CUVEX

CUVEX ACADEMY · 0.1

Lernen. Verstehen. Selbst entscheiden.

Bitcoin und Selbstverwahrung Schritt für Schritt. Kurs, Handbuch, Glossar und Übungen sind kostenlos und ohne Anmeldung zugänglich. Du entscheidest, wo du einsteigst.

Kostenlos · ohne Anmeldung

Alle Abschnitte

1. Deinen Lernplatz einrichten
2. Digitales Geld und die Vertrauensfrage
3. Geschichte und Grenzen von Bitcoin
4. Satoshis und fehlerfreies Rechnen
5. Dein Bedrohungsmodell
6. Knoten, Mining und Konsens
7. UTXOs und Wechselgeld einer Transaktion
8. Mempool, Bestätigungen und Reorganisationen
9. Gebühren, virtuelle Größe und Ersetzung
10. Netzwerke, Adressen und Zahlungsanforderungen
11. Hash, Signatur und Verschlüsselung
12. Seed, Passphrase und Passwort
13. Schlüsselableitung, xpub und Deskriptoren
14. Eine Wallet und ein Verwahrungsmodell wählen
15. Wiederherstellbare Sicherungen
16. Original und BIT kennenlernen
17. Einen Seed mit physischer Entropie erzeugen
18. Ein Geheimnis mit Cuvex ver- und entschlüsseln
19. Verschlüsselungsschwellen und Biometrie
20. Kopien klonen, aufbewahren und prüfen
21. Cuvex Desk installieren und schützen
22. Kryptogramme verknüpfen und WOW verwalten
23. Mirror mit Desk koppeln
24. NFC über Mirror, USB-C und das Lesen von QR-Codes
25. Öffentliche Anbieter und eigener Knoten
26. Bitcoin empfangen und die Adresse prüfen
27. UTXOs kennzeichnen, einfrieren und auswählen
28. Eine Zahlung vorbereiten und prüfen
29. Mit Original und mit BIT signieren
30. Finalisieren, veröffentlichen und Störungen beheben
31. Was sich bei Bitcoin beobachten lässt
32. Kontexte trennen und Wechselgeld verwalten
33. Privatsphäre im Netz, Tor und VPN
34. CoinJoin, Payjoin und heutige Grenzen
35. Lehren aus dokumentierten Vorfällen

36. Chat-Identität erstellen und Kontakte prüfen
37. Im Chat Satoshis anfordern und bezahlen
38. Kryptogramme bewusst weitergeben
39. Chat wiederherstellen und Metadaten verstehen
40. Alltagseinstellungen und Berechtigungen prüfen
41. Eine Multisig-Wallet entwerfen
42. Einladungen erstellen und Schlüssel beitragen
43. Richtlinien mit Mirror in beliebiger Reihenfolge prüfen
44. Signaturen koordinieren und Multisig-Transaktionen veröffentlichen
45. Eine Multisig-Wallet wiederherstellen und ändern
46. Firmware planmäßig aktualisieren
47. Verlust, Defekt und Wiederherstellung im Notfall
48. Phishing, Support und Betrug per Stimme
49. Privatsphäre, Recht und persönliche Aufzeichnungen
50. Erbschaft, Kontinuität und jährliche Übung
51. Preis, Sparen und Fundamentalanalyse
52. Einen Anbieter für den Bitcoin-Kauf wählen
53. Konten, Aufträge und Ausführungskosten
54. Kerzencharts, Indikatoren und Verzerrungen der technischen Analyse
55. Margin, Futures und Automatisierung
56. Lightning und weitere Schichten
57. Taproot, MuSig2 und die Zukunft der Post-Quanten-Kryptografie
58. Interoperabilität und Unabhängigkeit vom Hersteller
59. Technisches Labor mit Regtest
60. Abschlussprojekt und Kontinuitätsplan
61. Handbuch für Lernende
62. Glossar zu Bitcoin und Selbstverwahrung
63. Prüfe, was du gelernt hast

M01

Deinen Lernplatz einrichten

Lernziel

Bereite den Kurs vor, lerne die drei Geräte zu unterscheiden und kläre, welche Daten du dem Tutor niemals mitteilst.

Grundlagen

Du lernst, Bitcoin eigenständig zu empfangen, zu verwahren, auszugeben und wiederherzustellen. Am Ende sollst du eine Entscheidung erklären können, bevor du sie freigibst. Du kannst den Kurs allein lesen. Die Sprachbegleitung erklärt, stellt Fragen und unterstützt dich. Dafür braucht sie weder Einblick in dein Vermögen noch Kontrolle über deine Geräte.

Cuvex schützt Geheimnisse und autorisiert Vorgänge auf seinem Display. Desk verwaltet am Computer Kryptogramme, Beobachtungswallets, Zahlungen und deren Koordination. Mirror ist eine lokale Brücke für unterstützte Vorgänge und dient zum Datenvergleich. Es ist weder Signiergerät noch eigenständige Wallet. Welcher Ablauf möglich ist, hängt von Modell und Version ab.

Nutze möglichst einen Bildschirm für den Kurs und einen für Desk. Halte Telefon und Cuvex bereit. Hast du nur einen Bildschirm, wechsle zwischen den Anwendungen und teile ihn während der Eingabe von Geheimnissen nicht per Videoanruf. Ein Gespräch darf vor Abschluss einer Übung enden. Eine Pause ist kein Misserfolg. Halte lediglich Lektionskennung, erreichten Schritt und aufgetretene Schwierigkeit fest.

Weder menschliche Kursleitung noch KI dürfen Seeds, BIP39-Passphrasen, Passwörter, den Chat-Schlüssel, PINs, private Dateien oder vollständige Kaufcodes erhalten. Auch xpub, echter Deskriptor und Adresse sind unnötig. Sie erlauben zwar keine Ausgabe, verraten aber Aktivitäten. Beschreibe Fehlermeldungen und nutze die fiktiven Labordaten.

Übung

1. Bestimme vor Ort Computer, Telefon und Cuvex-Modell. Notiere ihre Versionen in deinen privaten Unterlagen.
2. Trenne eine Lernumgebung ohne Guthaben von deiner echten Verwahrung. Importiere zum Üben keinen produktiv genutzten Seed.
3. Öffne diese Lektion und suche Pause, Hilfe und Glossar. Fordert jemand ein Geheimnis, brich den Kontakt ab.

Zeig, was du kannst

Erkläre, wer signiert, wer das Netzwerk abfragt und wer Daten transportiert. Du kannst weitergehen, wenn du die Rollen ohne Hilfe unterscheidest.

Häufige Frage

Muss ich täglich mit dem Tutor sprechen? Nein. Du kannst allein lernen, Sitzungen wiederholen und gezielt bei einem Ablauf Hilfe holen. Kurszugang und Guthaben des Sprachdienstes sind getrennte Ansprüche.

Hier kannst du pausieren

L01 abgeschlossen, Geräte identifiziert, keine Geheimnisse im Kurs erfasst.

Der Tutor möchte deine Seed-Phrase hören, um deine Abschrift zu überprüfen. Was tust du?

1. Ich diktiere sie langsam.
2. Ich lehne die Anfrage ab und prüfe den Seed ausschließlich in meiner sicheren Umgebung.
3. Ich sende nur die ersten Wörter.

> **Antwort anzeigen: Ich lehne die Anfrage ab und prüfe den Seed ausschließlich in meiner sicheren Umgebung.**
> Auch Teile eines Geheimnisses gehören niemals in den Unterricht.

M01

Digitales Geld und die Vertrauensfrage

Lernziel

Verstehe vor dem Öffnen einer Wallet, welches Problem Bitcoin lösen will.

Grundlagen

Ein Bankguthaben ist ein Eintrag, den ein Institut verwaltet. Es authentifiziert den Kunden, entscheidet über Überweisungen und führt die Bücher. Eine gewöhnliche digitale Datei lässt sich leicht kopieren. Wer ein Foto verschickt, kann ein Exemplar behalten. Damit eine digitale Einheit als Geld funktioniert, muss verhindert werden, dass sie doppelt ausgegeben wird.

Bitcoin verbindet Validierungsregeln, Signaturen und eine gemeinsame Transaktionshistorie. Statt einem einzigen Institut das gesamte Register anzuvertrauen, können unabhängige Teilnehmer jede Transaktion auf Einhaltung der Regeln prüfen. Knappheit beruht auf der fortdauernden Prüfung und Akzeptanz dieser Regeln, weder auf dem Bild einer Münze noch auf dem Börsenkurs.

Selbstverwahrung verschiebt die Verantwortung. Du kannst ohne Erlaubnis eines Verwahrers ausgeben. Vernichtest du alle Sicherungen oder signierst eine falsche Zahlung, kannst du diese Möglichkeit verlieren. Auch bei eigenständigem Handeln brauchst du Schutz, Abstimmung und zum Senden eine Verbindung. Geltende Pflichten bleiben bestehen.

Unterscheide Bitcoin als Netzwerk und Protokoll von der Währungseinheit BTC. Andere Netzwerke können ebenfalls von Blockchain sprechen und andere Eigenschaften haben. Auch ein Unternehmensversprechen mit der Bezeichnung „Bitcoin“ ist etwas anderes als ein Bitcoin-Ausgang unter deinen eigenen Schlüsseln.

Übung

1. Vergleiche Bankguthaben, Börsenguthaben und einen UTXO unter deinen Schlüsseln.
2. Notiere jeweils, wer eine Verfügung verhindern und wer bei vergessenem Zugang helfen kann.
3. Beschreibe, was beim Kopieren eines Fotos und beim Versuch passiert, denselben Ausgang zweimal auszugeben.

Zeig, was du kannst

Erkläre in eigenen Worten den Unterschied zwischen einem Guthaben und der Fähigkeit zu signieren. Fachbegriffe brauchst du nicht auswendig zu lernen.

Häufige Frage

Verschwinden bei der Selbstverwahrung alle Vermittler? Für Kauf, Abfragen oder Kommunikation kannst du Dienste nutzen. Entscheidend ist, welche Befugnisse sie behalten und welche Daten sie erhalten.

Hier kannst du pausieren

Bewahre deinen Vergleich der Verantwortlichkeiten ohne echte Kontonamen auf.

Welches Geldproblem löst eine digitale Signatur allein nicht?

1. Den Versuch zu unterbinden, denselben Ausgang zweimal auszugeben.
2. Die Autorisierung mit einem Schlüssel nachzuweisen.
3. Eine Änderung an der signierten Nachricht zu erkennen.

> **Antwort anzeigen: Den Versuch zu unterbinden, denselben Ausgang zweimal auszugeben.**
> Signaturen autorisieren. Regeln und Konsens legen die Reihenfolge unvereinbarer Ausgaben fest.

M01

Geschichte und Grenzen von Bitcoin

Lernziel

Ordne die Entstehung von Bitcoin ein und trenne historische Fakten von Werbeaussagen.

Grundlagen

Satoshi Nakamotos Schrift erschien 2008, das Netzwerk startete 2009. Sie schlug elektronisches Bargeld von Person zu Person vor und griff frühere Ideen zu Kryptografie, Arbeitsnachweisen und digitalem Geld auf. Um Software oder Transaktionen zu überprüfen, brauchst du Satoshis bürgerliche Identität nicht zu kennen.

Die Weiterentwicklung beruht nicht darauf, dass ein Unternehmen einseitig Regeln austauscht. Entwickler schlagen Änderungen vor und prüfen sie, Betreiber wählen Software, Miner bauen Blöcke. Nutzer und Dienste entscheiden, was sie akzeptieren. Diese Aufgabenverteilung kann zu Konflikten führen. Eine Abspaltung und ein Anwendungsupdate sind verschiedene Vorgänge.

Ein Knoten kann einen regelwidrigen Block trotz großer investierter Rechenarbeit ablehnen. Konsens ist keine einfache Abstimmung nach Anzahl der Computer. Tausende Kopien eines Knotens geben nicht automatisch mehr Entscheidungsgewalt. Auch eine Mining-Mehrheit erhält dadurch keinen privaten Schlüssel eines Nutzers.

Bitcoin hat bewusst gewählte Grenzen und Zielkonflikte, etwa bei Blockkapazität, Prüfaufwand, variablen Bestätigungszeiten und öffentlichem Register. Es gibt keine administrative Rückabwicklung und standardmäßig keine umfassende Vertraulichkeit. Zusätzliche Schichten und Anwendungen bedienen einzelne Anwendungsfälle und schaffen dafür neue Abhängigkeiten.

Übung

1. Ordne auf einer Zeitachse die erste Veröffentlichung, den Netzwerkstart, die Einführung von SegWit und die Aktivierung von Taproot ein. Prüfe die Daten vor der Veröffentlichung anhand von Quellen.
2. Ordne „Ein Unternehmen garantiert den Preis“, „Ein Knoten validiert“ und „Ein Miner schlägt einen Block vor“ Werbeversprechen oder technischen Funktionen zu.
3. Nenne einen Vorteil und einen Nachteil davon, dass kein Administrator Zahlungen rückgängig machen kann.

Zeig, was du kannst

Unterscheide Konsensregel, lokale Richtlinie und Unternehmensentscheidung. Deine Anwendung bildet nur einen Teil des Netzwerks.

Häufige Frage

Ändert neue Software immer die Geldregeln? Nein. Versionen beheben auch Fehler, verbessern die Leistung oder ändern lokale Richtlinien. Lies die Versionshinweise und prüfe die Kompatibilität.

Hier kannst du pausieren

Notiere eine überprüfbare Eigenschaft und eine Behauptung, die weitere Belege erfordert.

Ein Block enthält eine Ausgabe ohne gültige Autorisierung. Macht ihn eine Mehrheit der Miner gültig?

1. Ja, wenn sie über 51 % liegt.
2. Nur wenn die Börse es bekannt gibt.
3. Nein, für einen Knoten, dessen Regeln den Block ablehnen, bleibt er ungültig.

> **Antwort anzeigen: Nein, für einen Knoten, dessen Regeln den Block ablehnen, bleibt er ungültig.**
> Die kumulierte Arbeit wird nur zwischen Historien verglichen, die nach den Regeln des Knotens gültig sind.

M01

Satoshis und fehlerfreies Rechnen

Lernziel

Rechne BTC in Satoshis um und umgekehrt. Prüfe Beträge unabhängig vom Wechselkurs.

Grundlagen

Ein BTC entspricht 100.000.000 Satoshis. „sat“ ist eine Einheit derselben Währung. Auf der Basiskette sind Beträge ganze Satoshis. 0,001 BTC sind 100.000 sat, 0,00001000 BTC sind 1.000 sat. Das Dezimaltrennzeichen einer Oberfläche hängt von der Sprache ab. Ergänze Nullen nie nach Augenmaß.

Ein Kurs rechnet BTC zu einem bestimmten Zeitpunkt in eine Währung wie EUR oder USD um. An der Anzahl deiner Satoshis ändert er nichts. Besitzt du 100.000 sat und der Kurs ändert sich, bleibt die Zahl deiner Satoshis gleich. Desk zeigt zum Orientierungskurs Quelle und Datum. Veraltete Daten können trotz richtigen BTC-Guthabens zu einer falschen wirtschaftlichen Entscheidung führen.

Unterscheide bei Zahlungen Empfängerbetrag, Netzwerkgebühr und Gesamtausgabe. Sendest du 50.000 sat mit 600 sat Gebühr, sinkt der Wert deiner Wallet um 50.600 sat, sofern keine weiteren eigenen Ausgänge zu berücksichtigen sind. „Alles senden“ ergibt gewöhnlich einen Nettobetrag unter dem verfügbaren Guthaben, da die Gebühr gedeckt werden muss.

Die Kursbeispiele sind Rechenübungen, keine Marktpreise oder Gebührenempfehlungen. Prüfe vor dem Signieren Einheit, Netzwerk, Empfänger und Gesamtkosten auf dem vorgesehenen Display. Die Stimme kann „fünfzigtausend Satoshis“ sagen und gleichzeitig „50.000 sat“ anzeigen. Eine unklare Transkription darf nie den Betrag festlegen.

Übung

1. Rechne 250.000 sat in BTC um: 0,0025 BTC. Rechne 0,00025000 BTC um: 25.000 sat.
2. Berechne eine Zahlung von 75.000 sat mit 900 sat Gebühr. Insgesamt sind es 75.900 sat.
3. Verwende im Simulator 120.000 sat, sende 70.000 bei 1.000 sat Gebühr und prüfe, dass 49.000 sat Wechselgeld entstehen.

Zeig, was du kannst

Lies einen Betrag in BTC und sat vor und erkläre, welcher Wert die Gebühr enthält. Pausiere bei Unsicherheit.

Häufige Frage

Muss ich einen ganzen Bitcoin kaufen? Nein. Bruchteile sind möglich, vorbehaltlich der Mindestmengen und Kosten des Anbieters.

Hier kannst du pausieren

Bewahre nur deine Übungsergebnisse auf.

Du hast 80.000 sat und sendest alles bei 1.200 sat Gebühr. Wie viel erhält der Empfänger?

1. 80.000 sat.
2. 78.800 sat.
3. 81.200 sat.

> **Antwort anzeigen: 78.800 sat.**
> Ohne weitere Ausgänge erhält der Empfänger hier das verfügbare Guthaben abzüglich Gebühr.

M01

Dein Bedrohungsmodell

Lernziel

Wähle angemessene Maßnahmen gegen Verlust, Diebstahl, Täuschung und Datenoffenlegung.

Grundlagen

Sicherheit bedeutet, nach deiner Absicht handeln zu können. Privatsphäre bedeutet Kontrolle darüber, wer deine Daten und Beziehungen kennt. Verfügbarkeit bedeutet Zugriff bei Bedarf. Ein für alle unzugänglicher Tresor kann auch dich ausschließen. Eine besonders bequeme Kopie kann zu viel preisgeben.

Bestimme schützenswerte Werte, mögliche Angreifer und Unfälle. Zu den Werten zählen Schlüssel, Sicherungen, Verlauf, Aufbewahrungsorte und Identität deiner Kontakte. Risiken sind Schadsoftware, Phishing, Feuer, Vergessen, Zwang, Defekte, Tod und eigene Fehler. Kein einzelnes Werkzeug mindert sie alle gleichermaßen.

Erstelle eine einfache Matrix aus ungefährer Wahrscheinlichkeit, Auswirkung und konkreter Maßnahme. Ein langes Passwort erschwert das Erraten, korrigiert aber keinen betrügerischen Empfänger, den du selbst freigibst. Zwei Kopien in einer Tasche helfen nicht bei deren Verlust. Kontrolliert eine Person sämtliche Geräte und Sicherungen einer Multisig, bleibt ein gemeinsamer Ausfallpunkt möglich.

Auch Kurs und Tutor gehören zum Modell. Käufe, Gespräche, Verbindungszeiten und Lernfortschritt erzeugen möglicherweise Metadaten. Die Kurswebsite soll für individuellen Unterricht weder Adressen noch Guthaben erfragen. Auch wenn Desk oder Mirror keine herkömmliche Registrierung fordern, können Shop, Sprachanbieter oder abgefragte Dritte Aktivitäten sehen.

Übung

1. Notiere deine drei wichtigsten Risiken ohne Vermögensbeträge und genaue Standorte.
2. Lege für jedes Prävention, Erkennung und Wiederherstellung fest. Beispiel Kartenverlust: zwei getrennte Kopien, Bestandsliste und Wiederherstellungstest.
3. Unterscheide, welche Person oder welches System Kauf, Gespräch, Guthabenabfrage und öffentliche Transaktion beobachten kann.

Zeig, was du kannst

Begründe, welches konkrete Risiko deine nächste Maßnahme mindert. Vermeide Komplexität, die du nicht pflegen oder deinen Erben erklären kannst.

Häufige Frage

Bedeuten mehr Geräte immer mehr Sicherheit? Nur wenn sie gemeinsame Abhängigkeiten verringern und du die Wiederherstellung testen kannst. Zusätzliche Geräte erhöhen auch Wartungsaufwand und Verwechslungsgefahr.

Hier kannst du pausieren

Bewahre den Plan in deinen privaten Unterlagen auf. Vermerke im Kurs nur „Bedrohungsmodell überprüft“.

Welche Maßnahme mindert das Risiko, bei einem örtlichen Brand alle Kopien zu verlieren, am besten?

1. Die Kartenfarbe ändern.
2. Zwei Kopien in dieselbe Schublade legen.
3. Geprüfte Kopien an Orten mit voneinander unabhängigen Risiken aufbewahren.

> **Antwort anzeigen: Geprüfte Kopien an Orten mit voneinander unabhängigen Risiken aufbewahren.**
> Redundanz muss dem Vorfall standhalten, der das Original bedroht.

M02

Knoten, Mining und Konsens

Lernziel

Erkläre, was Knoten überprüfen und welche Aufgabe Mining hat.

Grundlagen

Ein vollständiger Knoten empfängt Blöcke und Transaktionen, prüft die Regeln und führt eine eigene Sicht der Kette. Er muss der Saldoanzeige einer Webseite nicht vertrauen. Beim Mining werden mittels Arbeitsnachweis Blöcke vorgeschlagen. Miner wählen gültige Transaktionen aus und wetteifern darum, einen zulässigen Block zu finden.

Der Arbeitsnachweis macht das Umschreiben der Historie teuer. Bei mehreren gültigen Alternativen zählt die kumulierte Arbeit. Die bloße Blockanzahl berücksichtigt die Schwierigkeit nicht. Blockabstände schwanken. Zehn Minuten sind ein angestrebter Durchschnitt und kein Termin für die nächste Zahlung.

Die Mining-Vergütung besteht aus Blocksubvention und Gebühren. Die Subvention sinkt nach einem an Blockhöhen gebundenen Zeitplan. Gebühren stammen aus den aufgenommenen Transaktionen. Eine höhere Gebühr heilt keine ungültige Signatur. Ökonomische Sicherheit und Angriffskosten machen eine neue Zahlung mathematisch nicht unumkehrbar.

Ein eigener Knoten verringert Abfragen bei Drittanbietern und ermöglicht eigene Prüfungen. Betriebssystem, Zugriff und Verbindung brauchen weiterhin Schutz. Ein unsynchronisierter Knoten oder eine App, die trotz eigenem Knoten einen anderen Server befragt, bietet diese Vorteile nicht automatisch.

Übung

1. Ordne folgende Aufgaben zu: Signatur prüfen, Transaktionen für einen Block wählen, deinen Seed verwahren und über die Annahme einer Zahlung entscheiden.
2. Erkläre, weshalb „Der Miner verwahrt meine Bitcoins“ unzutreffend ist.
3. Beobachte im Labornetz Blockhöhe und Synchronisierung. Veröffentliche keine RPC-Zugangsdaten.

Zeig, was du kannst

Unterscheide Prüfen und Vorschlagen. Ein Vergleich ist möglich, schließe aber mit der korrekten technischen Funktion.

Häufige Frage

Muss ich minen, um Bitcoin zu nutzen? Nein. Auch ein eigener Knoten ist anfangs entbehrlich. Du musst jedoch wissen, wie weit du deinem Anbieter vertraust.

Hier kannst du pausieren

Notiere den Typ deines Laboranbieters ohne private URL.

Was bietet ein richtig konfigurierter vollständiger Knoten seinem Nutzer?

1. Die Regeln der akzeptierten Kette selbst zu prüfen.
2. Jeden verlorenen Schlüssel wiederherzustellen.
3. Einen Preisanstieg zu garantieren.

> **Antwort anzeigen: Die Regeln der akzeptierten Kette selbst zu prüfen.**
> Validierung und Verwahrung sind unterschiedliche Aufgaben.

UTXOs und Wechselgeld einer Transaktion

Lernziel

Lies eine Transaktion als Verbrauch und Erzeugung von Ausgängen.

Grundlagen

Ein UTXO ist ein noch nicht ausgegebener Ausgang einer früheren Transaktion. Eine Wallet ermittelt das Guthaben aus den Ausgängen, die sie kontrollieren kann. Es gibt kein allgemeines Konto, von dem wie im Bankbuch abgebucht wird. Jeder Eingang verweist über Transaktionskennung und Position auf einen früheren Ausgang.

Ein UTXO wird vollständig verbraucht. Zahlst du weniger als seinen Wert, erzeugst du gewöhnlich einen Ausgang zum Empfänger und einen Wechselgeldausgang unter deiner Kontrolle. Bei 120.000 sat Eingang, 70.000 sat Empfängerbetrag und 1.000 sat Gebühr bleiben 49.000 sat Wechselgeld. Die Summe der Eingänge entspricht allen Ausgängen plus Gebühr.

Eine Adresse ist kein UTXO. Auf derselben Adresse können mehrere Ausgänge eingehen. Auch steht sie nicht zwingend für eine Person. Eine Transaktionskennung kann öffentlich sein. Die Verknüpfung mit deiner Identität oder die Angabe, wem die Ausgänge gehören, verrät mehr als die Kette selbst.

Das hat Folgen für die Privatsphäre. Gemeinsame Eingänge können auf gemeinsame Kontrolle hindeuten. Wechselgeld kann spätere Zahlungen verknüpfen. Kollaborative Transaktionen zeigen, dass solche Schlüsse nicht immer beweiskräftig sind. Mit Coin Control wählst du Ausgänge bewusst aus und berücksichtigst die Folgen ihrer Kombination.

Übung

1. Zeichne drei fiktive Eingänge über 40.000, 60.000 und 200.000 sat. Zahle 70.000 mit 1.000 Gebühr und nutze nur die ersten beiden.
2. Prüfe, dass 29.000 sat Wechselgeld entstehen und der dritte Eingang unberührt bleibt.
3. Wiederhole es nur mit 200.000 sat. Es blieben 129.000. Vergleiche mögliche Kosten und Verknüpfungen, ohne gleiche Transaktionsgrößen vorauszusetzen.

Zeig, was du kannst

Finde Eingang, Empfänger, Wechselgeld und Gebühr im Kursdiagramm. Kannst du einen Ausgang nicht zuordnen, signiere keine echte Transaktion.

Häufige Frage

Ist alles, was in meine Wallet zurückkommt, Wechselgeld? Nein. Es kann eine Übertragung an eine andere eigene Adresse sein. Zur Zuordnung brauchst du Richtlinie und Ableitung. Der Betrag allein reicht nicht.

Hier kannst du pausieren

Bewahre die fiktive Skizze auf, niemals ein Bildschirmfoto deines Vermögens.

Ein Eingang über 100.000 sat erzeugt Ausgänge über 30.000 und 69.200. Wie hoch ist die Gebühr?

1. 69.200 sat.
2. 800 sat.
3. 30.000 sat.

> **Antwort anzeigen: 800 sat.**
> 100.000 minus 99.200 ergibt 800 sat.

Mempool, Bestätigungen und Reorganisationen

Lernziel

Unterscheide vorbereitete, veröffentlichte und bestätigte Transaktionen.

Grundlagen

Der Mempool enthält die unbestätigten Transaktionen, die ein Knoten nach seinen lokalen Richtlinien vorhält. Es gibt keinen weltweit identischen Mempool. Zeigt ein Explorer eine Zahlung, kennt dieser Dienst sie. Das garantiert weder die Annahme durch alle Knoten noch eine Bestätigung innerhalb einer bestimmten Frist.

Eine PSBT vorzubereiten veröffentlicht nichts. Die Signatur erteilt die Freigabe. Beim Finalisieren entsteht die übertragbare Transaktion. Veröffentlichen versucht, sie zu verbreiten. Eine Bestätigung bedeutet die Aufnahme in einen Block der Kette, die deine Prüfquelle akzeptiert. Die zweite Bestätigung ist ein weiterer Block darüber, keine zweite Unterschrift des Empfängers.

Bei einer Reorganisation ändert sich ein Kettenabschnitt. Eine Transaktion kann Bestätigungen verlieren oder wieder ausstehend sein. Bei größeren Risiken verlangen Beteiligte oft mehr Bestätigungen. Keine feste Anzahl beseitigt für alle Beträge und Situationen jedes Risiko.

Zeigt Desk einen gespeicherten Stand, prüfe den Synchronisierungszeitpunkt. Ein früherer Schnappschuss mit „Bestätigt“ muss heute nicht mehr stimmen. Fehlt eine Zahlung, bewahre die lokale Kennung auf und prüfe Veröffentlichung und Verlauf, bevor du sie neu vorbereitest. Ungeduld kann zu einer zweiten gültigen Zahlung führen.

Übung

1. Sortiere die Karten: Entwurf, PSBT, Signatur, finale Transaktion, Verbreitung, Aufnahme in einen Block.
2. Simuliere eine Verbindungsunterbrechung nach der Veröffentlichung. Entscheide, was vor einer erneuten Zahlung zu prüfen ist.
3. Erkläre einem Händler, warum „bezahlt“ im Chat keine Netzwerkprüfung ersetzt.

Zeig, was du kannst

Gib Status, Quelle und Zeitpunkt einer Transaktionsauskunft an, ohne daraus eine Garantie abzuleiten.

Häufige Frage

Bricht das Schließen von Desk eine veröffentlichte Transaktion ab? Nein. Andere Knoten und Teilnehmer können sie behalten. Das Verwerfen eines lokalen Entwurfs hat eine andere Reichweite.

Hier kannst du pausieren

Notiere den Simulationsstand. Teile dem Tutor keine echten Kennungen mit.

Nach dem Klick auf „Veröffentlichen“ verliert der Computer die Verbindung. Was tust du zuerst?

1. Dieselbe Zahlung von Grund auf neu vorbereiten.
2. Die Wallet löschen.
3. Die Verbindung wiederherstellen und Transaktion und Eingänge prüfen.

> **Antwort anzeigen: Die Verbindung wiederherstellen und Transaktion und Eingänge prüfen.**
> Eine ausbleibende Antwort beweist nicht, dass die Verbreitung gescheitert ist.

Gebühren, virtuelle Größe und Ersetzung

Lernziel

Schätze Kosten, verstehe sat pro virtuellem Byte sowie RBF und CPFP.

Grundlagen

Die Netzwerkgebühr ist die Differenz zwischen Ein- und Ausgängen. Ihre Wettbewerbsfähigkeit wird meist in sat/vB angegeben, also Satoshis je virtuellem Byte. Sie hängt nicht unmittelbar vom übertragenen Wert ab. Viele Eingänge können eine kleine Zahlung teuer machen. Eine große Zahlung mit wenigen Eingängen kann weniger Platz brauchen.

200 vB bei 5 sat/vB kosten 1.000 sat. Vor dem Signieren lässt sich die Gebühr nur schätzen, weil die endgültige Größe von Signaturen und Struktur abhängen kann. Desk bietet ungefähre Geschwindigkeitsstufen und manuelle Gebührensätze. „Schnell“ verspricht keine pünktliche Bestätigung.

RBF ermöglicht nach bestimmten Richtlinien das Ersetzen unbestätigter Transaktionen. Dabei wird eine konkurrierende Ausgabe mit höherer Gebühr vorgeschlagen. Knotenrichtlinien haben sich verändert. Ein Signal gegen Ersetzung ist keine Zahlungsgarantie. Eine Ersetzung erfordert erneute Prüfung und die nötigen Signaturen.

Bei CPFP wird ein Ausgang einer ausstehenden Transaktion ausgegeben, damit Eltern- und Kindtransaktion zusammen attraktiv sind. Du brauchst Kontrolle über einen ausgebbaren Ausgang, musst Richtlinien erfüllen und die Kosten tragen. Das Bitcoin-Konzept setzt keine CPFP-Schaltfläche in deiner Cuvex-Version voraus.

„Dust“ bezeichnet einen nach geltenden Richtlinien und geschätzten Ausgabekosten zu kleinen Ausgang. Es gibt keinen universellen Schwellenwert für alle Skripte. Lehre keine feste Zahl als Konsensregel. Ist Wechselgeld nicht sinnvoll, prüfe Betrag, Eingänge, vollständiges Leeren und effektive Gebühr.

Übung

1. Berechne 180 vB zu 8 sat/vB: 1.440 sat. Prüfe, ob das dein Laborbudget übersteigt.
2. Vergleiche einen mit zehn Eingängen. Erkläre, weshalb der Zahlbetrag zur Kostenschätzung nicht ausreicht.

3. Simuliere eine ausstehende Transaktion und wäge Warten, RBF oder die Prüfung von CPFP ab. Setze Unterstützung nie voraus.

Zeig, was du kannst

Begründe Gebührensatz, absolute Gebühr und ihr Verhältnis zum Zahlbetrag. Lehne eine Gebühr ab, die du nicht nachvollziehst.

Häufige Frage

Hebt RBF die erste Zahlung sicher auf? Nein. Die Versionen konkurrieren bis zur Bestätigung. Ihre Verbreitung spielt eine Rolle. Gib keine Waren gegen ein Stornierungsversprechen heraus.

Hier kannst du pausieren

Halte die Übungsentscheidung mit ihrer Begründung fest.

Welche Gebühr ergeben 250 vB zu 4 sat/vB?

1. 1.000 sat.
2. 254 sat.
3. 4 % des Zahlbetrags.

> **Antwort anzeigen: 1.000 sat.**
> Virtuelle Größe mal Gebührensatz ergibt die geschätzte Gebühr.

M02

Netzwerke, Adressen und Zahlungsanforderungen

Lernziel

Erkenne Netzwerk, Adressformat und Zahlungsanweisungen vor dem Kopieren oder Scannen.

Grundlagen

Im Mainnet werden Bitcoin mit wirtschaftlichem Wert bewegt. Testnetze dienen Entwicklung und Lernen, sind aber nicht untereinander austauschbar. Regtest ist ein vom Laborbetreiber kontrolliertes lokales Netz. Signet und Testnet haben eigene Regeln und Umgebungen. Einzelsignatur in Signet bedeutet nicht, dass das Cuvex-Multisig-Profil dieses Netz unterstützt.

Adressen kodieren Empfangsbedingungen. Im Mainnet beginnen gebräuchliche Formate mit 1, 3, bc1q oder bc1p. Das Präfix hilft bei der Einordnung, bestätigt aber weder Empfänger noch Signiererkompatibilität und ersetzt keine vollständige Formatprüfung.

Ein QR-Code ist ein visueller Datenbehälter. Er kann eine Adresse, Zahlungsanforderung, einen Deskriptor oder schädlichen Text enthalten. Ein Scan authentifiziert nicht den Ersteller. Ein bitcoin:-Link kann Betrag und Nachricht enthalten. Der aktuelle Standard BIP321 ersetzt BIP21. Die geprüfte Desk-Implementierung behält BIP21-Bezeichnungen und -Kompatibilität bei. Eine Standardverbesserung erweitert den Funktionsumfang der App nicht automatisch.

Eine Lightning-Rechnung ist keine On-Chain-Adresse. Sie kann Ablaufzeit und weitere Felder enthalten. Füge sie nicht in eine On-Chain-Zahlung ein, wenn die App keinen passenden Ablauf anbietet. Auch ein BTC benannter Token auf einer anderen Kette ist nicht automatisch nativer Bitcoin.

Übung

1. Ordne die beschrifteten Kursbeispiele ohne verwendbare Adressen zu: Adresse, bitcoin:-URI, Lightning-Rechnung und Deskriptor.
2. Bestimme das im Labor ausgewählte Netz. Das geprüfte Cuvex-Multisig-Profil unterstützt Mainnet und Regtest.
3. Vergleiche vor einem echten Vorgang die gesamte vom Empfänger mitgeteilte Zeichenfolge über einen authentifizierten Kanal.

Zeig, was du kannst

Lehne Anfragen mit unbekanntem Netz oder Verfahren ab und erkläre, was du prüfen musst.

Häufige Frage

Kann ich BTC über jedes von einer Börse angezeigte Netz senden? Nein. Auszahlungsnetz und tatsächlicher Empfang müssen übereinstimmen. Wähle nicht allein nach der niedrigsten Gebühr.

Hier kannst du pausieren

Erfasse nur den Typ des Lernnetzes.

Eine bc1-Empfangsadresse berechtigt nicht zur BTC-Auszahlung über ein anderes Tokennetz. Was fehlt?

1. Den Alias des Empfängers ändern.
2. Bestätigen, dass die Auszahlung Bitcoin on-chain nutzt und alle Angaben übereinstimmen.
3. Den Seed bei der Börse eingeben.

> **Antwort anzeigen: Bestätigen, dass die Auszahlung Bitcoin on-chain nutzt und alle Angaben übereinstimmen.**
> Vermögenswert, Netz und Empfangsmethode müssen zusammenpassen.

M03

Hash, Signatur und Verschlüsselung

Lernziel

Unterscheide Integrität, Autorisierung und Vertraulichkeit.

Grundlagen

Eine Hashfunktion bildet Daten auf einen Fingerabdruck fester Länge ab. Der Vergleich mit einem bekannten Wert hilft, Änderungen zu entdecken. Er verschlüsselt die Datei nicht und identifiziert für sich genommen auch nicht den Herausgeber. Stammen Datei und Hash von derselben kompromittierten Seite, könnten beide ersetzt sein.

Ein privater Schlüssel erzeugt Signaturen. Der zugehörige öffentliche Schlüssel erlaubt ihre Prüfung. Eine Signatur bindet nach den Regeln des Algorithmus eine Autorisierung an eine konkrete Nachricht. Sie verbirgt den signierten Inhalt nicht. Bei Bitcoin erfüllt eine gültige Signatur einen Teil der Ausgabebedingungen.

Verschlüsselung soll Inhalte nur mit der passenden Berechtigung lesbar machen. Authentifizierte Verschlüsselung erkennt zusätzlich Manipulationen. Bei Cuvex schützen Kryptogramme Geheimnisse, signierte Transaktionen autorisieren Ausgaben und verschlüsselte Kanäle transportieren Nachrichten. Das sind unterschiedliche Objekte, obwohl alle Kryptografie nutzen.

Ein menschliches Passwort durchläuft meist eine Ableitungsfunktion, bevor es als kryptografischer Schlüssel dient. „AES-256“ bezeichnet Algorithmus und Schlüssellänge, macht ein vorhersehbares Passwort aber nicht stark. Erzeugung, Implementierung, Aufbewahrung, Anzeige und Wiederherstellung tragen zur Gesamtsicherheit bei.

Ein komplex aussehender QR-Code ist nicht automatisch sicher. Prüfe Inhalt, Ersteller und beabsichtigte Verarbeitung durch die App. Bitte den Tutor vor der Freigabe um eine Erklärung des Zwecks, ohne das Geheimnis preiszugeben.

Übung

1. Ordne „Dateiänderung erkennen“, „Seed verbergen“ und „Zahlung autorisieren“ Hash, Verschlüsselung und Signatur zu.
2. Ändere einen Buchstaben eines fiktiven Textes und beobachte den neuen Hash. Nutze keine Geheimnisse.
3. Erkläre, weshalb eine Transaktion öffentlich und zugleich signiert sein kann.

Zeig, was du kannst

Beschreibe gewünschte Garantie und zugehörigen Mechanismus. Verwende „verschlüsselt“ nicht für alles, was sicher ist.

Häufige Frage

Belegt ein Firmware-Hash Fehlerfreiheit? Nein. Bei vertrauenswürdiger Referenz identifiziert er Bytes. Audit, Herstellersignatur und physischer Test beantworten unterschiedliche Fragen.

Hier kannst du pausieren

Halte die drei Zuordnungen fest.

Welcher Mechanismus verbirgt den Inhalt eines Geheimnisses?

1. Seinen Dateinamen veröffentlichen.
2. Es signieren, ohne es zu verschlüsseln.
3. Es mit einem geschützten Schlüssel korrekt verschlüsseln.

> **Antwort anzeigen: Es mit einem geschützten Schlüssel korrekt verschlüsseln.**
> Signatur und Fingerabdruck allein gewähren keine Vertraulichkeit.

M03

Seed, Passphrase und Passwort

Lernziel

Vermeide Verwechslungen zwischen den Zugangsdaten des Systems.

Grundlagen

Eine BIP39-Mnemonik stellt Entropie und Prüfsumme mit Wörtern einer Wortliste dar. Standardlängen sind 12, 15, 18, 21 oder 24 Wörter. Ein einprägsamer Satz, ein Liedtext oder von Menschen vermeintlich zufällig ausgesuchte Wörter ersetzen keine sichere Erzeugung. Die Prüfsumme erkennt manche Fehler, beweist aber weder den Urheber noch, dass sonst niemand den Seed kennt.

Die BIP39-Passphrase fließt in die Ableitung des binären Seeds ein. Eine andere Passphrase kann eine völlig andere, scheinbar leere Wallet öffnen. Eine Meldung „Falsche Passphrase“ muss nicht erscheinen. Die Passphrase muss kein Listenwort sein und ist nicht buchstäblich ein fünfundzwanzigstes Wort.

Das Cuvex-Kryptogrammpasswort schützt das gespeicherte Geheimnis. Das Desk-Passwort schützt den lokalen Datenspeicher. Die Kopplungs-PIN autorisiert eine Kommunikationssitzung. Der Chat-Schlüssel stellt eine Nachrichtenidentität wieder her. Keiner dieser Werte ist der Seed. Einen davon zu kennen erlaubt nicht automatisch die Rekonstruktion der anderen.

Seed und Passphrase im selben Kryptogramm können die Wiederherstellung erleichtern. Wer es entschlüsselt, erhält aber beides. Getrennte Aufbewahrung verlangt dir und deinen Erben mehr ab. Dokumentiere und teste die Entscheidung. Dass der Tutor etwas „fortgeschrittener“ findet, ist kein Grund.

Übung

1. Beschrifte fünf Papierkarten ohne Geheimwerte: Seed, Passphrase, Cuvex-Passwort, Desk-Passwort und Chat-Schlüssel.
2. Schreibe auf, was sich damit wiederherstellen lässt und was du bei Vergessen verlierst.
3. Entwirf einen Test mit einer leeren Wallet. Gib Wörter und Passphrase privat ein und teile dem Tutor nur das Ergebnis mit.

Zeig, was du kannst

Erkläre, weshalb der Kurs niemals zur „Lernkontrolle“ ein Passwort erfragen darf. Bestimme das für deinen Wiederherstellungsablauf benötigte Geheimnis.

Häufige Frage

Kann ich die Passphrase per E-Mail zurücksetzen? BIP39 sieht das nicht vor. Ein Verwahrdienst kann eine Kontowiederherstellung anbieten, arbeitet aber nach einem anderen Modell.

Hier kannst du pausieren

Halte „Zugangsdaten unterschieden“ fest, ohne ihre Werte aufzuschreiben.

Du änderst einen Buchstaben in einer BIP39-Passphrase und siehst ein Guthaben von null. Was ist die richtige Deutung?

1. Es kann eine andere gültige Wallet sein, die aus einer anderen Passphrase abgeleitet wurde.
2. Das Netzwerk hat mein Guthaben gelöscht.
3. Desk muss die ursprüngliche Passphrase erraten.

> **Antwort anzeigen: Es kann eine andere gültige Wallet sein, die aus einer anderen Passphrase abgeleitet wurde.**
> Eine andere Passphrase kann ohne Fehlermeldung eine andere Wallet erzeugen.

Schlüsselableitung, xpub und Deskriptoren

Lernziel

Verstehe, wie sich eine Wallet beschreiben lässt, ohne anderen die Möglichkeit zu geben, ihre Mittel auszugeben.

Grundlagen

Eine hierarchische Wallet leitet viele Schlüssel aus einer Wurzel ab. Der Pfad gibt den Zweig an. Im Mainnet verwendet BIP84 für das erste SegWit-Einzelsignaturkonto meist m/84'/0'/0', BIP48 P2WSH für das erste Multisig-Konto m/48'/0'/0'/2'. Der Apostroph kennzeichnet einen gehärteten Ableitungsschritt. Ein anderes Konto, Netzwerk oder Skript kann aus derselben Mnemonik andere Adressen ergeben.

Eine xpub ist ein erweiterter öffentlicher Schlüssel zur Ableitung bestimmter öffentlicher Nachfolgeschlüssel. Sie ist kein Ausgabepasswort, kann aber eine ganze Adressfamilie beobachtbar machen. Der Master-Fingerabdruck ist eine kurze Kennung für Zuordnungen. Er beweist allein keine Identität und schließt Kollisionen nicht aus.

Ein Deskriptor beschreibt, wie Skripte und Adressen aus Skripttyp, Schlüsseln, Ursprüngen und Ableitungen aufgebaut werden. Ein Watch-only-Deskriptor mit öffentlichen Schlüsseln erlaubt Beobachtung, keine Signatur. Die Bezeichnung garantiert nicht ausschließlich öffentliche Angaben. Manche Formate können private Schlüssel enthalten. Lade nie einen echten Deskriptor in den Kurs hoch.

Zur Multisig-Wiederherstellung reicht die Wortfolge eines einzelnen Signierers meist nicht aus. Du brauchst die vollständige Richtlinie. Bewahre Schwelle, Teilnehmer, xpubs, Pfade, Netzwerk, Skripttyp und Daten zur Adresssuche auf. Die Deskriptor-Prüfsumme erkennt Abschreibfehler, authentifiziert aber keine Teilnehmer.

Übung

1. Lies einen fiktiven Pfad und erkläre Verwendungszweck, Währung, Konto und Zweig. Gib keine echten Schlüssel ein.
2. Unterscheide Empfangsadresse, Teilnehmer-xpub und vollständigen Deskriptor.
3. Erstelle ein privates Wiederherstellungsblatt mit leeren, beschrifteten Feldern und einem getrennten Aufbewahrungsort für die Dokumentation.

Zeig, was du kannst

Erkläre, warum eine nach der Wiederherstellung leere Wallet noch keinen Verlust beweist. Prüfe Netz, Passphrase, Skript, Konto, Pfad und Adresssuche.

Häufige Frage

Kann ich eine xpub bedenkenlos veröffentlichen? Sie erlaubt allein normalerweise keine Ausgabe, legt aber private Zusammenhänge offen und kann in bestimmten kryptografischen Kombinationen weitere Risiken erhöhen.

Hier kannst du pausieren

Bewahre das Blatt im Kurs nur ohne sensible Werte auf.

Welche Angaben können fehlen, wenn du eine Multisig-Wallet nur mit einem Seed wiederherstellen möchtest?

1. Die Farbe des Geräts.
2. Die Richtlinie und die öffentlichen Schlüssel der übrigen Teilnehmer.
3. Das Passwort eines sozialen Netzwerks.

> **Antwort anzeigen: Die Richtlinie und die öffentlichen Schlüssel der übrigen Teilnehmer.** Die Rekonstruktion der Skripte erfordert die vollständige Richtlinie zusätzlich zur nötigen Anzahl privater Schlüssel.

M03

Eine Wallet und ein Verwahrungsmodell wählen

Lernziel

Vergleiche Werkzeuge anhand von Funktionen, Vertrauensannahmen und Wiederherstellung.

Grundlagen

Eine Wallet umfasst Werkzeuge zum Beschreiben, Beobachten und gegebenenfalls Autorisieren von Ausgaben. Eine Hot Wallet kann in einer verbundenen Umgebung signieren. Ein isolierter Signierer trennt Geheimnisse möglichst vom Gerät für Netzabfragen. Eine Watch-only-Wallet hält öffentliche Daten zum Beobachten und Vorbereiten. Zum Signieren braucht sie ein anderes System.

Bei Fremdverwahrung kann ein Konto einen Anspruch gegenüber einem Unternehmen darstellen. Bei Selbstverwahrung behältst du allein oder gemeinsam die technische Ausgabefähigkeit. Wiederherstellung per E-Mail und die Möglichkeit, Auszahlungen zu sperren, sprechen meist für Fremdverwahrung. Die Verantwortlichkeiten beider Modelle unterscheiden sich.

Vergleiche Netzwerk- und Skriptunterstützung, Prüfung am Display, Sicherungen, Updates, Interoperabilität, Wartung, Anbieterabfragen und Verständlichkeit von Fehlern. Münzlisten und Gehäusequalität allein reichen nicht. Auch ein Signiergerät schützt nicht davor, dass du eine falsche Adresse ungeprüft akzeptierst.

Cuvex trennt in Kryptogrammen geschützte Geheimnisse von Verwaltung und Abfragen in Desk. Du brauchst das Kryptogramm und seine Entsperrmittel. Schutz vor Geräteverlust hilft nicht, wenn auch sämtliche Kopien oder Passwörter verloren sind. Lerne den vollständigen Ablauf kennen, bevor du Vermögen überträgst.

Übung

1. Vergleiche Cuvex, Hot Wallet und Börse in einer Tabelle. Wer signiert, wer sieht Abfragen, wer kann Zugang wiederherstellen und was passiert bei einer Firmenschließung?
2. Wähle zwei Kriterien, für die du Belege statt Werbeaussagen benötigst.
3. Prüfe, dass deine Übungsumgebung keine Schlüssel mit deinem echten Ersparten teilt.

Zeig, was du kannst

Begründe die Wahl für einen konkreten Fall, ohne ein Werkzeug für unverwundbar zu erklären.

Häufige Frage

Macht eine Hardware-Wallet alle Transaktionen privat? Nein. Sie schützt vor allem die Signierfähigkeit und Teile der Prüfung. Kette, Abfragen und Gegenparteien liefern weiterhin Informationen.

Hier kannst du pausieren

Speichere die Kriterientabelle ohne Kontonamen.

Was kann eine korrekt eingerichtete Watch-only-Wallet mit öffentlichen Schlüsseln?

1. Vorgänge beobachten und vorbereiten, ohne sie allein signieren zu können.
2. Einen verlorenen Seed ändern.
3. Anonymität garantieren.

> **Antwort anzeigen: Vorgänge beobachten und vorbereiten, ohne sie allein signieren zu können.**
> Beobachten und Autorisieren sind trennbare Fähigkeiten.

M03

Wiederherstellbare Sicherungen

Lernziel

Plane eine vollständige Sicherung und weise die Wiederherstellung nach, bevor du dich darauf verlässt.

Grundlagen

Eine brauchbare Sicherung stellt eine Fähigkeit wieder her, nicht nur eine Datei. Bei Einzelsignatur können Mnemonik, Passphrase und Ableitungsdaten nötig sein. Multisig benötigt zusätzlich Richtlinie und ausreichend viele Signierer. Desk kann eine verschlüsselte Kopie und ihr Passwort benötigen. Eine wiederhergestellte Chat-Identität bringt nicht automatisch alte Nachrichten zurück.

Redundanz schützt vor zufälligem Verlust, Trennung vor gemeinsamem Zugriff. Verschiedene Medien und Orte können zusammenhängende Ausfälle verringern. Jede weitere Kopie braucht Zugangsschutz, Bestandsführung und Prüfung. Dateinamen und Etiketten dürfen weder Vermögen verraten noch das Auffinden aller Bestandteile erleichtern.

Ein Test sollte eine zuvor geprüfte Adresse bestätigen und in einer Lernumgebung die Signatur einer kontrollierten Transaktion ermöglichen. Eine lesbare Datei allein beweist nicht ihre Zugehörigkeit zur richtigen Wallet. Prüfe eine Kopie nicht durch Eingabe deines produktiven Seeds an einem beliebigen Rechner.

Dokumentiere bei jeder Kopie Umfang und Ausnahmen. Ein neues aktuelles Passwort ändert alte Kopien nicht automatisch. Wurde ein früheres Passwort bekannt, bleiben die zugehörigen Sicherungen betroffen. Auch das Löschen einer Datei auf modernem Speicher beseitigt nicht garantiert alle Kopien oder Versionen.

Übung

1. Fülle eine private Übersicht aus: Objekt, Inhalt, zugehöriges Passwort, unabhängiger Standort, Testdatum und verantwortliche Person.
2. Stelle eine Übungskopie in einer getrennten Umgebung wieder her. Prüfe Netzwerk, erste Adresse und Ableitung.
3. Simuliere zuerst den Verlust des Computers und dann des Geräts. Bestimme, welches Verfahren sich ändert.

Zeig, was du kannst

Stelle dein Testszenario ohne improvisierte Hilfe wieder her und erkläre, was für ein anderes Szenario noch fehlen würde.

Häufige Frage

Enthält die globale Desk-Sicherung alles? Davon darfst du nicht ausgehen. In der geprüften Fassung sind Chatverlauf und Chatsitzungen ausgeschlossen. Multisig-Richtlinien und private Schlüssel erfüllen verschiedene Aufgaben.

Hier kannst du pausieren

Halte Testdatum und Ergebnis fest, niemals den Inhalt der Kopie.

Du änderst das Desk-Passwort. Was passiert mit einer älteren Sicherung?

1. Sie aktualisiert sich selbst.
2. Sie verliert automatisch ihre Verschlüsselung.
3. Sie behält den Schutz und das Passwort, mit denen sie erstellt wurde.

> **Antwort anzeigen: Sie behält den Schutz und das Passwort, mit denen sie erstellt wurde.**
> Frühere Sicherungen sind eigenständige Objekte.

M04

Original und BIT kennenlernen

Lernziel

Wähle den richtigen Ablauf für dein Gerät und seine Version.

Grundlagen

Original transportiert Kryptogramme und unterstützte Vorgänge über NFC-Karten. Bluetooth dient zum Aktualisieren, USB-C beim dokumentierten Modell zur Stromversorgung. BIT tauscht Dateien per USB-C aus und bietet Biometrie für Kryptogramme, die sie voraussetzen. Übertrage die NFC- und Bluetooth-Anweisungen für Original nicht auf BIT.

Neben Einstellungen bietet das Gerät Verschlüsseln, Entschlüsseln, Wallet-Erstellung und Signieren. Original kann Karten klonen, BIT arbeitet mit Dateien auf dem USB-Medium. Bezeichnungen, Sprachen und Zugänge können sich mit der Version ändern. Der neue BIT-Eintrag „Richtlinien prüfen“ öffnet den unterstützten Ablauf, ohne die Zuständigkeit für die Autorisierung zu ändern.

Die geprüften redaktionellen Referenzen sind Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 und Mirror beta.12.12. Das sind Quellenstände. Signatur, Verteilung und physische Abnahme jeder Kombination sind mit dem Team zu prüfen. Ersetze deine Firmware nicht durch eine unsignierte Binärdatei aus einem Entwicklungspaket.

Prüfe vor der Nutzung Herkunft, Siegel, äußeren Zustand und Version. Rückverfolgbarkeit und eine Updatesignatur helfen gegen konkrete Gefahren, ersetzen aber nicht alle Kontrollen. Bei Manipulationsspuren oder unerwarteter Version pausiere die Einrichtung und kontaktiere den Support über einen eigenständig geprüften Kanal.

Übung

1. Identifiziere Modell und sichtbare Version, ohne Geheimnisse zu fotografieren.
2. Suche Verschlüsseln, Entschlüsseln, Wallet-Erstellung, PSBT und Einstellungen. Starte zum Erkunden weder Löschung noch Update.
3. Wähle im Kurs Original oder BIT und behalte die Auswahl während der Übung bei.

Zeig, was du kannst

Erkläre den Hin- und Rückweg eines Vorgangs für dein Modell und welches Medium vor Überschreiben zu schützen ist.

Häufige Frage

Ist BIT für jeden automatisch sicherer? Die Modelle verlangen unterschiedliche betriebliche Entscheidungen. Es kommt auf Bedrohungen, Wiederherstellung und richtige Nutzung an.

Hier kannst du pausieren

Notiere Modell und Version lokal. Für den Kurs genügt das gewählte Modell.

Du hast ein BIT. Eine Anleitung fordert dich auf, mit dem Gerät selbst eine NFC-Karte zu beschreiben. Was tust du?

1. Ich prüfe die Zuordnung der Anleitung zu meinem Modell und nutze den unterstützten USB-Ablauf.
2. Ich erzwinge das Original-Update.
3. Ich sende den Seed an das Telefon.

> **Antwort anzeigen: Ich prüfe die Zuordnung der Anleitung zu meinem Modell und nutze den unterstützten USB-Ablauf.**
> Die Anleitung muss zum tatsächlichen Übertragungsweg des Modells passen.

Einen Seed mit physischer Entropie erzeugen

Lernziel

Verstehe die Erzeugung und übe den Ablauf, ohne Kursdaten als eigene Schlüssel zu verwenden.

Grundlagen

Entropie bedeutet Unvorhersagbarkeit. Geeignete Würfel können Entropie liefern, wenn ihre Reihenfolge vor dem Wurf feststeht und die Umwandlung korrekt ist. Vom Verfahren verworfene Ergebnisse müssen genau nach Anweisung wiederholt werden. Das Ersetzen durch den Höchstwert oder ein selbst gewähltes Wort verzerrt die Verteilung.

Der geprüfte Cuvex-Ablauf nutzt eine Münze und vier Würfel. Die Funktion berechnet den Münzwert × 1.296 plus die Zahl zur Basis sechs, deren Ziffern den vier Würfelwerten minus jeweils eins entsprechen. Gültig sind die Indizes 0 bis 2.047. Liegt der Wert außerhalb der Wortliste, wirf Münze und alle vier Würfel neu. Nur die Würfel erneut zu werfen und den Münzwert zu behalten erzeugt eine Verzerrung. Dies beschreibt den geprüften Quellstand. Anzeige und Gesamtablauf sind für jede ausgelieferte Firmware zu validieren.

Das entspricht nicht der Wahl von Lieblingswörtern. Nutze öffentliche Demonstrationen nie zur Geldverwahrung. Jeder in Lehrmaterial gezeigte Seed gilt als bekannt. Das letzte Wort und seine Prüfung müssen aus dem vollständigen Gerätealgorithmus hervorgehen. Ergänze keine Mnemonik von Hand.

Bereite einen unbeobachteten Platz ohne Kameras, laufende Sprachassistenten in der Nähe oder Bildschirmaufnahme vor. Der Tutor pausiert bei der Eingabe und Prüfung des Geheimnisses. Er kann den Ablauf vorher erklären und danach Fragen stellen. Würfelergebnisse und Wörter darf er nicht hören.

Prüfe nach der Erzeugung die Sicherung, verschlüssele sie für das jeweilige Modell und teste die Wiederherstellung einer leeren Wallet. Eine Prüfadresse hilft beim Abgleich, ohne den Seed auf dem Rechner offenzulegen. Akzeptiert der Ablauf widersprüchliche Werte oder zeigt er unerwartete Wörter, stoppe und notiere nur Version, Anzeige und Fehler.

Übung

1. Folge im Test den Geräteschritten mit Material ohne Geldwert. Lege die Würfelreihenfolge fest und ändere keine Ergebnisse.

2. Wiederhole verworfene Eingaben wie angezeigt, ohne sie passend zu machen.
3. Prüfe den Inhalt privat, erstelle eine Kopie und bestätige die Wiederherstellung derselben Übungswallet.

Zeig, was du kannst

Erkläre, warum physische Entropie, korrekte Umwandlung und Geheimhaltung des Ergebnisses drei verschiedene Voraussetzungen sind.

Häufige Frage

Darf ich der KI meine Würfe zur Algorithmusprüfung nennen? Nicht für einen Seed, den du verwenden wirst. Die Lernhilfe nutzt andere, synthetische Beispiele.

Hier kannst du pausieren

Beende die Übung mit dem Gerät in sicherem Zustand. Lass in der Pause keinen Seed sichtbar.

Die Firmware verwirft eine Würfeleingabe. Welche Handlung entspricht dem Verfahren?

1. Ein Wort selbst wählen.
2. Nach Anweisung des Geräts erneut werfen, ohne das Ergebnis zu verzerren.
3. Die Zahl verringern, bis sie angenommen wird.

> **Antwort anzeigen: Nach Anweisung des Geräts erneut werfen, ohne das Ergebnis zu verzerren.**
> Verworfene Eingaben gehören zur Entropieumwandlung und dürfen nicht willkürlich ersetzt werden.

M04

Ein Geheimnis mit Cuvex ver- und entschlüsseln

Lernziel

Erstelle ein Übungskryptogramm und überprüfe die Wiederherstellung seines Inhalts.

Grundlagen

Wähle den passenden Inhaltstyp: BIP39, SLIP39, Monero oder, falls angeboten, Text. Die Formate unterscheiden sich. Das Verschlüsseln eines SLIP39-Texts macht Cuvex nicht zum Signierer aller Netze, die diesen Text nutzen könnten. Speicherung von Geheimnissen und Durchführung von Signaturprotokollen haben unterschiedliche Reichweiten.

Soll der Inhalt vernetzte Geräte nicht berühren, gib ihn direkt auf dem Gerät ein. Ein Import über Telefon oder PC kann ihn schon an der Quelle offengelegt haben, selbst wenn er später verschlüsselt wird. Prüfe vor dem Bestätigen Wörter, Reihenfolge, Groß- und Kleinschreibung sowie Felder auf dem Prüfbildschirm.

Wähle ein langes, einmaliges, nach deinem Plan wiederbeschaffbares Kryptogrammpasswort. Die geprüfte Eingabemaske zur Erstellung fasst 40 Zeichen. Der Validator verlangt mindestens 12 Zeichen, ASCII-Groß- und Kleinbuchstaben, eine Ziffer und ein anerkanntes Sonderzeichen. Die Desk-Regel von 12 bis 1.024 Zeichen gilt nicht automatisch auf der Cuvex-Tastatur. Für andere Wiederherstellungsfelder können andere Grenzen gelten. Prüfe Ablauf und Version.

Beschreibe bei Original eine geeignete leere Karte und halte sie bis zur Bestätigung ruhig. Bewahre bei BIT alle vom USB-Ablauf erzeugten Dateien auf, gegebenenfalls auch die erforderlichen biometrischen Komponenten. Benenne Dateien nicht auf Verdacht um und kombiniere sie nicht eigenmächtig. Lies und entschlüssele die Sicherung am Gerät zur Probe, ohne dem Tutor das Geheimnis zu nennen.

Übung

1. Verschlüssele einen eigens für diese Übung erstellten Text ohne Zugangsdaten oder wirtschaftlichen Wert.
2. Bestimme Medium und Ergebnisobjekt. Notiere Alias und Funktion privat.
3. Starte den Entschlüsselungsablauf neu, prüfe den Text auf dem vertrauenswürdigen Display und schließe anschließend die Anzeige.

Zeig, was du kannst

Unterscheide richtigen Inhalt, richtiges Schreiben und richtige Wiederherstellung. „Datei kopiert“ belegt nicht alle drei.

Häufige Frage

Ist der Kartenalias ein Passwort? Nein. Er dient der Organisation. Vermeide Guthaben oder Beschreibungen, die dein Vermögen erkennen lassen.

Hier kannst du pausieren

Lass keinen entschlüsselten Inhalt sichtbar. Halte nur Erfolg oder Misserfolg der Übung fest.

Was zeigt am besten, dass der Inhalt eines Testkryptogramms wiederherstellbar ist?

1. Es hat einen schönen Namen.
2. Die Datei liegt in zwei Ordnern.
3. Ich lese und entschlüssele es über den richtigen Ablauf und prüfe den Inhalt privat.

> **Antwort anzeigen: Ich lese und entschlüssele es über den richtigen Ablauf und prüfe den Inhalt privat.**
> Das Vorhandensein einer Kopie beweist weder Verwendbarkeit noch Zugehörigkeit.

Verschlüsselungsschwellen und Biometrie

Lernziel

Unterscheide den gemeinsamen Zugriffsschutz für ein Geheimnis von Bitcoin-Multisig.

Grundlagen

Ein Kryptogramm mit mehreren Passwörtern regelt, wer den Inhalt entschlüsseln kann. Eine Bitcoin-Multisig-Wallet bestimmt, welche Schlüssel eine Ausgabe im Netzwerk autorisieren müssen. Ein gemeinsam geschützter Seed kann zu einer Einzelsignatur-Wallet gehören. Umgekehrt kann jeder Multisig-Signierer ein eigenes, einzeln geschütztes Kryptogramm haben.

Entsperren mehrere Menschen gemeinsam einen einzigen Seed, der allein ausgeben kann, bleibt die Schwelle auf der Kette ein Schlüssel. Nach dem Offenlegen könnte jemand ihn behalten. Beschreibe dieses Verfahren nicht so, als verlange es für jede Zahlung mehrere koordinierte Signaturen.

Die BIT-Biometrie fügt bei unterstützten Formaten eine Zugangsbedingung hinzu. Ein Finger ist kein Seed und kein universeller Passwortersatz. Plane Verletzung, veränderten Fingerabdruck, Defekt, Geräteverfügbarkeit und Erbschaft ein. Bewahre den dokumentierten Wiederherstellungsweg für dieses Kryptogramm auf und teste ihn, bevor du darauf angewiesen bist.

Ein Wiederherstellungsexport kann gerade zur Notfallhilfe das Geheimnis auf einem Rechner offenlegen. Der PC wird damit nicht zu einer dem Gerät gleichwertigen Umgebung. Erhalte im Normalbetrieb die Trennung. Prüfe lokale Wiederherstellung bewusst und plane eine anschließende Migration, falls eine Offenlegung erfolgt ist.

Übung

1. Zeichne zwei Richtlinien: „zwei Passwörter zum Öffnen eines Seeds“ und „zwei von drei Schlüsseln zum Ausgeben“.
2. Bestimme in einem Test ohne Guthaben die für eine biometrische Kopie benötigten Dateien und den Ort der Wiederherstellungsprüfung.
3. Simuliere die Abwesenheit einer Person. Prüfe, ob die Schwelle deines Verfahrens das Fortfahren erlaubt.

Zeig, was du kannst

Erkläre, wer das Geheimnis kennen kann und wer nach der Entschlüsselung eine Ausgabe autorisieren kann.

Häufige Frage

Kann ich einen Teilnehmer durch Umbenennen entfernen? Nein. Unterscheide organisatorische Änderungen, neuen Zugriffsschutz für das Geheimnis und eine neue Ausgaberichtlinie.

Hier kannst du pausieren

Bewahre die Skizze ohne echte Namen oder biometrische Daten auf.

Drei Personen öffnen mit zwei Passwörtern ein Kryptogramm mit einem einzigen Einzelsignatur-Seed. Wie viele Schlüssel verlangt Bitcoin für die Ausgabe?

1. Einen, wenn die Wallet-Richtlinie das vorsieht.
2. Zwei, weil für die Datei zwei Passwörter vorgeschrieben waren.
3. Drei, weil drei Personen beteiligt sind.

> **Antwort anzeigen: Einen, wenn die Wallet-Richtlinie das vorsieht.**
> Die Verschlüsselungsschwelle ändert das Skript für die Coins nicht.

M04

Kopien klonen, aufbewahren und prüfen

Lernziel

Baue Redundanz auf, ohne die einzige gültige Kopie zu zerstören.

Grundlagen

Klonen kopiert verschlüsselte Daten. Es erzeugt weder neues Guthaben noch einen anderen Seed und beseitigt kein Problem mit einem offengelegten Passwort. Identische Kopien helfen beim Verlust des Mediums, nicht bei Offenlegung des ursprünglichen Geheimnisses. Wiederherstellung und Migration auf neue Schlüssel lösen verschiedene Probleme.

Unterscheide bei Original Kryptogrammkarte und PSBT-Transportkarte. Ein Transaktionsmedium kann dem Ablauf entsprechend wiederverwendet werden. Nutze dafür keine Sicherungskarte. Weist ein Vorgang eine Karte mit Kryptogramm zurück, umgehe den Schutz nicht und lösche den Datenkopf nicht von Hand.

Bei BIT muss eine Kopie alle erforderlichen Dateien und ihre Zuordnung erhalten. Ein Dateimanager kann eine abgeschlossene Übertragung anzeigen, obwohl das Gerät den Inhalt noch nicht validiert oder den Vorgang beendet hat. Warte auf die angegebenen Zustände und teste die Kopie mit kontrollierter Wiederherstellung.

Führe eine private Bestandsliste mit unauffälligen Kennungen, Formatversion, Datum und Ergebnis des letzten Tests. Trenne mindestens zwei Kopien gegenüber den von dir benannten Gefahren. Lade Sicherungen nicht zur Fehlerdiagnose in Supportkanäle. Teile bereinigte Metadaten und Fehlercodes mit.

Übung

1. Kopiere dein Übungskryptogramm mit dem richtigen Ablauf auf ein anderes Medium.
2. Trenne das ursprüngliche Medium und stelle den Übungstext aus der Kopie wieder her.
3. Dokumentiere dein Vorgehen bei Verlust, Dateischaden und offengelegtem Passwort. Es sind verschiedene Verfahren.

Zeig, was du kannst

Bestimme die geprüfte Kopie und erkläre, warum dabei das Original nicht überschrieben wurde.

Häufige Frage

Darf ich das Original löschen, sobald ich eine zweite Datei sehe? Prüfe zuerst Wiederherstellung und Umfang. Lösche nach Plan, nicht allein aufgrund der Kopienzahl.

Hier kannst du pausieren

Verwahre die Medien vor Sitzungsende und halte Sicherungskarten von Karten für Zahlungsübungen getrennt.

Jemand kennt das Passwort und hat eine Kryptogrammkopie. Was bewirken drei weitere Klone?

1. Sie widerrufen die Kopie des Angreifers.
2. Sie schaffen Redundanz, widerrufen seinen Zugriff aber nicht.
3. Sie ändern automatisch den Bitcoin-Seed.

> **Antwort anzeigen: Sie schaffen Redundanz, widerrufen seinen Zugriff aber nicht.**
> Vervielfältigung beseitigt keine bestehende Kompromittierung.

M05

Cuvex Desk installieren und schützen

Lernziel

Öffne eine Installation aus überprüfter Quelle und schütze ihren lokalen Speicher.

Grundlagen

Wähle das verfügbare Paket für System und Architektur: macOS Intel oder Apple Silicon, Windows x64 oder ARM64, Linux x64 oder ARM64. Quellcode-ZIP, Manager-Paket und Kundeninstallationsprogramm sind verschiedene Lieferungen. Der Kurs darf Lernende nicht zu einem privaten Signaturpaket schicken.

Prüfe Herkunft und Systemprüfungen. Eine technische Windows-Signatur begründet allein kein öffentliches Vertrauen in den Herausgeber. Auf dem Mac sind App-Signatur, Notarisierung und Prüfung beim Öffnen getrennte Kontrollen. Schalte auf Anruf eines angeblichen Supports keine allgemeinen Schutzfunktionen ab. Bei unerwarteter Warnung sichere den Text und nutze den offiziellen Kanal.

Desk erstellt einen lokalen, passwortverschlüsselten Speicher. In der geprüften Fassung sind neue Passwörter 12 bis 1.024 Zeichen lang. Bei Bestätigung müssen beide Felder übereinstimmen. Länge allein reicht nicht. Nutze eine einmalige Phrase ohne Wiederverwendung. Falls verfügbar, erleichtert die eigens einzurichtende Computerbiometrie den Zugang.

Richte eine Sperre bei Inaktivität und gegebenenfalls beim Wechsel in den Hintergrund ein. Verzögerungen nach Fehlversuchen und optionale Löschung beschreibt das Handbuch. Aktiviere bei Demonstrationen keine automatische Löschung. Die App kann ohne herkömmliches Nutzerkonto arbeiten. Abfragen, Chat und Downloads haben jeweils eigene Voraussetzungen und Kommunikationswege.

Übung

1. Prüfe Plattform, sichtbare Version und Paketherkunft, ohne private Kennungen an den Tutor zu geben.
2. Erstelle einen Übungsspeicher und prüfe Sperren und Wiederöffnen. Gib das Passwort privat ein.
3. Plane eine verschlüsselte Sicherung und verwahre das Passwort nach deinem Plan. Teste keine wiederholten Sperren in der echten Umgebung.

Zeig, was du kannst

Unterscheide lokales Passwort, Einkaufskonto und Zugangsdaten zusätzlich eingebundener Dienste.

Häufige Frage

Ändert mein Desk-Passwort auch die Kartenpasswörter? Nein. Die Schutzmechanismen sind unabhängig. Alte Kopien ändern sich ebenfalls nicht von selbst.

Hier kannst du pausieren

Sperre Desk und speichere die Lektionskennung ohne Zugangsdaten.

Das Installationsprogramm passt nicht zu deiner Systemarchitektur. Was ist der erste Schritt?

1. Schutzmechanismen abschalten und die Ausführung erzwingen.
2. Das passende offizielle Paket beschaffen und seine Anforderungen prüfen.
3. Zum Fortfahren den Seed auf einer Website importieren.

> **Antwort anzeigen: Das passende offizielle Paket beschaffen und seine Anforderungen prüfen.**
> Kläre Kompatibilität und Herkunft, bevor du Verwahrungsmaterial verwendest.

M05

Kryptogramme verknüpfen und WOW verwalten

Lernziel

Verknüpfe eine verschlüsselte Kopie und unterscheide sie von einem Beobachtungskonto.

Grundlagen

Desk ordnet Kryptogramme, die über NFC, USB oder eine unterstützte Sicherungsdatei verknüpft sind. Design und Alias helfen beim Wiedererkennen, liefern aber keinen kryptografischen Identitätsnachweis. Im Detailfenster stehen Herkunft und von der App interpretierte Eigenschaften wie Format, Größe und Zugangsmerkmale.

Die Verknüpfung importiert oder ordnet ein unterstütztes Objekt. Sie entschlüsselt es nicht am PC und prüft nicht sein Geheimnis. WOW ist eine über passende öffentliche Informationen zugeordnete Beobachtungswallet. Dieselben Geheimnisse können verschiedene Konten oder Ableitungen ergeben. Verknüpfe die Wallet, die du tatsächlich verwalten willst.

Aktiviere oder importiere das Konto mit dem Deskriptor oder den im Geräteablauf exportierten öffentlichen Angaben. Prüfe Netz, Skripttyp, Fingerabdruck, Pfad und Prüfadresse. Der Kontoname dient der Organisation. Eine davon abgeleitete Kennung bietet keine starke Anonymisierung, weil sich vorhersehbare Namen erraten lassen.

Die geprüfte Desk-Fassung speichert Konten mit ausstehender Zuordnung und bietet Export, Klonen und Löschen lokaler Einträge. Das Entfernen einer Karte aus der Oberfläche zerstört keine externen Kopien und bewegt keine Mittel. „Kein Backup“ heißt nur, dass die App nach ihren Kriterien keine Kopie nachweisen kann.

Übung

1. Verknüpfe das Übungskryptogramm über den gewählten Weg und prüfe seine Detailansicht.
2. Importiere ein kompatibles Übungskonto und prüfe Netz und Prüfadresse, ohne Schlüssel zu zeigen.
3. Unterscheide Kryptogrammeintrag, WOW-Konto und physisches Medium. Bestimme, was bei lokalem Löschen verschwindet.

Zeig, was du kannst

Erkläre, welche Angaben Desk für die Beobachtung braucht und welche im Normalbetrieb außerhalb des Computers bleiben müssen.

Häufige Frage

Garantiert eine verknüpfte .bin-Datei, dass sie meinen Seed enthält? Nein. Prüfe Herkunft und Wiederherstellung. Eine Dateiendung beglaubigt keinen Inhalt.

Hier kannst du pausieren

Halte nur den Zustand „Testverknüpfung geprüft“ fest.

Bewegt das lokale Löschen eines WOW-Kontos dessen Bitcoins?

1. Nein. Je nach Ablauf werden lokale Daten gelöscht. Die UTXOs werden nicht ausgegeben.
2. Ja. Sie werden dem Hersteller geschickt.
3. Es hebt sämtliche Signaturen auf, die jemand anders aufbewahrt.

> **Antwort anzeigen: Nein. Je nach Ablauf werden lokale Daten gelöscht. Die UTXOs werden nicht ausgegeben.**
> Lokaler Datenstand und Zustand der Kette sind verschieden.

M05

Mirror mit Desk koppeln

Lernziel

Stelle eine autorisierte lokale Verbindung her und beende sie, ohne die Codes zu verwechseln.

Grundlagen

Mirror ermöglicht lokale Vorgänge mit Desk über die in beiden Apps angezeigten Kopplungs-, PIN- und QR-Schritte. Die sechsstellige PIN gehört zur Sitzung. Sie ist weder Desk- oder Kryptogrammpasswort noch Wiederherstellungswort. Prüfe, welcher Bildschirm sie erzeugt und wo sie eingegeben wird. Verwende keinen von einer unbekannten Person gesendeten Code.

Beginne im passenden Desk-Kontext. Verknüpfen, QR-Lesen, PSBT-Transport und Firmware haben verschiedene Zwecke. Das Fenster meldet Suche, Verbindung, Erkennung, PIN, QR und Aktion auf Karte oder Datei. Ein in der Suche angezeigtes Gerät belegt keinen abgeschlossenen Vorgang.

Gewähre die benötigten Systemberechtigungen, etwa Kamera für optisches Lesen sowie Bluetooth oder NFC für die entsprechenden Abläufe. Fehlende Hardwarefähigkeiten lassen sich nicht durch eine App installieren. Unter iOS bestehen Unterschiede bei Adapter und Validierung. Ein kompilierbares Projekt ist kein Nachweis einer Auslieferung und Prüfung auf allen iPhones.

Bestimme bei Problemen die genaue Phase: nicht gefunden, gefunden ohne Verbindung, PIN abgelehnt, QR unlesbar, Karte nicht gelesen oder Antwort nicht erhalten. Beende alte Sitzungen, prüfe Versionen und Berechtigungen und versuche es kontrolliert erneut. Eine falsche PIN rechtfertigt weder Firmwaretausch noch Seed-Eingabe an anderer Stelle.

Übung

1. Starte einen Testlesevorgang in Desk und verbinde Mirror über die lokalen Anzeigen.
2. Prüfe den Zweck, bevor du einen Übungs-QR-Code oder eine Karte vorlegst.
3. Brich die Sitzung ab und bestätige, dass kein verspätetes Ergebnis eines früheren Kontexts übernommen wird. Öffne eine neue Sitzung.

Zeig, was du kannst

Beschreibe die fehlgeschlagene Phase und die beteiligten Geräte ohne aktive Codes oder sensible Inhalte.

Häufige Frage

Muss Mirror immer verbunden bleiben? Das hängt vom Vorgang ab. Behandle es nicht als Dauerdienst und setze nach Schließen oder Hintergrundwechsel keine weiter gültige Autorisierung voraus.

Hier kannst du pausieren

Beende die Kopplungssitzung und sperre die gerade nicht genutzten Apps.

Was soll der Tutor tun, wenn die Kopplung schon vor Anzeige der PIN scheitert?

1. Den Seed verlangen.
2. Erkennung, Berechtigungen, Sitzung und Versionen vor dem Weitergehen prüfen.
3. Die Verbindung als abgeschlossen betrachten.

> **Antwort anzeigen: Erkennung, Berechtigungen, Sitzung und Versionen vor dem Weitergehen prüfen.**
> Die Diagnose muss bei der beobachteten Phase ansetzen und darf keine erfolgreiche Verbindung unterstellen.

NFC über Mirror, USB-C und das Lesen von QR-Codes

Lernziel

Verwende jeden Übertragungsweg seinem Zweck entsprechend und behalte seine Prüfungen bei.

Grundlagen

NFC-Vorgänge in Cuvex Desktop erfordern Cuvex Mirror auf einem kompatiblen Smartphone, das per Bluetooth mit dem Computer gekoppelt ist. Cuvex Desktop unterstützt keine externen USB-NFC-Lesegeräte. Karte, Format und Kapazität müssen ebenfalls passen. Eine kleine Karte kann ein Kryptogramm aufnehmen, für eine PSBT mit früheren Transaktionen aber zu klein sein. Die tatsächliche Grenze hängt vom gesamten Inhalt ab, nicht allein von der Anzahl der Empfänger. Verwende eine Sicherungskarte nicht als Transportkarte.

Bei Original kann Mirror eine Anfrage auf eine Transaktionskarte schreiben. Das Gerät verarbeitet sie und schreibt eine Antwort, die Mirror an Desk zurückgibt. Die Schreibbestätigung belegt keinen Empfang durch Desk. Halte die Karte bis zur Rückmeldung ruhig. Respektiere die Ablehnung, wenn das System ein erkanntes Kryptogramm schützt.

BIT nutzt ein USB-Laufwerk oder einen Austauschordner. Das Laufwerk kann im Ablauf ausgehängt und erneut bereitgestellt werden. Desk muss das richtige Medium wählen, die Antwort validieren und den vorgesehenen Empfang quittieren. Eine Datei in einen gleichnamigen PC-Ordner zu kopieren liefert sie nicht an das Gerät.

Unscharfer Fokus, Spiegelungen, Größe, Bewegung oder Datendichte können einen QR-Scan verhindern. Vergrößere die Darstellung und verbessere Beleuchtung und Abstand. Ersetze lange Kennungen nicht durch Anfangszeichen und akzeptiere keine Teilabschrift. Nach dem erfolgreichen Scan beginnt erst die inhaltliche Prüfung.

Übung

1. Bestimme mit den Kursmaterialien Anfrage, Medium und Antwort für Original und BIT im Diagramm.
2. Brich eine QR-Lesung zur Probe ab, ohne verspätete Werte zu speichern. Wiederhole mit anderem Zweck.
3. Simuliere eine zu große Datei. Erkläre, weshalb der Vorgang vereinfacht oder ein geeignetes Medium gewählt werden muss, ohne Prüfungen zu streichen.

Zeig, was du kannst

Benenne das Gerät und die jeweils bestätigte Phase: Lesen, Schreiben, Validieren, Empfang oder Quittierung.

Häufige Frage

Beweist ein Hash oder eine erfolgreiche Kopiermeldung den richtigen Bitcoin-Empfänger? Nein. Prüfe Vorgang und Ausgänge auf dem Signiergerät.

Hier kannst du pausieren

Entferne und verwahre Sicherungskarten. Kennzeichne das Transportmedium.

Original meldet, die Antwort sei auf die Karte geschrieben. Was fehlt, bevor feststeht, dass Desk sie erhalten hat?

1. Die Karte anders anmalen.
2. Einen neuen Seed erzeugen.
3. Die Antwort auf dem vorgesehenen Weg in Desk einlesen und validieren.

> **Antwort anzeigen: Die Antwort auf dem vorgesehenen Weg in Desk einlesen und validieren.**
> Erfolgreiches Schreiben und erfolgreicher Empfang sind verschiedene Ereignisse.

Öffentliche Anbieter und eigener Knoten

Lernziel

Wähle eine Abfragequelle und verstehe, welche Daten sie preisgibt und wo ihre Grenzen liegen.

Grundlagen

Desk kann unterstützte öffentliche Anbieter oder einen selbst konfigurierten Bitcoin Core abfragen. Ein Anbieter sieht möglicherweise Anfragen, Reihenfolge und Verbindungsdaten. Keine vollständige xpub zu übermitteln vermindert eine konkrete Offenlegung. Auch Skripte und Skripthashes können miteinander verknüpft werden.

Desk 9.21 bietet neben REST-Alternativen und eigenem Knoten ausdrücklich Blockstream Electrum über TLS an. TLS schützt den Übertragungsweg vor bestimmten Netzbeobachtern. Der Anbieter selbst erhält die Anfragen weiterhin. Es gibt keinen unbemerkten Anbieterwechsel, der Anonymität garantiert. Wäge Privatsphäre gegen Komfort ab.

Konfiguriere für Core Endpunkt, Authentifizierung und Beobachtungswallet gemäß Anleitung. Veröffentliche den RPC-Port nicht und setze ihn nicht dem Internet aus, damit die App ihn „sieht“. Beschränke den Zugriff auf vertrauenswürdige Umgebungen und verwende einen geeigneten geschützten Übertragungsweg. Diktiere dem Tutor kein RPC-Passwort.

Erste Synchronisierung und erneuter Scan können dauern. Die Fortschrittsanzeige meldet laufende Arbeit, keinen vorweggenommenen Erfolg. Desk arbeitet im Hintergrund weiter. Das Schließen der Ansicht stoppt den Knoten nicht. Das dokumentierte historische Mindestfenster garantiert keine Erkennung älterer Aktivität. Bei älteren Wallets prüfe Importdatum und tatsächlichen Scanumfang.

Die Adresssuche stützt sich auf Historie, nicht auf positives Guthaben. Eine auf null geleerte Adresse wurde benutzt. Die geprüfte Multisig-Fassung nutzt je Zweig und Teilnehmer eine Lücke von 20 aufeinanderfolgenden Adressen ohne Historie und begrenzt die Ausgabe neuer Adressen. Übertrage kein pauschales Limit auf alle Wallets.

Übung

1. Wähle eine Übungsquelle und erkläre, was sie sehen kann.
2. Prüfe letzte Synchronisierung, Netzwerk und Fortschritt. Halte bei HTTP 429 die Pause ein und wechsle Anbieter nur bewusst.

3. Simuliere eine Wallet mit Nullsaldo und alter Historie. Erkläre den Unterschied zwischen „null“ und „unbenutzt“.

Zeig, was du kannst

Beurteile, ob deine Quelle Prüf- und Datenschutzbedarf deckt, und erkenne einen unvollständigen Stand.

Häufige Frage

Macht ein eigener Knoten anonym? Nein. Er verringert Abfrageabhängigkeiten. Verbindung, Gegenparteien, Veröffentlichung und andere Metadaten sind weiter zu berücksichtigen.

Hier kannst du pausieren

Halte nur Anbietertyp und ausstehenden Scanbedarf fest.

Eine Adresse hat ein Guthaben von null, hat aber Mittel empfangen und ausgegeben. Wie zählt sie bei der Wallet-Erkennung?

1. Als Adresse mit Historie.
2. Als nie verwendete Adresse.
3. Als ungültige Adresse.

> **Antwort anzeigen: Als Adresse mit Historie.**
> Ob eine Adresse benutzt wurde, bestimmt ihre Historie, nicht das heutige Guthaben.

Bitcoin empfangen und die Adresse prüfen

Lernziel

Erstelle eine Zahlungsanforderung und prüfe sie vor der Weitergabe.

Grundlagen

Öffne das richtige WOW-Konto und bestätige Netz und Richtlinie. Erzeuge oder lade eine Empfangsanforderung. Für deine Organisation kannst du Zweck, Beobachter und erwarteten Betrag ergänzen. Das sind lokale Angaben. Der erwartete Betrag hindert niemanden daran, anders zu zahlen.

Verifiziere die Adresse im verfügbaren Geräteablauf und im Kontext der Wallet. Fehlt ein physischer Test für deine Kombination, bleibt es bei der Simulation. Kläre den Ablauf, bevor du größere Beträge empfängst. Zwei aus derselben Quelle gespeiste Anzeigen sind keine voneinander unabhängigen Prüfungen.

Nutze für eine neue Zahlungsbeziehung nach Möglichkeit eine neue Adresse. Im geprüften Multisig-Ablauf werden bereits angezeigte Adressen weder neu vergeben noch ungültig, weil Zahlende sie später verwenden können. Ist das Limit aufeinanderfolgender neuer Adressen ohne Historie erreicht, rufe die passende frühere Anforderung auf und kläre den Grund des Limits. Setze Indizes nicht zurück.

Beobachte nach der Weitergabe den Eingang in deiner Prüfquelle. E-Mail, Börsenbeleg und Screenshot des Zahlenden beweisen keine Abwicklung. Prüfe Netz, txid, Ausgang, Betrag und risikogerechte Bestätigungen. Nutze nicht aus Bequemlichkeit einen öffentlichen Explorer mit deiner Adresse, wenn dein Plan private Abfragen verlangt.

Übung

1. Erzeuge im Labor eine Anforderung, prüfe Konto und Netz und erkläre, wie du die Adresse verifizieren würdest.
2. Speichere eine fiktive Bezeichnung und rufe dieselbe Anforderung nach Schließen der Ansicht wieder auf.
3. Simuliere einen abweichenden Zahlungseingang und entscheide, wie er ohne Änderung der Historie abzustimmen ist.

Zeig, was du kannst

Unterscheide erzeugte Adresse, geprüfte Adresse, geteilte Anforderung und bestätigten Zahlungseingang.

Häufige Frage

Wird eine alte Adresse beim Erstellen einer neuen ungültig? Normalerweise nicht. Mit fortgesetzter Adresssuche und Anforderungsprotokoll bleiben verspätete Zahlungen sichtbar.

Hier kannst du pausieren

Speichere den Zustand der Laboranforderung. Teile ihren Inhalt nicht mit dem Tutor.

Der Zahlende sendet einen Screenshot mit „Auszahlung abgeschlossen“. Was prüfst du vor Annahme der Zahlung?

1. Nur die Bildqualität.
2. Den zugehörigen Ausgang in einer verlässlichen Netzwerkquelle und die nötigen Bestätigungen.
3. Das Passwort des Zahlenden.

> **Antwort anzeigen: Den zugehörigen Ausgang in einer verlässlichen Netzwerkquelle und die nötigen Bestätigungen.**
> Ein Geschäftsbeleg oder Screenshot ersetzt nicht die Prüfung der Zahlung.

UTXOs kennzeichnen, einfrieren und auswählen

Lernziel

Bereite Eingänge vor, ohne versehentlich unterschiedliche Ursprünge zu vermischen.

Grundlagen

Kennzeichnungen speichern Kontext außerhalb der Kette, etwa Herkunft, Gegenpartei, Zweck und Nutzungsbeschränkungen. In Desk können UTXO-Label und Adressnotiz unterschiedliche Längen und Aufgaben haben. „Kunde A“ kann genügen. Ausweisnummer oder voller Name machen den Eintrag möglicherweise unnötig sensibel.

Ein in Desk eingefrorener UTXO wird bei bestimmten lokalen Auswahlen ausgeschlossen. Das blockiert die Ausgabe in Bitcoin nicht, ändert kein Skript und hindert andere Apps mit den Schlüsseln nicht an der Nutzung. Gesamt- und verfügbares Guthaben können abweichen. Prüfe, ob eine Münze eingefroren, durch einen Entwurf reserviert oder wirklich ausgegeben ist.

Die automatische Auswahl optimiert nach ihrem Algorithmus und Kontext. Sie kennt deine privaten Zusammenhänge nicht zwingend. Prüfe für jede Zahlung, ob ein Ausgang desselben Kontexts sinnvoller ist als die Verbindung von Erspartem, Gehalt und Geschäftstätigkeit. Effektive Trennung erfordert dauerhaft konsequente Entscheidungen.

Der Export von Labels in BIP329 erleichtert Sicherung und Migration. Das Format verschlüsselt nicht von selbst. Desk bietet eine verschlüsselte Exporthülle. Unterscheide die geschützte Datei von kompatiblem Klartext. Prüfe beim Import Wallet-Zuordnung und Umgang mit eingefrorenen Ausgängen, bevor du Informationen überschreibst.

Übung

1. Kennzeichne drei synthetische UTXOs als Erspartes, Geschäftstätigkeit und Spende.
2. Friere einen ein und vergleiche beobachtetes mit auswählbarem Guthaben.
3. Exportiere Labor-Labels mit Passwort, importiere sie in eine Kopie und prüfe das Ergebnis ohne echte private Daten.

Zeig, was du kannst

Begründe deine Eingangsauswahl nach Kosten und möglichen Offenlegungen. Erkenne Einfrieren als lokale Einstellung.

Häufige Frage

Wird ein Label bei Zahlung zum Empfänger gesendet? Nicht allein aufgrund seiner lokalen Existenz. Es kann beim Exportieren, Dateiteilen, Nutzen anderer Dienste oder Einfügen in Nachrichten offengelegt werden.

Hier kannst du pausieren

Speichere Übungslabels und Sperrstatus.

Was bewirkt das Einfrieren eines UTXO in Desk?

1. Es erzeugt eine Konsenssperre im Netzwerk.
2. Es überträgt ihn auf ein Sonderkonto.
3. Es schränkt die Auswahl lokal nach den Regeln der App ein.

> **Antwort anzeigen: Es schränkt die Auswahl lokal nach den Regeln der App ein.**
> Die Ausgabemöglichkeit anderer Schlüsselkopien wird nicht widerrufen.

M06

Eine Zahlung vorbereiten und prüfen

Lernziel

Erstelle eine nachvollziehbare PSBT und erkenne alle Kosten und Ausgänge.

Grundlagen

Wähle Konto, ausgebbare Eingänge, Empfänger und Beträge. Prüfe die Herkunft der Anforderung. Vergleiche beim Einfügen oder Scannen die vollständige Adresse und das Netzwerk. Zwischenablage und Bild könnten ausgetauscht sein. Verlasse dich nicht auf Anfang und Ende, wenn eine vollständige Prüfung möglich ist.

Wähle den Gebührensatz und prüfe absolute Gebühr, geschätzte Größe, Gesamtsumme und Wechselgeld. Bei „Alles senden“ zieht Desk die Gebühr vom verfügbaren Betrag ab. Beginnt die Zahlung im Chat und deckt der Nettobetrag die Anforderung nicht, entscheide bewusst über eine Teilzahlung. Die ursprüngliche Anforderung wird nicht geändert, um die Differenz zu verbergen.

Prüfe kleines Wechselgeld oder das Fehlen eines Wechselgeldausgangs. Verifiziere einen als eigenen markierten Ausgang anhand der Richtlinie statt anhand des Namens des Koordinators. Ist Wechselgeld nicht sinnvoll, prüfe die vollständige Übertragung oder ergänze einen passenden Eingang. Akzeptiere keine unbemerkte Umwandlung in eine unverhältnismäßige Gebühr.

PSBT transportiert Informationen und Signaturen. Das Format gewährleistet weder Privatsphäre noch authentische Herkunft. Es kann frühere Transaktionen, öffentliche Schlüssel, Pfade und Metadaten enthalten. In den geprüften Final-Firmwares verwendet das Multisig-Profil PSBT v0/BIP174. „Transaktionsversion 2“ bedeutet nicht „PSBT-Version 2“.

Übung

1. Erstelle im Simulator eine Zahlung mit 120.000 sat Eingang, 70.000 sat für den Empfänger und 1.000 sat Gebühr.
2. Zähle alle Ausgänge auf und erkläre das Wechselgeld von 49.000 sat. Wiederhole mit vollständiger Übertragung.
3. Verwirf den Entwurf und erkläre, was du lokal verworfen hast. Nutze diesen Simulator nicht zum Signieren oder Veröffentlichen.

Zeig, was du kannst

Erkläre vor dem Export Eingänge, Ausgänge, Empfänger, Kosten und noch fehlende Autorisierung.

Häufige Frage

Kann ich das gesamte angezeigte Guthaben senden? Nur wenn die App eine durchführbare Nettozahlung berechnet und die Gebühren gedeckt sind. Der Saldo kann nicht verfügbare Coins enthalten.

Hier kannst du pausieren

Speichere oder verwerfe einen Übungsentwurf. Lege nie eine echte PSBT im Kursportal ab.

Eine Anzeige meldet „transaction version 2“. Beweist das, dass die Datei PSBT v2 ist?

1. Nein. Die Angaben bezeichnen verschiedene Versionsfelder.
2. Ja, immer.
3. Es beweist die Verwendung von Taproot.

> **Antwort anzeigen: Nein. Die Angaben bezeichnen verschiedene Versionsfelder.**
> BIP370 unterscheidet die Version des Behälters von der Transaktionsversion.

Mit Original und mit BIT signieren

Lernziel

Schließe jeden Signaturablauf ab und empfange eine Antwort, die zum richtigen Vorgang gehört.

Grundlagen

Original: Übertrage die PSBT im unterstützten Ablauf mit Cuvex Mirror über die Transportkarte. Lies die Anfrage auf dem Gerät, lege das Kryptogramm vor und entsperre es privat. Prüfe alle Ausgänge, Beträge, Wechselgeld und Gebühr. Die Antwort wird auf die Karte geschrieben, anschließend in Desk eingelesen und validiert. Das erfolgreiche Beschreiben der Karte ersetzt den Rückweg nicht.

BIT: Wähle das richtige Laufwerk und liefere die Anfrage über USB-C. Der lokale Desk-Dienst wickelt den vorgesehenen Austausch ab, während du das Gerät bedienst. Lege das Kryptogramm nach Anzeige vor und prüfe auf BIT. „Von BIT empfangen“ importiert die Antwort. Desk validiert und speichert sie vor der Empfangsquittung. Nach einer Trennung ist derselbe Vorgang wiederaufzunehmen, kein nur ähnlich aussehender.

Bei Multisig-Signaturen in den Final-Firmwares prüfst du die erforderliche Zusammenfassung und Ausgänge, zutreffende Warnungen und die drei abschließenden Bestätigungen für „PSBT signieren“. Die optionale erweiterte Ansicht zeigt zusätzliche Parameter. „Nein“ hebt keine Pflichtprüfung auf. Die unabhängige Richtlinienprüfung ist ein eigener Ablauf mit eigenem Prüfumfang.

Zum Signieren ist ein kompatibles Kryptogramm mit überprüfbarer Echtheit erforderlich. Eine ältere Kopie kann noch der Wiederherstellung dienen, ohne zum Signieren zugelassen zu sein. Meldet das Gerät eine alte Kopie ohne geprüfte Echtheit, stelle das Geheimnis nach Anleitung wieder her, prüfe es und erstelle vor dem Signieren eine neue Kopie. Verändere keine Datenköpfe und umgehe die Ablehnung nicht.

Brich ab bei abweichender Adresse, unerwarteter Gebühr, fehlenden Daten, falschem Netz oder abgelehnter Richtlinie. Zeitdruck im Gespräch ist kein Grund zur Freigabe. Die KI drückt keine Tasten, erteilt keine Endbestätigung und erklärt ungeprüfte Schritte nicht für signiert.

Übung

1. Durchlaufe den Zweig deines Modells mit einer leeren Wallet oder in einem physisch abgenommenen Labor.

2. Simuliere einen Stopp vor den abschließenden Bestätigungen und erkläre, weshalb das keine Autorisierung ist.
3. Prüfe Rückweg, Bezug zum Entwurf und bei BIT Empfangs- und Quittungsstatus.

Zeig, was du kannst

Beschreibe den Ablauf ohne Zugangsdaten. Unterscheide Gerätefreigabe, importierte Antwort und veröffentlichte Transaktion.

Häufige Frage

Weiß das Offline-Gerät, ob die Eingänge noch unbenutzt sind? Es kann den aktuellen Kettenstand nicht allein prüfen. Die App muss die finale Transaktion mit ihrer Netzwerkquelle abgleichen.

Hier kannst du pausieren

Bei Unterbrechung brich ab oder lasse gemäß Ablauf einen eindeutig zugeordneten offenen Vorgang zurück, ohne sichtbare Geheimnisse.

BIT hat signiert, Desk bestätigt aber keinen Empfang. Von welchem Stand gehst du aus?

1. Die Zahlung ist endgültig veröffentlicht.
2. Empfang oder Prüfung der Antwort steht aus. Nimm denselben Vorgang wieder auf.
3. Die Wallet ist verloren.

> **Antwort anzeigen: Empfang oder Prüfung der Antwort steht aus. Nimm denselben Vorgang wieder auf.**
> Signieren, Empfangen und Veröffentlichen sind getrennte Schritte.

Finalisieren, veröffentlichen und Störungen beheben

Lernziel

Schließe den Zahlungsvorgang ohne Doppelzahlung ab und ordne Fehler der jeweiligen Phase zu.

Grundlagen

Nach dem Signaturimport muss Desk die Zuordnung zum Entwurf und die unveränderte Zahlungsabsicht prüfen. Bei Multisig kann die Schwelle noch fehlen. Auch bei Einzelsignatur entfällt die Prüfung nicht. Finalisieren erzeugt bei erfüllten Bedingungen die verbreitungsbereite Transaktion.

Veröffentliche erst nach der Endprüfung. Serverantwort oder txid melden ein Ergebnis der Anfrage. Prüfe anschließend Annahme und Kettenstand. Bleibt die Antwort aus, frage vor dem Wiederholen nach. Erstelle zur Behebung eines Anzeigeproblems keine neue Zahlung.

Prüfe bei einer ausstehenden Zahlung Gebührensatz, Gültigkeit, Konflikte und tatsächliche RBF-Möglichkeit. Ändern sich Richtlinie oder Empfänger, braucht der neue Vorschlag passende neue Signaturen. Ein lokaler Abbruch zerstört keine Signatur oder Transaktion, die jemand anders aufbewahrt, und widerruft keine Bestätigung.

Diagnostiziere nach Phasen: Vorbereitung, Transport, Entsperren, Prüfen, Signatur, Rückweg, Validierung, Finalisierung, Verbreitung und Bestätigung. Notiere System, Version, Modell, Phase, ungefähre Uhrzeit und Fehlercode. App-Diagnosen sollen sensible Angaben ausschließen. Prüfe sie vor Weitergabe und füge weder Kopien, QR-Codes, Chat-Schlüssel noch Zugangsdaten bei.

Übung

1. Ordne die Zustände einer fiktiven Zahlung und finde eine sichere Pausenstelle.
2. Löse drei Fälle: unzureichendes Guthaben, nicht empfangene USB-Antwort und Verbindungsabbruch bei Veröffentlichung.
3. Formuliere eine Supportanfrage mit synthetischen Daten und überprüfbarem Soll-Ergebnis.

Zeig, was du kannst

Bestimme, ob die nächste Handlung bei dir, dem Gerät, dem Koordinator oder dem Netz liegt. Vermeide eine unnötige zweite Zahlung.

Häufige Frage

Behebt ein wahlloses Firmwareupdate FIRMWARE_CAPABILITY_REQUIRED? Nein. Im dokumentierten Desk-Fall musste der Desk-Katalog korrigiert werden, damit er den Final-Build erkennt. Prüfe Version und Profil vor Geräteänderungen.

Hier kannst du pausieren

Speichere Stand und nächste Handlung. Bewahre den Nachweis einer außerhalb des Labors veröffentlichten echten Transaktion in deinen privaten Unterlagen auf.

Welche Handlung kann eine bereits bestätigte Transaktion für sich widerrufen?

1. Den lokalen Entwurf löschen.
2. Mirror schließen.
3. Keine dieser Handlungen.

> **Antwort anzeigen: Keine dieser Handlungen.**
> Lokales Löschen schreibt die Kette nicht um und zieht bereits verbreitete Autorisierungen nicht zurück.

Was sich bei Bitcoin beobachten lässt

Lernziel

Unterscheide öffentliche Daten, Rückschlüsse und Informationen, die du außerhalb der Kette ergänzt.

Grundlagen

Bitcoin-Transaktionen auf der Blockchain sind öffentlich. Skripte, darstellbare Adressen, Beträge, Beziehungen zwischen Ein- und Ausgängen und die Position in Blöcken sind analysierbar. Dein Name erscheint nicht zwangsläufig. Ein identifizierter Kauf, eine veröffentlichte Rechnung oder eine geteilte Adresse können dich aber mit der Historie verbinden.

Pseudonymität bedeutet, mit Kennungen zu arbeiten, die für sich genommen nicht deiner bürgerlichen Identität entsprechen. Anonymität erfordert eine Gruppe und Bedingungen, unter denen ihre Mitglieder nicht unterscheidbar sind. Eine App-Installation allein schafft sie nicht. Privatsphäre hängt vom Kontext ab. Ein Händler kennt deine Zahlung, eine Börse unter Umständen deine Auszahlung, ein Server die Anfragen und eine andere Person kann deine Geräte beobachten.

Unterscheide Fakten und Rückschlüsse. „Dieser Ausgang wurde in dieser Transaktion ausgegeben“ ist auf der Kette prüfbar. „Alle Eingänge gehören derselben Person“ ist eine fehlbare Faustregel. Identifizierung außerhalb der Kette kann eine Hypothese stützen, ohne alle Deutungen sicher zu machen.

Adresswiederverwendung erleichtert das Zusammenführen von Aktivitäten. Das Verbinden von UTXOs aus unterschiedlichen Kontexten kann Zusammenhänge offenlegen. Eine xpub macht mehr beobachtbar als eine einzelne Adresse. Eine mitgeteilte txid kann zusätzliche Ausgänge und Beziehungen verraten, die der Empfänger nicht kennen musste.

Übung

1. Markiere in einer fiktiven Transaktion öffentliche Daten und deine eigenen Kennzeichnungen.
2. Ergänze eine Rechnung mit Namen und beschreibe die neue Verknüpfung.
3. Formuliere eine Supportanfrage zur Fehlerbehebung ohne Adresse, Deskriptor oder Guthaben.

Zeig, was du kannst

Unterscheide „Das ist beobachtbar“ und „Das ist eine Schlussfolgerung“ und benenne fehlende Belege.

Häufige Frage

Bin ich anonym, wenn ich Adressen nie wiederverwende? Nein. Auswahl der Eingänge, Wechselgeld, Abfragen, Gegenparteien und andere Metadaten bleiben relevant.

Hier kannst du pausieren

Bewahre eine Übersicht der Beobachter ohne echte Identitäten oder Transaktionen auf.

Welche Angabe ermöglicht es häufig, eine Familie von Kontoadressen zu beobachten?

1. Die Farbe des Symbols.
2. Die xpub des Kontos zusammen mit ausreichendem Ableitungskontext.
3. Die Kabelmarke.

> **Antwort anzeigen: Die xpub des Kontos zusammen mit ausreichendem Ableitungskontext.**
> Erweiterte öffentliche Informationen sind für die Privatsphäre sensibel, selbst wenn sie allein keine Ausgabe autorisieren.

Kontexte trennen und Wechselgeld verwalten

Lernziel

Triff Ausgabeentscheidungen passend zur Herkunft deiner UTXOs.

Grundlagen

Die Trennung von Kontexten beginnt vor der Zahlung. Ordne einen Eingang Erspartem, beruflicher Tätigkeit, Alltagsausgaben oder einer bestimmten Beziehung zu. Halte diese Angaben in privaten Labels fest, damit du die Trennung bei späterer Auswahl nicht aus Unwissenheit aufgibst.

Labels trennen Ausgänge nicht kryptografisch. Gibst du zwei UTXOs aus verschiedenen Kontexten zusammen aus, veröffentlicht die Transaktion ihre Verbindung. Konsolidierung senkt die Zahl der Eingänge für spätere Zahlungen, verstärkt aber den Zusammenhang der zusammengefassten Ausgänge. Bei niedrigen Gebühren kann das effizient sein und dennoch deinem Datenschutzziel widersprechen.

Wechselgeld ist ein neuer Ausgang unter derselben Richtlinie und kein „unsichtbares Geld“. Spätere Verwendung kann frühere Zusammenhänge weitertragen. Markiere eine Adresse nicht wegen eines ungewöhnlichen Betrags als Wechselgeld. Bei echter Prüfung muss das Gerät die Zugehörigkeit zur Wallet verifizieren.

Vermeide mechanische Muster bei Beträgen, Zeitpunkten und wiederholten Übertragungen. Auch sie können erkennbar sein und zusätzliche Gebühren erzeugen. Prüfe, wer bereits welche Informationen hat und was die vorgeschlagene Transaktion neu veröffentlichen würde. Keine Abfolge löscht veröffentlichte Historie.

Übung

1. Erstelle fünf fiktive UTXOs aus drei Kontexten und bereite eine Zahlung mit möglichst wenigen nötigen Kontexten vor.
2. Bestimme den Wechselgeldausgang und wähle eine passende Kennzeichnung.
3. Vergleiche Kosten und mögliche Offenlegung bei vollständiger Konsolidierung und getrennter Aufbewahrung.

Zeig, was du kannst

Begründe die Konsolidierung oder ihre Ablehnung konkret, ohne eine allgemeingültige Regel zu unterstellen.

Häufige Frage

Trennt eine Überweisung an eine andere eigene Adresse die Historie? Nein. Sie veröffentlicht eine zusätzliche Verbindung und kann Kosten verursachen, ohne die Bedrohung zu mindern.

Hier kannst du pausieren

Bewahre die Begründung aus dem Labor und die gewählte Auswahlregel auf.

Was kann passieren, wenn du Gehalt und Spenden in einer Transaktion konsolidierst?

1. Eine Verbindung zwischen den Eingängen wird sichtbar.
2. Ihr öffentlicher Ursprung wird gelöscht.
3. Sie werden garantiert zu anonymem Bargeld.

> **Antwort anzeigen: Eine Verbindung zwischen den Eingängen wird sichtbar.**
> Das Verringern der UTXO-Zahl kann mehr Verbindungen sichtbar machen.

M07

Privatsphäre im Netz, Tor und VPN

Lernziel

Unterscheide die Privatsphäre der Verbindung von der Privatsphäre auf der Blockchain.

Grundlagen

Ein Abfrageserver kann Anfragen einer Verbindung zuordnen. Dein Internetanbieter sieht je nach Transport Ziele oder Muster. Ein VPN verlagert einen Teil des Vertrauens zum VPN-Betreiber. Es entfernt keine öffentlichen Bitcoin-Informationen und verhindert nicht, dass ein identifiziertes Konto dich wiedererkennt.

Tor leitet Daten über ein Netzwerk und vermindert bestimmte Verknüpfungen zwischen Ursprung und Ziel. Es macht keine Bitcoin-Adresse privat und schützt keine App, deren Daten nicht über Tor laufen. Das Starten von Tor Browser richtet Desk, Bitcoin Core und andere Computerprogramme nicht automatisch ein.

Prüfe Netzwerkpfad und Konfiguration vor einer Aussage über den Schutz. Die geprüfte Desk-Fassung setzt keinen eingebauten Tor-Schalter voraus. Der Einsatz eines Knotens oder Proxys erfordert technische Anleitung und Kontrolle des tatsächlichen Verkehrs. Ein Feld in einer anderen Wallet belegt kein entsprechendes Desk-Feld.

Auch DNS, Kontosynchronisierung, Explorer-Links und Kursdienste können Informationen offenlegen. Eine Einrichtung kann Saldoabfragen schützen und beim Öffnen eines öffentlichen Explorers Aktivitäten verraten. Definiere Umfang und Verhalten bei Verbindungsfehlern. Vermeide stille Wechsel zu einem weniger privaten Anbieter.

Übung

1. Zeichne den Weg vom Computer über Internetanbieter, möglichen Proxy und Knoten oder Dienst zum Bitcoin-Netzwerk.
2. Markiere, wer Abfragen erhält und wer deine Identität aus der Geschäftsbeziehung kennt.
3. Simuliere einen nicht antwortenden privaten Knoten. Entscheide bewusst zwischen Pause und Quellenwechsel unter Berücksichtigung der Datenoffenlegung.

Zeig, was du kannst

Erkläre, welche Bedrohung deine Konfiguration mindert und welche bestehen bleibt.

Häufige Frage

Garantiert Tor, dass mir niemand eine Zahlung zuordnen kann? Nein. Gegenparteien, geschäftliche Identifizierung, Muster und Bedienfehler können die Verbindung weiter offenlegen.

Hier kannst du pausieren

Dokumentiere den Schutzumfang ohne private Endpunkte oder Passwörter.

Zwingt das Öffnen von Tor Browser Desk dazu, über Tor abzufragen?

1. Ja, weil beide auf demselben Computer laufen.
2. Ja, wenn das Symbol sichtbar ist.
3. Nein. Der Netzwerkpfad jeder Anwendung muss eingerichtet und geprüft werden.

> **Antwort anzeigen: Nein. Der Netzwerkpfad jeder Anwendung muss eingerichtet und geprüft werden.**
> Der Schutz einer Anwendung überträgt sich nicht automatisch auf andere.

CoinJoin, Payjoin und heutige Grenzen

Lernziel

Verstehe gemeinsame Transaktionsverfahren, ohne ihnen unbelegte Anonymität oder Kompatibilität zuzuschreiben.

Grundlagen

Bei CoinJoin bringen mehrere Personen Eingänge in eine Transaktion ein, um bestimmte Rückschlüsse auf Ein- und Ausgänge zu erschweren. Das unterscheidet sich von der Übergabe an einen Verwahrdienst, der andere Coins verspricht. Prüfe je nach Aufbau Koordination, Verwahrung, Gebühren, Widerstandsfähigkeit gegen böswillige Teilnehmer und spätere Handhabung.

Payjoin kombiniert Eingänge von Zahlendem und Empfänger in einer gemeinsamen Zahlung und schwächt einige Annahmen über gemeinsame Kontrolle. Beide Seiten benötigen passende Unterstützung und ein konkretes Protokoll. Der Kurs erklärt die Technik. Die geprüften Quellen belegen keine integrierte, betriebsfähige Payjoin- oder CoinJoin-Funktion in Cuvex Desk.

Verfügbarkeit und Rechtslage ändern sich. Die Wasabi-Dokumentation verzeichnet die Schließung des zkSNACKs-Koordinators am 1. Juni 2024. Ein früherer Button garantiert keinen heutigen Dienst. Das US-Justizministerium meldete 2025 Schuldbekenntnisse und spätere Verurteilungen der Samourai-Gründer. Daraus folgt keine generelle Rechtswidrigkeit sämtlicher Datenschutztechniken in jedem Land.

Eine Technik kann einen Rückschluss erschweren und andere unberührt lassen. Eine bereits identifizierte Herkunft verschwindet nicht aus den Aufzeichnungen einer Gegenpartei. Spätere Neukombinationen, Metadaten und Fehler im Teilnehmerkreis können den Schutz schwächen. Manche Dienste verwenden für Coins mit bestimmter Historie unterschiedliche Geschäftsrichtlinien.

Übung

1. Vergleiche eine gewöhnliche Transaktion, eine gemeinsame Transaktion und einen Dienst mit Fremdverwahrung. Führe keine echten Vorgänge aus.
2. Prüfe für ein konkretes Werkzeug Version, Verantwortliche, Dienststatus und aktuelle Dokumentation, bevor du seinen Einsatz vorschlägst.

3. Unterscheide technische, verwahrungsbezogene und rechtliche Risiken. Der Tutor darf keine Umgehung von Kontrollen entwerfen und keine „unverfolgbaren Mittel“ versprechen.

Zeig, was du kannst

Erkläre einen begrenzten Vorteil und mindestens zwei Risiken oder Anforderungen einer Datenschutztechnik.

Häufige Frage

Braucht Cuvex für private Verwahrung einen Mixer? Nein. Die Kontrolle über Abfragen, Daten, Schlüssel und UTXO-Auswahl mindert bereits konkrete Risiken, ohne vollständige Verborgenheit zu versprechen.

Hier kannst du pausieren

Vermerke ohne Kompatibilitätsnachweis „untersucht“ und nicht „unterstützt“.

Welche Aussage ist vertretbar?

1. CoinJoin garantiert dauerhafte Anonymität.
2. Ein gemeinsames Verfahren kann bestimmte Rückschlüsse erschweren. Es hat Voraussetzungen und Grenzen.
3. Jeder als Mixer bezeichnete Dienst bewahrt die Selbstverwahrung.

> **Antwort anzeigen: Ein gemeinsames Verfahren kann bestimmte Rückschlüsse erschweren. Es hat Voraussetzungen und Grenzen.**
> Die Eigenschaften hängen von Protokoll, Umsetzung, Teilnehmern und späterer Nutzung ab.

Lehren aus dokumentierten Vorfällen

Lernziel

Leite aus dokumentierten Vorfällen überprüfbare Entscheidungen ab, ohne Wettbewerber anzugreifen oder den Schutz zu übertreiben.

Grundlagen

Mt. Gox: Eine Anklage des US-Justizministeriums von 2023 beschreibt unbefugte Zugriffe auf Server und Schlüssel und das anschließende Verschwinden von Kundengeldern. Eine Anklage enthält Vorwürfe und ist kein Urteil. Frage bei der Verwahrung, wer die Schlüssel tatsächlich kontrolliert und was bei Ausfall des Unternehmens geschieht.

Ledger Connect Kit, Dezember 2023: Ledger dokumentierte eine schädliche Veröffentlichung einer Bibliothek für dezentrale Anwendungen nach Kompromittierung des Zugangs eines früheren Mitarbeiters. Betroffen war die Softwarelieferkette. Nutzer von EVM-DApps wurden zum Signieren getäuscht. Der Vorfall belegt weder einen Bruch der Ledger-Hardware noch des Bitcoin-Konsenses.

Bybit, Februar 2025: Das FBI schrieb Nordkorea den Diebstahl virtueller Vermögenswerte im Wert von rund 1.500 Millionen US-Dollar zu. Betroffen waren eine Börse und Werte anderer Netzwerke. Das belegt keinen Bruch der Bitcoin-Kryptografie. Prüfe die Absicht einer Signatur und vermeide, dass mehrere Menschen blind demselben Bildschirm vertrauen.

Coinbase, Mai 2025: Das Unternehmen meldete Datendiebstahl durch bestochene Supportmitarbeiter zur Vorbereitung von Social Engineering. Nach seinen Angaben wurden weder Passwörter noch private Schlüssel offengelegt. Auch ein Betrüger kann echte Kundendaten kennen.

Auch Bitcoin Core veröffentlicht Softwarefehler. CVE-2024-35202 beschrieb eine aus der Ferne auslösbare Beendigung in Versionen vor 25.0. Regelprüfung ersetzt keine Softwarewartung. Aus dem Hinweis lässt sich kein Schlüsseldiebstahl ableiten.

Im Januar 2026 berichtete The Register über die Offenlegung von Bestell- und Kontaktdaten von Ledger-Käufern über Global-e. Bestätigungen wurden beiden Unternehmen zugeschrieben. Laut diesen Aussagen waren Wiederherstellungsschlüssel nicht betroffen. Ein Kauf kann den Gerätebesitz offenbaren, ohne dass die Hardware überwunden wurde.

Im April 2026 berichtete The Record über den Angriff auf Drift und die von der Plattform angekündigte Aussetzung von Ein- und Auszahlungen. Drift ist ein dezentrales Finanzprotokoll auf Solana. Es handelte sich nicht um einen Bruch von Bitcoin. Frühe Verlustschätzungen und spätere Wiederherstellungsmaßnahmen dürfen nicht als endgültige Summe oder garantierte Erstattung erscheinen.

Übung

1. Ordne jeden Vorfall Verwahrung, Oberfläche oder Verteilung, personenbezogenen Daten, Protokollen anderer Netze und Verfügbarkeit zu.
2. Nenne für jeden Vorfall eine Vorbeugung und eine Grenze dieser Vorbeugung.
3. Übe einen Betrugsanruf: „Ich kenne deinen Kauf. Verschiebe deine Mittel auf diese sichere Adresse.“ Lege auf und prüfe über einen selbst eingeleiteten Kontakt.

Zeig, was du kannst

Erkläre, warum kein Vorfall eine andere Marke als unverwundbar ausweist. Belege gelten für einen bestimmten Umfang.

Häufige Frage

Sind das alle neuesten Angriffe? Nein. Es ist eine für die Ausgabe vom 17. November 2026 geprüfte Auswahl, keine vollständige Liste oder Live-Beobachtung.

Hier kannst du pausieren

Notiere, welche Gewohnheit du ändern willst und wie du ihre Einhaltung prüfst.

Ein Anrufer kennt deinen Kauf und fordert eine Überweisung an eine „Rettungswallet“. Was belegt sein Wissen?

1. Die Information kann aus einem Datenleck stammen. Sie bestätigt weder seine Identität noch die Adresse.
2. Er ist zwingend ein legitimer Supportmitarbeiter.
3. Du musst deinen Seed teilen.

> **Antwort anzeigen: Die Information kann aus einem Datenleck stammen. Sie bestätigt weder seine Identität noch die Adresse.**
> Wahre Angaben können für eine glaubwürdige Täuschung eingesetzt werden.

Chat-Identität erstellen und Kontakte prüfen

Lernziel

Aktiviere eine Chat-Identität, ohne ihren Schlüssel offenzulegen, und prüfe die Gegenseite.

Grundlagen

Desk verknüpft den Chat über einen auf Cuvex erzeugten Chat-Schlüssel mit dem Kryptogramm. Auch wenn seine Darstellung wie eine xpub aussieht, bleibt er geheim. Behandle ihn nicht als öffentlichen Schlüssel eines WOW-Kontos. Der Tutor muss ihn weder lesen noch als QR-Code sehen.

Der Ablauf unterscheidet einen neuen Alias von Übertragung oder Wiederherstellung eines bestehenden. In der geprüften Implementierung wählst du das passende iOS- oder Android-Mobilprofil. Historisch abgeleitete Identitäten sind nicht beliebig austauschbar. DEV und Produktion sind getrennte Umgebungen. Ein Wechsel migriert Gespräche oder Aliase nicht automatisch.

Das Hinzufügen eines Alias prüft keine Identität. Vergleiche den Fingerabdruck über einen unabhängigen authentifizierten Kanal. Nutze bei Erkennungsfragen keine öffentlichen Angaben und keine Antworten, die Passwörter offenbaren. Stimmen lassen sich imitieren. Kombiniere in Risikosituationen vorher vereinbarte Verfahren.

Ändert sich die Identität eines Kontakts, pausiere Zahlungen und Koordination bis zur Klärung. Es kann eine legitime Wiederherstellung oder eine böswillige Ersetzung vorliegen. Ende-zu-Ende-Verschlüsselung schützt einen Kanal gemäß Protokoll und Umsetzung, beweist aber nicht, wer das Gerät der Gegenseite benutzt.

Übung

1. Erkläre in einer Testumgebung Erstellung oder Wiederherstellung, ohne den Chat-Schlüssel preiszugeben.
2. Füge einen Laborkontakt hinzu und vereinbare über einen anderen Kanal einen Fingerabdruckvergleich.
3. Simuliere einen Identitätswechsel und lege fest, wie du ihn vor einer Zahlung bestätigen würdest.

Zeig, was du kannst

Unterscheide Alias, öffentlichen Fingerabdruck, geheimen Chat-Schlüssel und persönliches Vertrauen.

Häufige Frage

Garantiert ein alter Alias dieselbe Person? Nein. Prüfe Kontinuität und Schlüsselwechsel im vorgesehenen Ablauf.

Hier kannst du pausieren

Speichere nur „Testkontakt verifiziert“ und die Methode, ohne Schlüssel und private Fragen.

Eine als Chat-Schlüssel bezeichnete Zeichenfolge sieht wie eine xpub aus. Wie behandelst du sie in Desk?

1. Als Angabe zum Veröffentlichen in Foren.
2. Als Geheimnis zur Wiederherstellung der Identität.
3. Als Bitcoin-Empfangsadresse.

> **Antwort anzeigen: Als Geheimnis zur Wiederherstellung der Identität.**
> Die äußere Form bestimmt weder Vertraulichkeit noch Zweck.

M08

Im Chat Satoshis anfordern und bezahlen

Lernziel

Wechsle vom Gespräch zur Zahlung, ohne Prüfschritte oder Kontext zu verlieren.

Grundlagen

Im Chat lassen sich Adressen anfordern, Empfangsadressen beantworten, Zahlungen anfragen und die Vorbereitung aus einem WOW-Konto öffnen. Der erhaltene Gesprächskontext vermeidet Kopierfehler zwischen Apps. Er macht nicht jede Nachricht zu einem authentifizierten Ausgabeauftrag.

Prüfe vor Antworten oder Bezahlen verifizierten Kontakt, Netz, Betrag und ursprüngliche Anfrage. Das gemeinsame Formular behält UTXO-Auswahl und Gebühr bei. Bei „Alles senden“ kann der Nettobetrag nach Gebühren unter der angeforderten Summe liegen. Kennzeichne die Zahlung gegebenenfalls als Teilzahlung.

Die Autorisierung bleibt auf Cuvex. Der Chat transportiert Absicht und Koordination und darf nicht automatisch signieren. Eine dem Kontakt gesendete Zahlungsmitteilung muss zwischen dem Empfang einer Nachricht und einer bestätigten Transaktion unterscheiden. Der Empfänger prüft über sein eigenes Konto oder seine Quelle.

Externe Links, angehängte QR-Codes und Adressen sind bis zur Prüfung unvertrauenswürdig. „In Mempool ansehen“ kann einen Drittanbieter öffnen und Abfragen offenlegen. Sieht dein Plan einen eigenen Knoten vor, nutze die unterstützte Prüfung in WOW und beurteile jeden Wechsel zu öffentlichen Diensten.

Übung

1. Spiele zwei Rollen: Ein Empfänger bittet um 50.000 sat, ein Zahlender bereitet die Zahlung ohne Veröffentlichung vor.
2. Simuliere einen verfügbaren Nettobetrag von 48.000 sat. Erkläre die noch nötige Zustimmung und Abstimmung für eine Teilzahlung.
3. Ändere in einer Testnachricht absichtlich das Netz und stoppe den Ablauf.

Zeig, was du kannst

Verfolge den Zusammenhang zwischen Anforderung, Adresse, Entwurf, Signatur und Bestätigung. „Der Chat sagt OK“ reicht nicht.

Häufige Frage

Bedeutet „Sats im Chat senden“ Lightning? Nein. Der dokumentierte WOW-Ablauf bereitet Bitcoin-On-Chain-Zahlungen vor. Sats bezeichnen eine Einheit, kein Transportnetz.

Hier kannst du pausieren

Verwirf den Laborentwurf oder halte den Status fest. Veröffentliche nichts nur zur Demonstration der Oberfläche.

Du erhältst im Chat eine Bestätigung. Welche Prüfung entscheidet über den Zahlungseingang?

1. Dass das Nachrichtensymbol grün ist.
2. Dass der Gesprächspartner „bestätigt“ sagt.
3. Die Transaktion und ihre Ausgänge über eine geeignete Quelle im Netzwerk prüfen.

> **Antwort anzeigen: Die Transaktion und ihre Ausgänge über eine geeignete Quelle im Netzwerk prüfen.**
> Nachrichtenstatus und Transaktionsstatus sind nicht gleichbedeutend.

Kryptogramme bewusst weitergeben

Lernziel

Verstehe, was es bedeutet, einer anderen Person eine verschlüsselte Kopie zu geben.

Grundlagen

Das Teilen eines Kryptogramms übermittelt eine Kopie des verschlüsselten Objekts. Es überträgt nicht zwangsläufig Bitcoin und fügt für sich keinen Signierer hinzu. Erhält der Empfänger genügend Entsperrmittel, kann er gemäß Schutzschema auf den Inhalt zugreifen. Entscheide vorher, welche Fähigkeit du weitergibst.

Ende-zu-Ende-Verschlüsselung des Chats und Dateiverschlüsselung schützen unterschiedliche Ebenen. Nach dem Download kann der Empfänger das Objekt außerhalb des Chats speichern. Das Löschen deiner Nachricht oder deines lokalen Eintrags zieht nicht alle Kopien zurück. Ein im selben Kanal mitgeteiltes Passwort führt Schutzkomponenten auf einem Weg zusammen.

Prüfe vor dem Senden Identität, Format und Zweck. Die Verknüpfung eines empfangenen Kryptogramms ordnet eine Kopie. Sie belegt nicht, dass jede Datei gefahrlos zu entschlüsseln ist. Verwende keine Anhänge, die auf einer externen Seite Seed oder Passwort verlangen.

Für die Wiederherstellung braucht es eine Vereinbarung: Wer verwahrt welche Komponente, wer kann sie öffnen, wie erkennt man eine Offenlegung und wie ändert sich die Verwahrung bei Ende der Beziehung? Für eine normale Zahlung reicht meist eine geprüfte Adresse ohne Weitergabe des Kryptogramms.

Übung

1. Plane die Übertragung eines verschlüsselten Übungstexts an einen Laborkontakt.
2. Zähle auf, was der Empfänger vor und nach Kenntnis des Passworts weiß und tun könnte.
3. Simuliere das Ende der Beziehung. Erkläre, warum das Löschen der Nachricht Kopie und Schlüssel nicht widerruft.

Zeig, was du kannst

Unterscheide „Daten geteilt“, „Zugang zu einem Geheimnis geteilt“ und „Ausgabe signiert“.

Häufige Frage

Kann eine verschlüsselte Datei folgenlos zirkulieren? Sie kann Metadaten offenlegen, Passwortversuche erleichtern und unbegrenzt aufbewahrt werden. Prüfe, ob Weitergabe nötig ist.

Hier kannst du pausieren

Lasse keine Verwahrungsanhänge im Kurs. Halte nur die Erkenntnis der Übung fest.

Ist das Versenden eines Kryptogramms im Chat eine Bitcoin-Zahlung?

1. Nein. Es überträgt ein Objekt mit einem andersartigen Inhalt und Zugriff.
2. Ja, wenn sein Name auf .bin endet.
3. Es aktiviert automatisch eine neue Multisig.

> **Antwort anzeigen: Nein. Es überträgt ein Objekt mit einem andersartigen Inhalt und Zugriff.**
> Geheimnisse zu transportieren und UTXOs zu bewegen sind unterschiedliche Vorgänge.

M08

Chat wiederherstellen und Metadaten verstehen

Lernziel

Plane einen Gerätewechsel und unterscheide die Wiederherstellung von Identität und Nachrichten.

Grundlagen

Desk gibt an, Chatverlauf und Sitzungen lokal zu verschlüsseln und von seiner globalen Sicherung auszunehmen. Der Chat-Schlüssel ermöglicht die Wiederherstellung der Identität, garantiert aber keine vollständigen früheren Unterhaltungen. Die App kennt Zustände und Aktionen für ausstehende Aktivierung, Schlüsselpflege und lokale Wiederherstellung bei passendem Material.

Laut geprüfter Anleitung darf jeder Alias jeweils nur auf einem Gerät genutzt werden. Aktiviere ihn nicht zugleich auf zwei Geräten, um eine nicht unterstützte Synchronisierung zu testen. Halte beim Umzug das Verfahren ein und prüfe die Kontinuität mit den Kontakten.

„Ausstehend“, „vom Server angenommen“, „empfangen“ und „Entschlüsselung fehlgeschlagen“ bezeichnen verschiedene Phasen. Versende nichts blind erneut, solange der erste Empfang ungeklärt ist. Fehlt ein Sitzungsschlüssel oder ändert sich die Identität, ist eine gespeicherte wartende Nachricht noch nicht gelesen.

Verschlüsselter Inhalt verbirgt nicht zwangsläufig Zeiten, Größe, Zustellbeziehungen, Aliase oder Verbindungsdaten vor allen beteiligten Systemen. Ähnliches gilt für Sprache. Transportverschlüsselung macht einen gewöhnlichen Anruf nicht zum geeigneten Kanal für Geheimnisse. Nutze nur die zum Lernen und zur Fehlerklärung nötigen Daten.

Übung

1. Simuliere den Verlust des PCs und erkläre, was jedes vorhandene Material wiederherstellt.
2. Ordne Nachrichtenzustände und entscheide, wann du eine Zahlungsanforderung nicht erneut sendest.
3. Entwirf einen Hinweis auf Gerätewechsel, den Kontakte über einen unabhängigen Kanal prüfen können.

Zeig, was du kannst

Erkläre, welches Gespräch verloren geht und welche Identität sich wiederherstellen lässt, ohne über die Sicherung hinauszugehen.

Häufige Frage

Löscht lokales Entfernen des Chats die Nachrichten auf der Gegenseite? Setze das nicht voraus. Empfänger können Nachrichten und Dateien selbstständig aufbewahren.

Hier kannst du pausieren

Bewahre einen Umzugsplan mit leeren, beschrifteten Feldern ohne Chat-Schlüssel auf.

Was gewährleistet der Chat-Schlüssel allein laut der geprüften Anleitung?

1. Sämtliche früheren Gespräche auf jedem beliebigen PC.
2. Die Identität über den unterstützten Ablauf wiederherstellen zu können, nicht sämtliche älteren Nachrichten.
3. Automatischen Zugriff auf die Bitcoin-Schlüssel der Kontakte.

> **Antwort anzeigen: Die Identität über den unterstützten Ablauf wiederherstellen zu können, nicht sämtliche älteren Nachrichten.**
> Identität und historisches Nachrichtenarchiv sind getrennte Fähigkeiten.

M08

Alltagseinstellungen und Berechtigungen prüfen

Lernziel

Verwalte die Desk-Einstellungen und unterscheide Komfort von Schutz.

Grundlagen

Desk bietet Nacht-, Tages- und Systemdesign, automatische Synchronisierung alle 3 oder 5 Minuten, Transaktionstöne, Chathintergrund, Sprache und Referenzwährung. Diese Einstellungen ändern Darstellung oder Abfragehäufigkeit. Sie verändern keine Bitcoin-Signatur und schaffen keine zusätzliche Anonymität.

Die geprüften Sicherheitseinstellungen umfassen Inaktivitätssperre, Sperre beim Hintergrundwechsel, maximale Verzögerung nach Fehlern und optionale Löschung. Das Inaktivitätsschema erlaubt 30 bis 86.400 Sekunden. Die Oberfläche kann eine engere Auswahl zeigen. Lies Standardwerte in deiner laufenden Version ab, statt sie aus einer aufgezeichneten Lektion abzuleiten.

Die Integration von bitcoin:-Links öffnet eine Anforderung zum Entsperren, zur Kontowahl und Prüfung. Sie gibt keine Zahlung automatisch frei. Unter Linux unterscheidet die Anleitung bei der Linkregistrierung zwischen integrierter Installation und AppImage. Eine Lightning-Rechnung benötigt einen anderen unterstützten Ablauf. Desk als Standard-App reicht dafür nicht.

Kurs, Preisgrafik und Informationslinks können externe Dienste abfragen. Sie dienen der Information und sind kein Kaufsignal. Prüfe Datum und Quelle für die Umrechnung. Dunkles Design oder kleines Fenster dürfen Abschlussschaltflächen, Adresse oder Gebühr nicht verdecken. Halte andernfalls an und melde das Darstellungsproblem.

Übung

1. Ändere Darstellung und Sperre im Übungsspeicher und teste den erneuten Zugang.
2. Prüfe die aktivierten Automatismen. Synchronisierung, Töne und Firmwareprüfung sind getrennte Funktionen.
3. Öffne eine fiktive bitcoin:-Anforderung und brich vor der Vorbereitung eines echten Vorgangs ab.

Zeig, was du kannst

Erkläre die Wirkung jeder Einstellung und identifiziere solche mit Abfragen oder sensiblen Aktionen.

Häufige Frage

Ersetzt die PC-Biometrie meine Wiederherstellungskopie? Nein. Sie kann vom Gerät und vom sicheren Systemspeicher abhängen. Behalte eine unabhängige Wiederherstellungsmöglichkeit.

Hier kannst du pausieren

Sperre Desk und notiere nur, welche Einstellungen du geändert hast.

Was ändert sich bei einer Synchronisierung alle drei Minuten?

1. Die vorgesehene Abfragehäufigkeit, während die Funktion läuft.
2. Die Signaturrichtlinie auf der Blockchain.
3. Der Seed des Geräts.

> **Antwort anzeigen: Die vorgesehene Abfragehäufigkeit, während die Funktion läuft.**
> Es handelt sich um eine Betriebseinstellung, nicht um eine Änderung der Verwahrung.

M09

Eine Multisig-Wallet entwerfen

Lernziel

Wähle eine Schwelle, die plausible Verluste und Kompromittierungen verkraftet.

Grundlagen

In einer M-von-N-Richtlinie zählt N die Teilnehmer mit unterschiedlichen Schlüsseln und M die nötigen Signaturen. Bei 2 von 3 darf ein Schlüssel ausfallen. Zwei kompromittierte Schlüssel können aber eine Ausgabe autorisieren. Liegen alle drei Seeds am selben Ort oder sind sie derselben Offenlegung ausgesetzt, sinkt ihre Unabhängigkeit.

Das geprüfte Cuvex-Multisig-Profil verwendet natives P2WSH mit sortedmulti und BIP48-Ableitung. Die Struktur von Original erlaubt bis zu sechs Richtlinienschlüssel, BIT bis zu fünfzehn. Bei gemischter Nutzung gelten die Grenzen des eingeschränkteren Teilnehmers und die tatsächliche Transportkapazität. Strukturelle Höchstwerte garantieren nicht, dass viele Schlüssel und Eingänge auf das Medium passen.

Die App erlaubt Schwellen gemäß den Beziehungen der Richtlinie. Bei 1 von N braucht eine Ausgabe jedoch keine Zusammenarbeit. Die Firmware zeigt dazu besondere Risikohinweise. Größere Zahlen erhöhen auch Koordination, Kosten, Wiederherstellungsaufwand und Sperrrisiko.

MuSig2 ist ein anderes Verfahren zur Aggregation von Schnorr-Signaturen. Für sich genommen ist es N von N, kein beliebiges 3 von 5. Die untersuchten Final-Firmwares implementieren weder das Signieren von Taproot-Eingängen noch MuSig2 oder Miniscript. P2TR als Empfänger zu unterstützen beweist keine Ausgabesignatur aus einer Taproot-Wallet.

Übung

1. Entwirf eine fiktive 2-von-3-Richtlinie mit voneinander unabhängigen Risiken für die Teilnehmer.
2. Simuliere den Verlust eines Schlüssels und die Kompromittierung eines Schlüssels. Erkläre, was möglich bleibt.
3. Prüfe vor Wahl einer größeren Richtlinie die Modellgrenzen.

Zeig, was du kannst

Benenne Verlusttoleranz, Angriffsschwelle und gemeinsame Abhängigkeiten deines Entwurfs.

Häufige Frage

Müssen bei Multisig alle die Seeds der anderen kennen? Nein. Jeder soll seine private Signierfähigkeit behalten. Gemeinsam geteilt werden die öffentlichen Daten zur Erstellung und Wiederherstellung der Richtlinie.

Hier kannst du pausieren

Speichere den Entwurf mit fiktiven Teilnehmern und Zuständigkeiten.

Wie viele private Schlüssel reichen bei 2 von 3 unabhängigen Schlüsseln aus, um die Ausgabe gemäß dieser Richtlinie zu autorisieren?

1. Einer.
2. Zwei.
3. Immer alle drei.

> **Antwort anzeigen: Zwei.**
> Die Schwelle verlangt zwei. Auch die übrigen Bedingungen und Prüfungen müssen erfüllt sein.

Einladungen erstellen und Schlüssel beitragen

Lernziel

Erstelle mit geprüften Teilnehmern eine Richtlinie, ohne Seeds weiterzugeben.

Grundlagen

Der Ersteller wählt Name, Netz, M, N, Kontakte, eigene öffentliche Angaben und die Betriebsbedingungen der Einladung. Der geprüfte Ablauf unterstützt Mainnet und Regtest, vor Anwendung der Gerätegrenzen 2 bis 15 Teilnehmer sowie 1 bis 720 Stunden Gültigkeit. Diese Bereiche ersetzen keine Kapazitätsprüfung.

Jeder Teilnehmer prüft die Einladung, nimmt sie an oder lehnt ab und liefert über den unterstützten Ablauf seinen erweiterten öffentlichen Schlüssel mit Fingerabdruck und BIP48-Pfad. Nicht benötigt werden Seeds, private Schlüssel, einzelne Adressen oder vollständige Deskriptoren anderer Wallets. Eine scheinbar gültige xpub im falschen Kontext kann eine andere Richtlinie ergeben.

Der Ersteller koordiniert. Jeder Signierer muss selbst prüfen. Vor der Finanzierung müssen alle dieselben Parameter und eine Prüfadresse rekonstruieren und verifizieren können. Die Annahme eines Chatkontakts gibt dessen spätere Richtlinien nicht automatisch frei.

Die Einladungsfrist ist eine Koordinationsregel der App. Sie ändert kein bereits finanziertes Skript, löscht keine fremd gespeicherten Signaturen und ist keine zeitliche Konsenssperre. Einen Vorschlag abzubrechen und Mittel aus einer bestehenden Richtlinie abzuziehen sind verschiedene Handlungen.

Übung

1. Erstelle im vorbereiteten Regtest-Labor mit Testkontakten einen 2-von-3-Vorschlag.
2. Spiele Annahme, Ablehnung und einen Beitrag für das falsche Netz durch. Prüfe den Stopp im letzten Fall.
3. Zähle auf, was alle vor der Finanzierung aufbewahren müssen: Netz, Schwelle, öffentliche Schlüssel, Ursprünge, Skript und geprüfte Adresse.

Zeig, was du kannst

Erkenne eine unvollständige Einladung und benenne die fehlende Freigabe. Ein bestehender Chat ist kein Nachweis.

Häufige Frage

Verhindert die Ablauffrist spätere Ausgaben? Nicht als Einladungsfeld. Eine zeitliche Bitcoin-Beschränkung erfordert bestimmte Skript- oder Transaktionsbedingungen und tatsächliche Unterstützung.

Hier kannst du pausieren

Speichere die Übungskennung des Vorschlags und die ausstehende Freigabe.

Was verlangt der dokumentierte Ablauf für deinen Beitrag zur Multisig?

1. Den Seed jedes Teilnehmers.
2. Eine beliebige Empfangsadresse.
3. Deinen erweiterten öffentlichen Schlüssel mit passendem Fingerabdruck und BIP48-Ursprung.

> **Antwort anzeigen: Deinen erweiterten öffentlichen Schlüssel mit passendem Fingerabdruck und BIP48-Ursprung.**
> Mit korrektem öffentlichem Material entsteht die Richtlinie ohne Offenlegung privater Schlüssel.

Richtlinien mit Mirror in beliebiger Reihenfolge prüfen

Lernziel

Vergleiche vollständige Felder und verstehe genau, was das Resultat belegt.

Grundlagen

Die unabhängige Prüfung zeigt Schwelle, Netz, Profil, SIGHASH, Richtlinien-ID, erste Adresse, Nutzerposition und Daten jedes Teilnehmers. Sie prüft Absicht und Konsistenz. Daraus folgt keine dauerhafte Registrierung der Richtlinie im Gerät. Der dokumentierte Umfang gilt für „diese Prüfung“.

In Mirror 12.12 kannst du zuerst den QR-Code von Cuvex oder Desk lesen und jeden Datenpunkt wählen. Du musst weder bei Schritt 1 beginnen noch alles scannen oder eine Reihenfolge einhalten. Einen von Hand geprüften, nicht gescannten Text kennzeichnet Mirror nicht als selbst geprüft.

Der Vergleich zeigt den vollständigen Wortlaut. Leerzeichen, Zeilenumbrüche, Groß- und Kleinschreibung und Unicode-Unterschiede zählen. „Übereinstimmung“ bestätigt nur die Gleichheit des Paares. Es authentifiziert keine Quelle, beweist nicht dieselbe Richtlinie und aktiviert keine Wallet. Endfreigabe und zugeordnete Antwort laufen weiterhin über Cuvex und Desk.

Heutige Desk-QR-Codes enthalten nur den Wert, keine Schrittnummer und keine Sitzung. Mirror kann den Schritt nicht immer ableiten. „Desk-Schritt angeben“ ergänzt manuell erfassten Kontext und muss so erscheinen. Bei N Teilnehmern umfasst die dokumentierte Zuordnung 7 + 4N Felder: 8+4k Fingerabdruck, 9+4k Pfad, 10+4k xpub und 11+4k Schlüssel-ID, beginnend mit k gleich null. Bei N=2 ist Schritt 15 die ID des zweiten Schlüssels. Du kannst damit anfangen.

Übung

1. Vergleiche mit synthetischen Daten zuerst eine als Schritt 15 gekennzeichnete ID, dann Netz und Schwelle.
2. Ändere ein Zeichen. Prüfe „Keine Übereinstimmung“ und beginne das nächste Paar ohne Übernahme des Ergebnisses.
3. Vergleiche „2 / 3“ und erkläre, weshalb der Text allein Schwelle und Nutzerposition nicht immer unterscheidet.

Zeig, was du kannst

Benenne geprüftes Feld, zugeordneten Kontext und ausstehende Freigaben. Teilübereinstimmungen sind keine Gesamtfreigabe.

Häufige Frage

Muss ich alle QR-Codes für das Weiterlernen scannen? Nein. Der Vergleich ist frei. Verpflichtende Prüfungen und Freigaben des Signierers haben ihren eigenen Ablauf.

Hier kannst du pausieren

Schließe den Vergleich. Laut geprüftem Entwurf müssen die Werte beim Verlassen oder Wechsel in den Hintergrund gelöscht werden.

Mirror vergleicht zwei QR-Codes aus Schritt 15 und meldet „Übereinstimmung“. Was belegt das?

1. Zeichengleiche Übereinstimmung dieses Paars in dem festgestellten oder angegebenen Kontext.
2. Freigabe der gesamten Richtlinie.
3. Authentifizierung der Herkunft beider QR-Codes.

> **Antwort anzeigen: Zeichengleiche Übereinstimmung dieses Paars in dem festgestellten oder angegebenen Kontext.**
> Der Vergleich ersetzt weder Authentifizierung noch Gesamtprüfung oder Hardwareantwort.

Signaturen koordinieren und Multisig-Transaktionen veröffentlichen

Lernziel

Bringe einen Vorschlag bis zur Signaturschwelle, ohne Absicht oder Kontrolle aus den Augen zu verlieren.

Grundlagen

Ein Multisig-Vorgang enthält Eingänge, Empfänger, Beträge, Gebührensatz, Ersetzung und betriebliche Hinweise. Der Ersteller kann unterstützte Teilnehmer um Signaturen bitten. Jeder Signierer prüft auf eigene Verantwortung Netz, Richtlinie, Eingänge, alle Ausgänge und Gebühr vor Freigabe am Gerät.

Eine Teilsignatur bewegt ohne erreichte Schwelle noch keine Mittel. Sobald die Schwelle erreicht ist, kann der Koordinator nach Vorgabe kombinieren und finalisieren. Berichte anderer Teilnehmer oder des Koordinators dienen der Abstimmung. Sie ersetzen keine selbst vorgenommene lokale Prüfung. Die App muss ihre Herkunft unterscheiden.

Die geprüfte Fassung bietet erneuten Versuch, Signaturannahme, Quittung, Ablehnung und Übergabe der Koordination. Letztere ändert weder Schlüssel noch Schwelle auf der Kette. Ordne eine gespeicherte Antwort der Anfrage und dem tatsächlich verwendeten Profil zu. Wähle keine ähnliche Richtlinie oder einfach den ersten Katalogeintrag.

Bei geänderten Empfängern oder maßgeblichen Bedingungen prüfe einen neuen Vorschlag und hole die passenden Signaturen ein. Entferne nicht manuell Sicherheitsdaten aus einer PSBT, damit sie auf eine NFC-Karte passt. Die Firmware verlangt kompatibles Profil und Prüfungen und begrenzt Eingänge, Ausgänge und Größe.

Prüfe vor Veröffentlichung die vereinbarte Transaktion und eine mögliche bereits verbreitete Version. Verfolge danach Bestätigungen über die gewählte Quelle. Eine Ablehnung in deiner App widerruft keine bereits bei anderen gespeicherten Signaturen und verhindert nicht jede Handlung, die mit der verbleibenden Schwelle zulässig ist.

Übung

1. Spiele 2 von 3 mit drei fiktiven Rollen durch. Eine signiert, eine lehnt ab, die dritte bittet um Klärung.

2. Ändere die Adresse der Testzahlung und erkläre, warum eine frühere mündliche Zustimmung nicht ausreicht.
3. Simuliere nach dem Speichern der Signatur eine fehlgeschlagene Quittung. Nimm denselben Vorgang wieder auf, ohne Zahlung oder Profil zu ändern.

Zeig, was du kannst

Benenne Koordinator, Signierer und Finalisierenden und den Nachweis jeder Phase.

Häufige Frage

Sind zwei „OK“ im Chat zwei Signaturen? Nein. Die Schwelle wird durch gültige kryptografische Autorisierungen gemäß Richtlinie erfüllt, nicht durch Nachrichten.

Hier kannst du pausieren

Vermerke Stand, ausstehende Signaturen und nächste Zuständigkeit ohne private Inhalte.

Ein 2-von-3-Vorgang hat eine gültige Signatur und zwei Nachrichten mit „einverstanden“. Ist die Schwelle erreicht?

1. Ja, weil drei Personen beteiligt sind.
2. Nein. Eine weitere gültige kryptografische Signatur fehlt.
3. Ja, wenn der Koordinator es verkündet.

> **Antwort anzeigen: Nein. Eine weitere gültige kryptografische Signatur fehlt.**
> Zustimmung im Gespräch und gültige Signatur sind unterschiedliche Nachweise.

Eine Multisig-Wallet wiederherstellen und ändern

Lernziel

Rekonstruiere die Richtlinie und plane den Verlust oder Austausch von Teilnehmern.

Grundlagen

Zur Wiederherstellung brauchst du Daten zur Rekonstruktion der Richtlinie und ausreichend private Signiermöglichkeiten. Eine Richtlinienkopie mit xpubs kann die Historie offenlegen, ohne Seeds zu enthalten. Eine verschlüsselte Kopie schützt die Datei zusätzlich und braucht ihr Passwort. Die Endung .cuvexms beweist keine Verschlüsselung. Prüfe das konkrete Format und den Export.

In Desk 9.21 verlangt die Wiederherstellung den vom Teilnehmergerät exportierten erweiterten öffentlichen Schlüssel mit Fingerabdruck und BIP48-Pfad. Der unterstützte Ablauf liest ihn per Webcam oder Mirror ein. Ersetze diesen Beitrag nicht durch eine Empfangsadresse und sende keinen Seed an den Support.

Geht bei 2 von 3 ein Schlüssel verloren, können die anderen beiden weiterhin ausgeben. Die alte Richtlinie bleibt bestehen. Um einen Teilnehmer wirksam zu entfernen und andere Schlüssel einzusetzen, wird gewöhnlich eine neue Richtlinie erstellt und das Guthaben mit den erforderlichen Freigaben übertragen. Ein neuer Alias oder das Löschen einer Wallet aus Desk ändert bestehende UTXOs nicht.

Sicherungen müssen beide Zweige rekonstruierbar und die Historie auffindbar machen. Bewahre Indizes, ausgegebene Anforderungen und nötigen Kontext auf, damit Adressen nicht wiederverwendet und unvollständige Scans nicht als leere Wallet interpretiert werden. Nutze bei Wiederherstellung und Fortsetzung eines offenen Vorgangs das ursprünglich mit ihm gespeicherte Profil.

Übung

1. Exportiere und rekonstruiere eine Laborrichtlinie mit der dokumentierten Funktion. Prüfe Netz und bekannte Adresse.
2. Simuliere den Ausfall eines Teilnehmers und plane den Austausch, ohne echtes Guthaben zu bewegen.
3. Simuliere einen Verlust, bei dem die verfügbaren Schlüssel unter der Schwelle liegen. Support und KI können die fehlenden Signaturen nicht herstellen.

Zeig, was du kannst

Stelle das Testszenario wieder her und unterscheide die Wiederherstellung von Informationen von einer Änderung der Kontrolle über Coins.

Häufige Frage

Deaktiviert das Löschen der Multisig in Desk die Wallet für alle? Nein. Der lokale Zustand wird gemäß Ablauf entfernt. Andere Personen und Kopien können richtliniengemäß handlungsfähig bleiben.

Hier kannst du pausieren

Bewahre geprüfte Kopie und Plan privat auf. Vermerke im Kurs nur das Ergebnis.

Du willst jemanden aus einer bereits mit Guthaben versehenen Richtlinie entfernen. Genügt das Löschen des Namens in Desk?

1. Ja.
2. Ja, wenn auch der Chat gelöscht wird.
3. Nein. Plane eine neue Richtlinie und gegebenenfalls eine autorisierte Übertragung der Mittel.

> **Antwort anzeigen: Nein. Plane eine neue Richtlinie und gegebenenfalls eine autorisierte Übertragung der Mittel.**
> Die Skripte bestehender UTXOs ändern sich nicht durch das Bearbeiten lokaler Einträge.

M10

Firmware planmäßig aktualisieren

Lernziel

Bereite ein kompatibles Update vor und prüfe das Ergebnis auf dem Gerät.

Grundlagen

Ein Update verändert vertrauenswürdige Software. Prüfe Modell, Hardwarerevision, Version, Herkunft und Authentifizierungsverfahren des Herstellers. Ein vollständiger Download oder mit einer Website übereinstimmender Hash ersetzt keine Signatur- und Kompatibilitätsprüfung. Installiere keine unsignierte Firmwareanwendung für Entwickler als Kundenveröffentlichung.

Original aktualisiert im dokumentierten Ablauf per Bluetooth, BIT per USB-C. Mirror bietet passende Vorbereitungs- und Transportabläufe. Eine bestimmte Kombination aus PC, Telefon und Gerät ist erst nach physischer Abnahme bestätigt. Der bekannte Fall eines Original-Updates unter Windows erfordert gezielte Diagnose. Ein Fortschritt von 99 % belegt keinen Erfolg.

Prüfe vorher wiederherstellbare Sicherungen, stabile Stromversorgung und Abwesenheit anderer Vorgänge. Lege die offizielle Datei oder eine zuvor gemäß App geprüfte Kopie bereit. Unterscheide Übertragung, Validierung, Installation, Neustart und Versionsprüfung. Der Fortschrittsbalken ist kein Abschlussnachweis.

Prüfe anschließend die sichtbare Geräteversion und vermerke Datum und Ergebnis. Der Desk-Katalog misst die Firmware nicht aus der Ferne: firmwareAttestation bleibt false. Auswahl eines Final-Profils belegt nicht die wirklich installierten Bytes. Folge bei Fehlern der dokumentierten Wiederherstellung und notiere Phase und Fehler, ohne mitten in einem kritischen Schritt blind zu trennen.

Übung

1. Prüfe die Vorbereitungsliste, ohne während der Übung ein echtes Update zu starten.
2. Ordne die Zustände und erkläre den Unterschied zwischen „übertragen“ und „installiert“.
3. Verfasse einen fiktiven Fehlerbericht über einen Abbruch bei 99 % mit Modell, Version, System, Phase und letzter Meldung.

Zeig, was du kannst

Benenne richtige Datei, Übertragungsweg und abschließendes Erfolgskriterium.

Häufige Frage

Soll ich nur wegen eines Desk-Fehlers aktualisieren? Kläre zuerst die Ursache. Eine Kataloginkompatibilität kann eine Desk-Korrektur bei unveränderter validierter Firmware erfordern.

Hier kannst du pausieren

Pausiere ein echtes Update nur an einer im Verfahren ausdrücklich sicheren Stelle, nicht wegen des Gesprächsendes.

Was belegt der ausdrückliche Desk-Katalog für sich genommen?

1. Die unterstützten Kompatibilitätsreferenzen, ohne die installierte Firmware aus der Ferne zu messen.
2. Eine physische Attestierung aller angeschlossenen Geräte.
3. Das Fehlen von Schwachstellen.

> **Antwort anzeigen: Die unterstützten Kompatibilitätsreferenzen, ohne die installierte Firmware aus der Ferne zu messen.**
> Kompatibilität, Signatur, Messung und physische Abnahme sind unterschiedliche Nachweise.

M10

Verlust, Defekt und Wiederherstellung im Notfall

Lernziel

Wähle eine zum Vorfall passende Wiederherstellung und sichere aussagekräftige Nachweise.

Grundlagen

Ordne bei einem Vorfall zuerst den Verlust oder die Offenlegung zu: Computer, Gerät, Karte, Datei, Passwort, Seed, Passphrase oder Richtlinie. „Ich komme nicht hinein“ heißt nicht automatisch „Ich wurde bestohlen“. Gib bei Verdacht auf Kompromittierung keine weiteren Geheimnisse auf dem verdächtigen Rechner ein.

Ein verlorenes Gerät kann mit passenden Medien und Wiederherstellungszugängen ersetzbar sein. Beim Computerverlust können die Wiederherstellung des Desk-Speichers und der Beobachtung nötig sein. Fehlen alle Entsperrmittel oder genügend Schlüssel, um die Schwelle zu erreichen, gibt es möglicherweise keine technische Lösung. Keine KI kann die Rettung nicht vorhandener Schlüssel garantieren.

Desk bietet für unterstützte Formate lokale Wiederherstellung und Export des zugehörigen Materials. Entschlüsseln am PC kann das Geheimnis Betriebssystem oder Schadsoftware offenlegen. Nutze dieses Ausnahmeverfahren mit vorbereiteter Umgebung, passendem Material und Plan zur Übertragung auf neue Schlüssel bei möglicher Offenlegung. Es ist nicht gleichwertig mit der üblichen Cuvex-Isolierung.

Ein neues Desk-Passwort widerruft keinen offengelegten Seed. Prüfe die autorisierte Übertragung in eine neue Wallet und sichere sie auf vertrauenswürdigem Gerät. Veröffentliche keine für Angreifer nützlichen Vorfallsdetails. Meide Dienste, die für eine Wiederherstellung einen anderen Seed oder betrügerische Vorschüsse verlangen.

Übung

1. Löse vier fiktive Fälle: verlorener PC, defekte Karte mit gültiger Kopie, vergessenes Passwort und offengelegter Seed.
2. Benenne jeweils erforderliches Material, Handlungsrisiko und Nachweis der Wiederherstellung.
3. Übe nur mit Lerndaten. Lade keine echten Notfalldateien beim Tutor hoch.

Zeig, was du kannst

Wähle zwischen Wiederherstellung, Neueinrichtung der Beobachtung, Übertragung der Kontrolle und Einschaltung eines Fachkundigen. Versprich keine unmögliche Lösung.

Häufige Frage

Verschlüsselt ein neues Passwort alle schon gesehenen Geheimnisse erneut? Nein. Eine Klartextkopie oder ein bekannter Seed bleibt bekannt.

Hier kannst du pausieren

Speichere Vorfallskategorie und nächste sichere Handlung. Beende die Sprachbegleitung vor der Arbeit mit Geheimnissen.

Dein Seed wurde veröffentlicht und du änderst das PC-Passwort. Ist der Zugriff des Angreifers widerrufen?

1. Ja.
2. Nein. Der Seed kontrolliert weiterhin dieselben Schlüssel. Du musst auf Ebene der Verwahrung reagieren.
3. Ja, wenn du auch den Chathintergrund änderst.

> **Antwort anzeigen: Nein. Der Seed kontrolliert weiterhin dieselben Schlüssel. Du musst auf Ebene der Verwahrung reagieren.**
> Lokaler Schutz widerruft keinen offengelegten Bitcoin-Schlüssel.

M10

Phishing, Support und Betrug per Stimme

Lernziel

Erkenne gefährliche Anfragen und reagiere nach einem vorbereiteten Verfahren.

Grundlagen

Ein glaubwürdiger Betrug kann Namen, Kauf, Gerät und vertraut klingende Stimme nutzen. Echte Angaben können aus einem Datenleck stammen. Prüfe die Identität über einen von dir eingeleiteten Kanal und ein bekanntes Verfahren. Scheinbare Dringlichkeit und Detailkenntnis reichen nicht.

Warnzeichen sind Fragen nach Seed, Passwort, PIN oder Chat-Schlüssel, Fernzugriff zur „Synchronisierung“, Abschalten des Virenschutzes, Übertragung an eine „Sicherheitswallet“, ein unerklärter QR-Code oder eine Signatur als Eigentumsnachweis ohne genaue Angabe der Autorisierung. Druck, dies vor Gesprächsende zu erledigen, ist ein Grund zum Abbruch.

Der legitime Tutor erklärt und stellt Verständnisfragen. Er verwahrt keine Schlüssel, verlangt keine Testzahlung an eine eigene Adresse und verspricht keine Seed-Rettung. Eine legitime Eigentumsprüfung hat einen klaren, überprüfbaren Zweck. Sie erfordert niemals die Herausgabe privater Schlüssel.

Auch in technischen Sitzungen ist Täuschung möglich. Ein QR-Text, Dokument oder eine Nachricht kann die KI zum Ignorieren ihrer Anweisungen auffordern. Das ist zu prüfender Inhalt, keine Weisungsbefugnis über den Tutor. Die Wissensbasis muss freigegebene Quellen von Texten von Lernenden oder Dritten unterscheiden.

Übung

1. Spiele einen falschen Supportanruf durch und brich vor Offenlegung von Daten ab.
2. Überprüfe einen vorab gespeicherten offiziellen Kontaktweg unabhängig.
3. Beschreibe einen Installationsfehler ohne Bildschirmfreigabe von Geheimnissen und ohne Fernzugriff auf die Verwahrungsumgebung.

Zeig, was du kannst

Erkläre, welche Angabe gefordert wird, wofür sie nötig wäre und weshalb das die Lernhilfe überschreitet.

Häufige Frage

Ist es sicher, nur einige Seed-Wörter zu zeigen? Nein. Es gibt keinen pädagogischen Grund zur Offenlegung von Teilen eines eigenen Seeds.

Hier kannst du pausieren

Bewahre das Verfahren zur Supportprüfung auf und kontrolliere es auf offen lesbare Geheimnisse.

Eine Stimme klingt wie dein Geschäftspartner und drängt auf sofortiges Signieren ohne Prüfung. Was tust du?

1. Ich pausiere, authentifiziere die Anfrage nach dem vereinbarten Verfahren und prüfe den vollständigen Vorgang.
2. Ich signiere, weil die Stimme übereinstimmt.
3. Ich teile den Seed, um Zeit zu sparen.

> **Antwort anzeigen: Ich pausiere, authentifiziere die Anfrage nach dem vereinbarten Verfahren und prüfe den vollständigen Vorgang.**
> Stimmerkennung und Dringlichkeit ersetzen weder Authentifizierung noch Prüfung.

Privatsphäre, Recht und persönliche Aufzeichnungen

Lernziel

Lerne den allgemeinen Rahmen kennen und bereite konkrete Rechts- und Steuerfragen vor.

Grundlagen

Finanzielle Privatsphäre beseitigt keine Steuerpflichten und keine anwendbaren Identifizierungs-, Sanktions- oder Kriminalpräventionspflichten. Maßgeblich sind Wohnsitz, Tätigkeit, Gegenpartei und Dienst. Die KI soll allgemeine Informationen mit Quelle und Datum geben und Einzelfallentscheidungen an zuständige Fachleute verweisen.

In der EU regelt MiCA bestimmte Kryptowerte und Dienstleistungen. Die allgemeine Anwendung begann am 30. Dezember 2024. Die in der Verordnung vorgesehene maximale Übergangsfrist reichte vorbehaltlich nationaler Entscheidungen bis zum 1. Juli 2026. Prüfe Zulassung und Umfang in aktuellen amtlichen Registern. Ein alter Registrierungshinweis reicht nicht. Eine Zulassung garantiert weder Preis, Zahlungsfähigkeit noch vollständige Entschädigung.

Die Verordnung 2023/1113 bestimmt, welche Informationen Transfers begleiten, wenn verpflichtete Anbieter beteiligt sind. Bei Transfers über 1.000 Euro mit selbstverwahrten Adressen sieht sie Maßnahmen zur Prüfung von Eigentum oder Kontrolle vor. Die Schwelle schafft darunter keine allgemeine Ausnahme von der Identifizierung. Transfers zwischen Personen ohne Anbieter sind vom Anwendungsbereich dieser Verordnung ausgenommen. Andere Pflichten bleiben bestehen.

Bewahre für deinen Fall ausreichende Belege zu Käufen, Verkäufen, Gebühren und Herkunft geschützt vor unnötigen Zugriffen auf. Für private Aufzeichnungen musst du nicht die gesamte Historie veröffentlichen. Der Kurs lehrt weder Aufteilung zur Kontrollumgehung noch Falschangaben oder Verheimlichen von Einkünften.

Bei Sprachaufzeichnung oder -transkription und zuordenbarem Lernfortschritt muss der Dienst Zweck, Rechtsgrundlage, Aufbewahrung, Zugriff, Auftragsverarbeiter und anwendbare Rechte festlegen. Prüfe die Datenschutzkonfiguration vor dem Verkauf, nicht improvisiert im Gespräch.

Übung

1. Entwirf für einen Berater einen fiktiven Fall mit Wohnsitz, Tätigkeit und Vorgängen, ohne Schlüssel.
2. Kläre, wo Zulassung des Anbieters und Datum der Auskunft überprüfbar sind.
3. Entwirf ein privates Transaktionsverzeichnis und eine auf das Nötigste beschränkte Richtlinie für Lerndaten.

Zeig, was du kannst

Unterscheide Rechtsregel, Börsenrichtlinie und technische Bitcoin-Fähigkeit.

Häufige Frage

Ist jede Selbstverwahrung in der EU verboten? Das folgt nicht aus den genannten Vorschriften. Vermeide pauschale Schlagzeilen und prüfe den konkreten Wortlaut und Geltungsbereich.

Hier kannst du pausieren

Notiere offene Fragen für die Beratung, ohne persönliche Dokumente beim Tutor einzugeben.

Entfallen unterhalb der für bestimmte Adresskontrollen genannten Schwelle von 1.000 Euro alle Pflichten?

1. Ja.
2. Nur wenn du den Vorgang aufteilst.
3. Nein. Sie ist keine allgemeine Ausnahme von Identifizierung oder anderen Pflichten.

> **Antwort anzeigen: Nein. Sie ist keine allgemeine Ausnahme von Identifizierung oder anderen Pflichten.**
> Maßnahme und Geltungsbereich bestimmen die Auslegung. Eine einzelne Schwelle ist keine allgemeine Befreiung.

Erbschaft, Kontinuität und jährliche Übung

Lernziel

Erstelle einen Plan, mit dem berechtigte Personen handeln können, ohne vorzeitig sämtliche Geheimnisse offenzulegen.

Grundlagen

Beim Vererben müssen rechtliche Berechtigung, Auffindbarkeit der Materialien und technische Handlungsfähigkeit zusammenpassen. Erbberechtigte können eine Wallet vielleicht nicht rekonstruieren. Ein Schlüsselinhaber ist umgekehrt nicht unbedingt nutzungsberechtigt. Kläre beide Seiten mit geeigneter Beratung.

Trenne allgemein zugängliche Hinweise vom Geheimniszugang. Das Inventar nennt vorhandene Objekte, Kontakte und Prüfungen. Lege nicht alle Schlüssel und Passwörter in einem breit zugänglichen Dokument ab. Veröffentliche keine Seeds in Testamenten oder Unterlagen, die außerhalb deiner Kontrolle zirkulieren können.

Plane bei Multisig Verwahrung von Richtlinie und Kopien, erreichbare Schwelle nach Verlust und Folgen des Todes einer Schlüsselperson. Genügend Komponenten bei einem Verwahrer können eine einzelne Missbrauchsmöglichkeit schaffen. Zu komplizierte Verteilung kann das Vermögen unwiederbringlich machen.

Plane Wiederherstellung der Kryptogrammpasswörter und einer vorhandenen Passphrase, Ableitungsdaten, Gerätekompatibilität und das Vorgehen bei Betriebsaufgabe des Herstellers. Verlass dich nicht auf ein proprietäres Dateiformat oder biometrischen Abdruck ohne Vorbereitung. Erprobe Interoperabilität mit Testdaten und dokumentierten Formaten.

Prüfe den Plan nach Änderungen in Familie, Wohnort, Richtlinie, Software oder Teilnehmerkreis und übe regelmäßig. Eine Vertrauensperson sollte die Anweisung verstehen können, ohne Vermögen offenzulegen oder unnötig Geld zu bewegen.

Übung

1. Fülle eine private Vorlage mit Zuständigkeiten, Komponenten, berechtigtem Zugang und Vertretungen aus.
2. Gib einer anderen Person Laboranweisungen ohne mündliche Erklärung und beobachte, wo sie nicht weiterkommt.

3. Beseitige Unklarheiten und vermerke einen Prüftermin. Der Kurs erstellt nicht automatisch Erinnerungen.

Zeig, was du kannst

Erkläre, was bei deiner Abwesenheit geschieht und welche Informationen jede Rolle je Phase benötigt.

Häufige Frage

Ersetzt 2 von 3 den Nachlassplan? Nein. Es ist ein technisches Werkzeug. Erben benötigen weiterhin Kontext, Materialien, Abstimmung und Berechtigung.

Hier kannst du pausieren

Bewahre den Plan außerhalb des Kurses auf und markiere nur „Übung überprüft“.

Woran lässt sich ein Nachlassplan sinnvoll messen?

1. Eine berechtigte Person kann eine dokumentierte Übung ohne Improvisation und vorzeitige Offenlegung von Geheimnissen durchführen.
2. Er hat viele Seiten.
3. Er hängt ausschließlich vom Erinnern eines Passworts ab.

> **Antwort anzeigen: Eine berechtigte Person kann eine dokumentierte Übung ohne Improvisation und vorzeitige Offenlegung von Geheimnissen durchführen.**
> Wiederherstellbarkeit und Zugangsschutz müssen praktisch geprüft werden.

M11

Preis, Sparen und Fundamentalanalyse

Lernziel

Analysiere Anlageargumente und unterscheide sie von überprüfbaren technischen Eigenschaften.

Grundlagen

Preise entstehen aus Geschäften an konkreten Märkten und können je Plattform abweichen. Liquidität, Kurswährung, Markttiefe, Bankbetriebszeiten und Nachfrage beeinflussen den tatsächlich ausführbaren Kurs. Die Bildschirmanzeige ist kein garantiertes Angebot für deine Menge.

Die Fundamentalanalyse betrachtet Verbreitung, Nachfrage, Konkurrenz, wirtschaftliche Sicherheit, Regulierung und Angebot. Der Emissionsplan allein legt keine künftigen Preise fest. Bewertungen des monetären Nutzens oder „inneren Werts“ hängen von Annahmen ab. Es gibt keine objektive Zahl, welche die KI als universelle Gewissheit ausgeben kann.

Regelmäßige Käufe verteilen Einstiegszeitpunkte, garantieren aber weder Gewinn noch Schutz vor langen Verlustphasen. Langfristiges Sparen braucht auch Liquidität für Verpflichtungen, Tragfähigkeit von Schwankungen und einen Verwahrungsplan. Der Kurs schreibt keinen Vermögensanteil vor und entscheidet nicht für dich.

Trenne drei Fragen: Verstehe ich den Vermögenswert? Kann ich ihn verwahren und wiederherstellen? Kann ich das wirtschaftliche Risiko tragen? Schlüsselkompetenz beantwortet die dritte Frage nicht automatisch. Eine Kursprognose oder historische Grafik wird durch Unterricht nicht zur persönlichen Empfehlung.

Übung

1. Formuliere eine fiktive These, ihre Annahmen und Tatsachen, die sie widerlegen würden.
2. Simuliere einen Rückgang um 50 % bei gleichzeitigem Liquiditätsbedarf ohne echte Vermögensangaben.
3. Trenne nachprüfbare Angaben von Erwartungen.

Zeig, was du kannst

Diskutiere Anlagen ohne Renditeversprechen und ohne Überzeugung mit Belegen zu verwechseln.

Häufige Frage

Sichert Knappheit einen Preisanstieg? Nein. Nachfrage und weitere Bedingungen bleiben für den Marktpreis entscheidend.

Hier kannst du pausieren

Bewahre die Laborannahmen auf, keinen automatischen Kaufauftrag.

Was garantiert regelmäßiges Kaufen?

1. Langfristigen Gewinn.
2. Keine Rendite. Es verteilt Kaufzeitpunkte nach einer gewählten Regel.
3. Schutz vor Schlüsselverlust.

> **Antwort anzeigen: Keine Rendite. Es verteilt Kaufzeitpunkte nach einer gewählten Regel.**
> Die Verteilung der Einstiege beseitigt weder wirtschaftliche noch betriebliche Risiken.

Einen Anbieter für den Bitcoin-Kauf wählen

Lernziel

Beurteile einen Anbieter anhand von Zulassung, Kosten, Auszahlung, Privatsphäre und Verwahrungsrisiko.

Grundlagen

Vergleiche überprüfbare Kriterien: Rechtsträger und Rechtsordnung, zugelassene Dienste, Auszahlungsnetz, Gebühren, Handelsspanne, Limits, Support, Authentifizierung und Datenverarbeitung. Marke und Sponsoring beweisen keine Zulassung für den konkreten Dienst.

Gesamtkosten können Einzahlung, Umrechnung, Spread, Handel, Auszahlung und Bankgebühren umfassen. „Gebührenfreier“ Handel kann einen größeren Spread haben. Prüfe Nettobeträge und Referenzwährung. Ist Selbstverwahrung das Ziel, plane die Auszahlung dorthin finanziell ein.

Bei einem verwahrten Guthaben bleibst du vom Anbieter abhängig. Ein Reservenachweis allein belegt weder sämtliche Verbindlichkeiten noch Eigentum an Mitteln oder künftige Zahlungsfähigkeit. Prüfe Beschränkungen und teste einen neuen Ablauf mit einer kleinen verkraftbaren Auszahlung.

Geschäftliche Identifizierung kann dich mit einer Auszahlung verbinden. Späterer Datenschutz löscht das Wissen des Anbieters nicht. Mache keine falschen Angaben und nutze den Kurs nicht zur Pflichtenumgehung. Auch der Kauf eines Lerncodes erzeugt einen geschäftlichen Eintrag unabhängig von deiner Wallet.

Übung

1. Erstelle eine fiktive Tabelle für zwei Anbieter mit Gesamtkosten, Netz, Mindestauszahlung, Zulassung und benötigten Daten.
2. Berechne die Nettosumme eines Übungsvorgangs mit allen angegebenen Kosten.
3. Plane eine Testauszahlung an eine zuvor geprüfte Adresse, ohne sie von der Kursseite auszuführen.

Zeig, was du kannst

Begründe eine Wahl für deinen Fall und erkenne veraltete oder ungeprüfte Informationen.

Häufige Frage

Empfiehlt der Kurs eine für alle beste Börse? Nein. Zulassungen, Gebühren, bediente Länder und Bedingungen ändern sich. Der Vergleich braucht Stichtag und Anwendungsfall.

Hier kannst du pausieren

Bewahre die Tabelle ohne Zugangsdaten und Ausweisdokumente auf.

Was sagt mehr aus als allein die Handelsgebühr?

1. Die gesamten Kosten bis zum Eingang der BTC im gewünschten Netz an der gewünschten Adresse.
2. Die Zahl der Follower des Anbieters.
3. Die Farbe seiner App.

> **Antwort anzeigen: Die gesamten Kosten bis zum Eingang der BTC im gewünschten Netz an der gewünschten Adresse.**
> Der Endpreis umfasst möglicherweise Posten, die in der beworbenen Gebühr fehlen.

Konten, Aufträge und Ausführungskosten

Lernziel

Verstehe grundlegende Auftragstypen und schütze das Konto, ohne den Kurs als Handelsplattform zu nutzen.

Grundlagen

Eine Marktorder priorisiert die verfügbare Ausführung und birgt das Risiko einer Kursabweichung. Eine Limitorder legt einen Höchstkauf- oder Mindestverkaufspreis fest, kann aber ganz oder teilweise offenbleiben. Eine Stoporder löst nach Anbieterregeln eine weitere Aktion aus und garantiert keinen Endpreis.

Das Orderbuch zeigt verfügbare Angebote, nicht die dauerhafte Verfügbarkeit aller Mengen. Bei Kursfall oder geringer Liquidität kann das Ergebnis vom letzten Kurs abweichen. Stop-Market riskiert einen schlechteren Preis, Stop-Limit eine ausbleibende Ausführung.

Schütze den Zugang mit einmaligem Passwort, nach Möglichkeit phishingresistenter Authentifizierung, Sitzungsprüfung und geeigneten Auszahlungskontrollen. Verwahre die Wiederherstellung des zweiten Faktors unabhängig. Ein API-Schlüssel zur Automatisierung kann mehr und gefährlichere Rechte haben als zum Lesen nötig. Gib ihn weder im Tutor noch auf der Kursseite ein.

Prüfe vor Auszahlung Vermögenswert, Bitcoin-Netz, eigene Wallet-Adresse und Nettobeträge. Plattformen verwenden mitunter dieselben Kürzel für verschiedene Produkte. Bewahre Belege zu Kauf, Ausführung, Gebühren und Auszahlung entsprechend deinem Fall auf. Eine Auszahlung an deine Wallet ist kein neuer Kauf.

Übung

1. Simuliere ein Orderbuch mit 1 Einheit zu 100 und einer weiteren zu 102. Erkläre, weshalb zwei Einheiten per Marktorder keinen Durchschnitt von 100 garantieren.
2. Entwirf eine Limitorder und beschreibe einen Fall ohne vollständige Ausführung.
3. Prüfe die Rechte einer fiktiven API und entferne Auszahlungsrechte, wenn nur Abfragen nötig sind.

Zeig, was du kannst

Beschreibe je Auftrag Priorität, Preis und Risiko der Nichtausführung.

Häufige Frage

Begrenzt ein Stop-Loss Verluste immer exakt? Nein. Kurslücken, Liquidität, Kursabweichung und Anbieterregeln können das verhindern.

Hier kannst du pausieren

Speichere das Übungsergebnis ohne echte Aufträge und API-Schlüssel.

Welches Risiko bleibt bei einem limitierten Kaufauftrag zu 100?

1. Er wird vielleicht nie oder nur teilweise ausgeführt.
2. Er muss zu jedem beliebigen Preis ausgeführt werden.
3. Er legt automatisch eine Sicherung an.

> **Antwort anzeigen: Er wird vielleicht nie oder nur teilweise ausgeführt.**
> Preiskontrolle kann dazu führen, dass die Ausführung ausbleibt.

M11

Kerzencharts, Indikatoren und Verzerrungen der technischen Analyse

Lernziel

Lies Diagramme als historische Daten und bewerte eine Strategie, ohne Muster mit Vorhersagen zu verwechseln.

Grundlagen

Eine Kerze fasst Eröffnungs-, Höchst-, Tiefst- und Schlusskurs eines Zeitraums zusammen. Das Volumen hängt von der Quelle ab. Plattform, Währung, Zeitzone und Intervall beeinflussen die Darstellung. Die zeitliche Reihenfolge aller Bewegungen innerhalb der Kerze ist nicht ersichtlich.

Ein gleitender Durchschnitt glättet vergangene Preise. Ein Momentum-Indikator formt beobachtete Daten nach einer Formel um. Keiner kennt die Zukunft. Zwei aus derselben Reihe berechnete Indikatoren können trotz verschiedener Farben und Namen stark korrelierte Informationen liefern.

Lege Einstieg, Ausstieg, Ungültigkeitskriterium, Kosten, Positionsgröße und Daten vor der Ergebnisbetrachtung fest. Vermeide das Herausgreifen von Gewinnern, nachträgliches Anpassen der Parameter und die Nutzung späterer Daten bei früheren Entscheidungen. Trenne Trainingsdaten von zeitlich nachgelagerten Validierungsdaten.

Ein Backtest muss Spread, Gebühren, Kursabweichung, Datenverfügbarkeit und mögliche Ausführung berücksichtigen. Bruttorendite, Trefferquote, Höchstverlust und Verlustverteilung beantworten unterschiedliche Fragen. Wenige große Verluste können viele kleine Gewinne übersteigen. Kein Kauf- oder Verkaufssignal wird als sicher gelehrt.

Übung

1. Lies eine fiktive Kerze und erkläre, welche Zeitinformation fehlt.
2. Notiere vor der Auswertung von zehn synthetischen Ergebnissen eine Regel mit Kosten und Fehlerkriterium.
3. Vergleiche 9 Gewinne von je 1 mit einem Verlust von 15. Trotz 90 % Trefferquote beträgt das Bruttoergebnis -6.

Zeig, was du kannst

Hinterfrage ein attraktives Ergebnis anhand von Auswahl, Kosten und Risiko, ohne handeln zu müssen.

Häufige Frage

Garantieren viele Indikatoren ein besseres Signal? Nein. Sie können Überanpassung und Komplexität erhöhen, ohne unabhängige Informationen hinzuzufügen.

Hier kannst du pausieren

Bewahre Regel und Laborergebnisse auf, keine Marktorder.

Neun Geschäfte gewinnen je 1, eines verliert 15. Was ist das Ergebnis vor Kosten?

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

> **Antwort anzeigen: -6.**
> Neun gewonnene abzüglich fünfzehn verlorener Einheiten ergeben sechs Einheiten Verlust.

Margin, Futures und Automatisierung

Lernziel

Erkenne Positionsrisiko, Liquidation und Automatisierungsfehler, bevor du komplexe Produkte erwägst.

Grundlagen

Hebel erhöht das Engagement im Verhältnis zum eingesetzten Kapital. Bei 100 Margin für eine Position von 1.000 entspricht eine ungünstige Bewegung des Basiswerts um 5 % vor Kosten einem Verlust von 50, der Hälfte der ursprünglichen Margin. Tatsächliche Regeln für Mindestdeckung, Liquidation, Sicherheiten und Gebühren können das Ergebnis verschlechtern und früher greifen als erwartet.

Futures und unbefristete Kontrakte können Fälligkeit, Differenzausgleich, Finanzierungssätze und vom letzten Handel abweichende Referenzpreise haben. Sie entsprechen keiner Auszahlung nativer Bitcoin an Cuvex. Die Verwahrung eines Seeds schützt keine Position vor Liquidation oder Ausfall einer Gegenpartei.

Ein Bot automatisiert Regeln samt ihren Fehlern. Er braucht Positionsgrenzen, minimale Rechte, idempotente Aufträge, Abgleich, Verlustkontrolle, Not-Aus und Aufsicht. Wiederholung einer Anfrage nach Zeitüberschreitung kann die Position verdoppeln, wenn das frühere Ergebnis ungeklärt ist.

Die KI kann Begriffe erklären und Widersprüche in fiktiven Fällen erkennen. Sie soll keine API-Schlüssel erhalten, keinen Handel aktivieren und keine rentable Strategie versprechen. Wer Risiken versteht, kann sich im Sinne des Kursziels gegen unverstandene Produkte entscheiden.

Übung

1. Löse das Beispiel zu Position und Margin, ohne eine Liquidation exakt bei 10 % zu unterstellen.
2. Simuliere eine API, die einen Auftrag ausführt, dessen Antwort verloren geht. Begründe den Abgleich vor Wiederholung.
3. Entwirf einen Stoppknopf, der neue Aufträge sperrt und bereits offene prüft, ohne sich mit einem Broker zu verbinden.

Zeig, was du kannst

Benenne ein trotz Stop verbleibendes Risiko, eines trotz Bot und eines trotz Selbstverwahrung anderer Mittel.

Häufige Frage

Beseitigt Automatisierung emotionale Fehler und garantiert dadurch Ergebnisse? Nein. Sie kann impulsive Eingriffe verringern und zugleich Entwurfs- oder Ausführungsfehler vervielfachen.

Hier kannst du pausieren

Markiere diese Vertiefung als verstanden, ohne komplexe Produkte freizuschalten.

Eine Position von 1.000 ist mit 100 Margin unterlegt. Was bedeuten 5 % Verlust auf die Position vor Kosten?

1. 5 Verlust.
2. 50 Verlust, also 50 % der Margin.
3. Mit einem Bot kein Verlust.

> **Antwort anzeigen: 50 Verlust, also 50 % der Margin.**
> Hebel und Kosten bewirken, dass das Ergebnis bezogen auf die Margin von der Kursbewegung des Basiswerts abweicht.

M12

Lightning und weitere Schichten

Lernziel

Verstehe Kanalzahlungen und erkenne, welche Funktionen der geprüfte Cuvex-Ablauf nicht bietet.

Grundlagen

Lightning verwendet Kanäle und Aktualisierungsmechanismen für Zahlungen, ohne jeden einzelnen Austausch in der Basiskette zu protokollieren. Kanaleröffnung, Schließung und bestimmte Wiederherstellungen können On-Chain-Transaktionen erfordern. Verfügbarkeit, ein- und ausgehende Liquidität und Überwachung hängen von Wallet-Aufbau und Diensten ab.

Eine Lightning-Rechnung kann Betrag, Beschreibung und Ablauf enthalten. Je nach Kontext wird in Satoshis oder Millisatoshis gerechnet. Letztere bedeuten keine Ausgänge unter einem Satoshi in der Basiskette. Die Zahlung braucht Unterstützung und eine verfügbare Route. Ein QR-Code garantiert keine Bezahlbarkeit mit jeder App.

Verwahrende und nicht verwahrende Dienste unterscheiden sich erheblich. Übliche Geschwindigkeit beweist keine Risikofreiheit. Lightning bedeutet auch keine vollständige Anonymität. Beobachter, Routen, Gegenparteien und Metadaten spielen eine Rolle.

Der Cuvex-Chat kann Sats-Anforderungen koordinieren, die über das WOW-Konto on-chain bezahlt werden. Diese Ausgabe schreibt Desk weder einen Lightning-Knoten noch Kanalverwaltung oder Signatur von Lightning-Rechnungen zu. Bei mehreren Zahlungsarten prüfe, welche du verstehst und welche die App ausführen wird.

Übung

1. Ordne eine On-Chain-Adresse, einen bitcoin:-URI und eine Lightning-Übungsrechnung zu.
2. Vergleiche Ketten- und Kanalzahlung hinsichtlich Bestätigung, Liquidität, Verwahrung und Wiederherstellung.
3. Erkläre, warum eine abgelaufene Rechnung mit dem Empfänger zu klären ist und nicht als Adresse umgedeutet wird.

Zeig, was du kannst

Lehne eine inkompatible Zahlungsart ab, ohne Schlüssel offenzulegen oder Cuvex fälschlich einen Fehler zuzuschreiben.

Häufige Frage

Laufen alle Sats-Zahlungen über Lightning? Nein. Satoshis geben den Wert an. Der Zahlungsweg hängt vom Protokoll ab.

Hier kannst du pausieren

Speichere die Zahlungsart der Übung ohne echte Rechnungen.

Woran lässt sich erkennen, dass eine Anforderung per Lightning bezahlt wird?

1. Am Wort „sats“.
2. An der Zustellung im Chat.
3. An kompatiblem Format und Zahlungsart, nicht bloß an Einheit oder Nachrichtenkanal.

> **Antwort anzeigen: An kompatiblem Format und Zahlungsart, nicht bloß an Einheit oder Nachrichtenkanal.**
> Recheneinheit und Zahlungsnetz sind verschiedene Merkmale.

Taproot, MuSig2 und die Zukunft der Post-Quanten-Kryptografie

Lernziel

Unterscheide Standards, Vorschläge und implementierte Fähigkeiten.

Grundlagen

Taproot ermöglicht Ausgabebedingungen über Schlüssel- und Skriptpfade. Schnorr-Signaturen und Aggregation können bestimmte Konstruktionen verbessern. Privatsphäre hängt von Einrichtung und Ausgabe ab. Eine bc1p-Adresse beweist weder die Abwesenheit weiterer Teilnehmer noch verrät sie alle verborgenen Bedingungen.

MuSig2 ermöglicht einer Gruppe das Aggregieren von Schlüsseln und interaktive Erzeugen einer kompatiblen Schnorr-Signatur. Das Grundverfahren ist N von N. Für beliebige Schwellen M von N ist eine andere Konstruktion oder ein zusätzliches Protokoll nötig. Nonces und Sitzungen müssen sorgfältig verwaltet werden. Informeller Nachrichtenaustausch ersetzt das Protokoll nicht.

PSBT v2 ordnet Informationen anders als v0. Eine Datei mit Transaktionsversion 2 verwendet dadurch nicht automatisch das neuere Behälterformat. Die Final-Firmwares dieser Ausgabe verwenden im Multisig-Profil PSBT v0, P2WSH/sortedmulti und SIGHASH_ALL. Künftige Fähigkeiten benötigen eigene Spezifikation und Validierung.

NIST veröffentlichte 2024 die ersten abgeschlossenen Post-Quanten-Standards. Das ändert keine Bitcoin-Signaturen. Ein Post-Quanten-Verfahren zur Firmware-Authentifizierung würde diese Ebene schützen. Es würde ECDSA- oder Schnorr-Signaturen eines UTXO nicht automatisch postquantensicher machen. Der Tutor kann auch kein künftiges Angriffsdatum sicher vorhersagen.

Übung

1. Ordne fünf Aussagen als Standard, geprüfte Umsetzung, Vorschlag oder Werbung ein.
2. Erkläre, warum „unterstützt einen Taproot-Empfänger“ nicht „signiert einen Taproot-Eingang“ belegt.
3. Zeichne getrennte Ebenen für Firmware-Signatur, Geheimnisverschlüsselung, Chat und Bitcoin-Ausgabesignatur.

Zeig, was du kannst

Fordere einen Nachweis für eine bestimmte Ebene und übertrage Garantien nicht zwischen Protokollen.

Häufige Frage

Soll ich wegen einer Schlagzeile über Quantencomputer alle Mittel migrieren? Eine echte Entscheidung braucht aktuelle technische Belege, prüfbare Unterstützung, Risikobewertung und sicheren Migrationsplan. Der Kurs ordnet keine Transfers wegen Schlagzeilen an.

Hier kannst du pausieren

Notiere technische Fragen ohne automatischen Ausgabeplan.

Würde eine implementierte und validierte Post-Quanten-Signatur im Bootloader die Signaturbedingungen eines bestehenden UTXO ändern?

1. Nein. Das sind verschiedene Schichten.
2. Ja. Sie stellt das gesamte Netzwerk auf einen anderen Algorithmus um.
3. Sie macht Sicherungen überflüssig.

> **Antwort anzeigen: Nein. Das sind verschiedene Schichten.**
> Die Authentifizierung eines Updates schreibt Bitcoins Ausgabebedingungen nicht um.

Interoperabilität und Unabhängigkeit vom Hersteller

Lernziel

Plane den Weiterbetrieb bei Wechsel von Software, Gerät oder Anbieter.

Grundlagen

Eine Liste von Kürzeln beweist keine Interoperabilität. Netz, Skript, Ableitung, Schlüssel, Richtlinie, Transaktionsformat und Bedeutung der Signaturen müssen erhalten bleiben. Zwei BIP174-fähige Apps können unterschiedliche Felder, Größen oder Eingangstypen unterstützen.

Um unabhängig von einer Oberfläche zu werden, bewahre dokumentierte Wiederherstellungsdaten auf und übe mit Lernwallets. Eine standardisierte Wortfolge kann Schlüssel ableiten. Für Multisig brauchst du außerdem die vollständige Richtlinie. BIP329-Labels ergänzen privaten Kontext, der Chatverlauf hat einen anderen Umfang.

Lege bei einem Kompatibilitätstest keinen echten Seed offen. Prüfe zuerst den öffentlichen Deskriptorexport und die Watch-only-Wiederherstellung. Müssen im Notfall Schlüssel rekonstruiert werden, nutze eine dafür vorgesehene Umgebung und erwäge danach eine Migration. Eine inkompatible Wallet mit Nullanzeige belegt keinen Verlust.

Bewahre eine prüfbare Kopie von Dokumentation, Kursversion und nötigen Werkzeugen auf. App-Signaturen, abgelaufene Zertifikate und Systemänderungen können die Installation beeinflussen. Verfügbarer Quellcode garantiert keinen späteren Build ohne erhaltene Abhängigkeiten und Kenntnisse.

Übung

1. Entwirf für ein leeres Konto einen Ausstiegstest mit identischem Netzwerk, Richtlinie und Prüfadresse in zwei kompatiblen Implementierungen.
2. Unterscheide standardisierte Bestandteile von solchen, die einen Konverter oder eine Cuvex-Formatbeschreibung brauchen.
3. Lege den Nachweis für Kompatibilität fest und benenne noch ausstehende Hardware- oder echte Signaturtests.

Zeig, was du kannst

Beschreibe einen Wiederherstellungsweg unabhängig vom Fortbestand desselben Unternehmensdienstes.

Häufige Frage

Spielt bei Open Source der Hersteller keine Rolle mehr? Doch. Verteilung, Wartung, Hardware und Betriebserfahrung bleiben wichtig. Offenheit ermöglicht Prüfung und mögliche Kontinuität, garantiert sie aber nicht.

Hier kannst du pausieren

Bewahre Laborergebnisse mit Versionen und beobachteten Grenzen auf.

Welcher Nachweis spricht am stärksten für Interoperabilität?

1. Beide Apps zeigen das Wort „Bitcoin“.
2. Dieselbe Richtlinie und Adresse werden im Labor mit festgehaltenen Versionen rekonstruiert und geprüft.
3. Die Symbole sehen ähnlich aus.

> **Antwort anzeigen: Dieselbe Richtlinie und Adresse werden im Labor mit festgehaltenen Versionen rekonstruiert und geprüft.**
> Die Prüfung muss die maßgeblichen Bedingungen und ein überprüfbares Ergebnis festhalten.

Technisches Labor mit Regtest

Lernziel

Verstehe ein reproduzierbares Labor und unterscheide synthetische Tests von physischer Nutzung.

Grundlagen

Regtest erzeugt eine kontrollierte lokale Kette für Blöcke und Transaktionsversuche ohne wirtschaftlichen Wert. Nutze getrennte Verzeichnisse und Zugangsdaten, ohne echtes Material zu importieren. Die Ergebnisse belegen allein keine USB-, NFC-, Bluetooth- oder Kamerakompatibilität physischer Geräte.

Ein vollständiges Labor protokolliert Versionen, Netzkonfiguration, Richtlinie, Testeingänge, PSBT, Signaturen, finale Transaktion und Annahme. Es kann die Wertsumme, Ablehnung einer veränderten Signatur und Aufnahme einer gültigen Zahlung in einen lokalen Block prüfen. Teste auch Fehlerfälle.

Die Validierung von Desk 9.21 berichtet über Bitcoin Core 31 in Regtest sowie automatisierte Tests des Transaktionsmoduls und einer simulierten Oberfläche. Diese Ausgabe nutzt die Berichte als Dokumentation und behauptet weder eine Wiederholung der Versuche noch eigene Gerätevorgänge. Eine Paketprüfung belegt keine Installation auf allen Systemen.

Vor einer technischen Lektion muss das technische Team ein eingerichtetes Labor und einen zur Lernendenversion passenden Ablauf bereitstellen. Öffne RPC nicht zum Internet, damit der Tutor es steuern kann. Die KI kann synthetische Ergebnisse erklären, soll aber weder Zugangsdaten noch Administratorrechte erhalten.

Übung

1. Beobachte im vorbereiteten Labor eine gültige Transaktion und eine mit veränderter Signatur. Notiere Annahme oder Ablehnung.
2. Prüfe einen Fall mit falschem Wechselgeld und einen mit inkompatiblem Netz.
3. Unterscheide im Bericht „Test des Transaktionsmoduls“, „simulierte Oberfläche“ und „physische Hardware“.

Zeig, was du kannst

Beschreibe genau, was geprüft wurde und was offen ist, ohne eine Simulation als Zertifizierung auszugeben.

Häufige Frage

Darf ich den Kurs nach erfolgreichem Regtest für alle Geräte als validiert verkaufen? Nein. Tests physischer Abläufe, Installation, Barrierefreiheit, Wiederherstellung und kommerzieller Dienst stehen noch aus.

Hier kannst du pausieren

Beende und speichere das Labor nach Anleitung und bewahre nur synthetische Daten auf.

Beweist ein Regtest des Transaktionsmoduls, dass ein bestimmtes Telefon NFC tatsächlich lesen kann?

1. Ja, weil beide Bitcoin verwenden.
2. Ja, wenn die PSBT klein ist.
3. Nein. Dafür ist ein eigener physischer Test erforderlich.

> **Antwort anzeigen: Nein. Dafür ist ein eigener physischer Test erforderlich.**
> Die verschiedenen Testumgebungen haben unterschiedliche Aussagekraft.

Abschlussprojekt und Kontinuitätsplan

Lernziel

Zeige selbstständiges Handeln von der Vorbereitung bis zur Wiederherstellung und zum Schutz der Privatsphäre.

Grundlagen

Ziel ist, die Absicht zu erklären, das Ergebnis zu prüfen und bei einem unverstandenen Vorgang anzuhalten. Dafür musst du kein Menü auswendig lernen. Bewertet werden Konzepte, angeleitete Übungen und ein selbstständig gelöster Fall. Seeds, Vermögensangaben und persönliche Adressen sind niemals dem Prüfer offenzulegen.

Fall A: Richte eine Lernumgebung ein, bestimme Modelle und Versionen, schütze Desk, verknüpfe ein Übungskryptogramm und rekonstruiere ein Watch-only-Konto. Erkläre notwendige Sicherungen und die für deinen Anbieter sichtbaren Daten.

Fall B: Entwirf eine Zahlung mit fiktiven UTXOs verschiedener Kontexte, begründe die Auswahl, prüfe Empfänger, Wechselgeld und Gebühr und beschreibe den Signaturablauf deines Geräts. Löse eine Unterbrechung auf dem Rückweg und bei der Veröffentlichung ohne Doppelzahlung. Fehlt physisch abgenommene Hardware, vermerke den Teil als simuliert und weiterhin offen.

Fall C: Entwirf 2 von 3, spiele Einladung und Prüfung durch, vergleiche in Mirror ein frei gewähltes Feld und erkläre die Aussage des OK. Stelle die Übungsrichtlinie wieder her, simuliere den Ausfall einer Person und plane Kontinuität und Erbschaft.

Vorgeschlagen sind mindestens 80 % im Wissenstest und richtige Ausführung sämtlicher kritischen Kontrollen: keine Geheimnisse preisgeben, Netz und Ausgänge prüfen, Phasen unterscheiden und Wiederherstellung sichern. Kritische Fehler erfordern Nacharbeit und neue Übung. Richtige Marktfragen gleichen sie nicht aus. Ein etwaiges kommerzielles Zertifikat muss nennen, was geprüft wurde und ob eine physische Beobachtung oder nur eine Simulation stattfand.

Übung

1. Bearbeite alle drei Fälle mit synthetischen Daten und eigener Erklärung.
2. Löse den Abschlusstest im Anhang und prüfe jede falsche Antwort.

3. Gib nur ein Ergebnisblatt ohne Geheimnisse ab, mit Nachweisen zum Umfang und offenen Punkten.

Zeig, was du kannst

Halte selbstständig an, wenn ausreichende Belege fehlen, und benenne, was du zum Weitergehen brauchst.

Häufige Frage

Bin ich nach Lesen aller Seiten für beliebig große Beträge vorbereitet? Nein. Fähigkeiten sind praktisch zu prüfen und Risiken für die eigene Situation zu bewerten. Lesen und Üben garantieren keine künftigen Ergebnisse.

Hier kannst du pausieren

Bewahre Prüfplan und offene Übungen auf. Bei Bedarf kannst du ein einzelnes Kapitel wiederholen.

Was ist eine wesentliche Voraussetzung für den Abschluss der praktischen Schulung?

1. Alle Seiten einmal geöffnet zu haben.
2. Wiederherstellung und Prüfung von Vorgängen in einem dokumentierten Umfang nachweisen, ohne Geheimnisse zu offenbaren.
3. Den Preis des nächsten Monats vorhersagen.

> **Antwort anzeigen: Wiederherstellung und Prüfung von Vorgängen in einem dokumentierten Umfang nachweisen, ohne Geheimnisse zu offenbaren.**
> Lernerfolg zeigt sich an geprüften Fähigkeiten und Grenzen, nicht an Seitenaufrufen oder Vorhersagen.

Handbuch für Lernende

Cuvex-Bedienhandbuch

Dieses Handbuch begleitet die Lektionen. Jedes Verfahren beschreibt den in den geprüften Quellen vorgefundenen Ablauf, seine Kontrollen und den Haltepunkt. Die Ausgabe ist für einen Pilotversuch vorgesehen. Sie belegt keine eigenen physischen Tests mit Original, BIT, Telefonen oder allen Desktop-Plattformen. Vor Unterricht mit echtem Guthaben muss das Team die Abnahmematrix vervollständigen und abweichende Beschriftungen oder Ansichten anpassen.

Referenzstände sind Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 und Mirror 1.0.0-beta.12.12. Die Profilauswahl in Desk gibt erklärte Kompatibilität an und misst keine Firmware aus der Ferne. Die enthaltenen Mirror-Screenshots stammen vom Android-Emulator des Pakets 12.12. Die Produktfotos sind Firmenmaterial und belegen keine auf einem heutigen Gerät angezeigte Version.

P01 | Herkunft und Version prüfen | Cuvex | L16,L21 | C01,C02

Vorbereitung: Halte Kaufunterlagen und einen unabhängig überprüfbaren offiziellen Kontaktweg bereit. Gib noch keine Geheimnisse ein.

1. Prüfe Verpackung und Siegel. Stoppe bei Manipulationsspuren die Inbetriebnahme und bewahre nicht sensible Belege auf.
2. Nutze die Integritäts- und Siegelprüfung der zur Lieferung passenden App. Gib Codes nur dort ein, niemals beim Tutor.
3. Bestimme Original oder BIT und den verfügbaren Revisionsstand. Prüfe die sichtbare Version von Gerät und Apps.
4. Vergleiche mit der vom Team veröffentlichten Matrix. Weder Katalog noch Hash ersetzen Firmware-Authentifizierung oder physische Abnahme.

Ergebnis: Modell und Versionen sind bekannt, die Herkunft ist ohne Offenlegung von Geheimnissen geprüft. Sind die Codes ungültig oder weicht die Oberfläche ab, erzwinge die Nutzung nicht mit einer alten Anleitung.

Pause vor dem Laden von Verwahrungsmaterial. Die geschäftliche Rückverfolgbarkeit allein schließt fortgeschrittene Manipulationen nicht aus.

P02 | Original über Bluetooth aktualisieren | Original | L46 | C01,C02,C03

Vorbereitung: wiederherstellbare Kopien, stabile Stromversorgung, kompatibles offizielles Paket und für dein System abgenommener Ablauf. Dieser Kurs belegt nicht die vollständige physische Verfügbarkeit auf jeder Plattform.

1. Wähle in der Geräte- oder Firmwareansicht der App Original und den offiziellen Download oder die passende authentische lokale Datei.
2. Versetze das Gerät über sein Menü in den Updatemodus und verbinde es im App-Ablauf. Bleibe in Reichweite und vermeide konkurrierende Sitzungen.
3. Gib den auf Original angezeigten Code im vorgesehenen Feld ein. Verwechsle ihn nicht mit dem Kryptogrammpasswort.
4. Verfolge Übertragung, Validierung, Installation und Neustart. Die Prozentanzeige belegt keine Installation.
5. Prüfe die endgültige Version auf Original und trage sie in der App ein, falls ein entsprechendes Feld vorhanden ist.

Ergebnis: Version nach Neustart am Display geprüft und Abschluss des Ablaufs bestätigt. Scheitert er vor PIN, bei den Paketen oder am Ende, notiere Phase und Code. Trenne nichts und wechsle nicht auf Verdacht Software, um „über 99 %“ zu kommen.

P03 | BIT über USB aktualisieren | BIT | L46 | C01,C02,C03

Vorbereitung: Bestimme das echte BIT-Medium, Stromversorgung und kompatibles offizielles Paket. Sichere die Daten vor einem Softwarewechsel.

1. Wähle BIT im unterstützten Firmwareablauf von Desk oder Mirror.
2. Verbinde das Gerät mit geeignetem Datenkabel und Adapter. Erlaube auf Anforderung der App den Zugriff auf Laufwerk oder Ordner.
3. Wähle die authentische Firmware für das Modell. Prüfe vor der Übertragung Version und Kompatibilitätsangaben.
4. Warte auf Übertragung und Gerätevalidierung. Das Laufwerk kann gemäß Protokoll verschwinden und erneut eingebunden werden.
5. Prüfe nach Neustart die Version auf BIT und die Abschlussmeldung der App.

Ergebnis: Die Installation ist am Gerät bestätigt. Fehlt das Laufwerk, prüfe Gerätemodus, Datenkabel, Berechtigungen, Einbindung und andere aktive Sitzungen. Ersetze es nicht durch einen gleichnamigen PC-Ordner. Nach fehlgeschlagenem Update brauchst du das offizielle Wiederherstellungsverfahren dieser Hardware.

P04 | Wallet mit Münze und Würfeln erzeugen | Cuvex | L17 | C01

Vorbereitung: privater Raum, geeignete Würfel und Münze, keine Kameras und kein aktives Tutormikrofon. Nutze eine Übungswallet.

1. Öffne die Wallet-Erstellung und den Entropieablauf der Firmware. Lege vorher die Reihenfolge der vier Würfel fest.
2. Gib Münze und jeden Würfel wie angezeigt ein. Ändere keine Ergebnisse nach Belieben.
3. Die geprüfte Quelle berechnet Index = Münze × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Zulässig sind ausschließlich die Indizes 0 bis 2.047.
4. Wirf bei Ablehnung Münze und sämtliche Würfel neu. Die Meldung behält frühere Wörter bei und verlangt die Wiederholung des gesamten Satzes.
5. Schließe den Gerätealgorithmus einschließlich Endprüfung ab, schütze die Wortfolge und teste die Wiederherstellung privat.

Ergebnis: Die Wallet ist im vollständigen Ablauf entstanden, ohne Wörter manuell auszuwählen. Weichen Anzeige und Quelle ab, stoppe. Nutze öffentliche Beispiele von Würfen, Seeds oder Schlüsseln niemals als eigenes Material.

P05 | Ein Geheimnis verschlüsseln | Cuvex | L18,L19 | C01

Vorbereitung: Wähle Modell, Inhaltsformat und Schutz. Eingabe am PC oder Telefon legt das Geheimnis dort offen, auch wenn das Ziel verschlüsselt wird.

1. Wähle Verschlüsseln und BIP39, SLIP39, Monero oder unterstützten Text. Vertausche keine Wortlisten. Die geprüfte Klartexteingabe unterstützt bis zu 500 Zeichen. Das Speichern eines anderen Formats bedeutet keine Signierfähigkeit in seinem Netz.
2. Gib den Inhalt direkt am Gerät ein, um die Trennung zu erhalten. Prüfe Reihenfolge, Zeichen und Zusatzfelder auf seinem Display.
3. Wähle je nach Ablauf individuellen oder gemeinsamen Schutz und auf BIT gegebenenfalls Biometrie. Unterscheide diese Schwelle vom Bitcoin-Schwellenwert.
4. Gib die Passwörter gemäß Firmwareprüfung privat ein und bestätige sie. Übertrage die Desk-Regeln nicht automatisch.
5. Beschreibe bei Original eine kompatible leere Karte. Bewahre bei BIT die Exportobjekte des USB-Ablaufs auf. Warte auf Bestätigung.
6. Öffne eine Probewiederherstellung, prüfe den Inhalt und schließe am Ende die Geheimnisanzeige.

Ergebnis: Kryptogramm mit geprüfter Wiederherstellung. Scheitert Schreiben oder Lesen, schütze das Original und folge der Wiederholungsanweisung am Display. Lösche keine Datenköpfe und erzwinge kein Überschreiben.

P06 | Auf dem Gerät entschlüsseln | Cuvex | L18 | C01,C02

Vorbereitung: Sichtschutz und ausreichende Entsperrkomponenten. Deaktiviere Mikrofon und Bildschirmaufnahme in der Nähe des Geheimnisses.

1. Starte die Entschlüsselung im richtigen Modell und liefere das Kryptogramm bei Original über NFC, bei BIT über den USB-Ablauf.
2. Prüfe Alias und Objektkennung, bevor du Zugangsdaten eingibst.
3. Gib die nötigen Passwörter und bei entsprechendem Format Biometrie ein. Versuche es nach Fehlern nicht automatisch weiter. Es bestehen Zugriffskontrolle und Sperren.
4. Prüfe den Inhalt nur auf dem vorgesehenen Display. Ein Geheimnis als QR-Code ist genauso sensibel wie sein Text.
5. Schließe oder beende den Vorgang gemäß Gerät und verwahre Medium und Zugangsdaten nach Plan getrennt.

Ergebnis: Inhalt privat wiederhergestellt und Sitzung beendet. Bei unbekanntem Format, gescheiterter Authentifizierung oder unerwartetem Inhalt nutze keine unbekannte App zur „Reparatur“. Beschreibe dem Support Version, Format und Fehler ohne Anhang des Geheimnisses.

P07 | Wiederherstellung eines biometrischen Kryptogramms vorbereiten | BIT | L19,L47 | C01,C02

Vorbereitung: Übungskryptogramm und Dokumentation seines Formats. Das Vorhandensein einer .bin-Kopie belegt keine Wiederherstellung.

1. Prüfe in der Desk-Detailansicht biometrische Komponenten und verfügbaren Wiederherstellungsexport.
2. Bewahre den zusammengehörigen Dateisatz und eine unabhängige Kopie unter unauffälligen Kennungen auf.
3. Teste die normale Entsperrung auf BIT und dokumentiere benötigte Passwörter und Bedingungen.
4. Prüfe die lokale Notfallwiederherstellung und ihre unterstützten Formate. Stelle vorher sicher, dass alles Nötige vorhanden ist.
5. Übe mit Material ohne Guthaben den Fall eines defekten Geräts oder nicht verfügbaren Fingerabdrucks.

Ergebnis: getesteter Plan mit Grenzen für genau dieses Format. Nicht jede Biometrie lässt sich überspringen und kein Fingerabdruck ersetzt Sicherungen. Nach Wiederherstellung eines Geheimnisses am PC beurteile die Offenlegung und die Notwendigkeit einer anschließenden Kontrollmigration.

P08 | Eine Kryptogrammkopie erstellen und prüfen | Cuvex und Desk | L20 | C01,C02

Vorbereitung: identifizierte Ausgangskopie und kompatibles Ziel ohne zu erhaltende Daten.

1. Nutze für Original die Klonfunktion des Geräts oder die unterstützte Desk-Funktion und lege Quelle und Ziel in der angegebenen Reihenfolge vor.
2. Halte die Karten ruhig und respektiere die Ablehnung eines Mediums, das bereits Kryptogramme enthält.
3. Exportiere bei BIT oder einer Datei sämtliche zugehörigen Komponenten und erhalte benötigte Namen oder Zuordnungen.
4. Trenne die Ausgangskopie und teste Lesen und Wiederherstellung ausschließlich mit der neuen Kopie.
5. Notiere Datum, Format und Ergebnis privat. Verwahre Kopien an Orten mit unabhängigen physischen Risiken.

Ergebnis: eine zweite geprüfte Kopie. Das erzeugt weder eine andere Wallet noch widerruft es Passwörter oder schützt vor einem schon offengelegten Seed. Scheitert das Ziel, bewahre die Quelle auf. „Repariere“ sie nicht, um beide anzugleichen.

P09 | Desk-Speicher erstellen und entsperren, Passwort ändern | Desk | L21,L40 | C02

Vorbereitung: geprüftes Installationsprogramm, passende Architektur und Sicherungsplan für den Speicher.

1. Erstelle den Speicher mit einmaligem Passwort von 12 bis 1.024 Zeichen und übereinstimmender Bestätigung.
2. Sperre den Speicher und öffne ihn erneut als Zugangstest. Gib das Passwort nur in Desk ein.
3. Prüfe unter Sicherheit und „Zugang und Sperre“ Inaktivität und Hintergrundwechsel. Aktiviere während einer Vorführung keine optionale Löschung.
4. Gib zum Ändern das aktuelle Passwort ein und bestätige im vorgesehenen Ablauf das neue.
5. Richte zuvor genutzte PC-Biometrie nach Anweisung neu ein. Erstelle eine aktuelle Sicherung und dokumentiere den Bezug zu früheren Kopien.

Ergebnis: Zugang geprüft. Frühere Kopien behalten das ursprüngliche Passwort und die Verschlüsselung. PC- und BIT-Biometrie sind unterschiedliche Verfahren. Bei Zugangsfehlern stoppe Wiederholungen und prüfe Wiederherstellung, ohne dem Tutor Zugangsdaten anzuvertrauen.

P10 | Ein Kryptogramm in Desk verknüpfen und prüfen | Desk | L22 | C02

Vorbereitung: Testkryptogramm bekannter Herkunft und verfügbarer Übertragungsweg.

1. Öffne Kryptogramme oder Karten und wähle Verknüpfen über NFC, USB oder eine kompatible Kopie.
2. Wähle Design und Quelle. Für NFC nutze Cuvex Mirror auf einem per Bluetooth mit dem Computer gekoppelten Smartphone. Für Cuvex BIT nutze das über USB-C angeschlossene Laufwerk. Cuvex Desktop unterstützt keine externen USB-NFC-Lesegeräte.
3. Prüfe Alias, Herkunft, Größe, Format und interpretierte Bedingungen in der Detailansicht. Das sind Metadaten und keine entschlüsselten Inhalte.
4. Prüfe auf gespeicherte, noch nicht zugeordnete Konten und verknüpfe nur das verifizierte Konto.
5. Exportiere bei unzureichender Sicherungsabdeckung eine Kopie und erprobe die Wiederherstellung getrennt.

Ergebnis: Objekt lokal eingeordnet. „Verknüpft“ belegt weder Authentifizierung des Seeds noch Guthaben. Prüfe bei einem unbekannten Objekt Format und Version. Ändere nicht die Endung und lösche keine Daten, um die Annahme zu erzwingen.

P11 | Ein WOW-Beobachtungskonto aktivieren | Desk und Cuvex | L13,L22 | C01,C02

Vorbereitung: öffentliche Angaben aus dem Geräteablauf und privat geprüfte Herkunft.

1. Öffne die WOW-Aktivierung oder das Hinzufügen eines Kontos aus dem richtigen Kryptogramm.
2. Importiere Deskriptor oder unterstütztes öffentliches Material je nach Funktion per Datei, Webcam oder Mirror.
3. Prüfe Netz, Skript, Ursprung, Fingerabdruck, Pfad und gegebenenfalls Prüfsumme. Gib keinen Seed und keine xprv ein.
4. Benenne das Konto und wähle die Abfragequelle nach bewusster Zustimmung.
5. Prüfe eine Kontrolladresse und den Umfang der Adresssuche vor der Interpretation des Guthabens.

Ergebnis: zugeordnete Beobachtungswallet. Bei Nullanzeige prüfe Netz, ursprüngliche Passphrase, Ableitung, Konto, Anbieter und Scan. Schließe nicht vorschnell auf Verlust. Allgemeine Netzwerkunterstützung der Oberfläche gilt nicht zwangsläufig für das Multisig-Profil. Beachte den jeweiligen Kontext.

P12 | Knoten und Synchronisierung konfigurieren | Desk | L25,L33 | C02

Vorbereitung: Entscheidung zum Datenschutz und bei Core Zugang zu einem geschützten synchronisierten Knoten.

1. Wähle unter Sicherheit und „Datenschutz und Knoten“ das WOW-Konto und prüfe seinen Anbieter.
2. Wähle ausdrücklich einen unterstützten öffentlichen Anbieter oder Core. Gib für Core Endpunkt, Wallet und Zugangsdaten nur in der App ein.
3. Autorisiere die Abfrage in Kenntnis der Daten, die jeder Dienst erhält. TLS verbirgt die Abfrage nicht vor dem Anbieter.
4. Synchronisiere und prüfe Zeitpunkt, Kettenspitze, Fortschritt und Vollständigkeit. Prüfe bei erneutem Scan den abgedeckten Zeitraum und das Fortlaufen der Arbeit.
5. Halte bei 429 die Pause ein. Unterstelle nach einem Fehler keinen Wechsel auf einen anderen Knoten. Die Konfiguration wechselt nicht stillschweigend.

Ergebnis: Quelle und Stand sind bekannt. Öffne RPC nicht zum Internet, teile kein Passwort und beschränke die Adresssuche nicht auf Adressen mit Guthaben. Eine leere Historie kann ein Teilergebnis sein.

P13 | Empfangsanforderung erzeugen und wieder aufrufen | Desk und Cuvex | L26 | C01,C02

Vorbereitung: Konto, Netz und Richtlinie sind geprüft.

1. Öffne Empfangen und erzeuge die passende Anforderung oder rufe sie wieder auf.
2. Ergänze Beobachter, Zweck und erwarteten Betrag nur bei Bedarf an diesen lokalen Metadaten.
3. Prüfe die Adresse vor einem wesentlichen Zahlungseingang im unterstützten Geräteablauf. Fehlt die physische Abnahme, bleibe bei der Simulation.
4. Teile ausschließlich notwendige Daten über den authentifizierten Kanal des Empfängers.
5. Prüfe Eingang, Betrag und Bestätigungen in deiner Netzwerkquelle.

Ergebnis: abgestimmter Zahlungseingang, über die bloße Anforderung hinaus. Bei Multisig bleiben angezeigte Adressen für spätere Zahlungen erhalten und werden nicht neu vergeben. Ist die Grenze neuer Adressen ohne Historie erreicht, rufe frühere Anforderungen auf. Erzwinge keine Indizes von Hand.

P14 | Labels, Einfrieren und BIP329 | Desk | L27 | C02,B13

Vorbereitung: Laborkonto mit UTXOs und Passwort für den geschützten Export.

1. Kennzeichne einen Eingang nach Kontext ohne unnötige personenbezogene Angaben.
2. Friere bewusst ein oder hebe die Sperre auf und prüfe das ausgebbare Guthaben. Die Beschränkung gilt lokal.
3. Exportiere Labels mit der geschützten Funktion. Unterscheide das Format BIP329 von der Dateiverschlüsselung.
4. Importiere in eine kompatible Kopie und gleiche Verweise, Labels und eingefrorene Ausgänge ab.
5. Bewahre eine aktuelle Metadatensicherung und das zugehörige Passwort entsprechend deinem Plan auf.

Ergebnis: Kontext ist erhalten und die Auswahl nachvollziehbar. Ein Import darf eingefrorene Coins nicht ungeprüft automatisch entsperren. Sende dem Tutor keine Labeldatei. Auch ohne Ausgabeschlüssel kann sie Gegenparteien und Beziehungen offenlegen.

P15 | Zahlung vorbereiten und alles senden | Desk | L28 | C02

Vorbereitung: geprüfte Anforderung und Konto mit ausreichend ausgebbaren Eingängen.

1. Öffne Bezahlen über WOW, UTXOs oder Chat und bestätige Konto und Netz.
2. Wähle Eingänge, Empfänger und Beträge. Prüfe die dadurch verbundenen Kontexte.
3. Wähle den Gebührensatz und prüfe absolute Gebühr, Wechselgeld und Warnungen. Prüfe bei Dust Alternativen, ohne eine verborgene Gebühr zu akzeptieren.
4. Prüfe bei vollständiger Übertragung den Nettobetrag nach Gebühr. Bestätige im Chat eine Teilzahlung ausdrücklich, wenn sie die Anforderung nicht deckt.
5. Bereite den Entwurf vor und prüfe vor dem Signatur-Export alle Angaben.

Ergebnis: nachvollziehbare Absicht und PSBT des Vorgangs. Ein allgemeines Formular kann mehr Eingänge oder Empfänger zulassen als die Hardware. Es gelten tatsächliche Grenzen des Signierers und Transports. Änderungen an Ausgängen oder Bedingungen verlangen erneute Prüfung.

P16 | Eine PSBT mit Original signieren und zurückgeben | Original und Mirror | L29 | C01,C02,C03

Vorbereitung: richtiger Entwurf, kompatible Transportkarte, kompatibles authentifiziertes Kryptogramm und privat verfügbare Entsperrmittel. Eine ältere Kopie ohne geprüfte Echtheit kann vor Signatur eine geprüfte Wiederherstellung und neue Kopie erfordern. Das Bearbeiten des Datenkopfs löst das nicht.

1. Exportiere die Anfrage über den unterstützten NFC-Ablauf von Desk/Mirror.
2. Bringe sie zu Original. Lege das angeforderte Kryptogramm vor und entsperre es, ohne Zugangsdaten zu diktieren.
3. Prüfe Netz, Zusammenfassung, vollständige Ausgänge, Gebühr, Wechselgeld und Pflichtwarnungen.
4. Entscheide bei Final-Multisig über die erweiterte Ansicht. Gib die drei abschließenden Bestätigungen nur, wenn alles übereinstimmt.
5. Warte auf das Schreiben und erneute Lesen der Antwort auf der Karte.
6. Lies die Antwort mit Cuvex Mirror und validiere sie im zugehörigen Desk-Vorgang.

Ergebnis: Signatur empfangen und dem Entwurf zugeordnet. Die Veröffentlichung ist ein weiterer Schritt. Bewahre bei Schreibfehler den Stand und folge dem Wiederholungsablauf. Nutze die Sicherungskarte nie als entbehrliches Zahlungsmedium.

P17 | Mit BIT signieren, empfangen und quittieren | BIT und Desk | L29 | C01,C02

Vorbereitung: richtiger Entwurf, kompatibles authentifiziertes Kryptogramm und ausgewähltes echtes BIT-Laufwerk. Wird eine alte Kopie zum Signieren abgelehnt, folge der vorgesehenen Wiederherstellung und Erneuerung, ohne das Format zu erzwingen.

1. Übertrage die Anfrage über den Desk-Dienst per USB-C und folge für das Kryptogramm den Gerätehinweisen.
2. Entsperre privat und prüfe Zusammenfassung, alle Ausgänge, Gebühr und Warnungen.
3. Prüfe bei Final-Multisig gegebenenfalls erweiterte Details und autorisiere mit den vorgeschriebenen Endbestätigungen.
4. Nutze in Desk „Von BIT empfangen“, um die Antwort dieses Vorgangs zu importieren und zu validieren.
5. Prüfe Speicherung und Quittung. Scheitert diese nach dem Empfang, wiederhole denselben Vorgang, keinen anhand des Modells neu gewählten.

Ergebnis: geprüfte Signatur und konsistenter Austauschzustand. Behalte bei Trennung vor Empfang oder nach Speicherung das Profil der Anfrage bei. Wechsle nicht auf eine andere Katalog-Firmware, um eine wartende Antwort passend zu machen.

P18 | Einen Vorgang finalisieren, veröffentlichen und verfolgen | Desk | L30,L44 | C02

Vorbereitung: geprüfte Signaturen und gegebenenfalls erreichte Schwelle.

1. Prüfe erneut Absicht, Eingänge, Ausgänge, Gebühr und Netzwerk.
2. Finalisiere mit der zugehörigen Aktion und prüfe, dass keine Signaturen oder Bedingungen fehlen.
3. Autorisiere die Verbreitung und speichere das lokale Ergebnis. Bleibt die Netzwerkantwort aus, prüfe den Stand vor Wiederholung.
4. Verfolge Mempool und Bestätigungen beim gewählten Anbieter mit Synchronisierungszeitpunkt.
5. Prüfe bei erwogenem RBF die neue Transaktion und beschaffe die erforderlichen Signaturen. Setze keine integrierte CPFP-Funktion voraus.

Ergebnis: Kettenstand über seine Quelle geprüft. Das Verwerfen eines Entwurfs widerruft keine schon exportierten Signaturen und ändert keine bestätigten Zahlungen. Weder Chatnachricht noch Screenshot ersetzen die Nachverfolgung.

P19 | Zwei Richtlinien-QR-Codes frei vergleichen | Mirror | L43 | C03,C02

Vorbereitung: Feld auf Desk und Cuvex sichtbar. Nutze für die Übung nur die synthetischen Kursbeispiele.

1. Öffne „Richtlinien vergleichen“ und lies zuerst eine beliebige der beiden Seiten.
2. Wähle den zu prüfenden Wert. Du kannst bei Schritt 15 beginnen und andere, manuell geprüfte Felder überspringen.
3. Lies den Gegenwert und prüfe beide Texte vollständig. Nutze bei unklarem Schritt „Desk-Schritt angeben“. Dieser Kontext wird manuell gesetzt.
4. Beziehe „Übereinstimmung“ bzw. „Keine Übereinstimmung“ nur auf dieses Textpaar. Leerzeichen, Groß- und Kleinschreibung und Kodierung zählen.
5. Beginne ein weiteres Paar in beliebiger Reihenfolge. Beende durch Verlassen oder Hintergrundwechsel entsprechend dem geprüften Löschverhalten.

Ergebnis: punktueller lokaler Vergleich. Er belegt weder Herkunft oder Sitzung noch Gesamtfreigabe oder Aktivierung. Kläre Abweichungen an den Quellen, ohne den Text für ein OK zu normalisieren.

P20 | Chat aktivieren, wiederherstellen und umziehen | Desk und Cuvex | L36,L39 | C02

Vorbereitung: DEV oder Produktion ist gewählt. Alias und Chat-Schlüssel befinden sich auf dem Gerät, niemals im Kurs.

1. Öffne Aktivierung oder Wiederherstellung des Chats aus dem Kontext des Kryptogramms.
2. Wähle neuen Alias oder Übertragung eines bestehenden und das von der App angegebene kompatible Mobilprofil.
3. Gib oder lies den Chat-Schlüssel ausschließlich im geschützten Ablauf ein. Verwende weder Seed noch PIN oder WOW-Schlüssel.
4. Prüfe die Aktivierung beim Dienst. Nutze bei offenem Status die Funktion zum Abschließen oder Prüfen, ohne Erfolg zu unterstellen.
5. Prüfe nach einem Umzug die Kontinuität mit Kontakten und vermeide die gleichzeitige Nutzung desselben Alias auf mehreren Geräten.

Ergebnis: Chat-Identität in richtiger Umgebung aktiviert oder wiederhergestellt. Frühere Sitzungen und Verlauf werden weder durch Chat-Schlüssel noch globale Desk-Sicherung automatisch wiederhergestellt. Beachte die Grenzen des vorhandenen Materials.

P21 | Identität eines Kontakts prüfen | Desk | L36,L48 | C02

Vorbereitung: vorab mit der Person vereinbarter unabhängiger Kanal.

1. Füge den Alias hinzu und rufe die öffentliche Identität in der App ab.
2. Vergleiche den Fingerabdruck über den authentifizierten Kanal, nicht allein im gerade erstellten Gespräch.
3. Vermeide bei Erkennungsfragen öffentliche Angaben oder Geheimnisse aus anderen Diensten.
4. Bestätige erst nach Klärung von Abweichungen. Stoppe bei Identitätswechsel Zahlungen und Koordination bis zur Prüfung.
5. Dokumentiere die Prüfmethode ohne Speichern sensibler Antworten im Kurs.

Ergebnis: kontextbezogenes Vertrauen in den Kontakt, keine Garantie für alle künftigen Anfragen. Eine Stimme kann imitiert und ein legitimes Gerät kompromittiert werden. Jede Transaktion braucht ihre eigene Prüfung.

P22 | Adresse anfragen, Zahlung anfordern und im Chat bezahlen | Desk und Cuvex | L37 | C02,C01

Vorbereitung: verifizierter Kontakt und kompatibles WOW-Konto.

1. Wähle je nach Absicht Adresse anfordern, mit Adresse antworten oder Zahlung anfordern.
2. Prüfe ursprüngliche Anforderung, Netz, Betrag und Notiz vor dem Senden.
3. Öffne zum Bezahlen die Vorbereitung aus dem richtigen Konto, wähle UTXOs und Gebührensatz und prüfe die Nettosumme.
4. Autorisiere auf Cuvex nach dem Verfahren deines Modells. Der Chat signiert nicht automatisch.
5. Verfolge Veröffentlichung und Bestätigung über deine Quelle. Gleiche ausdrückliche Teilzahlungen mit der ursprünglichen Anforderung ab.

Ergebnis: Koordination ohne Verzicht auf die Prüfungen der Verwahrung. Nachrichten- und Transaktionsstatus sind verschieden. Ein Explorer-Link kann Informationen an Dritte senden. Prüfe vor dem Öffnen, ob du ihn verwenden willst.

P23 | Ein empfangenes Kryptogramm teilen und verknüpfen | Desk | L38 | C02

Vorbereitung: konkreter Bedarf an Weitergabe, geprüfter Kontakt und festgelegte Entsperrmittel, die er erhalten soll.

1. Wähle die Chataktion zum Teilen eines Kryptogramms und prüfe das Objekt.
2. Hänge weder Passwort, Seed noch Chat-Schlüssel als Kommentar an.
3. Der Empfänger prüft die Herkunft und verknüpft das kompatible Objekt über seine Empfangsfunktion.
4. Beurteile, was er damit bereits tun kann und was ihm ausreichende Zugangsdaten zum Entsperren ermöglichen würden.
5. Plane einen realistischen Widerruf. Löschen von Nachrichten zieht keine externen Kopien zurück und macht bekannte Schlüssel nicht unbekannt.

Ergebnis: bewusste Übertragung eines verschlüsselten Objekts. Sie ist keine Zahlung und fügt allein keinen Schlüssel zu einer Multisig hinzu. Verlangt der Anhang zur Entschlüsselung eine unbekannte Webseite, stoppe den Ablauf.

P24 | Globale Desk-Sicherung und Wiederherstellung | Desk | L15,L21 | C02

Vorbereitung: Übungsspeicher und kontrolliertes Sicherungsziel.

1. Öffne die Speicher-Sicherungsfunktion und lege das geforderte Passwort fest. Bewahre die Zuordnung zu genau dieser Kopie auf.
2. Verwahre die Kopie außerhalb des einzigen genutzten Geräts und prüfe Herkunft und Integrität im vorgesehenen Ablauf.
3. Stelle in einer getrennten Testumgebung wieder her und prüfe Konten, Konfiguration und abgedeckte Daten.
4. Prüfe Ausnahmen. Setze die Sicherung von Chat, Sitzungen und Verlauf nicht voraus. Multisig-Richtlinie und private Schlüssel sind nicht austauschbar.
5. Wiederhole nach wesentlichen Änderungen und bewahre die Wiederherstellungsanweisungen auf.

Ergebnis: Sicherung mit bekanntem Umfang und Passwort. Alte Kopien behalten frühere Passwörter. Prüfe bei Zugangsänderung oder Offenlegung auch diese Kopien. Das Ändern des aktuellen Speichers allein reicht nicht.

P25 | Eine Multisig erstellen und annehmen | Desk und Cuvex | L41,L42 | C01,C02

Vorbereitung: unabhängige Teilnehmer, verifizierte Kontakte sowie vereinbartes Netz und tatsächliche Grenzen.

1. Der Ersteller wählt Namen, M/N, Netzwerk, Teilnehmer und betriebliche Gültigkeitsdauer.
2. Liefere den richtigen erweiterten öffentlichen Schlüssel mit Fingerabdruck und BIP48-Pfad über den unterstützten Ablauf.
3. Jeder Teilnehmer prüft, nimmt an oder lehnt ab und liefert sein öffentliches Material. Der Seed wird niemals geteilt.
4. Erstelle die vollständige Richtlinie und bereite ihre Prüfung auf jedem Gerät vor.
5. Bewahre vor Finanzierung Richtlinienkopien auf. Prüfe Kontrolladresse und Wiederherstellbarkeit.

Ergebnis: vollständiger, prüfbarer Vorschlag. Die Annahme der Einladung ersetzt die Hardwareprüfung nicht. Bei Beteiligung von Original beachte höchstens sechs Schlüssel und die NFC-Kapazität. BIT erweitert keine Grenzen der übrigen Teilnehmer.

P26 | Richtlinie prüfen und Bestätigung empfangen | Desk und Cuvex | L43 | C01,C02,C03

Vorbereitung: dieselbe vollständige Richtlinie für alle, richtiges Firmwareprofil und keine konkurrierenden Vorgänge auf dem Gerät.

1. Starte die Richtlinienprüfung im unterstützten Kontext. Original verlangt die ausdrückliche Auswahl des installierten Profils, BIT handelt Fähigkeiten gemäß seiner Spezifikation aus.
2. Liefere die Anfrage je nach Modell über NFC/Mirror oder USB-C.
3. Prüfe die Richtlinienfelder auf dem Gerät. Nutze Mirror bei Bedarf für frei gewählte Wertepaare ohne vorgeschriebene Reihenfolge.
4. Schließe die Gerätebestätigung ab und gib die Antwort über den passenden Weg zurück.
5. Validiere in Desk die zur Anfrage gehörende Antwort. Ersetze das nicht durch ein sichtbares OK im Vergleich.

Ergebnis: zugeordnete Prüfung mit auf diesen Durchlauf begrenzter Aussage. Der Katalog attestiert Firmware nicht aus der Ferne. Das Gerät wird nicht als dauerhafter Richtlinienspeicher dargestellt. Prüfe bei FIRMWARE_CAPABILITY_REQUIRED zuerst Desk-Version und Kombination aus Modell und Build.

P27 | Signaturen anfordern, empfangen und Koordination übergeben | Desk und Cuvex | L44 | C01,C02

Vorbereitung: geprüfte Richtlinie, identifizierter Vorgang und vereinbarte Empfänger.

1. Bereite Eingänge, Ausgänge, Gebühr und Notizen vor und bitte unterstützte Teilnehmer um Signaturen.
2. Jeder Teilnehmer prüft und signiert auf seinem Gerät über den für ihn vorgesehenen Übertragungsweg.
3. Empfange, prüfe und speichere jede Signatur. Kläre offene Quittungen ohne Wechsel des gespeicherten Profils.
4. Bei Übergabe nimmt der neue Koordinator den Ablauf an und prüft den Stand. M/N und Schlüsseleigentum ändern sich dadurch nicht.
5. Prüfe und finalisiere nach Erreichen der Schwelle vor dem Veröffentlichen. Verfolge die Transaktion im Netz.

Ergebnis: Koordination mit unterscheidbaren Nachweisen. Ein Fortschrittsbericht des Koordinators ist keine eigene lokale Prüfung. Abbrechen oder Ablehnen in einer App zerstört nicht zwangsläufig bei Dritten gespeicherte Signaturen.

P28 | Multisig exportieren, wiederherstellen und lokal entfernen | Desk | L45 | C02

Vorbereitung: bekannte Richtlinie und verschlüsselte Kopie mit einmaligem Passwort.

1. Exportiere die Wiederherstellungsdaten mit der Desk-Funktion. Der aktuelle Ablauf nutzt dafür den authentifizierten Behälter CVXMSBK1.
2. Verwahre Kopie und Passwort so, dass sie unabhängigen Risiken ausgesetzt sind. Schließe bei alten Dateien nicht aus der Endung auf Verschlüsselung.
3. Liefere zur Wiederherstellung Kopie, Passwort und öffentlichen Teilnehmerschlüssel mit richtigem Ursprung, bei Bedarf über Webcam oder Mirror.
4. Prüfe vor der Nutzung Richtlinie, Netz, Adresse und Adresssuche.
5. Lies vor lokaler Löschung Umfang und Bestätigung. Bewahre bei gewünschter Wiederherstellbarkeit eine Kopie. Eine spätere Wiederherstellung musst du ausdrücklich auslösen.

Ergebnis: wiederherstellbare Richtlinie oder bewusste lokale Löschung. Diese bewegt keine Mittel, löscht keine fremden Signierschlüssel und annulliert allein keine von anderen aufbewahrten Vorgänge.

P29 | Außergewöhnliche Wiederherstellung am PC | Desk | L47 | C02

Vorbereitung: unterstütztes Format, vorbereitete saubere Umgebung und Sicherung. Der Vorgang kann dem PC ein Geheimnis offenlegen. Verwende im Kurs nur Übungsdaten.

1. Starte die lokale Wiederherstellung aus dem richtigen Kontext und lies Formatgrenzen und Warnungen.
2. Akzeptiere das Risiko bewusst und trenne das Netz wie vorgeschrieben. Das Fenster prüft den Zustand vor Freigabe des nächsten Schrittes.
3. Gib nur die nötigen Zugangsdaten im privaten Fenster ein. Diktiere sie nicht, füge sie nicht im Kurs ein und teile sie nicht mit dem Support.
4. Zeige das Geheimnis nur ohne Kameras oder mithörende Assistenten an. Beachte Zeitbegrenzung und Schließen.
5. Beende den Vorgang, prüfe mögliche Offenlegung und plane gegebenenfalls eine Migration auf neue Schlüssel.

Ergebnis: außergewöhnliche Wiederherstellung ohne Garantie forensisch sicherer Löschung oder Gleichwertigkeit mit isolierter Hardware. Fehlt Authentifizierung, Format oder Zugriffsmaterial, teste keine Internetwerkzeuge mit deiner echten Kopie.

P30 | Einstellungen, Biometrie und Sperre prüfen | Desk | L40 | C02

Vorbereitung: bekanntes Passwort und getestete Sicherung vor Sicherheitsänderungen.

1. Prüfe unter „Zugang und Sperre“ Passwort, verfügbare Biometrie, Inaktivitätssperre und Sperre beim Hintergrundwechsel.
2. Kläre vor einer Änderung die Verzögerung nach Fehlversuchen und den eingestellten Höchstwert.
3. Lass die optionale Löschung deaktiviert, bis du Bedingungen, Schwelle und Wiederherstellung verstehst. Erprobe sie nicht im Produktivbetrieb.
4. Stelle in den Einstellungen Sprache, Design, Währung, Synchronisierung von 3 oder 5 Minuten und Töne ein.
5. Registrierst du bitcoin:-Links, prüfe beim Öffnen einer Anforderung Entsperrung, Auswahl und Prüfung. Der Link zahlt nicht selbst.

Ergebnis: Konfiguration nachvollziehbar. Betriebssystembiometrie hängt vom Gerät ab und ersetzt weder Passwort noch Sicherung. Optische Einstellungen ändern keine Bitcoin-Richtlinie.

P31 | Einträge löschen und ihre Reichweite verstehen | Desk | L22,L45 | C02

Vorbereitung: Bestimme, ob du lokales Kryptogramm, Konto, WOW, Chat oder Multisig entfernen willst, und welche Kopie du behältst.

1. Lies das gewählte Objekt und den Warnhinweis. Bestätige den genauen Alias oder die ausdrückliche Bedingung, wenn die App dies verlangt.
2. Exportiere und teste eine Kopie, falls du den Zustand später wiederherstellen musst.
3. Entferne nur das vorgesehene Objekt und prüfe, welche Zuordnungen erhalten bleiben oder aufgehoben werden.
4. Prüfe verbleibende Vorgänge oder externe Teilnehmer. Setze nicht voraus, dass Nachrichten, Signaturen oder Dateien auf anderen Geräten verschwinden.
5. Dokumentiere die Änderung in deiner privaten Bestandsliste ohne sensible Angaben im Kurs.

Ergebnis: bewusst verwalteter lokaler Zustand. Keine dieser Handlungen ändert allein die Skripte finanzierter UTXOs, löscht einen Dritten bekannten Seed oder macht bestätigte Transaktionen rückgängig.

P32 | Fehler diagnostizieren, ohne Geheimnisse offenzulegen | Desk und Mirror | L23,L30,L48 | C02,C03

Vorbereitung: Notiere ungefähre Uhrzeit, System, Architektur, Version und Phase. Wiederhole sensible Vorgänge nicht fortlaufend, solange der Zustand unklar ist.

1. Ordne den Fehler Suche, Kopplung, Lesen, Schreiben, Validierung, Signatur, Rückweg, Netz oder Anzeige zu.
2. Kopiere Fehlercode und -text ohne QR-Codes oder private Angaben. Nutze gegebenenfalls die App-Diagnose.
3. Prüfe die Datei vor der Weitergabe. Hänge keine Speicherkopie, Kryptogramme, Seeds, Chat-Schlüssel, Deskriptoren oder RPC-Zugangsdaten an.
4. Dokumentiere bei Oberflächenfehlern Fenstergröße, Zoom und verdeckte Bedienelemente in einer synthetischen Szene.
5. Sende das erwartete Ergebnis und nachstellbare Schritte über den offiziellen Kanal. Der Kurs sendet nicht automatisch Supportnachrichten.

Ergebnis: untersuchbarer Bericht mit möglichst wenigen Daten. Fehlt ein Nachweis für einen Schritt, vermerke „ausstehend“ und nicht „abgeschlossen“. Die Sprachbegleitung braucht keinen Fernzugriff auf dein Verwahrungsgerät.

Glossar zu Bitcoin und Selbstverwahrung

Bitcoin

Netzwerk und Regelwerk zur Übertragung von Werten und zur Prüfung ihrer Geschichte ohne zentrale Registerverwaltung.

BTC

Geldeinheit von Bitcoin. Ein BTC entspricht hundert Millionen Satoshis.

Satoshi

Einheit der Basiskette im Wert eines Hundertmillionstels eines BTC.

Blockchain

Historie miteinander verknüpfter und nach Regeln geprüfter Blöcke. Der Begriff allein beschreibt nicht alle Eigenschaften eines Netzwerks.

Block

Datenmenge mit Transaktionen und einem überprüfbaren Blockkopf.

Vollständiger Knoten

Software, die Blöcke und Transaktionen vor der Annahme auf Einhaltung ihrer Regeln prüft.

Mining

Erzeugen von Blöcken durch Arbeitsnachweise nach den Netzwerkregeln.

Arbeitsnachweis

Mechanismus, der für einen Blockvorschlag überprüfbare Rechenarbeit verlangt.

Konsens

Übereinstimmung der Teilnehmer über Regeln und die als gültig anerkannte Historie.

Mempool-Richtlinie

Lokale Annahme- und Weiterleitungsregeln. Sie müssen keine Konsensregeln sein.

Mempool

Lokale Menge unbestätigter Transaktionen, die ein Knoten vorhält.

Bestätigung

Aufnahme in einen Block der akzeptierten Kette und die anschließend erreichte Tiefe dieses Blocks.

Reorganisation

Wechsel eines Abschnitts der akzeptierten Kette, der Bestätigungen verändern kann.

UTXO

Noch nicht ausgegebener Transaktionsausgang, der gemäß seinen Bedingungen ausgegeben werden kann.

Eingang

Verweis auf einen früheren Ausgang und die zur Freigabe seiner Ausgabe nötigen Daten.

Ausgang

Von einer Transaktion erzeugter Wert samt Ausgabebedingung.

Wechselgeld

Ausgang, der den nach Zahlung und Gebühr verbleibenden Teil der Eingänge wieder unter eigene Kontrolle bringt.

Gebühr

Differenz zwischen dem Wert der Ein- und Ausgänge einer Transaktion.

vByte

Einheit der virtuellen Größe zur Angabe der relativen Kosten einer Transaktion.

sat pro vByte

Gebührensatz in Satoshis je Einheit virtueller Größe.

Dust

Kleiner Ausgang gemessen an Richtlinien und Ausgabekosten. Die Schwelle hängt von Kontext und Skript ab.

RBF

Ersetzen einer unbestätigten Transaktion nach unterstützenden Richtlinien. Eine Annullierung ist nicht garantiert.

CPFP

Verwendung einer Kindtransaktion, um einen stärkeren Anreiz für die gemeinsame Aufnahme mit ihrer Elterntransaktion zu schaffen.

Hash

Datenfingerabdruck für Integritätsprüfungen. Er verschlüsselt nicht und identifiziert allein keinen Urheber.

Privater Schlüssel

Kryptografische Möglichkeit, nach dem jeweiligen Verfahren Autorisierungen zu erteilen.

Öffentlicher Schlüssel

Daten zur Signaturprüfung und zur Konstruktion bestimmter Bedingungen ohne Offenlegung des privaten Schlüssels.

Digitale Signatur

Kryptografischer Nachweis der Autorisierung einer bestimmten Nachricht. Ihr Inhalt bleibt sichtbar.

Verschlüsselung

Schutz der Vertraulichkeit mit einem Schlüssel und einem Algorithmus.

Authentifizierte Verschlüsselung

Verschlüsselungsverfahren, das gemäß seinem Entwurf auch Veränderungen erkennt.

AES GCM

Familie authentifizierter Verschlüsselungsverfahren in Formaten des Ökosystems. Ihre Eigenschaften hängen von Implementierung und Schlüsselhandhabung ab.

Mnemonik

Wortdarstellung von Ausgangsmaterial und Prüfinformation nach einem bestimmten Format.

Seed

Ausgangsmaterial für die Schlüsselableitung. Umgangssprachlich steht der Begriff auch für die Wörter, daher ist der Kontext zu klären.

Entropie

Unvorhersagbarkeit des Ausgangsmaterials. Die Wahl einprägsamer Wörter erzeugt sie nicht.

Prüfsumme

Prüfwert zur Erkennung bestimmter Fehler. Er authentifiziert keinen Urheber.

BIP39

Spezifikation für Mnemoniken und die Seed-Ableitung mit optionaler Passphrase.

BIP39-Passphrase

Zusätzliche Eingabe für die Ableitung. Eine andere Passphrase kann eine andere gültige und leere Wallet ergeben.

BIP32

Spezifikation für die hierarchische Schlüsselableitung.

Ableitungspfad

Folge von Zweigen, über die aus einer Wurzel Schlüssel gewonnen werden.

Gehärtete Ableitung

Ableitungsschritt, gewöhnlich mit Apostroph oder h gekennzeichnet, mit anderen Eigenschaften als eine gewöhnliche öffentliche Ableitung.

xpub

Erweiterter öffentlicher Schlüssel mit Kontext für die Ableitung. Für die Privatsphäre sensibel.

xprv

Erweiterter privater Schlüssel. Teile ihn nicht und importiere ihn niemals in einen Kurs.

Master-Fingerabdruck

Kurze Wurzelkennung zur Zuordnung. Als alleiniger Identitätsnachweis reicht sie nicht aus.

Deskriptor

Ausdruck zur Skripterstellung aus Schlüsseln und Ableitungen. Er kann öffentlich sein oder privates Material enthalten.

Watch-only

Beobachtungswallet ohne ausreichendes privates Schlüsselmaterial zum eigenständigen Signieren.

WOW

Bezeichnung für Beobachtungskonten und Wallet-Verwaltung im Cuvex-Ökosystem.

Hot Wallet

Werkzeug mit Signierfähigkeit in einer verbundenen Umgebung.

Selbstverwahrung

Modell, in dem Nutzer die technische Möglichkeit zur alleinigen oder gemeinsamen Ausgabe nach ihrer Richtlinie behalten.

Verwahrer

Stelle, die im Auftrag des Kunden die Ausgabe kontrolliert und ihre Zugangsbedingungen anwendet.

Cuvex-Kryptogramm

Verschlüsseltes Objekt zum Schutz eines Geheimnisses. Es ist für sich weder Transaktion noch Guthaben.

Desk-Passwort

Zugangsschutz für den lokalen Speicher. Es entspricht weder Seed noch Kryptogrammpasswort.

Chat-Schlüssel

Geheimnis zur Wiederherstellung der Chat-Identität. Es kann wie eine öffentliche Angabe aussehen und bleibt dennoch geheim.

Kopplungs-PIN

Vorübergehender Code einer Verbindungssitzung. Er ist kein Passwort zur Verwahrung.

Air Gap

Betriebliche Trennung von Umgebungen. Übertragene Daten müssen weiterhin geprüft werden.

NFC

Nahbereichskommunikation mit kompatiblen Karten und Lesegeräten.

USB Mass Storage

Dateiaustauschschnittstelle des BIT-Modells. Sie erfordert eigenes Protokoll, Prüfungen und Empfangsbestätigungen.

PSBT

Behälter für Daten und Signaturen zur Koordination der Erstellung und Autorisierung von Transaktionen.

PSBT v0

In BIP174 definiertes Format des geprüften Final-Multisig-Profils.

PSBT v2

In BIP370 definierte Formatversion. Transaktionsversion 2 lässt für sich nicht auf die Version des Behälters schließen.

SIGHASH ALL

Im geprüften Profil genutzter Modus, der bestimmt, was die Signatur bindet. Sein technischer Umfang ist Teil der Transaktionsprüfung.

P2WPKH

SegWit-Bedingung mit einem Schlüssel, üblicherweise mit BIP84-Konten verbunden.

P2WSH

SegWit-Bedingung, die ein Skript bindet. Das geprüfte Final-Multisig-Profil verwendet sie.

P2TR

Taproot-Ausgangstyp. Unterstützung als Empfängeradresse bedeutet keine Unterstützung beim Signieren einer Ausgabe daraus.

sortedmulti

Multisig-Konstruktion, die Skripte mit deterministischer Schlüsselreihenfolge erzeugt.

Schwelle M von N

Zahl M der nach einer konkreten Richtlinie erforderlichen Autorisierungen unter N Beteiligten.

MuSig2

Protokoll zur Aggregation von Schnorr-Signaturen mit N-von-N-Grundschema. Es entspricht keiner beliebigen Schwelle.

Taproot

Bitcoin-Mechanismen für Ausgaben und kryptografische Bindungen mit Schlüssel- und Skriptpfaden.

Miniscript

Sprache zur Beschreibung und Analyse bestimmter Skriptrichtlinien. Im geprüften Final-Profil nicht implementiert.

Regtest

Lokales Labornetz unter Kontrolle des Betreibers der Umgebung und ohne wirtschaftlichen Wert.

Signet

Testnetz mit eigenen Eigenschaften. Es ist nicht ohne Weiteres mit Regtest austauschbar.

Mainnet

Bitcoin-Netzwerk für echte wirtschaftliche Nutzung.

Gap Limit

Kriterium zur Adresssuche anhand einer Lücke aufeinanderfolgender Adressen ohne Historie. Der Geltungsbereich hängt von der Wallet ab.

Coin Control

Bewusste Auswahl der auszugebenden UTXOs.

Konsolidierung

Zusammenführen von Ausgängen, um Fragmentierung zu verringern. Das beeinflusst Kosten und Privatsphäre.

Pseudonymität

Nutzung von Kennungen, die nicht direkt dem bürgerlichen Namen entsprechen. Das schafft nicht automatisch Anonymität.

Anonymität

Kontextabhängige Ununterscheidbarkeit gegenüber festgelegten Beobachtern. Eine App-Bezeichnung garantiert sie nicht.

Metadaten

Informationen über Kommunikation oder Aktivitäten, etwa Zeitpunkte, Größen und Beziehungen, getrennt vom Inhalt.

CoinJoin

Gemeinschaftliche Transaktionskonstruktion, die bestimmte Rückschlüsse erschwert, ohne dauerhafte Anonymität zu garantieren.

Payjoin

Gemeinsame Zahlung mit Eingängen von Zahlendem und Empfänger nach einem unterstützten Protokoll.

Tor

Netzwerk und Werkzeuge zum Verbindungsschutz. Ihre Nutzung ist für jede Anwendung einzurichten und zu prüfen.

VPN

Kanal, der einen Teil des Vertrauens in die Verbindung auf den Betreiber verlagert. Er verbirgt die Blockchain nicht.

Lightning

Zahlungssystem über Kanäle mit anderen Voraussetzungen und Risiken als bei einer On-Chain-Zahlung.

Invoice

Strukturierte Zahlungsanforderung. Format und Zahlungsart müssen bestimmt werden.

RPC

Schnittstelle für Aufrufe an einen Dienst wie Bitcoin Core. Sie erfordert Authentifizierung und Schutz.

TLS

Transportschutz vor bestimmten Bedrohungen. Der empfangende Server sieht die Anfragen weiterhin.

SRTP

Schutz für Audio auf bestimmten VoIP-Strecken. Er gewährleistet nicht automatisch Vertraulichkeit gegenüber dem Betreiber.

Idempotenz

Eigenschaft, die bei Wiederholung einer identifizierten Anfrage eine doppelte Wirkung verhindert.

Webhook

Zwischen Servern übertragenes Ereignis, dessen Echtheit und mögliche Wiederholung geprüft werden müssen.

RAG

Abruf von Wissensausschnitten, um eine Antwort auf Kontext und Version zu stützen.

Teach-back

Lernkontrolle, bei der Lernende das Verstandene in eigenen Worten erklären.

Phishing

Täuschung mit vorgetäuschter Identität und glaubwürdigem Kontext, um Zugriff zu erlangen oder eine Handlung auszulösen.

Social Engineering

Manipulation menschlicher Entscheidungen, die echte Informationen und Zeitdruck nutzen kann.

Notarisierung

Apples Vertriebskontrolle. Sie unterscheidet sich von einem Produktaudit oder einem physischen Test sämtlicher Abläufe.

Attestierung

Zustandsnachweis nach einem konkreten Verfahren. Der Desk-Kompatibilitätskatalog führt keine Fernmessung durch.

MiCA

Europäischer Rahmen für bestimmte Kryptowerte und Dienstleistungen. Er garantiert weder Rendite noch vollständige Entschädigung.

Travel Rule

Informationspflichten für erfasste Übertragungen. Selbstverwahrung hebt sie nicht auf.

Lernstand

Stelle für die Wiederaufnahme des Lernens mit minimalen Daten ohne Wallet-Informationen.

Prüfe, was du gelernt hast

Übe ohne echtes Guthaben. Der Selbsttest ist frei zugänglich und erfordert kein Konto.

Wer autorisiert bei der üblichen Nutzung von Cuvex die Ausgabe?

1. Das Gerät nach Prüfung durch den Nutzer
2. Der Sprachtutor
3. Der Kursserver

> **Antwort anzeigen: Das Gerät nach Prüfung durch den Nutzer**
> Die Freigabe erfolgt weiterhin auf Cuvex.

Wie vielen Satoshis entsprechen 0,001 BTC?

1. 1.000
2. 100.000
3. 1.000.000

> **Antwort anzeigen: 100.000**
> Ein BTC entspricht 100.000.000 sat.

Die Eingänge betragen 120.000 sat, die Ausgänge 119.000 sat. Wie hoch ist die Gebühr?

1. 1.000 sat
2. 119.000 sat
3. Ohne weitere Angaben 1 sat/vB

> **Antwort anzeigen: 1.000 sat**
> Die Differenz der Werte ergibt die absolute Gebühr.

Welchen Status hat eine signierte, noch nicht verbreitete Transaktion?

1. Bestätigt
2. Durch die Signatur unumkehrbar
3. Autorisiert, aber nicht zwingend veröffentlicht

> **Antwort anzeigen: Autorisiert, aber nicht zwingend veröffentlicht**
> Signatur und Veröffentlichung sind verschiedene Schritte.

Was kosten 200 vB bei 6 sat/vB?

1. 206 sat
2. 1.200 sat
3. 6 % des Zahlbetrags

> **Antwort anzeigen: 1.200 sat**
> Multipliziere virtuelle Größe und Gebührensatz.

Was musst du vor der Auszahlung von einer Börse prüfen?

1. Nur die niedrigste Gebühr
2. Ob Vermögenswert, Netzwerk, Adresse und Nettobetrag zusammenpassen
3. Den Seed der Gegenpartei

> **Antwort anzeigen: Ob Vermögenswert, Netzwerk, Adresse und Nettobetrag zusammenpassen**
> Nicht jedes Netz mit dem Kürzel BTC ist Bitcoin on-chain.

Was leistet eine digitale Signatur für sich genommen?

1. Sie verbirgt die ganze Nachricht
2. Sie autorisiert eine nach ihrem Verfahren überprüfbare Nachricht
3. Sie löscht veröffentlichte Daten

> **Antwort anzeigen: Sie autorisiert eine nach ihrem Verfahren überprüfbare Nachricht**
> Vertraulichkeit erfordert einen anderen Mechanismus.

Was kann eine Änderung der BIP39-Passphrase bewirken?

1. Eine andere gültige, scheinbar leere Wallet erzeugen
2. Sich immer per E-Mail zurücksetzen lassen
3. Das öffentliche Register früherer Zahlungen verändern

> **Antwort anzeigen: Eine andere gültige, scheinbar leere Wallet erzeugen**
> Die Passphrase fließt in die Ableitung ein.

Wie solltest du die xpub eines Kontos behandeln?

1. Als Angabe ohne jede Auswirkung
2. Als identischen privaten Seed
3. Als für die Privatsphäre sensible Information

> **Antwort anzeigen: Als für die Privatsphäre sensible Information**
> Sie kann eine umfassendere Beobachtung der Aktivitäten erlauben.

Warum kann ein einzelner Seed bei Multisig unzureichend sein?

1. Es fehlen die Richtlinie und die vom Schwellenwert geforderten Freigaben
2. Bitcoin erlaubt keinerlei Wiederherstellung
3. Die ursprüngliche Farbe der App ist erforderlich

> **Antwort anzeigen: Es fehlen die Richtlinie und die vom Schwellenwert geforderten Freigaben**
> Das Bewahren der Richtlinie und das Bewahren privater Signiermöglichkeiten sind unterschiedliche Anforderungen.

Der geprüfte Final-Algorithmus verwirft einen Würfelwurf. Was tust du?

1. Nur den Münzwurf wiederholen, bis er akzeptiert wird
2. Münze und alle vier Würfel erneut werfen
3. Ein bekanntes Wort auswählen

> **Antwort anzeigen: Münze und alle vier Würfel erneut werfen**
> Nur einen Teil erneut zu werfen kann die Zuordnung verzerren.

Was bedeuten zwei Passwörter zum Öffnen eines Seeds für Einzelsignatur?

1. Zwei zwingend erforderliche Schlüssel auf der Blockchain
2. Eine Taproot-Multisig
3. Eine Zugriffsschwelle für das Geheimnis, die unabhängig von der Bitcoin-Signaturschwelle ist

> **Antwort anzeigen: Eine Zugriffsschwelle für das Geheimnis, die unabhängig von der Bitcoin-Signaturschwelle ist**
> Die Verschlüsselung verändert das Skript nicht.

Was solltest du über ein vollständiges Desk-Backup wissen?

1. Es enthält zwingend den gesamten Chat
2. Es hat einen bestimmten Umfang und Ausnahmen. Der Chat ist nicht ohne Weiteres eingeschlossen
3. Es aktualisiert alle alten Kopien

> **Antwort anzeigen: Es hat einen bestimmten Umfang und Ausnahmen. Der Chat ist nicht ohne Weiteres eingeschlossen**
> Identität und Nachrichten wiederherzustellen sind unterschiedliche Aufgaben.

Was leistet ein richtig eingerichteter eigener Knoten?

1. Er beseitigt alle Datenlecks
2. Er verringert Abhängigkeiten bei Abfragen an Dritte und ermöglicht eigene Prüfungen
3. Er stellt verlorene Schlüssel wieder her

> **Antwort anzeigen: Er verringert Abhängigkeiten bei Abfragen an Dritte und ermöglicht eigene Prüfungen**
> Er garantiert weder Anonymität noch die Wiederherstellung von Geheimnissen.

Was bewirkt das Einfrieren eines UTXO in Desk?

1. Eine lokale, von der App verwaltete Beschränkung
2. Eine Änderung der Konsensbedingung
3. Den Widerruf anderer Seed-Kopien

> **Antwort anzeigen: Eine lokale, von der App verwaltete Beschränkung**
> Es handelt sich nicht um eine globale Ausgabesperre.

Die Verbindung bricht beim Veröffentlichen ab. Was tust du?

1. Sofort erneut zahlen
2. Die Wallet löschen
3. Zuerst prüfen, ob die Zahlung bereits verbreitet wurde

> **Antwort anzeigen: Zuerst prüfen, ob die Zahlung bereits verbreitet wurde**
> Eine Zeitüberschreitung beweist nicht, dass der Vorgang wirkungslos blieb.

Welche Folge kann die Wiederverwendung von Adressen oder das Verbinden von UTXOs verschiedener Kontexte haben?

1. Es kann beobachtbare Zusammenhänge offenlegen
2. Es löscht die Historie
3. Es garantiert Anonymität

> **Antwort anzeigen: Es kann beobachtbare Zusammenhänge offenlegen**
> Privatsphäre hängt von Kontext und späterer Verwendung ab.

Konfiguriert das Öffnen von Tor Browser automatisch Desk?

1. Ja
2. Nein
3. Nur bei dunklem Design

> **Antwort anzeigen: Nein**
> Der Netzwerkpfad ist für jede Anwendung zu prüfen.

Was ist der Chat-Schlüssel, der wie eine xpub aussieht?

1. Zur Veröffentlichung bestimmt
2. Eine Empfangsadresse
3. Ein Geheimnis der Chat-Identität

> **Antwort anzeigen: Ein Geheimnis der Chat-Identität**
> Der Verwendungszweck bestimmt die Schutzbedürftigkeit.

Was gilt bei einer Chatnachricht mit dem Text „bezahlt“?

1. Sie ersetzt Bestätigungen
2. Die Zahlung muss unabhängig im Netz überprüft werden
3. Sie ändert das Netzwerk der Zahlungsanforderung

> **Antwort anzeigen: Die Zahlung muss unabhängig im Netz überprüft werden**
> Der Status der Nachricht ist nicht der Status der Zahlung.

Welche Technik nutzt das geprüfte Final-Multisig-Profil?

1. MuSig2 und PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Beliebige Bitcoin-Skripte

> **Antwort anzeigen: P2WSH sortedmulti BIP48 PSBT v0**
> Wünsche oder Produktnamen erweitern den unterstützten Funktionsumfang nicht.

Womit kannst du den Vergleich in Mirror 12.12 beginnen?

1. Nur mit Schritt 1
2. Mit jedem gewählten Datenpunkt, auch mit Nummer 15
3. Nur mit dem letzten, nachdem alle anderen erledigt sind

> **Antwort anzeigen: Mit jedem gewählten Datenpunkt, auch mit Nummer 15**
> Jeweils zwei Werte werden frei und unabhängig verglichen.

Was belegt die Anzeige „Übereinstimmung“ in Mirror?

1. Globale Freigabe
2. Echte Herkunft beider QR-Codes
3. Zeichengleiche Übereinstimmung des Wertepaares

> **Antwort anzeigen: Zeichengleiche Übereinstimmung des Wertepaares**
> Die übrigen Prüfungen und die Antwort stehen noch aus.

Ein Seed wurde offengelegt. Was bewirkt ein neues Desk-Passwort?

1. Es entzieht dem Angreifer den Zugriff
2. Es widerruft die aus diesem Seed abgeleiteten Schlüssel nicht
3. Es löscht alle Kopien

> **Antwort anzeigen: Es widerruft die aus diesem Seed abgeleiteten Schlüssel nicht**
> Ein sicherer Übergang zu neuer Kontrolle muss geprüft werden.

Was sollte der Abschluss der praktischen Ausbildung festhalten?

1. Was gelesen, simuliert und physisch getestet wurde und was noch aussteht
2. Nur die verkauften Stunden
3. Das Versprechen einer unverwundbaren Verwahrung

> **Antwort anzeigen: Was gelesen, simuliert und physisch getestet wurde und was noch aussteht**
> Die einzelnen Nachweise haben unterschiedliche Aussagekraft.