. Nie oznacza innego portfela, unieważnienia haseł ani ochrony po wcześniejszym wycieku frazy. Przy błędzie celu zachowaj oryginał i nie „naprawiaj” go, aby zrównać obie kopie.

P09 | Tworzenie i odblokowanie magazynu Desk oraz zmiana hasła | Desk | L21,L40 | C02

Przygotowanie: zweryfikowany instalator, właściwa architektura i plan kopii magazynu.

1. Utwórz magazyn z unikalnym hasłem od 12 do 1 024 znaków i identycznym potwierdzeniem.
2. Zablokuj i ponownie otwórz, by sprawdzić dostęp. Hasło wpisuj tylko w Desk.
3. W ustawieniach bezpieczeństwa oraz „Dostęp i blokada” sprawdź bezczynność i przejście w tło. Nie włączaj opcjonalnego kasowania podczas demonstracji.
4. Aby zmienić hasło, podaj obecne i potwierdź nowe właściwą procedurą.
5. Jeśli używano biometrii komputera, skonfiguruj ją ponownie według instrukcji. Utwórz bieżącą kopię i zachowaj jej związek z wcześniejszymi.

Wynik: dostęp sprawdzony. Dawne kopie zachowują oryginalne hasło i szyfrowanie. Biometria komputera i BIT to inne mechanizmy. Przy błędzie przerwij ponawianie i sprawdź odzyskiwanie bez powierzania tutorowi danych dostępu.

P10 | Łączenie i sprawdzanie kryptogramu w Desk | Desk | L22 | C02

Przygotowanie: próbny kryptogram znanego pochodzenia i dostępny sposób przesyłania.

1. Otwórz kryptogramy lub karty i wybierz powiązanie przez NFC, USB albo zgodną kopię.
2. Wybierz wzór i źródło. Dla NFC użyj Cuvex Mirror połączonego z komputerem przez Bluetooth, a dla Cuvex BIT woluminu podłączonego przez USB-C. Cuvex Desktop nie obsługuje zewnętrznych czytników NFC na USB.
3. Sprawdź alias, pochodzenie, rozmiar, format i zinterpretowane warunki w szczegółach. To metadane, nie odszyfrowana treść.
4. Sprawdź zachowane konta oczekujące na powiązanie i połącz tylko zweryfikowane konto.
5. W razie braków kopii wyeksportuj egzemplarz i osobno przetestuj odzyskanie.

Wynik: obiekt uporządkowany lokalnie. „Powiązany” nie dowodzi uwierzytelnienia frazy ani salda. Przy nierozpoznanym obiekcie sprawdź format i wersję, bez zmiany rozszerzenia lub kasowania danych w celu wymuszenia akceptacji.

P11 | Aktywacja konta obserwacyjnego WOW | Desk i Cuvex | L13,L22 | C01,C02

Przygotowanie: dane publiczne uzyskane w procedurze urządzenia i prywatnie sprawdzone pochodzenie.

1. Otwórz aktywację WOW lub dodanie konta z właściwego kryptogramu.
2. Zaimportuj deskryptor lub obsługiwane dane publiczne z pliku, kamery internetowej albo Mirror, zależnie od funkcji.
3. Sprawdź sieć, skrypt, pochodzenie, odcisk, ścieżkę i, gdzie dotyczy, sumę kontrolną. Nie wpisuj frazy seed ani xprv.
4. Nazwij konto i świadomie zatwierdź wybór źródła zapytań.
5. Przed interpretacją salda sprawdź adres kontrolny i zakres odkrywania adresów.

Wynik: powiązany portfel obserwacyjny. Przy zerowym saldzie sprawdź sieć, pierwotne hasło dodatkowe, wyprowadzanie, konto, dostawcę i skan bez wnioskowania o utracie monet. Ogólna obsługa sieci przez interfejs nie musi dotyczyć profilu wielopodpisowego. Uwzględniaj kontekst.

P12 | Konfiguracja węzła i synchronizacji | Desk | L25,L33 | C02

Przygotowanie: decyzja dotycząca prywatności i, przy Core, dostęp do zabezpieczonego i zsynchronizowanego węzła.

1. W sekcji bezpieczeństwa oraz „Prywatność i węzły” wybierz konto WOW i sprawdź jego dostawcę.
2. Wybierz wyraźnie zgodnego publicznego dostawcę albo Core. Dla Core wpisz punkt końcowy, portfel i dane uwierzytelniające tylko w aplikacji.
3. Autoryzuj zapytanie, rozumiejąc dane otrzymywane przez każdą usługę. TLS nie ukrywa zapytania przed dostawcą.
4. Zsynchronizuj i sprawdź datę, wierzchołek łańcucha, postęp i pełny stan. Przy ponownym skanie sprawdź zakres historyczny i ciągłość pracy.
5. Przy 429 respektuj przerwę. Po błędzie nie zakładaj włączenia innego węzła. Konfiguracja nie przełącza się po cichu.

Wynik: znane źródło i stan. Nie udostępniaj RPC w internecie, nie podawaj hasła i nie ograniczaj odkrywania do adresów z dodatnim saldem. Pusta historia może być wynikiem częściowym.

P13 | Generowanie i odszukiwanie żądania płatności | Desk i Cuvex | L26 | C01,C02

Przygotowanie: sprawdzone konto, sieć i polityka.

1. Otwórz odbiór i utwórz albo odszukaj właściwe żądanie.
2. Dodaj obserwatora, cel i oczekiwaną kwotę tylko wtedy, gdy potrzebujesz tych lokalnych metadanych.
3. Przed istotnym wpływem sprawdź adres obsługiwaną ścieżką urządzenia. Przy braku fizycznego odbioru pozostań przy symulacji.
4. Przekaż wyłącznie potrzebne dane uwierzytelnionym kanałem odbiorcy.
5. Sprawdź wpływ, kwotę i potwierdzenia w swoim źródle sieciowym.

Wynik: uzgodniony wpływ, a nie tylko wystawione żądanie. W wielopodpisie pokazane adresy pozostają dostępne dla późniejszych płatności i nie są przydzielane ponownie. Po osiągnięciu limitu nowych adresów bez historii odszukaj wcześniejsze żądania. Nie wymuszaj indeksów ręcznie.

P14 | Etykiety, zamrażanie i BIP329 | Desk | L27 | C02,B13

Przygotowanie: konto laboratoryjne z UTXO i hasło do chronionego eksportu.

1. Opisz wejście jego kontekstem bez zbędnych danych osobowych.
2. Świadomie zamroź lub odmroź i sprawdź saldo dostępne do wydania. Ograniczenie jest lokalne.
3. Wyeksportuj etykiety za pomocą chronionej funkcji. Odróżnij format BIP329 od szyfrowania pliku.
4. Zaimportuj do zgodnej kopii i sprawdź zgodność odwołań, etykiet i zamrożeń.
5. Zachowaj aktualną kopię metadanych i jej hasło zgodnie ze swoim planem.

Wynik: zachowany kontekst i zrozumiany wybór. Import nie powinien automatycznie odmrażać monet bez kontroli. Nie wysyłaj tutorowi pliku etykiet. Może ujawniać kontrahentów i powiązania mimo braku kluczy wydawania.

P15 | Przygotowanie płatności i wysłanie całości | Desk | L28 | C02

Przygotowanie: zweryfikowane żądanie i konto z wystarczającymi dostępnymi wejściami.

1. Otwórz płatność z WOW, UTXO lub czatu i potwierdź konto oraz sieć.
2. Wybierz wejścia, odbiorców i kwoty. Sprawdź, które konteksty zostaną powiązane.
3. Wybierz stawkę i sprawdź bezwzględną opłatę, resztę oraz ostrzeżenia. Przy dust przeanalizuj alternatywy bez akceptowania ukrytej opłaty.
4. Przy wysłaniu całości sprawdź kwotę netto po opłacie. Wyraźnie potwierdź na czacie częściową płatność, jeśli nie pokrywa żądania.
5. Przygotuj szkic i sprawdź wszystkie dane przed eksportem do podpisu.

Wynik: zrozumiała intencja i PSBT danej operacji. Ogólny formularz może dopuszczać więcej wejść lub odbiorców niż sprzęt. Stosuj rzeczywiste limity podpisującego i transportu. Zmiana wyjść lub warunków rozpoczyna nową weryfikację.

P16 | Podpisanie i zwrócenie PSBT za pomocą Original | Original i Mirror | L29 | C01,C02,C03

Przygotowanie: właściwy szkic, zgodna karta transportowa, zgodny uwierzytelniony kryptogram i prywatne środki odblokowania. Stara kopia bez zweryfikowanej autentyczności może wymagać sprawdzonego odzyskania i utworzenia nowej przed podpisem. Edycja nagłówka tego nie naprawi.

1. Wyeksportuj żądanie zgodną ścieżką NFC z Desk/Mirror.

2. Przenieś je do Original. Podaj kryptogram na żądanie i odblokuj bez dyktowania danych.
3. Sprawdź sieć, podsumowanie, całe wyjścia, opłatę, resztę i wymagane ostrzeżenia.
4. W wielopodpisie Final zdecyduj o przeglądzie rozszerzonych parametrów. Wykonaj trzy końcowe potwierdzenia tylko przy pełnej zgodności.
5. Poczekaj na zapis i ponowny odczyt odpowiedzi na karcie.
6. Odczytaj odpowiedź za pomocą Cuvex Mirror i zweryfikuj ją w odpowiedniej operacji Desk.

Wynik: podpis odebrany i powiązany ze szkicem, nadal odrębny od publikacji. Po błędzie zapisu zachowaj stan i ponów według procedury. Nigdy nie używaj karty z kopią jako zbędnego nośnika płatności.

P17 | Podpisywanie, odbiór i potwierdzenie z BIT | BIT i Desk | L29 | C01,C02

Przygotowanie: właściwy szkic, zgodny uwierzytelniony kryptogram i wybrany rzeczywisty wolumin BIT. Jeśli stara kopia zostanie odrzucona przy podpisie, przeprowadź wskazane odzyskanie i odnowienie, nie wymuszając formatu.

1. Przekaż żądanie przez USB-C usługą Desk i postępuj zgodnie z ekranem urządzenia dla kryptogramu.
2. Odblokuj prywatnie i sprawdź podsumowanie, wszystkie wyjścia, opłatę oraz ostrzeżenia.
3. W wielopodpisie Final opcjonalnie sprawdź rozszerzone szczegóły i autoryzuj wymaganymi końcowymi potwierdzeniami.
4. W Desk użyj „Odbierz z BIT”, by zaimportować i zweryfikować odpowiedź dotyczącą tej pracy.
5. Sprawdź zapis i pokwitowanie. Przy błędzie pokwitowania po odbiorze ponów tę samą operację, nie nową dobraną według modelu.

Wynik: sprawdzony podpis i spójny stan wymiany. Przy odłączeniu przed odbiorem lub po zapisaniu zachowaj profil żądania. Nie przełączaj na inne firmware z katalogu w celu dopasowania oczekującej odpowiedzi.

P18 | Finalizowanie, publikacja i śledzenie operacji | Desk | L30,L44 | C02

Przygotowanie: zweryfikowane podpisy i, gdzie dotyczy, osiągnięty próg.

1. Ponownie sprawdź intencję, wejścia, wyjścia, opłatę i sieć.
2. Sfinalizuj odpowiednim działaniem i sprawdź komplet podpisów i warunków.
3. Autoryzuj rozesłanie i zachowaj wynik lokalny. Jeśli zginie odpowiedź sieciowa, sprawdź stan przed ponowieniem.

4. Obserwuj mempool i potwierdzenia u wybranego dostawcy z datą synchronizacji.
5. Przy rozważaniu RBF sprawdź nową operację i uzyskaj wymagane podpisy. Nie zakładaj wbudowanej funkcji CPFP.

Wynik: stan łańcucha sprawdzony z jego źródłem. Anulowanie szkicu nie unieważnia wyeksportowanych podpisów ani nie przepisuje potwierdzonych płatności. Wiadomość na czacie i zrzut nie zastępują śledzenia.

P19 | Dowolne porównywanie dwóch kodów QR polityki | Mirror | L43 | C03,C02

Przygotowanie: pole widoczne w Desk i Cuvex. W ćwiczeniu używaj wyłącznie syntetycznych przykładów kursu.

1. Otwórz „Porównaj polityki” i odczytaj najpierw dowolną stronę.
2. Wybierz sprawdzaną wartość. Możesz zacząć od kroku 15 i pominąć inne pola sprawdzone ręcznie.
3. Odczytaj odpowiednik i sprawdź oba teksty w całości. Przy niejednoznacznym kroku użyj „Podaj krok Desk”. Ten kontekst podaje się ręcznie.
4. Odnoś „Zgodne” lub „Niezgodne” tylko do tej dosłownej pary. Liczą się spacje, wielkość liter i kodowanie.
5. Zacznij inną parę w dowolnej kolejności. Wyjdź lub przejdź w tło zgodnie ze sprawdzonym mechanizmem kasowania.

Wynik: pojedyncze porównanie lokalne. Nie potwierdza pochodzenia, sesji, globalnego zatwierdzenia ani aktywacji. Wyjaśnij różnicę u źródeł bez normalizowania tekstu w celu wymuszenia OK.

P20 | Aktywacja, odzyskanie i przeniesienie czatu | Desk i Cuvex | L36,L39 | C02

Przygotowanie: wybrane środowisko DEV lub produkcyjne, alias i klucz czatu na urządzeniu, nigdy w kursie.

1. Otwórz aktywację lub odzyskiwanie czatu z kontekstu kryptogramu.
2. Wybierz nowy alias albo przeniesienie istniejącego i zgodny profil mobilny wskazany przez aplikację.
3. Wprowadź lub odczytaj klucz czatu wyłącznie w prywatnej procedurze. Nie używaj frazy seed, PIN-u ani klucza WOW.
4. Sprawdź aktywację w usłudze. Jeśli oczekuje, użyj funkcji dokończenia lub kontroli, nie zakładając powodzenia.
5. Po przeniesieniu zweryfikuj ciągłość z kontaktami i unikaj jednoczesnego użycia tego samego aliasu na kilku urządzeniach.

Wynik: tożsamość aktywowana lub odtworzona we właściwym środowisku. Dawna historia i sesje nie są automatycznie odzyskiwane kluczem czatu ani pełną kopią Desk. Uwzględnij ograniczenia dostępnego materiału.

P21 | Weryfikacja tożsamości kontaktu | Desk | L36,L48 | C02

Przygotowanie: niezależny kanał wcześniej uzgodniony z daną osobą.

1. Dodaj alias i odczytaj jego publiczną tożsamość w aplikacji.
2. Porównaj odcisk przez uwierzytelniony kanał, nie tylko w nowo utworzonej rozmowie.
3. Przy pytaniach rozpoznawczych unikaj publicznych informacji i sekretów używanych w innych usługach.
4. Potwierdź dopiero po wyjaśnieniu różnic. Po zmianie tożsamości wstrzymaj płatności i koordynację do weryfikacji.
5. Udokumentuj metodę weryfikacji bez zapisywania wrażliwych odpowiedzi w kursie.

Wynik: zaufanie do kontaktu w danym kontekście, nie gwarancja wszystkich przyszłych żądań. Głos można naśladować, a prawdziwe urządzenie przejąć. Każda operacja nadal wymaga weryfikacji.

P22 | Proszenie o adres, żądanie płatności i płacenie z czatu | Desk i Cuvex | L37 | C02,C01

Przygotowanie: zweryfikowany kontakt i zgodne konto WOW.

1. Zależnie od intencji wybierz prośbę o adres, odpowiedź adresem lub żądanie płatności.
2. Przed wysłaniem sprawdź pierwotne żądanie, sieć, kwotę i notatkę.
3. Aby zapłacić, otwórz przygotowanie z właściwego konta, wybierz UTXO i stawkę oraz sprawdź kwotę netto.
4. Autoryzuj na Cuvex procedurą swojego modelu. Czat nie podpisuje automatycznie.
5. Śledź publikację i potwierdzenie w swoim źródle. Uzgodnij jawnie określone płatności częściowe z pierwotnym żądaniem.

Wynik: koordynacja z zachowaniem weryfikacji pieczy. Stan wiadomości i transakcji nie są równoważne. Link do eksploratora może przekazać dane stronie trzeciej. Oceń użycie przed otwarciem.

P23 | Udostępnianie i powiązanie otrzymanego kryptogramu | Desk | L38 | C02

Przygotowanie: konkretna potrzeba udostępnienia, zweryfikowany kontakt i określone środki dostępu, które otrzyma.

1. Wybierz udostępnienie kryptogramu z działania czatu i sprawdź obiekt.
2. Nie dołączaj haseł, frazy seed ani klucza czatu jako komentarza.
3. Odbiorca sprawdza pochodzenie i wiąże zgodny obiekt za pomocą działania odbioru.
4. Oceń, co może zrobić teraz i co będzie mógł zrobić po zdobyciu wystarczających danych odblokowania.
5. Zachowaj realistyczny plan odebrania dostępu. Kasowanie wiadomości nie wycofuje zewnętrznych kopii ani poznanych kluczy.

Wynik: świadome przekazanie zaszyfrowanego obiektu. Nie jest to płatność ani dodanie klucza do wielopodpisu. Jeśli załącznik odsyła do nieznanej strony w celu odszyfrowania, zatrzymaj proces.

P24 | Pełna kopia i przywracanie Desk | Desk | L15,L21 | C02

Przygotowanie: magazyn szkoleniowy i kontrolowane miejsce docelowe kopii.

1. Otwórz funkcję kopii magazynu i ustaw wskazane hasło. Zachowaj powiązanie z tym konkretnym egzemplarzem.
2. Przechowuj kopię poza jedynym używanym urządzeniem. Sprawdź pochodzenie i integralność właściwą procedurą.
3. Odtwórz w osobnym środowisku testowym i sprawdź konta, konfigurację oraz objęte dane.
4. Sprawdź wyłączenia. Nie zakładaj objęcia czatu, jego sesji i historii. Polityka wielopodpisu i klucze prywatne nie są zamienne.
5. Powtarzaj po istotnych zmianach i zachowaj instrukcje odzyskiwania.

Wynik: kopia o znanym zakresie i haśle. Stare kopie zachowują wcześniejsze hasła. Przy zmianie dostępu lub ujawnieniu oceń również te kopie. Sama zmiana bieżącego magazynu nie wystarcza.

P25 | Tworzenie i przyjmowanie wielopodpisu | Desk i Cuvex | L41,L42 | C01,C02

Przygotowanie: niezależni uczestnicy, zweryfikowane kontakty, uzgodniona sieć i rzeczywiste limity.

1. Twórca wybiera nazwę, M/N, sieć, uczestników i okres ważności operacyjnej.
2. Przekaż właściwy rozszerzony klucz publiczny z odciskiem i ścieżką BIP48 obsługiwaną procedurą.
3. Każdy uczestnik sprawdza, przyjmuje lub odrzuca i przekazuje swój publiczny materiał. Nigdy nie udostępnia frazy seed.
4. Zbuduj pełną politykę i przygotuj weryfikację na każdym urządzeniu.
5. Przed wpłatą zachowaj kopie polityki. Sprawdź adres kontrolny i możliwość odtworzenia.

Wynik: kompletna i sprawdzalna propozycja. Przyjęcie zaproszenia nie zastępuje kontroli sprzętowej. Przy udziale Original obowiązuje limit sześciu kluczy i pojemność NFC. BIT nie rozszerza możliwości pozostałych uczestników.

P26 | Weryfikacja polityki i odbiór potwierdzenia | Desk i Cuvex | L43 | C01,C02,C03

Przygotowanie: ta sama pełna polityka dla wszystkich, właściwy profil firmware i urządzenie bez konkurencyjnych operacji.

1. Rozpocznij weryfikację polityk we właściwym kontekście. Original wymaga jawnego wyboru zainstalowanego profilu, a BIT negocjuje możliwości zgodnie ze swoją specyfikacją.
2. Przekaż żądanie zależnie od modelu przez NFC/Mirror lub USB-C.
3. Sprawdź pola polityki na urządzeniu. Opcjonalnie użyj Mirror do porównania wybranych par bez narzuconej kolejności.
4. Dokończ potwierdzenie na urządzeniu i zwróć odpowiedź właściwym transportem.
5. W Desk zweryfikuj odpowiedź powiązaną z żądaniem. Nie zastępuj tego wizualnym OK porównywarki.

Wynik: skojarzone sprawdzenie o zakresie ograniczonym do tej weryfikacji. Katalog nie poświadcza zdalnie firmware, a urządzenie nie jest przedstawiane jako trwały magazyn polityk. Przy FIRMWARE_CAPABILITY_REQUIRED najpierw sprawdź wersję Desk oraz kombinację modelu i kompilacji.

P27 | Żądanie i odbiór podpisów oraz przekazywanie koordynacji | Desk i Cuvex | L44 | C01,C02

Przygotowanie: sprawdzona polityka, rozpoznana operacja i uzgodnieni odbiorcy.

1. Przygotuj wejścia, wyjścia, opłatę i notatki. Poproś zgodnych uczestników o podpisy.
2. Każdy uczestnik weryfikuje i podpisuje na swoim urządzeniu ścieżką jego transportu.
3. Odbierz, zweryfikuj i zachowaj każdy podpis. Rozwiąż sprawę oczekujących potwierdzeń bez zmiany zapisanego profilu.
4. Po przekazaniu koordynacji odbiorca przyjmuje procedurę i sprawdza stan. Nie zmienia to M/N ani własności kluczy.
5. Po osiągnięciu progu sprawdź i sfinalizuj przed publikacją. Śledź transakcję w sieci.

Wynik: koordynacja z rozróżnionymi dowodami. Raport postępu koordynatora nie stanowi twojej lokalnej weryfikacji. Anulowanie lub odmowa w aplikacji nie musi zniszczyć podpisów już zachowanych przez innych.

P28 | Eksport, odtworzenie i lokalne usunięcie wielopodpisu | Desk | L45 | C02

Przygotowanie: znana polityka i zaszyfrowana kopia z unikalnym hasłem.

1. Wyeksportuj materiał odzyskiwania funkcją Desk. Obecna procedura używa do tego uwierzytelnionego kontenera CVXMSBK1.
2. Przechowuj kopię i hasło przy niezależnych zagrożeniach. Nie wnioskuj o szyfrowaniu starszych plików z samego rozszerzenia.
3. Do odtworzenia podaj kopię, hasło i klucz publiczny uczestnika o właściwym pochodzeniu, w razie potrzeby kamerą internetową lub przez Mirror.
4. Przed działaniem sprawdź politykę, sieć, adres i odkrywanie.
5. Przed lokalnym usunięciem przeczytaj zakres i potwierdzenie. Zachowaj kopię, jeśli chcesz móc odtworzyć stan. Późniejsze przywrócenie wymaga jawnego działania.

Wynik: odtwarzalna polityka lub świadome lokalne usunięcie. Usunięcie nie przenosi środków, nie kasuje kluczy pozostałych podpisujących ani samo nie anuluje operacji zachowanych przez innych.

P29 | Awaryjne odzyskiwanie na komputerze | Desk | L47 | C02

Przygotowanie: materiał w obsługiwanym formacie, przygotowane czyste środowisko i kopia. Operacja może ujawnić komputerowi sekret. W kursie używaj danych ćwiczeniowych.

1. Rozpocznij odzyskiwanie lokalne z właściwego kontekstu. Przeczytaj ograniczenia formatu i ostrzeżenia.
2. Świadomie zaakceptuj ryzyko i odłącz sieć zgodnie z procedurą. Okno sprawdza stan przed umożliwieniem kontynuacji.
3. Wpisz tylko potrzebne dane w prywatnym oknie. Nie dyktuj ich, nie wklejaj w kursie i nie podawaj wsparciu.
4. Włącz podgląd wyłącznie bez kamer i nasłuchujących asystentów. Przestrzegaj limitu czasu i zamknięcia.
5. Zakończ, oceń możliwe ujawnienie i w razie potrzeby zaplanuj migrację na nowe klucze.

Wynik: wyjątkowe odzyskanie, bez gwarancji usunięcia odpornego na analizę śledczą czy równoważności z izolowanym sprzętem. Przy braku uwierzytelnienia, formatu lub materiału dostępu nie testuj narzędzi z internetu na rzeczywistej kopii.

P30 | Przegląd preferencji, biometrii i blokady | Desk | L40 | C02

Przygotowanie: znane hasło i przetestowana kopia przed zmianą zabezpieczeń.

1. W „Dostęp i blokada” sprawdź hasło, dostępną biometrię, bezczynność i blokowanie po przejściu w tło.
2. Przed zmianą poznaj opóźnienie po błędach i skonfigurowane maksimum.
3. Nie włączaj opcjonalnego kasowania, dopóki nie rozumiesz warunków, progu i odzyskiwania. Nie testuj go produkcyjnie.
4. W preferencjach dopasuj język, motyw, walutę, synchronizację co 3 lub 5 minut oraz dźwięki.
5. Przy rejestracji linków bitcoin: sprawdź, czy otwarcie żądania zachowuje odblokowanie, wybór i weryfikację. Sam link nie płaci.

Wynik: zrozumiana konfiguracja. Biometria systemu zależy od urządzenia i nie zastępuje hasła ani kopii. Preferencje wizualne nie zmieniają polityki Bitcoin.

P31 | Usuwanie wpisów z uwzględnieniem zakresu | Desk | L22,L45 | C02

Przygotowanie: ustal, czy usuwasz lokalny kryptogram, konto, WOW, czat czy wielopodpis i którą kopię zachowasz.

1. Sprawdź wybrany obiekt i ostrzeżenie. Na żądanie aplikacji potwierdź dokładny alias lub jawny warunek.
2. Wyeksportuj i przetestuj kopię, jeśli później potrzebujesz odtworzyć stan.
3. Usuń tylko zamierzony obiekt. Sprawdź, które powiązania procedura zachowuje lub usuwa.
4. Sprawdź pozostałe operacje lub zewnętrznych uczestników. Nie zakładaj zniknięcia wiadomości, podpisów czy plików na innych urządzeniach.
5. Udokumentuj zmianę w prywatnym spisie bez danych wrażliwych w kursie.

Wynik: świadomie zarządzany stan lokalny. Żadne z tych działań samo nie zmienia skryptów UTXO ze środkami, nie niszczy frazy znanej innym ani nie cofa potwierdzonych transakcji.

P32 | Diagnozowanie bez ujawniania sekretów | Desk i Mirror | L23,L30,L48 | C02,C03

Przygotowanie: zapisz przybliżony czas, system, architekturę, wersję i fazę. Nie ponawiaj wciąż wrażliwej operacji bez znajomości stanu.

1. Przypisz usterkę do wyszukiwania, parowania, odczytu, zapisu, walidacji, podpisu, powrotu, sieci lub wyświetlania.
2. Skopiuj kod i treść błędu bez QR i prywatnych danych. W razie potrzeby użyj diagnostyki aplikacji.
3. Sprawdź plik przed udostępnieniem. Nie załączaj kopii magazynu, kryptogramu, frazy seed, klucza czatu, deskryptora ani danych dostępu RPC.
4. Przy błędzie interfejsu zapisz rozmiar okna, powiększenie i ukryte elementy sterujące na syntetycznym przykładzie.
5. Przekaż oficjalnym kanałem oczekiwany wynik i odtwarzalne kroki. Kurs nie wysyła zgłoszeń do wsparcia automatycznie.

Wynik: raport umożliwiający zbadanie sprawy na podstawie minimalnych danych. Przy braku dowodu etapu wpisz „oczekuje”, nie „ukończony”. Wsparcie głosowe nie wymaga zdalnego dostępu do urządzenia przechowującego sekrety.

Słownik Bitcoina i samodzielnego przechowywania

Bitcoin

Sieć i zbiór reguł do przekazywania wartości i weryfikacji jej historii bez jednego administratora rejestru.

BTC

Jednostka pieniężna Bitcoina. Jeden BTC to sto milionów satoshi.

Satoshi

Jednostka łańcucha bazowego równa jednej stumilionowej BTC.

Blockchain

Historia powiązanych bloków weryfikowanych według określonych reguł. Sam termin nie opisuje wszystkich cech sieci.

Blok

Zbiór danych obejmujący transakcje i nagłówek podlegający weryfikacji.

Pełny węzeł

Oprogramowanie sprawdzające reguły dla przyjmowanych bloków i transakcji.

Wydobycie

Budowanie bloków za pomocą dowodu pracy zgodnie z regułami sieci.

Dowód pracy

Mechanizm wymagający sprawdzalnej pracy obliczeniowej przy proponowaniu bloku.

Konsensus

Zgodność uczestników co do reguł i akceptowanej prawidłowej historii.

Polityka mempoola

Lokalne reguły przyjmowania i przekazywania transakcji, które nie muszą być regułami konsensusu.

Mempool

Lokalny zbiór niepotwierdzonych transakcji przechowywanych przez węzeł.

Potwierdzenie

Włączenie do bloku akceptowanego łańcucha i późniejsza głębokość tego bloku.

Reorganizacja

Zmiana fragmentu akceptowanego łańcucha, która może wpłynąć na potwierdzenia.

UTXO

Niewydane wyjście transakcji, które można wydać po spełnieniu jego warunków.

Wejście

Odwołanie do wcześniejszego wyjścia i dane potrzebne do autoryzacji jego wydania.

Wyjście

Wartość i warunek wydania utworzone przez transakcję.

Reszta

Wyjście zwracające pod własną kontrolę część wartości wejść pozostałą po płatności i opłacie.

Opłata

Różnica między wartością wejść i wyjść transakcji.

vbyte

Jednostka rozmiaru wirtualnego służąca do wyrażania względnego kosztu transakcji.

sat za vbyte

Stawka opłaty w satoshi za jednostkę rozmiaru wirtualnego.

Dust

Małe wyjście według polityki i kosztu wydania. Próg zależy od kontekstu i skryptu.

RBF

Zastąpienie niepotwierdzonej transakcji zgodnie ze zgodnymi politykami. Anulowanie nie jest gwarantowane.

CPFP

Użycie transakcji potomnej do zwiększenia zachęty do jej włączenia razem z transakcją nadrzędną.

Skrót

Odcisk danych przydatny do weryfikacji integralności. Nie szyfruje i sam nie identyfikuje autora.

Klucz prywatny

Środek kryptograficzny pozwalający tworzyć upoważnienia według danego schematu.

Klucz publiczny

Dane pozwalające sprawdzać podpisy i tworzyć pewne warunki bez ujawniania klucza prywatnego.

Podpis cyfrowy

Kryptograficzny dowód autoryzacji konkretnej wiadomości. Nie ukrywa treści.

Szyfrowanie

Ochrona poufności za pomocą klucza i algorytmu.

Szyfrowanie uwierzytelnione

Szyfrowanie z kontrolą modyfikacji przewidzianą w jego konstrukcji.

AES GCM

Rodzina metod szyfrowania uwierzytelnionego stosowana w formatach tego środowiska. Jej właściwości zależą od implementacji i sposobu postępowania z kluczami.

Mnemonik

Słowne przedstawienie materiału generacyjnego i kontrolnego według określonego formatu.

Seed

Materiał, z którego wyprowadza się klucze. Potocznie termin oznacza również słowa, dlatego trzeba określić kontekst.

Entropia

Nieprzewidywalność materiału generacyjnego. Nie uzyskuje się jej przez wybieranie łatwych do zapamiętania słów.

Suma kontrolna

Wartość wykrywająca niektóre błędy. Nie uwierzytelnia autora.

BIP39

Specyfikacja mnemoników i wyprowadzania ziarna z opcjonalnym hasłem dodatkowym.

Dodatkowe hasło BIP39

Dodatkowe dane wejściowe do wyprowadzania. Inne hasło może dać inny prawidłowy i pusty portfel.

BIP32

Specyfikacja hierarchicznego wyprowadzania kluczy.

Ścieżka wyprowadzania

Sekwencja gałęzi używana do uzyskiwania kluczy z korzenia.

Wyprowadzanie utwardzone

Krok wyprowadzania oznaczany zwykle apostrofem lub literą h, o właściwościach innych niż zwykłe wyprowadzanie publiczne.

xpub

Rozszerzony klucz publiczny zawierający kontekst wyprowadzania. Wrażliwy z punktu widzenia prywatności.

xprv

Rozszerzony klucz prywatny. Nie należy go udostępniać ani importować do kursu.

Odcisk klucza głównego

Krótki identyfikator korzenia przydatny do kojarzenia danych. Sam nie jest wystarczającym dowodem tożsamości.

Deskryptor

Wyrażenie określające budowę skryptów z kluczy i ścieżek. Może być publiczne lub zawierać materiał prywatny.

Watch-only

Portfel obserwacyjny bez wystarczającego materiału prywatnego do samodzielnego podpisywania.

WOW

Nazwa kont obserwacyjnych i zarządzania portfelem w środowisku Cuvex.

Gorący portfel

Narzędzie umożliwiające podpisywanie w środowisku podłączonym do sieci.

Samodzielne przechowywanie

Model, w którym użytkownik zachowuje techniczną możliwość samodzielnego lub wspólnego wydania zgodnie z przyjętą polityką.

Powiernik

Podmiot kontrolujący możliwość wydawania na rzecz klienta i stosujący własne warunki dostępu.

Kryptogram Cuvex

Zaszyfrowany obiekt chroniący sekret. Sam nie jest transakcją ani saldem.

Hasło Desk

Zabezpiecza dostęp do lokalnego magazynu. Nie jest frazą seed ani hasłem kryptogramu.

Klucz czatu

Sekret odtwarzający tożsamość czatu. Może przypominać dane publiczne, lecz nimi nie jest.

PIN parowania

Tymczasowy kod sesji połączenia, odrębny od hasła do przechowywanych sekretów.

Air gap

Operacyjne odseparowanie środowisk. Przenoszone dane nadal wymagają weryfikacji.

NFC

Technologia komunikacji zbliżeniowej z kompatybilnymi kartami i czytnikami.

USB Mass Storage

Interfejs wymiany plików modelu BIT. Wymaga właściwego protokołu, weryfikacji i potwierdzeń.

PSBT

Kontener danych i podpisów służący do koordynowania budowania i autoryzacji transakcji.

PSBT v0

Wersja formatu z BIP174 stosowana w sprawdzonym profilu wielopodpisowym Final.

PSBT v2

Wersja z BIP370. Wersja 2 samej transakcji nie określa wersji kontenera.

SIGHASH ALL

Tryb określający zakres zobowiązania podpisu w sprawdzonym profilu. Weryfikacja operacji obejmuje jego zakres techniczny.

P2WPKH

Rodzaj warunku SegWit z jednym kluczem, zwykle związany z kontami BIP84.

P2WSH

Warunek SegWit wiążący skrypt, stosowany przez sprawdzony wielopodpis Final.

P2TR

Typ wyjścia Taproot. Obsługa go jako odbiorcy nie oznacza obsługi podpisania wydatku z niego.

sortedmulti

Konstrukcja wielopodpisowa o deterministycznej kolejności kluczy przy generowaniu skryptów.

Próg M z N

Liczba M wymaganych upoważnień spośród N uczestników według danej polityki.

MuSig2

Protokół agregacji Schnorra, którego podstawowy schemat to N z N. Nie jest dowolnym progiem.

Taproot

Zestaw mechanizmów wydawania i zobowiązań kryptograficznych Bitcoina ze ścieżkami klucza i skryptu.

Miniscript

Język opisu i analizy wybranych polityk skryptów. Nie został wdrożony w sprawdzonym profilu Final.

Regtest

Lokalna sieć ćwiczeniowa bez wartości ekonomicznej, kontrolowana przez organizatora środowiska.

Signet

Sieć testowa o własnych cechach, domyślnie niewymienna z regtest.

Mainnet

Sieć Bitcoin używana do rzeczywistych operacji o wartości ekonomicznej.

Gap limit

Kryterium odkrywania adresów na podstawie luki kolejnych adresów bez historii. Jego zakres zależy od portfela.

Coin control

Świadomy wybór UTXO przeznaczonych do wydania.

Konsolidacja

Łączenie wyjść w celu zmniejszenia rozdrobnienia, mające skutki dla kosztów i prywatności.

Pseudonimowość

Używanie identyfikatorów innych niż bezpośrednio imię i nazwisko. Nie oznacza automatycznej anonimowości.

Anonimowość

Zależna od kontekstu nierozróżnialność dla określonych obserwatorów. Etykieta aplikacji jej nie gwarantuje.

Metadane

Informacje o komunikacji lub aktywności, np. czasy, rozmiary i powiązania, odrębne od treści.

CoinJoin

Wspólne tworzenie transakcji utrudniające określone wnioskowanie bez gwarancji trwałej anonimowości.

Payjoin

Wspólna płatność z wejściami płatnika i odbiorcy według obsługiwanego protokołu.

Tor

Sieć i narzędzia chroniące połączenie. Użycie należy skonfigurować i sprawdzić osobno w każdej aplikacji.

VPN

Kanał przenoszący część zaufania do połączenia na operatora. Nie ukrywa łańcucha.

Lightning

System płatności kanałowych o wymaganiach i ryzyku odmiennych od płatności on-chain.

Invoice

Ustrukturyzowane żądanie płatności, którego format i tryb trzeba rozpoznać.

RPC

Interfejs wywołań usługi, np. Bitcoin Core. Wymaga uwierzytelniania i zabezpieczenia.

TLS

Ochrona transportu przed określonymi zagrożeniami. Serwer odbierający nadal widzi żądania.

SRTP

Ochrona dźwięku na określonych odcinkach VoIP. Nie zapewnia automatycznie tajemnicy względem operatora.

Idempotencja

Właściwość zapobiegająca powieleniu skutku po ponowieniu zidentyfikowanego żądania.

Webhook

Zdarzenie przesyłane między serwerami. Należy sprawdzić autentyczność i ewentualne powtórzenie.

RAG

Wyszukiwanie fragmentów wiedzy w celu oparcia odpowiedzi na kontekście i wersji.

Teach-back

Sprawdzenie zrozumienia przez poproszenie uczestnika o wyjaśnienie zagadnienia własnymi słowami.

Phishing

Oszustwo wykorzystujące podszywanie się i wiarygodny kontekst, by uzyskać dostęp lub skłonić do działania.

Socjotechnika

Manipulowanie ludzkimi decyzjami, które może wykorzystywać prawdziwe informacje i presję czasu.

Notaryzacja

Kontrola dystrybucyjna Apple odrębna od audytu produktu i fizycznego sprawdzenia wszystkich procedur.

Atestacja

Dowód stanu według konkretnego mechanizmu. Katalog zgodności Desk nie stanowi zdalnego pomiaru.

MiCA

Europejskie ramy dla określonych kryptoaktywów i usług. Nie gwarantują zysku ani pełnej rekompensaty.

Travel Rule

Obowiązki informacyjne dotyczące transferów objętych regulacją. Samodzielne przechowywanie nie pozwala ich obejść.

Punkt wznowienia

Miejsce wznowienia nauki z minimalnymi danymi, bez informacji o portfelu.

Sprawdź, co już potrafisz

Ćwicz bez prawdziwych środków. Sprawdzian jest ogólnodostępny i nie wymaga konta.

Kto upoważnia do wydania środków przy zwykłym użyciu Cuvex?

1. Urządzenie po sprawdzeniu przez użytkownika
2. Tutor głosowy
3. Serwer kursu

> **Pokaż odpowiedź: Urządzenie po sprawdzeniu przez użytkownika**
> Zatwierdzenie nadal odbywa się w Cuvex.

Ile satoshi to 0,001 BTC?

1. 1 000
2. 100 000
3. 1 000 000

> **Pokaż odpowiedź: 100 000**
> Jeden BTC to 100 000 000 sat.

Wejścia wynoszą 120 000 sat, a wyjścia 119 000 sat. Jaka jest opłata?

1. 1 000 sat
2. 119 000 sat
3. 1 sat/vB bez dodatkowych danych

> **Pokaż odpowiedź: 1 000 sat**
> Różnica wartości to bezwzględna wysokość opłaty.

Jaki status ma podpisana, lecz jeszcze nierozesłana transakcja?

1. Potwierdzona
2. Nieodwracalna dzięki podpisowi
3. Autoryzowana, ale niekoniecznie opublikowana

> **Pokaż odpowiedź: Autoryzowana, ale niekoniecznie opublikowana**
> Podpis i publikacja są oddzielnymi etapami.

Ile kosztuje 200 vB przy stawce 6 sat/vB?

1. 206 sat
2. 1 200 sat
3. 6% wysyłanej kwoty

> **Pokaż odpowiedź: 1 200 sat**
> Pomnóż rozmiar wirtualny przez stawkę.

Co trzeba sprawdzić przed wypłatą z giełdy?

1. Tylko najniższą opłatę
2. Zgodność aktywa, sieci, adresu i kwoty netto
3. Frazę seed drugiej strony

> **Pokaż odpowiedź: Zgodność aktywa, sieci, adresu i kwoty netto**
> Nie każda sieć z symbolem BTC to Bitcoin on-chain.

Co samodzielnie zapewnia podpis cyfrowy?

1. Ukrywa całą wiadomość
2. Autoryzuje wiadomość, którą można zweryfikować według reguł danego schematu
3. Kasuje opublikowane dane

> **Pokaż odpowiedź: Autoryzuje wiadomość, którą można zweryfikować według reguł danego schematu**
> Poufność wymaga innego mechanizmu.

Jaki skutek może mieć zmiana dodatkowego hasła BIP39?

1. Utworzenie innego prawidłowego i pozornie pustego portfela
2. Możliwość zresetowania go zawsze przez e-mail
3. Zmiana publicznego zapisu wcześniejszych płatności

> **Pokaż odpowiedź: Utworzenie innego prawidłowego i pozornie pustego portfela**
> Dodatkowe hasło uczestniczy w wyprowadzaniu kluczy.

Jak należy traktować xpub konta?

1. Jako dane bez żadnych konsekwencji
2. Jako identyczną prywatną frazę seed
3. Jako dane wrażliwe z punktu widzenia prywatności

> **Pokaż odpowiedź: Jako dane wrażliwe z punktu widzenia prywatności**
> Mogą rozszerzyć zakres obserwacji aktywności.

Dlaczego jedna fraza seed może nie wystarczyć w portfelu wielopodpisowym?

1. Brakuje polityki i upoważnień wymaganych przez próg
2. Bitcoin nie pozwala niczego odzyskać
3. Potrzebny jest oryginalny kolor aplikacji

> **Pokaż odpowiedź: Brakuje polityki i upoważnień wymaganych przez próg**
> Zachowanie polityki i zachowanie prywatnej możliwości podpisywania to odrębne wymagania.

Sprawdzony algorytm Final odrzucił wynik kości. Co robisz?

1. Powtarzam tylko rzut monetą aż do akceptacji
2. Powtarzam rzut monetą i wszystkimi czterema kośćmi
3. Wybieram znane słowo

> **Pokaż odpowiedź: Powtarzam rzut monetą i wszystkimi czterema kośćmi**
> Powtórzenie tylko części zestawu może zaburzyć rozkład wyników.

Co oznaczają dwa hasła otwierające frazę seed portfela z jednym podpisem?

1. Dwa wymagane klucze w łańcuchu
2. Wielopodpis Taproot
3. Próg dostępu do sekretu odrębny od progu podpisów Bitcoin

> **Pokaż odpowiedź: Próg dostępu do sekretu odrębny od progu podpisów Bitcoin**
> Szyfrowanie nie zmienia skryptu.

Co trzeba uwzględnić przy ocenie pełnej kopii Desk?

1. Zawsze zawiera cały czat
2. Ma określony zakres i wyłączenia. Nie zakładaj, że obejmuje czat
3. Aktualizuje wszystkie stare kopie

> **Pokaż odpowiedź: Ma określony zakres i wyłączenia. Nie zakładaj, że obejmuje czat**
> Odtworzenie tożsamości i odtworzenie wiadomości to dwie różne czynności.

Co daje prawidłowo skonfigurowany własny węzeł?

1. Usuwa wszystkie wycieki
2. Ogranicza zależność od zapytań do stron trzecich i umożliwia samodzielną weryfikację
3. Odzyskuje utracone klucze

> **Pokaż odpowiedź: Ogranicza zależność od zapytań do stron trzecich i umożliwia samodzielną weryfikację**
> Nie gwarantuje anonimowości ani odzyskania sekretów.

Co oznacza zamrożenie UTXO w Desk?

1. Lokalne ograniczenie stosowane przez aplikację
2. Zmianę warunku konsensusu
3. Unieważnienie innych kopii frazy seed

> **Pokaż odpowiedź: Lokalne ograniczenie stosowane przez aplikację**
> Nie jest to ogólnoświatowa blokada wydania.

Podczas publikacji tracisz połączenie. Co robisz?

1. Natychmiast płacę ponownie
2. Kasuję portfel
3. Najpierw sprawdzam, czy płatność została już rozesłana

> **Pokaż odpowiedź: Najpierw sprawdzam, czy płatność została już rozesłana**
> Przekroczenie limitu czasu nie dowodzi braku skutku.

Co może spowodować ponowne używanie adresów lub łączenie UTXO z różnych kontekstów?

1. Ułatwić dostrzeżenie powiązań
2. Skasować historię
3. Zagwarantować anonimowość

> **Pokaż odpowiedź: Ułatwić dostrzeżenie powiązań**
> Prywatność zależy od kontekstu i dalszego użycia.

Czy uruchomienie Tor Browser automatycznie konfiguruje Desk?

1. Tak
2. Nie
3. Tylko przy ciemnym motywie

> **Pokaż odpowiedź: Nie**
> Trzeba sprawdzić drogę połączenia każdej aplikacji.

Czym jest klucz czatu przypominający xpub?

1. Informacją do publikacji
2. Adresem do odbierania płatności
3. Sekretem tożsamości

> **Pokaż odpowiedź: Sekretem tożsamości**
> O wrażliwości decyduje zastosowanie.

Co oznacza wiadomość „zapłacono” na czacie?

1. Zastępuje potwierdzenia
2. Wymaga niezależnego sprawdzenia płatności w sieci
3. Zmienia sieć wskazaną w żądaniu

> **Pokaż odpowiedź: Wymaga niezależnego sprawdzenia płatności w sieci**
> Stan wiadomości nie jest stanem płatności.

Czego używa sprawdzony profil wielopodpisowy Final?

1. MuSig2 i PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Dowolnego skryptu Bitcoin

> **Pokaż odpowiedź: P2WSH sortedmulti BIP48 PSBT v0**
> Życzenia i nazwy handlowe nie rozszerzają obsługi.

Od czego możesz rozpocząć porównanie w Mirror 12.12?

1. Wyłącznie od kroku 1
2. Od dowolnych wybranych danych, także pozycji 15
3. Tylko od ostatniej pozycji po przejściu wszystkich poprzednich

> **Pokaż odpowiedź: Od dowolnych wybranych danych, także pozycji 15**
> Każdą parę można porównywać niezależnie i w dowolnej kolejności.

Co poświadcza komunikat „Zgodne” w Mirror?

1. Zatwierdzenie całości
2. Autentyczne pochodzenie obu kodów QR
3. Dosłowną zgodność porównanej pary

> **Pokaż odpowiedź: Dosłowną zgodność porównanej pary**
> Pozostałe kontrole i odpowiedź wciąż wymagają wykonania.

Fraza seed została ujawniona. Co daje zmiana hasła Desk?

1. Odbiera napastnikowi dostęp
2. Nie unieważnia kluczy wyprowadzonych z tej frazy
3. Kasuje wszystkie kopie

> **Pokaż odpowiedź: Nie unieważnia kluczy wyprowadzonych z tej frazy**
> Trzeba ocenić sposób bezpiecznego przeniesienia kontroli.

Co należy wskazać na zakończenie szkolenia praktycznego?

1. Co przeczytano, zasymulowano i przetestowano fizycznie oraz co pozostaje do zrobienia
2. Tylko liczbę sprzedanych godzin
3. Obietnicę przechowywania odpornego na każde zagrożenie

> **Pokaż odpowiedź: Co przeczytano, zasymulowano i przetestowano fizycznie oraz co pozostaje do zrobienia**
> Poszczególne dowody mają różny zakres.