CUVEX

CUVEX ACADEMY · 0.1

学ぶ。理解する。自分で管理する。

Bitcoinと自己管理を一歩ずつ学びましょう。講座、マニュアル、用語集、演習は登録不要ですべて無料です。好きなところから始められます。

無料・登録不要

すべてのセクション

1. 学習環境を整える
2. デジタル通貨と信頼の問題
3. Bitcoinの歴史と限界
4. サトシ単位で正確に計算する
5. 自分の脅威モデル
6. ノード、マイニング、コンセンサス
7. UTXOと取引のお釣り
8. メモリプール、承認、チェーン再編成
9. 手数料、仮想サイズ、取引の置換
10. ネットワーク、アドレス、インボイス
11. ハッシュ、署名、暗号化
12. シード、パスフレーズ、パスワード
13. 鍵の導出、xpub、ディスクリプタ
14. ウォレットと保管方式の選び方
15. 復旧できるバックアップ
16. OriginalとBITの違い
17. 物理的エントロピーでシードを作る
18. Cuvexで秘密情報を暗号化・復号する
19. 暗号化の閾値と生体認証
20. コピーを複製・保管・検証する
21. Cuvex Deskのインストールと保護
22. 暗号文の関連付けとWOWの整理
23. MirrorとDeskのペアリング
24. Mirror経由のNFC、USB-C、QRの読み取り
25. 公開プロバイダーと自分のノード
26. ビットコインの受け取りとアドレス確認
27. UTXOへのラベル付け、凍結、選択
28. 支払いの準備と確認
29. OriginalとBITによる署名
30. 最終化、配信、トラブル対応
31. Bitcoinで観察できる情報
32. 用途を分け、お釣りを管理する
33. ネットワークのプライバシー、Tor、VPN
34. CoinJoin、Payjoinと現在の限界
35. 実際のインシデントから学ぶ

36. チャットのアイデンティティ作成と連絡先確認
37. チャットからサトシを請求・支払う
38. 暗号文を理解して共有する
39. チャットの復旧とメタデータ
40. 日常の設定と権限の見直し
41. マルチシグウォレットを設計する
42. 招待の作成と鍵の提供
43. Mirrorで任意の順にポリシーを照合する
44. マルチシグの署名調整と配信
45. マルチシグの復旧と変更
46. 手順に沿ってファームウェアを更新する
47. 紛失、故障、緊急時の復旧
48. フィッシング、サポート詐称、音声詐欺
49. プライバシー、法令、個人の記録
50. 相続、継続計画、年次訓練
51. 価格、貯蓄、ファンダメンタル分析
52. ビットコインの購入先を選ぶ
53. 口座、注文、約定コスト
54. ローソク足、指標、テクニカル分析の偏り
55. 証拠金、先物、自動化
56. Lightningとその他のレイヤー
57. Taproot、MuSig2、耐量子技術の展望
58. 相互運用性とメーカーに依存しない復旧
59. regtestを使う技術演習
60. 最終課題と継続計画
61. 受講者マニュアル
62. Bitcoinと自己管理の用語集
63. 学んだことを確認しよう

M01

学習環境を整える

学習目標

講座を始める準備をし、3つの機器の役割を区別し、チューターに決して伝えない情報を確認します。

解説

ビットコインの受け取り、保管、支払い、復旧を自分で判断できるように学びます。最終目標は承認の前に判断の理由を説明できることです。独学でも受講できます。音声チューターは説明や質問で学習を支えます。資産を見ることも機器を操作することも必要ありません。

秘密情報を保護し、画面で操作を承認する機器はCuvexです。Deskはパソコンで暗号文、監視専用ウォレット、支払い、共同作業を管理します。Mirrorは対応操作を仲介するローカルな橋渡し役で、データを照合できます。署名機でも独立したウォレットでもありません。使える手順はモデルとバージョンで決まります。

講座とDeskに画面を1つずつ用意し、電話とCuvexを手元に置きます。画面が1つなら切り替えてください。秘密情報を入力する間はビデオ通話で画面を共有しません。演習の途中で通話が終わってもかまいません。中断するときはレッスン番号、到達した手順、つまずいた点だけを保存します。

人間の講師にもAIにも、シード、BIP39パスフレーズ、パスワード、チャットキー、PIN、非公開ファイル、購入コード全体を渡してはいけません。実際のxpub、ディスクリプタ、アドレスも不要です。これらで支払えなくても活動が明らかになります。エラーは文章で説明し、演習用の架空データを使ってください。

演習

1. パソコン、電話、Cuvexの実機とモデルを確認し、バージョンを自分だけのノートに記録します。
2. 資金のない練習環境と実際の保管環境を分けます。練習のために本番シードを取り込まないでください。
3. このレッスンで一時停止、ヘルプ、用語集の場所を確認します。秘密を尋ねられたら、そのやり取りを止めてください。

理解を確認する

誰が署名し、誰がネットワークに照会し、誰がデータを運ぶのか説明してください。助けなしに区別できたら先に進めます。

よくある質問

毎日チューターと話す必要がありますか。いいえ。自習したり、同じ回を繰り返したり、特定の手順だけを質問したりできます。講座へのアクセスと音声サービスの残り時間は別々です。

中断するとき

L01完了。機器を確認し、講座には秘密を記録していません。

シードフレーズを書き間違えていないか確かめたいとチューターに言われたら？

1. ゆっくり読み上げる。
2. 要求を断り、自分の安全な環境だけで確認する。
3. 最初の数語だけ送る。

> **答えを表示: 要求を断り、自分の安全な環境だけで確認する。**
> 秘密はその一部でも学習サービスの対象外です。

M01

デジタル通貨と信頼の問題

学習目標

ウォレットを開く前に、Bitcoinがどんな問題を解決しようとしているかを理解します。

解説

銀行残高は金融機関が管理する記録です。銀行が本人を認証し、処理する送金を決め、帳簿を管理します。普通のデジタルファイルは簡単に複製できます。写真を送っても手元にコピーを残せます。デジタルな単位を通貨として使うには二重支払いを防ぐ仕組みが必要です。

Bitcoinは検証規則、署名、共有された取引履歴を組み合わせます。単一の機関に帳簿全体を任せず、それぞれの参加者が取引と規則の整合性を確認できます。希少性を支えるのは規則が継続して検証され受け入れられることです。コインの画像や取引所の価格が希少性を生むわけではありません。

自己管理では責任の所在が変わります。保管業者の許可なく使える反面、すべてのバックアップを破棄したり誤送金に署名したりすれば失い得ます。自由に操作できても、安全対策、関係者との調整、配信時のネット接続、適用される義務の履行は必要です。

ネットワークとプロトコルを指すBitcoinと、その通貨単位BTCを区別してください。「ブロックチェーン」を名乗る他のネットワークには異なる性質があります。企業が「ビットコイン」と呼ぶ約束を得ることと、自分の鍵でBitcoinの出力を支配することも異なります。

演習

1. 銀行残高、取引所残高、自分の鍵で管理するUTXOの3例を比較します。
2. それぞれ、移動を止められる人と、アクセス方法を忘れた際に助けられる人を書き出します。
3. 写真をコピーした場合と、同じ出力を二度使おうとした場合に何が起きるかを説明します。

理解を確認する

残高と署名できることが別である理由を自分の言葉で説明します。専門用語を暗記する必要はありません。

よくある質問

自己管理なら仲介者はすべて不要ですか。購入、照会、連絡のサービスは自分で選べます。それらが持つ権限と受け取るデータが重要です。

中断するとき

実在の口座名を除き、責任を比較した結果を保存します。

電子署名だけでは解決できない通貨上の問題はどれですか。

1. 同じ出力を二度使おうとするのを防ぐ。
2. 鍵による承認を証明する。
3. 署名されたメッセージの変更を検出する。

> **答えを表示: 同じ出力を二度使おうとするのを防ぐ。**
> 署名は承認を示し、競合する支払いの順序は規則とコンセンサスで決まります。

M01

Bitcoinの歴史と限界

学習目標

Bitcoinの起源を知り、史実と宣伝文句を区別します。

解説

サトシ・ナカモトの論文は2008年に発表され、ネットワークは2009年に稼働しました。先行する暗号技術、プルーフ・オブ・ワーク、デジタル通貨の研究を生かした個人間電子現金の提案です。ソフトウェアや取引の検証にサトシの実名は不要です。

一社が一方的に規則を入れ替えて発展してきたわけではありません。開発者が変更を提案・審査し、運営者がソフトウェアを選び、マイナーがブロックを作り、利用者やサービスが何を受け入れるか決めます。意見が分かれることもあります。フォークとアプリの更新は別物です。

大量の仕事量が投入されていても、ノードは自分の規則に反するブロックを拒否できます。コンセンサスはコンピューターの台数による単純多数決ではありません。ノードを何千個も複製しても自動的に決定権は増えず、マイナーの多数派も利用者の秘密鍵を手に入れられません。

ブロック容量、検証コスト、不定の承認時間、公開台帳には設計上の限界と折り合いがあります。管理者による支払いの取消しや、初期状態での完全な秘匿性は提供されません。各種レイヤーやアプリは特定用途を支える代わりに、新たな依存先を生みます。

演習

1. 最初の論文、ネットワークの開始、SegWitの採用、Taprootの有効化を年表に置きます。公表前に日付を資料で確認してください。
2. 「企業が価格を保証する」「ノードが検証する」「マイナーがブロックを提案する」を商業上の約束か技術的役割に分類します。
3. 支払いを取り消す管理者がいないことの利点と代償を1つずつ説明します。

理解を確認する

コンセンサス規則、ローカルポリシー、企業の判断を区別してください。使っているアプリはネットワークの一部分です。

よくある質問

最新ソフトウェアは常に通貨規則を変えますか。いいえ。バグ修正、性能改善、ローカルポリシーの変更もあります。リリースノートと互換性を確認してください。

中断するとき

検証できる性質を1つ、追加の証拠が要る主張を1つ書きます。

有効な承認のない支払いを含むブロックは、マイナーの多数決で有効になりますか。

1. はい、51%を超えれば有効です。
2. 取引所が発表した場合に限ります。
3. 拒否規則を適用するノードにとっては無効です。

> **答えを表示: 拒否規則を適用するノードにとっては無効です。**
> 累積仕事量を比較するのは、そのノードの規則上で有効な履歴同士です。

M01

サトシ単位で正確に計算する

学習目標

BTCとサトシを換算し、相場に頼らず数量を確かめます。

解説

1 BTCは100,000,000サトシです。satは別の通貨ではなく単位です。ベースチェーンの金額は整数のサトシで計上します。0.001 BTCは100,000 sat、0.00001000 BTCは1,000 satです。小数点の表示は言語で異なるので、目分量でゼロを足さないでください。

為替レートはその時点のBTCをEURやUSDなどに換算するもので、管理しているサトシ数には影響しません。100,000 satは値動きしても100,000 satです。Deskの相場表示には出典と日時があります。BTC残高が正しくても古い相場で経済的判断を誤ることがあります。

支払いでは受取額、ネットワーク手数料、支出総額を分けます。50,000 satを送り手数料が600 satなら、ほかに自己宛て出力がない場合の支出は50,600 satです。「全額送金」の受取額は通常、手数料の分だけ利用可能残高より少なくなります。

例は計算練習であり、市場価格や推奨手数料ではありません。署名前に該当画面で単位、ネットワーク、宛先、総額を確認します。音声で「5万サトシ」と読み、同時に「50,000 sat」と表示できますが、不確かな文字起こしから金額を決めてはいけません。

演習

1. 250,000 satをBTCに換算すると0.0025 BTCです。0.00025000 BTCは25,000 satです。
2. 75,000 satを手数料900 satで送ると支出は75,900 satです。
3. シミュレーターで120,000 satから70,000 satを手数料1,000 satで送り、お釣りが49,000 satになることを確かめます。

理解を確認する

金額をBTCとsatで読み、どの金額が手数料込みか説明します。疑問があれば操作を中断します。

よくある質問

1 BTC丸ごと買う必要がありますか。いいえ。サービスごとの最低額や費用の範囲内で端数を購入できます。

中断するとき

演習の計算結果だけを残します。

80,000 satを、手数料1,200 satを差し引いて全額送ると、受取人にはいくら届きますか。

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

> **答えを表示: 78,800 sat。**
> ほかに出力がないこの例では、受取額は利用可能残高から手数料を引いた額です。

M01

自分の脅威モデル

学習目標

紛失、盗難、詐欺、データ流出に対し、リスクに見合う対策を選びます。

解説

セキュリティは意図どおりに行動できる状態を守ること、プライバシーは誰に自分の情報や関係を知られるか管理すること、可用性は必要時にアクセスできることです。誰にも開けられない金庫は自分にも開けられず、便利すぎるコピーは情報を明かしすぎる場合があります。

守る対象、攻撃者、事故を洗い出します。鍵、バックアップ、履歴、複製の保管場所、連絡先の身元が対象です。マルウェア、フィッシング、火災、失念、脅迫、故障、死亡、自分のミスには異なる対処が必要です。

おおよその発生確率、影響、具体策を表にします。長いパスワードは推測を難しくしても、自分で承認した詐欺宛先を訂正できません。同じバッグ内のコピー2つはバッグの紛失に弱く、マルチシグでも全機器とバックアップを一人が握れば共通の障害点が残ります。

講座とチューターも対象です。購入、通話、接続時間、進捗からメタデータが生じます。授業の個別化にサイトがアドレスや残高を求める必要はありません。DeskやMirrorで通常の登録が不要でも、ストア、音声事業者、照会先第三者に活動が伝わる場合があります。

演習

1. 資産額や正確な場所を含めずに、自分にとって大きなリスクを3つ書きます。
2. 各リスクについて予防、検知、復旧を決めます。例はカードの紛失、コピー2つの分散、棚卸し、復元テストです。
3. 購入、通話、残高照会、公開取引を観察できる人やシステムを区別します。

理解を確認する

次の対策がどのリスクを減らすか説明します。維持できない仕組みや相続人に説明できない複雑さを加えないでください。

よくある質問

機器を増やせば常に安全ですか。共通の依存先が減り、復旧を試せる場合に限ります。機器が増えると保守や取り違えも増えます。

中断するとき

計画は個人の資料に保管し、講座には「脅威モデルを確認済み」とだけ記録します。

一か所の火災ですべてのコピーを失うリスクを最も減らす対策は？

1. カードの色を変える。
2. 同じ引き出しにコピーを2つ入れる。
3. 確認済みのコピーを、同じ事故に巻き込まれにくい別々の場所に保管する。

> **答えを表示: 確認済みのコピーを、同じ事故に巻き込まれにくい別々の場所に保管する。**
> 冗長化には、原本を脅かす事故が起きても耐えられることが必要です。

M02

ノード、マイニング、コンセンサス

学習目標

ノードが何を検証し、マイニングが何を提供するかを説明します。

解説

フルノードはブロックと取引を受け取り、規則を検証し、チェーンの状態を把握します。ウェブサイトの残高表示を信じる必要はありません。マイニングはプルーフ・オブ・ワークでブロックを提案する過程です。マイナーは有効な取引を選び、受理されるブロックを探して競います。

プルーフ・オブ・ワークは履歴を書き直すコストを高めます。有効な候補同士では難易度を無視したブロック数ではなく累積仕事量を比較します。ブロック間隔にはばらつきがあります。10分は目標平均であって、次の支払いの予定時刻ではありません。

マイニング報酬はブロック高に応じて減額される補助金と、収録取引の手数料から成ります。高い手数料でも誤った署名を有効にはできません。経済的安全性や攻撃コストがあっても、新しい支払いが数学的に不可逆になるわけではありません。

自分のノードなら第三者への照会が減り、自分で検証できます。ただしOS、アクセス権、接続の保護が必要です。同期していないノードや、別のサーバーに照会するアプリでは、起動するだけでこの利点は得られません。

演習

1. 署名検証、ブロックの収録取引の選定、シードの保管、支払いの受諾判断の担当を挙げます。
2. 「マイナーが私のビットコインを預かる」という説明が誤りである理由を述べます。
3. 演習用ネットワークでブロック高と同期状態を確認します。RPC認証情報は公開しません。

理解を確認する

検証と提案の違いを説明します。たとえを使っても、最後に正確な技術的役割を述べます。

よくある質問

Bitcoinを使うにはマイニングが必要ですか。いいえ。始めるのに自分のノードも必須ではありませんが、利用先をどこまで信頼するかは把握してください。

中断するとき

演習用プロバイダーの種類だけを記録し、非公開URLは記載しません。

正しく設定したフルノードで何ができますか。

1. 受け入れるチェーンの規則を検証する。
2. どんな紛失鍵も復元する。
3. 値上がりを保証する。

> **答えを表示: 受け入れるチェーンの規則を検証する。**
> 検証と資産の保管は異なる役割です。

M02

UTXOと取引のお釣り

学習目標

取引を、出力を消費して新しい出力を作る処理として読みます。

解説

UTXOは過去の取引で生じた未使用の出力です。ウォレットは管理できる出力を特定して残高を計算します。銀行のように共通の口座残高から引く仕組みではなく、入力は取引IDと位置で過去の出力を参照します。

UTXOを使うと全額が消費されます。一部だけ払うなら通常、受取人への出力と自分が管理するお釣り出力を作ります。入力120,000 sat、受取額70,000、手数料1,000なら、お釣りは49,000です。入力合計＝出力合計＋手数料です。

アドレスとUTXOは異なり、1アドレスが複数の出力を受け取れます。アドレスは必ずしも一人を表しません。取引IDは公開でも、身元や各出力の所有者を結び付けて明かせば、チェーンのみでは分からない情報を加えます。

入力をまとめると同じ人が管理していると推測され、お釣りは将来の支払いを結び付け得ます。共同取引もあるので推測は万能の証拠ではありません。コインコントロールとは、組み合わせによる影響を理解して使う出力を選ぶことです。

演習

1. 架空の入力40,000、60,000、200,000 satを描き、最初の2つだけで70,000を手数料1,000で支払います。
2. お釣りは29,000 satで、3つ目の入力が使われないことを確認します。
3. 200,000だけで支払うとお釣りは129,000です。取引サイズが同じと仮定せず、費用と結び付きの違いを比べます。

理解を確認する

図で入力、宛先、お釣り、手数料を指し示します。判別できない出力がある実取引には署名しないでください。

よくある質問

自分のウォレットに戻るものはすべてお釣りですか。自分の別アドレスへの送金かもしれません。金額から推測せず、ポリシーと導出情報を確認します。

中断するとき

架空の図だけを保存し、自分の資産の画面は保存しません。

入力100,000 satから30,000と69,200の出力ができました。手数料はいくらですか。

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

> **答えを表示: 800 sat。**
> 100,000から99,200を引くと800 satです。

M02

メモリプール、承認、チェーン再編成

学習目標

取引の作成、配信、承認の状態を区別します。

解説

メモリプールはノードが自分のポリシーで保持する未承認取引の集合です。世界共通のものはありません。エクスプローラーに支払いが表示されても、そのサービスが認識しただけで、全ノードの受理や一定時間内の承認は保証されません。

PSBT作成では何も配信されません。署名は承認を与え、最終化は配信可能な取引を組み立て、公開で送信を試みます。承認数1は検証元が受け入れるチェーンのブロックに入ったことです。2承認はその上にもう1ブロックが積まれたことで、受取人の追加署名ではありません。

再編成でチェーンの一部が変わり、取引の承認数が減ったり未承認に戻ったりします。リスクが大きい支払いほど当事者は多くの承認を求める傾向があります。すべての金額・状況でリスクを消せる承認数はありません。

Deskが保存済み状態を表示するなら同期日時を確認します。古い「承認済み」は現在の状態を必ずしも表しません。送金が見当たらなければローカルIDを残し、配信状況と履歴を確認してから再作成します。焦って繰り返すと有効な支払いが二重に生じ得ます。

演習

1. 下書き、PSBT、署名、最終取引、配信、ブロック収録のカードを順に並べます。
2. 公開直後の切断を模擬し、再送金の前に何を確認するか決めます。
3. チャットの「支払済み」がネットワーク検証に代わらない理由を店舗に説明します。

理解を確認する

取引状態、その情報源と日時を、保証と取り違えずに伝えます。

よくある質問

Deskを閉じれば配信済み取引は取り消せますか。いいえ。他のノードや参加者が保持していることがあります。ローカルの下書きの取消しとは範囲が違います。

中断するとき

模擬取引の状態だけを記録し、チューターには本物のIDを渡しません。

公開を押した直後にパソコンが切断されました。最初に何をしますか。

1. 同じ支払いを最初から作り直す。
2. ウォレットを削除する。
3. 再接続して取引とその入力を確認する。

> **答えを表示: 再接続して取引とその入力を確認する。**
> 応答がなかったことは配信失敗の証拠ではありません。

M02

手数料、仮想サイズ、取引の置換

学習目標

費用を見積もり、仮想バイト当たりのsat、RBF、CPFPを理解します。

解説

ネットワーク手数料は入力と出力の差です。通常その競争力は仮想バイト当たりのサトシ数（sat/vB）で表します。送金額には直接依存しません。少額でも入力が多ければ高くなり、大口でも入力が少なければサイズは小さくなり得ます。

200 vBを5 sat/vBで送れば手数料は1,000 satです。最終サイズは署名や構造に左右され、署名前は見積もりです。Deskでは速度の目安と手動設定が使えます。「速い」表示は時刻を保証しません。

RBFは条件を満たす未承認取引を置き換えるポリシーです。より高い手数料の競合取引を提案できます。ノードのポリシーは変化しており、置換不可の合図は入金保証になりません。置換には改めて内容確認と必要な署名を行います。

CPFPは未承認取引の出力を使い、親子をまとめて取り込む採算を高める方法です。使える出力の管理権、ポリシーの順守、費用が必要です。Bitcoinの仕組みであって、利用中のCuvexにCPFPボタンがあるとは限りません。

「ダスト」は適用ポリシーと予想支出コストに比べ小さすぎる出力です。全スクリプト共通の閾値はなく、固定額をコンセンサス規則として教えません。お釣りが成立しなければ金額、入力、全額送金、実際の手数料を見直します。

演習

1. 180 vB×8 sat/vB＝1,440 satです。演習予算内か確認します。
2. 入力1つと10個を比べ、送金額だけで費用を見積もれない理由を説明します。
3. 未承認取引を模擬し、対応を決めつけずに、待機、RBF、CPFPの検討から選びます。

理解を確認する

手数料率、手数料総額、送金額に占める費用を説明し、納得できない手数料なら拒否します。

よくある質問

RBFなら元の支払いは確実に消えますか。いいえ。承認まで候補が競合し、伝播状況も影響します。取消しの約束だけで商品を渡さないでください。

中断するとき

演習で選んだ方法と理由を保存します。

250 vBを4 sat/vBとした手数料はいくらですか。

1. 1,000 sat。
2. 254 sat。
3. 送金額の4%。

> **答えを表示: 1,000 sat。**
> 仮想サイズに手数料率を掛けると推定手数料になります。

M02

ネットワーク、アドレス、インボイス

学習目標

コピーやスキャンの前にネットワーク、アドレス形式、支払い指示を識別します。

解説

mainnetでは経済的価値を持つビットコインが移動します。開発や学習用のテストネットワークは互換ではありません。regtestは演習の設置者が制御するローカル網、signetとtestnetにはそれぞれの規則と環境があります。signetで単一署名が使えてもCuvexのマルチシグ対応を意味しません。

アドレスは受け取り条件を符号化します。mainnetには1、3、bc1q、bc1pで始まる形式があります。接頭辞は種類を見分ける目安ですが、受取人の確認、署名機の互換性、形式全体の検証にはなりません。

QRは視覚的な容器で、アドレス、請求書、ディスクリプタ、悪意あるテキストも運べます。スキャンしても作成者は認証されません。bitcoin: リンクには金額やメッセージも指定できます。BIP321がBIP21の後継ですが、確認したDesk実装はBIP21の用語と互換性を保ちます。規格の更新だけではアプリの対応範囲は広がりません。

Lightningインボイスはオンチェーンのアドレスとは別で、有効期限などの項目を含み得ます。対応フローがなければオンチェーン送金欄に貼らないでください。別ネットワークのBTCというトークンも、ネイティブなビットコインとは限りません。

演習

1. 使える本物のアドレスを避け、講座の例をアドレス、bitcoin: URI、Lightningインボイス、ディスクリプタに分類します。
2. 演習のネットワークを確認します。確認済みのCuvexマルチシグプロファイルはmainnet/regtestに対応します。
3. 実取引の前に認証済みの経路で受取人が指定した全文を照合します。

理解を確認する

ネットワークや方法が不明な依頼は断り、何を確認すべきかを説明します。

よくある質問

取引所に表示されるどのネットワークでもBTCを送れますか。いいえ。出金網と実際の受取網が一致する必要があります。手数料の安さだけで選ばないでください。

中断するとき

演習用ネットワークの種類だけを記録します。

受取先がbc1アドレスであることだけでは別のトークン網からBTCを出金できません。ほかに何が必要ですか。

1. 受取人の表示名を変える。
2. 出金がBitcoinオンチェーンを使い、すべての情報が一致することを確認する。
3. 取引所にシードを入力する。

> **答えを表示: 出金がBitcoinオンチェーンを使い、すべての情報が一致することを確認する。**
> 資産、ネットワーク、受け取り方法が適合する必要があります。

M03

ハッシュ、署名、暗号化

学習目標

完全性、承認、機密性の違いを理解します。

解説

ハッシュ関数はデータを固定長の指紋に変換します。既知の指紋との照合は変更の検出に役立ちますが、ファイルを暗号化したり発行者を特定したりはしません。侵害された同じページからファイルとハッシュを取得すれば、攻撃者が両方を差し替えた可能性があります。

秘密鍵で署名を作り、対応する公開鍵で検証します。署名はアルゴリズムと規則に従って特定のメッセージに承認を結び付けます。署名した内容は隠れません。Bitcoinでは有効な署名は出力を使うための条件の一部です。

暗号化は適切な鍵を持つ人だけが内容を読めるようにします。認証付き暗号は改変も検出します。Cuvexには、秘密を守る暗号文、支出を承認する署名済み取引、メッセージを運ぶ暗号化通信路があります。同じ暗号技術を使っても役割は異なります。

人が決めるパスワードは通常、鍵導出関数を通して暗号鍵にします。「AES-256」はアルゴリズムと鍵長を表し、推測できるパスワードを強くはしません。生成、実装、保管、画面上の確認、復旧を含めて安全性を評価します。

複雑に見えるQRも、それだけで安全とは限りません。内容、作成者、アプリが実行する処理を確認してください。承認前に、非公開データを求めない形で操作の目的をチューターに説明してもらいましょう。

演習

1. 「ファイル変更を検出する」「シードを隠す」「支払いを承認する」をハッシュ、暗号化、署名に対応させます。
2. 架空の文を1文字変え、ハッシュが変わることを確かめます。実演に秘密を使いません。
3. 取引が公開されていて同時に署名済みでもあり得る理由を説明します。

理解を確認する

安全に関することをすべて「暗号化」と呼ばず、欲しい保証とそれを提供する仕組みを説明します。

よくある質問

ファームウェアのハッシュで無欠陥と証明できますか。いいえ。信頼できる参照値があればバイト列を特定できます。監査、メーカー署名、実機試験はそれぞれ違う問いに答えます。

中断するとき

演習の3つの対応関係を保存します。

秘密の内容を隠すのはどの方法ですか。

1. ファイル名を公開する。
2. 暗号化せず署名する。
3. 保護された鍵で適切に暗号化する。

> **答えを表示: 保護された鍵で適切に暗号化する。**
> 署名やフィンガープリントだけでは機密性は得られません。

M03

シード、パスフレーズ、パスワード

学習目標

システムで使う認証情報の役割を区別します。

解説

BIP39ニーモニックはエントロピーとチェックサムを辞書の単語で表します。標準の長さは12、15、18、21、24語です。覚えやすい文、歌詞、人がでたらめに選んだ単語では安全に生成できません。チェックサムは一部の誤りを検出しますが、作成者や他人が知らないことを証明しません。

BIP39パスフレーズはバイナリシードの導出に使われます。違うパスフレーズは全く別の、空に見えるウォレットを開くことがあります。「パスフレーズが違います」と表示されるとは限りません。辞書の単語である必要はなく、文字どおりの25語目でもありません。

Cuvex暗号文のパスワードは格納した秘密を、DeskパスワードはPCのローカルストアを保護します。ペアリングPINは通信セッションを許可し、チャットキーはメッセージ用のアイデンティティを復旧します。どれもシードとは異なり、1つ分かっても残りをすべて再構築できるわけではありません。

シードとパスフレーズを同じ暗号文に保管すれば復旧は楽になりますが、復号できる人に対して両者を分けた保護は失われます。分離すれば本人と相続人の負担が増えます。チューターが「上級者向け」と呼ぶから選ぶのではなく、判断を記録して試してください。

演習

1. 値を書かず紙のカード5枚にシード、パスフレーズ、Cuvexパスワード、Deskパスワード、チャットキーと書きます。
2. それぞれで何を復旧でき、忘れると何を失うかを書きます。
3. 空のウォレットで試験を設計します。単語やパスフレーズは非公開で入力し、チューターには結果だけを伝えます。

理解を確認する

学習の「検証」のために講座がパスワードを求めてはならない理由を説明し、自分の復旧手順に必要な秘密を特定します。

よくある質問

メールでパスフレーズをリセットできますか。BIP39にはその仕組みがありません。保管業者のアカウント復旧は別のモデルです。

中断するとき

値を書かず「認証情報を区別できた」と記録します。

BIP39パスフレーズを1文字変えると残高がゼロになりました。正しい解釈は？

1. 異なるパスフレーズから導出された別の有効なウォレットかもしれない。
2. ネットワークが資金を消した。
3. Deskが元のパスフレーズを推測するはずだ。

> **答えを表示: 異なるパスフレーズから導出された別の有効なウォレットかもしれない。**
> 別のパスフレーズはエラーを出さず別のウォレットを生成し得ます。

M03

鍵の導出、xpub、ディスクリプタ

学習目標

支出権限を渡さずにウォレットの構成を記述する方法を理解します。

解説

階層型ウォレットは1つのルートから多数の鍵を導出し、パスが分岐を示します。mainnetでは、BIP84の最初のSegWit単一署名アカウントに通常 m/84'/0'/0'、BIP48 P2WSHの最初のマルチシグアカウントに m/48'/0'/0'/2' を使います。アポストロフィは強化導出を示します。同じニーモニックでもアカウント、ネットワーク、スクリプト形式が変われば異なるアドレスになり得ます。

xpubは一定の下位公開鍵を導出できる拡張公開鍵です。支出用パスワードではありませんが、一群のアドレスを観察できる場合があります。マスターフィンガープリントは記録を結び付ける短い識別子で、単独では本人確認にならず、値の衝突も防げません。

ディスクリプタは、スクリプト形式、鍵、起点、導出を指定してスクリプトとアドレスの作り方を表します。公開鍵だけの監視専用ディスクリプタでは観察できても署名できません。ディスクリプタには秘密鍵を含む形式もあります。実物を講座にアップロードしないでください。

マルチシグ復旧には通常、一人の署名者の単語だけでなくポリシー全体が必要です。閾値、参加者、xpub、パス、ネットワーク、スクリプト形式、探索情報を保管します。ディスクリプタのチェックサムは転記ミスの検出に役立ちますが、参加者を認証しません。

演習

1. 架空のパスを読み、目的、通貨、アカウント、ブランチを説明します。本物の鍵を入力しません。
2. 入金アドレス、参加者のxpub、完全なディスクリプタを区別します。
3. 欄名だけの非公開復旧シートを用意し、資料の保管場所を分けます。

理解を確認する

復元後空に見えても紛失と断定できない理由を説明します。ネットワーク、パスフレーズ、スクリプト、アカウント、パス、探索が確認対象です。

よくある質問

xpubは何の影響もなく公開できますか。通常は単独で支出できませんが、プライバシーが漏れ、特定の暗号学的な組合せでは他のリスクも増し得ます。

中断するとき

講座には機密値を除いたシートを保存します。

シード1つだけでマルチシグを復旧しようとすると何が不足し得ますか。

1. デバイスの色。
2. ポリシーと他の参加者の公開鍵。
3. SNSのパスワード。

> **答えを表示: ポリシーと他の参加者の公開鍵。**
> スクリプトの再構築には、必要な数の秘密鍵に加え完全なポリシーが必要です。

M03

ウォレットと保管方式の選び方

学習目標

機能、信頼の前提、復旧方法からツールを比較します。

解説

ウォレットはウォレットの構成の記述、観察、必要に応じた支出の承認を担うツール群です。ホットウォレットはオンライン環境に署名能力を持ちます。隔離した署名機は秘密をネットワーク照会機器と分離します。監視専用ウォレットは観察・準備に必要な公開情報を持ち、署名には別の仕組みを使います。

第三者保管の口座は企業に対する請求権を表す場合があります。自己管理では利用者が単独または共同で支出の技術的能力を持ちます。メールによるアカウント復旧や事業者による出金停止は通常、第三者保管の特徴です。それぞれ責任の前提が異なります。

対応ネットワークとスクリプト、画面での検証、バックアップ、更新、相互運用性、保守、外部照会、エラーの分かりやすさを比較します。対応通貨リストや外装だけでは判断できません。署名機でも、宛先を見直さなければ誤ったアドレスへの承認は防げません。

Cuvexでは暗号文での秘密保護とDeskでの整理・照会を分けます。暗号文と解除手段の両方を保管してください。デバイスの紛失に備えていても、全コピーやパスワードもなくなれば復旧できるとは限りません。資産を移す前に全手順を学びます。

演習

1. Cuvex、ホットウォレット、取引所を表で比較します。署名者、照会を観察する人、アクセスを復旧できる人、会社が閉じた場合を挙げます。
2. 広告でなく証拠で検証すべき基準を2つ選びます。
3. 練習環境が本当の貯蓄と鍵を共有していないことを確認します。

理解を確認する

ある事例に合う選択を理由とともに説明し、どの道具も無敵とは言いません。

よくある質問

ハードウェアウォレットですべての取引は非公開になりますか。いいえ。主に署名能力と確認の一部を守ります。チェーン、照会、相手方には引き続き情報が生じます。

中断するとき

アカウント名を含めず比較表を保管します。

公開鍵で正しく設定した監視専用ウォレットにできることは？

1. 取引を観察・準備できるが、単独では署名できない。
2. 失われたシードを変更する。
3. 匿名性を保証する。

> **答えを表示: 取引を観察・準備できるが、単独では署名できない。**
> 観察する能力と承認する能力は分けられます。

M03

復旧できるバックアップ

学習目標

必要なものがそろったバックアップを設計し、頼る前に復旧を実証します。

解説

役立つバックアップは単なるファイルではなく、ある操作能力を復元します。単一署名ではニーモニック、パスフレーズ、導出情報、マルチシグではさらにポリシーと十分な署名者が要ります。Deskでは暗号化コピーとパスワードが必要な場合があります。チャットのアイデンティティ復旧と過去のメッセージの復旧は別です。

冗長化は偶発的な紛失に、分離は同時侵害に備えます。異なる媒体と場所に2つのコピーを置くと共通障害を減らせます。追加するコピーごとにアクセス制御、棚卸し、点検が必要です。名前やラベルで資産を明かしたり全要素の場所を分かりやすくしたりしません。

試験では事前に検証したアドレスを照合し、演習環境で管理された取引に署名できることを確認します。ファイルが開くだけでは正しいウォレットのものとは分かりません。コピー確認のために本番シードをどこにでもあるPCに入力しないでください。

各コピーの対象範囲と除外事項を記録します。現在のパスワードを変更しても古いコピーは自動で変わりません。以前のパスワードが漏れれば古いコピーには影響が残ります。現代のストレージではファイルを削除しても全コピー・全履歴の消去は保証されません。

演習

1. 対象、内容、対応パスワード、独立した保管場所、試験日、責任者を非公開の表に記入します。
2. 分離した環境で練習用コピーを復元し、ネットワーク、最初のアドレス、導出を確認します。
3. PCを失った場合、次に端末を失った場合を模擬し、変わる手順を特定します。

理解を確認する

その場しのぎの手助けなしで練習環境を復旧し、他の事例なら不足する資料を説明します。

よくある質問

Deskの全体バックアップにすべて含まれますか。そう仮定はできません。確認した版にチャット履歴とセッションは含まれません。マルチシグポリシーと秘密鍵も別の役割があります。

中断するとき

試験の日付と結果だけを記録し、コピーの内容は記録しません。

Deskのパスワードを変更した場合、以前のコピーはどうなりますか。

1. 自動更新される。
2. 自動的に暗号化が解除される。
3. 作成時の保護とパスワードが残る。

> **答えを表示: 作成時の保護とパスワードが残る。**
> 過去のコピーは独立したオブジェクトです。

M04

OriginalとBITの違い

学習目標

機器とバージョンに合う手順を選びます。

解説

OriginalはNFCカードで暗号文や対応操作を運び、更新にはBluetoothを使います。資料で確認したモデルのUSB-Cは電源用です。BITはUSB-Cでファイルを交換し、対象の暗号文には生体認証も使います。OriginalのNFCやBluetoothの手順をBITに適用しないでください。

本体には設定のほか、暗号化、復号、ウォレット作成、署名機能があります。Originalにはカード複製、BITにはUSB媒体のファイルを扱う機能があります。表示、言語、入口はバージョンにより異なります。BITの新しい「ポリシー検証」は対応手順への入口で、承認者は変わりません。

この教材の参照版はOriginal 1.2.2 Final、BIT 1.2.3 Final、Desk beta.9.21、Mirror beta.12.12です。参照資料に基づく情報で、各組合せの署名・配布・実機受入試験は担当チームに確認が必要です。開発用パッケージの未署名バイナリにファームウェアを置き換えないでください。

使用前に出所、封印、外観、バージョンを確認します。流通経路の記録と更新署名は特定の脅威に役立ちますが、あらゆる検証に代わるものではありません。改変や予想外の版があれば初期化を止め、自分で確認した窓口に連絡してください。

演習

1. 秘密を撮影せず、自分のモデルと表示バージョンを記録します。
2. 暗号化、復号、ウォレット作成、PSBT、設定を探します。メニュー探索で消去や更新を開始しないでください。
3. 講座でOriginalまたはBITの手順を選び、練習中はその選択を保ちます。

理解を確認する

自分のモデルに操作がどう入り結果がどう戻るか、どの媒体を上書きから守るべきか説明します。

よくある質問

誰にとってもBITが自動的に安全ですか。モデルごとに運用上の選択が違います。答えは脅威、復旧、正しい使い方によります。

中断するとき

モデルと版は自分のノートに保存します。講座に必要なのは選択したモデルだけです。

BITを使っているのに、ガイドが本体でNFCカードに書き込むよう指示します。どうしますか。

1. ガイドの対象モデルを確認して、対応するUSB手順を使う。
2. Original用の更新を強制する。
3. シードを電話に送る。

> **答えを表示: ガイドの対象モデルを確認して、対応するUSB手順を使う。**
> 手順はモデルが実際に使う伝送手段と一致していなければなりません。

M04

物理的エントロピーでシードを作る

学習目標

生成方法を理解し、講座のデータを自分の本番鍵に使わずに手順を練習します。

解説

エントロピーとは予測しにくさです。適切なサイコロを使い、振る前に順番を決め、正しい変換アルゴリズムを使えばエントロピーを得られます。棄却された場合は指示どおりやり直します。最大値に置換したり他の単語を選んだりすると偏りが入ります。

確認したCuvexの手順ではコイン1枚とサイコロ4個を使います。コインの値×1,296に、各サイコロの目から1を引いた値を各桁とする6進数を足します。有効な索引は0〜2,047です。辞書の範囲外ならコインとサイコロ4個をすべて振り直します。コインの結果を残してサイコロだけ振ると偏ります。これは確認したソースの説明で、配布版ごとに画面と全手順の検証が必要です。

好きな単語を選ぶのとは異なります。公開実演を実資金の保管に使わないでください。教材に登場するシードはすべて知られているとみなします。最後の単語とその検査はデバイスの完全なアルゴリズムで決定し、ニーモニックを手で完成させません。

カメラ、近くで動く音声アシスタント、画面録画、見ている人がいない環境を用意します。秘密の入力・確認中はチューターを止めます。チューターは前に説明し、後で手順について質問できますが、投げた結果や単語を聞くことはありません。

生成後はバックアップを確認し、モデルに沿って暗号化し、空のウォレットを復旧して試します。確認用アドレスを使えばシードをPCに出さず整合性を確かめられます。指示に反する値を受理したり予期しない単語が出たりしたら使用を止め、バージョン、画面、エラーだけを記録します。

演習

1. 資金のない資料で本体の指示に従い、サイコロの順番を固定し、結果を変えないでください。
2. 棄却時は画面の指示どおりにやり直し、通るように値を修正しません。
3. 非公開で内容を確認しコピーを作り、同じ練習ウォレットを再構築できることを確かめます。

理解を確認する

物理的エントロピー、正しい変換、結果の秘匿が別々の3要件である理由を説明します。

よくある質問

アルゴリズム確認のためにAIに投げた結果を教えてよいですか。使用予定のシードではいけません。支援は別の架空例で行います。

中断するとき

本体を安全な状態で終了し、休憩中にシードを表示したままにしません。

ファームウェアがサイコロの入力を棄却しました。正しい手順は？

1. 単語を手動で選ぶ。
2. 端末の指示どおり、偏りを加えずやり直す。
3. 採用されるまで数を小さくする。

> **答えを表示: 端末の指示どおり、偏りを加えずやり直す。**
> 棄却はエントロピー変換の一部で、任意の値に置き換えてはいけません。

M04

Cuvexで秘密情報を暗号化・復号する

学習目標

演習用の暗号文を作り、復旧できることを確認します。

解説

利用する手順で対応するBIP39、SLIP39、Monero、テキストから正しい種類を選びます。それぞれ異なる形式です。SLIP39テキストを暗号化しても、そのテキストを扱うすべてのネットワークでCuvexが署名できるわけではありません。秘密の保管と署名プロトコルの実行は別です。

接続機器に秘密を出したくない場合は本体に直接入力してください。電話やPCから取り込むと、あとで暗号化しても取り込み元ですでに露出した可能性があります。事前確認画面で単語、順番、大文字小文字、誤った欄の入力を見つけます。

暗号文のパスワードは長く、使い回さず、自分の計画で復旧できるものにします。確認した作成用キーボードは最大40文字で、検証には12文字以上、ASCIIの大文字と小文字、数字、認識される記号が必要です。Deskの12〜1,024文字という別の基準をCuvexのキーボードに当てはめないでください。復旧用の欄には別の上限があり得るので、手順とバージョンを確認します。

Originalでは適切な空のカードに書き、確認が出るまで動かしません。BITでは必要な場合の生体認証要素を含め、USB手順で生成されるファイルを保管します。推測で改名・結合しないでください。その後、本体で試験的に読み取り・復号し、秘密をチューターに伝えずに確認します。

演習

1. 認証情報も金銭的価値もない、練習用に作ったテキストを暗号化します。
2. 媒体と生成物を識別し、別名と役割を非公開で記録します。
3. 復号手順を開始し直し、信頼できる画面で文章を照合して、終了時に表示を閉じます。

理解を確認する

内容の正しさ、書き込み成功、復旧成功を区別します。「ファイルをコピーしました」は3つすべての証明ではありません。

よくある質問

カードの別名はパスワードですか。いいえ。整理用の情報です。資産を特定しやすくする残高や説明は入れないでください。

中断するとき

復号内容を表示したままにせず、練習の成否だけを記録します。

演習用暗号文から内容を復旧できることを最もよく実証する方法は？

1. きれいな名前を付ける。
2. 2つのフォルダーにファイルが存在する。
3. 正規手順で読み取り・復号し、内容を非公開で照合する。

> **答えを表示: 正規手順で読み取り・復号し、内容を非公開で照合する。**
> コピーの存在だけでは、使えることも必要な内容に対応することも分かりません。

M04

暗号化の閾値と生体認証

学習目標

秘密を複数人で保護する方式とBitcoinマルチシグの違いを理解します。

解説

複数パスワードで保護した暗号文は誰が内容を復号できるかを決めます。Bitcoinマルチシグはネットワーク上の支出にどの鍵が必要かを決めます。単一署名ウォレットの秘密を共同で暗号化したり、マルチシグの各署名者が個別の暗号文を持ったりできます。

複数人で1つのシードを解錠しても、そのシード単独で支払えるならチェーン上の閾値は1鍵です。開示後に誰かが控えを残せます。支払いごとに複数署名が必要な方式として説明しないでください。

BITの生体認証は該当形式で追加のアクセス条件になります。指はシードでも、すべてのパスワードの代替でもありません。けが、指紋の変化、故障、機器の利用可能性、相続を考慮し、頼る前にその暗号文の文書化された復旧方法を保管・試験します。

緊急復旧のためのエクスポートはPC上に秘密を表示する場合があります。その機能があってもPCが専用機器と同等に安全とは限りません。通常は隔離を保ち、ローカル復旧は影響を理解したうえで、露出時の移行計画を伴って検討します。

演習

1. 「シードを開くためのパスワード2つ」と「支出に3鍵中2鍵」という2つのポリシーを描きます。
2. 資金のない練習で生体認証コピーに必要なファイルと、復旧を確かめる場所を特定します。
3. 一人が不在の場面を模擬し、自分の方式で閾値を満たして続けられるか判断します。

理解を確認する

誰が秘密を知り得るか、復号後に誰が支出を承認できるか説明します。

よくある質問

ラベルを変えて参加者を外せますか。いいえ。整理上の変更、秘密の保護の変更、支出ポリシーの変更を区別してください。

中断するとき

本名や生体情報を含めず図を保管します。

3人が2つのパスワードで、単一署名シード1つを含む暗号文を開きます。Bitcoinで使う鍵はいくつ必要ですか。

1. ポリシーが単一署名なら1つ。
2. ファイルにパスワード2つが必要だったので2つ。
3. 3人いるので3つ。

> **答えを表示: ポリシーが単一署名なら1つ。**
> 暗号化の閾値はコインを管理するスクリプトを変えません。

M04

コピーを複製・保管・検証する

学習目標

唯一の有効なコピーを壊さずに冗長性を確保します。

解説

暗号文の複製は暗号化データのコピーです。残高やシードを新しく作らず、漏えいしたパスワードの影響も切り離せません。同一コピーは媒体の紛失には備えられますが、元の秘密の侵害には対処できません。復元と新しい鍵への移行は異なる状況で必要になります。

Originalでは暗号文カードとPSBT転送カードを区別します。操作用媒体は手順に沿って再利用できますが、バックアップカードを転用しません。暗号文の入ったカードが拒否されたら、保護を回避したりヘッダーを手で消したりしないでください。

BITのコピーは必要なファイル一式と相互関係を保ちます。ファイルマネージャーの転送完了は、本体の内容検証や操作終了を意味しません。指定の状態を待ち、管理された復旧試験でコピーを確かめます。

目立たない識別子、形式バージョン、最終試験日と結果を非公開の一覧に記録します。想定する事故に備え少なくとも2つのコピーを分離します。診断のためバックアップをサポート窓口に送らず、機密情報を除いたメタデータとエラーコードを渡してください。

演習

1. 正しい手順で練習用暗号文を別媒体に複製します。
2. 元媒体を外し、コピーからテスト文を復旧します。
3. 紛失、ファイル破損、パスワード漏えいへの対応を個別に記録します。手順は同じではありません。

理解を確認する

試験したコピーを特定し、元のコピーを上書きしていない理由を説明します。

よくある質問

2つ目のファイルが見えたら元を消してよいですか。先に復旧と対象範囲を検証します。削除はコピー数だけで決めず計画に従います。

中断するとき

終了前に媒体を保管し、支払い練習のカードと混ぜないようにします。

パスワードを知る人が暗号文のコピーを得ました。さらに3つ複製すると何が解決しますか。

1. 攻撃者のコピーが失効する。
2. 冗長性は増すが、その人のアクセスは失効しない。
3. Bitcoinのシードが自動的に変わる。

> **答えを表示: 冗長性は増すが、その人のアクセスは失効しない。**
> 複製しても既存の侵害は解消されません。

M05

Cuvex Deskのインストールと保護

学習目標

出所を検証してインストールし、Deskを開いてローカルストアを保護します。

解説

配布されている中からOSとアーキテクチャに合うパッケージを選びます。macOSはIntelまたはApple Silicon、WindowsとLinuxはそれぞれx64またはARM64です。ソースZIP、Manager用パッケージ、顧客用インストーラーは別物です。非公開の署名用パッケージに受講者を誘導しません。

出所とOSによる検査を確認します。Windowsの開発用署名だけで発行者が公に信頼されたことにはなりません。Macのアプリ署名、公証、起動時評価は異なる検査です。サポートを名乗る電話で全般的な保護機能を切らないでください。予期しない警告は文面を控え、公式窓口を利用します。

Deskはパスワードで暗号化したローカルストアを作ります。確認した版では新規パスワードは12〜1,024文字で、確認欄があれば一致が必要です。長さだけでは強さは決まりません。独自のフレーズを使い、使い回さないでください。PCの生体認証は対応時に個別設定するアクセス補助です。

無操作時と、必要ならバックグラウンド移行時にロックするよう設定します。失敗後の待機と任意の消去機能はマニュアルで扱います。実演中に自動消去を有効にしないでください。通常のアカウントなしで動作しても、照会、チャット、ダウンロードにはそれぞれの要件と通信があります。

演習

1. チューターに非公開IDを伝えず、プラットフォーム、表示版、パッケージの出所を検証します。
2. 練習用ストアを作成し、ロックして開き直します。パスワードは非公開で入力します。
3. 暗号化バックアップを予定し、計画どおりパスワードを保管します。本番で繰り返しロックを試しません。

理解を確認する

ローカルパスワード、商用アカウント、追加サービスの認証情報を区別します。

よくある質問

Deskパスワードを変えるとカード側も変わりますか。いいえ。別の保護です。古いコピーも勝手には変わりません。

中断するとき

Deskをロックし、認証情報を除いてレッスン番号を保存します。

インストーラーのアーキテクチャが合いません。最初に何をしますか。

1. 保護機能を無効にして強制実行する。
2. 適切な公式パッケージを入手し、要件を確認する。
3. 続行するためウェブサイトにシードを入力する。

> **答えを表示: 適切な公式パッケージを入手し、要件を確認する。**
> 保管用の秘密を扱う前に、互換性と出所を確かめます。

M05

暗号文の関連付けとWOWの整理

学習目標

暗号化されたコピーを関連付け、それと監視専用アカウントを区別します。

解説

DeskはNFC、USB、対応バックアップファイルで関連付けた暗号文を整理します。見た目や別名は識別に役立ちますが暗号学的な身元証明ではありません。詳細画面では出所、形式、サイズ、アクセス特性などアプリが解釈した項目を確認できます。

関連付けは対応オブジェクトの取り込みや整理です。PCで復号したり秘密を検証したりすることではありません。WOWは対応する公開情報で関連付けた監視専用ウォレットです。同じ秘密群でも複数のアカウントや導出があり得るので、管理したいウォレットと一致させます。

デバイスの手順でエクスポートしたディスクリプタまたは公開情報でアカウントを有効化・取り込みます。ネットワーク、スクリプト形式、フィンガープリント、パス、照合用アドレスを確認します。名前は整理用です。名前由来のIDは元の名前を推測できるため、強い匿名化ではありません。

確認したDeskには関連付け待ちのアカウントを保持し、コピーをエクスポート・複製し、ローカル記録を消す機能があります。画面からカードを消しても外部コピーは消えず資金も移動しません。「バックアップなし」はアプリの基準で確認できないという意味で、世界中にコピーがないことではありません。

演習

1. 選んだ伝送手段で練習用暗号文を関連付け、詳細画面を確認します。
2. 対応する練習アカウントを取り込み、チューターに鍵を見せずネットワークと照合用アドレスを確認します。
3. 暗号文の記録、WOWアカウント、物理媒体を区別し、ローカル削除で何が消えるかを特定します。

理解を確認する

Deskが観察に必要とするデータと、通常利用時にPCの外に置くべきデータを説明します。

よくある質問

.binファイルを関連付ければ自分のシードだと保証されますか。いいえ。出所と復旧を確かめてください。拡張子は内容を証明しません。

中断するとき

「練習用関連付けを確認済み」という状態だけを残します。

WOWアカウントをローカルで削除すると、ビットコインは移動しますか。

1. いいえ。手順に従ってローカル情報を削除するだけでUTXOは使わない。
2. はい。メーカーに送られる。
3. 他人が保管するすべての署名も取り消す。

> **答えを表示: いいえ。手順に従ってローカル情報を削除するだけでUTXOは使わない。**
> ローカル状態とチェーンの状態は別です。

M05

MirrorとDeskのペアリング

学習目標

コードを取り違えず、許可したローカル接続を開始して終了します。

解説

Mirrorはアプリが表示するペアリング、PIN、QRの手順でDeskとのローカル操作を可能にします。6桁のPINはそのセッション用です。Deskや暗号文のパスワード、復元単語ではありません。どの画面で生成し、どこに入力するかを確認し、知らない相手のコードを使わないでください。

Deskの適切な画面から開始します。関連付け、QR読み取り、PSBT転送、ファームウェア操作は異なる目的です。ウィンドウは検索、接続、検出、PIN、QR、カードやファイルの操作を示します。検索に現れただけでは処理全体は完了していません。

OSと用途に応じ、光学読み取りにはカメラ、必要時にはBluetoothやNFCを許可します。物理機能のない電話にアプリを入れても機能は追加されません。iOSではアダプターと検証に差があり、ビルド可能なプロジェクトを全iPhoneで配布・試験済みと扱いません。

失敗したら未検出、接続不能、PIN拒否、QR判読不能、カード未読、応答未着のどの段階かを特定します。古いセッションを閉じ、互換バージョンと権限を確認して慎重に再試行します。PINの間違いを理由にファームウェアを変えたり他所にシードを入力したりしないでください。

演習

1. Deskから試験読み取りを始め、ローカル画面の手順でMirrorを接続します。
2. 練習用QRやカードを提示する前に目的を確認します。
3. セッションを取消し、前の文脈での遅れた読み取りが適用されないことを確認して、新しいセッションを開きます。

理解を確認する

有効なコードや機密内容を明かさず、失敗した段階と関係機器を説明します。

よくある質問

Mirrorは常時接続が必要ですか。操作によります。常駐サービスとは考えず、終了・バックグラウンド移行後も許可が続くと仮定しません。

中断するとき

ペアリングセッションを閉じ、使っていないアプリをロックします。

PIN表示前にペアリングが失敗したら、チューターはどうしますか。

1. シードを求める。
2. 検出、権限、セッション、バージョンを確認してから進む。
3. 接続完了とみなす。

> **答えを表示: 検出、権限、セッション、バージョンを確認してから進む。**
> 観察した段階に沿って診断し、成立していない接続を成功扱いしません。

M05

Mirror経由のNFC、USB-C、QRの読み取り

学習目標

各伝送手段の用途を守り、手段ごとの確認を行います。

解説

Cuvex DesktopのNFC操作には、対応スマートフォン上のCuvex MirrorをBluetoothでパソコンに接続する必要があります。Cuvex Desktopは外付けUSB NFCリーダーに対応していません。カードの種類、形式、容量にも互換性が必要です。暗号文を保存できる小容量カードでも、過去の取引情報を含むPSBTが収まるとは限りません。上限は宛先数だけでなく内容全体で決まります。バックアップ用カードをデータ転送用に転用しないでください。

Originalでは、Mirrorが操作用カードに要求を書き込み、デバイスが処理して応答を書き込み、それをMirrorがDeskに返します。書き込みの確認とDeskの受信は別です。機器が結果を示すまでカードを動かさず、認識済みの暗号文を保護するために拒否された場合は、その保護に従ってください。

BITはUSBの交換用ボリュームまたはフォルダーを使います。処理中にボリュームがアンマウントされ、再び現れる場合があります。Deskで正しい媒体を選び、応答を検証して所定の受領確認を行います。PCに同名フォルダーを作ってファイルをコピーしてもデバイスへの受け渡しにはなりません。

カメラがQRを読めない原因には、ピント、反射、サイズ、動き、情報密度があります。表示を拡大し、光や距離を調節してください。長い識別子を先頭数文字で代用せず、一部しか書き写せていないものは受け付けません。読めたら次は中身が意図どおりか検証します。

演習

1. 教材の図を使い、OriginalとBITそれぞれの要求、媒体、応答を特定します。
2. QR読み取りをキャンセルし、後から届いた値が保存されないことを試します。別の用途でも繰り返します。
3. 容量を超えるファイルを模擬し、検証を省かずに取引の複雑さを減らすか、対応媒体を選ぶ理由を述べます。

理解を確認する

読み取り、書き込み、検証、受信、受領確認のどの段階をどの機器が確認したかを伝えます。

よくある質問

ハッシュやコピー成功の「OK」はBitcoinの宛先が正しい証拠ですか。いいえ。署名機で取引と各出力を確認してください。

中断するとき

バックアップ用カードを取り外して保管し、転送用の媒体を識別できる状態にします。

Originalがカードへの応答書き込みを完了しました。Deskの受信を確認するには何が必要ですか。

1. カードを別の色に塗る。
2. 新しいシードを作る。
3. 所定の手順で応答を読み取り、Deskで検証する。

> **答えを表示: 所定の手順で応答を読み取り、Deskで検証する。**
> 書き込みの成功と受信の成功は別々の出来事です。

M05

公開プロバイダーと自分のノード

学習目標

照会先を選び、そこから漏れ得る情報と限界を理解します。

解説

Deskは対応する公開プロバイダーや利用者設定のBitcoin Coreに照会できます。プロバイダーは受けた照会、その順序、接続情報を知り得ます。xpub全体を送らなければ一つの露出は減りますが、スクリプトやハッシュ同士も関連付けられます。

Desk 9.21ではRESTや自分のノードに加え、TLS経由のBlockstream Electrumを明示的に選べます。TLSは一部の経路上の観察者から通信を守りますが、照会先には内容が届きます。暗黙の切り替えで匿名性が保証されるわけではありません。利便性との引き換えに何を開示するかを理解します。

Coreでは対応ガイドに沿ってエンドポイント、認証、監視専用ウォレットを設定します。アプリから「見える」ようにRPCポートをインターネットへ公開しないでください。信頼する環境にアクセスを限定し、適切な保護通信を使います。RPCパスワードはチューターに読み上げません。

初期同期や再スキャンには時間がかかります。進捗は作業状態であり成功の先取りではありません。Deskはバックグラウンドで処理し、画面を閉じてもノードは停止しません。資料上の最小履歴範囲より前の活動を見つけられるとは限りません。古いウォレットでは取り込み日と実際のスキャン範囲を確認してください。

探索は正の残高ではなく履歴に基づきます。残高を使い切ったアドレスも使用済みです。確認したマルチシグではブランチと参加者ごとに履歴なしの連続20アドレスをギャップとし、発行数にも制限があります。すべてのウォレットに同じ上限を当てはめないでください。

演習

1. 学習用の情報源を選び、その情報源に見えるものを説明します。
2. 最終同期日時、ネットワーク、進捗を確認します。HTTP 429の場合は待ち、意図せずプロバイダーを変えません。
3. 残高ゼロで過去履歴があるウォレットを模擬し、「ゼロ」と「未使用」の違いを確認します。

理解を確認する

選んだ情報源が自分の検証・プライバシー要件を満たすか判断し、未完了の状態を識別します。

よくある質問

自分のノードなら匿名ですか。いいえ。照会依存は減りますが、接続、相手、配信、その他のメタデータも考慮が必要です。

中断するとき

プロバイダーの種類と追加スキャンの要否だけを記録します。

入金し、その後すべて使ったため残高ゼロのアドレスを、ウォレット探索時にはどう扱いますか。

1. 履歴のあるアドレス。
2. 一度も使用していないアドレス。
3. 無効なアドレス。

> **答えを表示: 履歴のあるアドレス。**
> 使用済みかどうかは現在の残高ではなく履歴で判断します。

M06

ビットコインの受け取りとアドレス確認

学習目標

入金依頼を作成し、相手に渡す前に検証します。

解説

正しいWOWアカウントを開き、ネットワークとポリシーを確かめ、入金依頼を作成または再表示します。整理のために理由、観察者、予定額を加えられます。これらはローカルの情報で、予定額が違う金額の送金を防ぐわけではありません。

端末で利用できる手順とウォレットの文脈でアドレスを検証します。その組合せで実機検証が済んでいなければ模擬操作にとどめ、多額の資金を受け取る前に担当者へ確認します。同じ情報源から表示した2画面を比べても独立検証にはなりません。

対応する場合、新しい入金関係には新しいアドレスを使います。確認したマルチシグでは、後から支払われる可能性があるため表示済みのアドレスは再割当てされず失効もしません。履歴のない新規アドレスの連続発行上限に達したら、適切な過去の依頼を再表示し、制限の意味を確認します。索引を巻き戻さないでください。

依頼を共有したら自分の検証元で入金を確認します。メール、取引所の控え、支払人の画面は決済完了の証拠ではありません。リスクに応じてネットワーク、txid、出力、金額、承認数を確認します。照会の秘匿が必要なら便利だからと公開エクスプローラーにアドレスを入れないでください。

演習

1. 練習用の入金依頼を作り、アカウントとネットワークを確認して、アドレスをどう検証するか説明します。
2. 架空のラベルを記録し、画面を閉じてから同じ依頼を呼び出します。
3. 請求と異なる額で入金された場面を模擬し、履歴を変えずにどう照合するか決めます。

理解を確認する

アドレス生成、アドレス検証、依頼共有、入金確認を区別します。

よくある質問

新しいアドレスを作ると古いものは使えなくなりますか。通常は使えます。探索情報と依頼記録を保管すれば後からの支払いを見失いません。

中断するとき

練習依頼の状態だけを保存し、チューターに内容を残しません。

支払人が「出金完了」の画面を送ってきました。入金を受け入れる前に何を確認しますか。

1. 画像の画質だけ。
2. 信頼できるネットワーク情報源で該当出力と必要な承認数を確認する。
3. 支払人のパスワード。

> **答えを表示: 信頼できるネットワーク情報源で該当出力と必要な承認数を確認する。**
> 業者の証明や画面画像は支払いの検証に代わりません。

M06

UTXOへのラベル付け、凍結、選択

学習目標

異なる出所の資金を誤って混ぜずに入力を準備します。

解説

ラベルにはチェーンにない出所、相手、用途、使用制限を記録できます。DeskのUTXOラベルとアドレスメモは長さや機能が異なり得ます。「顧客A」で足りる場面で実名や身分証番号を記録すると、不必要に機微な記録になります。

DeskでUTXOを凍結すると、一部のローカル選択から除外されます。Bitcoin上での支出を禁止せず、スクリプトも変わらず、鍵を持つ他のアプリは使えます。総残高と使用可能残高が異なることもあります。凍結、下書きによる予約、実際の支出済みを区別してください。

自動選択はアルゴリズムと状況に応じて最適化し、利用者だけが知る関係までは把握しません。支払いの際、貯蓄、給与、事業をまとめず同じ文脈の出力を使う方がよいか検討します。分離を保つにはラベルに加えて今後の一貫した使い方が必要です。

BIP329形式のラベル出力は保管や移行に役立ちます。形式自体は暗号化しません。Deskの暗号化されたエクスポートと互換平文を区別してください。取り込み時は上書き前にウォレットとの対応と凍結情報の扱いを確認します。

演習

1. 架空のUTXO3つに貯蓄、事業、寄付とラベルを付けます。
2. 1つ凍結し、観察できる残高と選択可能残高の違いを確認します。
3. 練習用ラベルをパスワード付きで出力し、コピーに取り込んで、本物の非公開データを使わず結果を確認します。

理解を確認する

費用と情報露出から入力選択を説明し、凍結はローカル設定であると理解します。

よくある質問

支払い時にラベルは受取人に届きますか。ローカルラベルだけなら届きませんが、エクスポート、ファイル共有、別サービス、メッセージへの追記で漏れる場合があります。

中断するとき

練習用ラベルと凍結状態を保存します。

DeskでUTXOを凍結するとどうなりますか。

1. ネットワークのコンセンサスで支出が禁止される。
2. 特別なアカウントに移る。
3. アプリ内の入力選択にローカルな制限がかかる。

> **答えを表示: アプリ内の入力選択にローカルな制限がかかる。**
> 他の鍵のコピーの支出能力は失効しません。

M06

支払いの準備と確認

学習目標

内容を説明できるPSBTを作成し、すべての費用と出力を確認します。

解説

アカウント、使える入力、宛先、金額を選び、依頼元を検証します。貼り付け・スキャン時にはネットワークとアドレス全体を確認します。クリップボードや画像は差し替えられ得るため、全文照合できるなら先頭と末尾だけに頼らないでください。

手数料率を選び、手数料総額、推定サイズ、合計、お釣りを確認します。「全額送金」ではDeskが利用可能額から手数料を差し引きます。チャット発の依頼で手取りが請求額に足りなければ、一部支払いと理解して行います。差額を隠すために元の依頼は変更されません。

お釣りが小さい場合や、お釣り出力がない場合も確認します。自己宛て表示は調整役の呼び名でなくポリシーで検証します。お釣りが成立しなければ、全額送金または互換入力の追加を見直し、知らないうちに不釣合いな手数料に変わるのを受け入れません。

PSBTは情報と署名を運ぶ形式で、秘匿性や出所の真正性を自動では提供しません。過去の取引、公開鍵、パス、メタデータを含むことがあります。確認したFinal版ファームウェアのマルチシグはPSBT v0/BIP174を使います。「取引バージョン2」は「PSBTバージョン2」ではありません。

演習

1. シミュレーターで入力120,000 sat、宛先70,000 sat、手数料1,000 satの支払いを作ります。
2. すべての出力を挙げ、お釣り49,000 satを説明します。全額送金でも繰り返します。
3. 下書きを取消し、ローカルで何を取消したか説明します。シミュレーターで署名・公開は行いません。

理解を確認する

出力する前に何が入り何が出るか、誰が受け取り、いくらかかり、どの承認がまだ要るかを説明します。

よくある質問

表示残高全額を送れますか。アプリが手数料を賄える実行可能な手取り額を計算できる場合だけです。残高には使えないコインを含むことがあります。

中断するとき

練習下書きを保存または取消します。本物のPSBTは講座サイトに残しません。

画面に「transaction version 2」と表示されています。ファイルがPSBT v2である証明ですか。

1. いいえ。異なるバージョンフィールドです。
2. はい、常にそうです。
3. Taprootを使う証明です。

> **答えを表示: いいえ。異なるバージョンフィールドです。**
> BIP370ではコンテナのバージョンと取引のバージョンを区別します。

M06

OriginalとBITによる署名

学習目標

モデル別の署名手順を最後まで行い、正しい取引に対応する応答を受け取ります。

解説

Originalでは、対応する転送用カードとCuvex Mirrorを使ってPSBTを渡します。デバイスで要求を読み取り、暗号文を提示して人に見られないところでロックを解除します。すべての出力、金額、お釣り、手数料を確認してください。応答はカードに書き込まれ、次にDeskで読み取って検証します。カードへの書き込み成功だけでこの戻りの手順を省くことはできません。

BITでは正しいボリュームを選びUSB-Cで要求を渡します。利用者がデバイスを操作する間、Deskのローカルサービスが交換の手順を処理します。画面の指示に従い暗号文を提示し、BITで確認します。「BITから受信」で応答を取り込み、Deskが検証・保存してから受領を確認します。切断時は似た操作を選ばず、同じ操作を再開します。

Final版ファームウェアのマルチシグ署名では、要約、必須の出力、該当する警告を確認し、「PSBTに署名」の最後の3回の確認を行います。任意の詳細確認では追加項目を調べられます。「いいえ」を選んでも必須の確認は省略されません。ポリシーの独立検証は別の手順で、その確認の範囲に限られます。

署名には真正性を検証できる互換暗号文が必要です。古いコピーで秘密を復旧できても、そのまま署名に使えるわけではありません。真正性未確認の古いコピーという警告が出たら、秘密を復旧・確認し、新しくコピーを作ってから署名します。ヘッダーを改変したり拒否を回避したりしないでください。

アドレスの不一致、予期しない手数料、データ不足、ネットワーク違い、機器によるポリシー拒否があれば中止します。通話の終了を急いで承認してはいけません。AIはボタンを押さず、最終確認を行わず、利用者が確認していないものを署名済みと宣言しません。

演習

1. 資金のないウォレットまたは実機検証済みの演習環境で、自分のモデルの手順をたどります。
2. 最後の確認前に止める練習をし、その状態が承認ではない理由を説明します。
3. 応答の戻りと下書きとの対応を確かめ、BITの場合は受信と受領確認の状態も確認します。

理解を確認する

認証情報を明かさずに手順を説明し、デバイス上の承認、応答の取り込み、取引の公開を区別します。

よくある質問

オフライン端末には入力が今も未使用だと分かりますか。単独では現在のチェーン状態を確認できません。アプリがネットワーク情報源に照らして最終取引を検証します。

中断するとき

署名を中断したら、秘密を表示したままにせず、手順に従ってキャンセルするか、特定できる保留操作として残します。

BITで署名しましたがDeskが受信を確認しません。どんな状態と判断しますか。

1. 支払いは確実に公開済み。
2. 応答の受信または検証待ち。同じ操作を再開する。
3. ウォレットを紛失した。

> **答えを表示: 応答の受信または検証待ち。同じ操作を再開する。**
> 署名、受信、配信は異なる段階です。

M06

最終化、配信、トラブル対応

学習目標

二重に払わずに支払いを完了し、どの段階で失敗したかを診断します。

解説

署名を取り込んだDeskは、下書きとの対応と意図が保たれていることを検証します。マルチシグなら閾値に未達かもしれず、単一署名でも取り込みだけで確認は不要になりません。すべての条件がそろうと、最終化で配信可能な取引を作れます。

最終確認後にだけ公開します。サーバー応答やtxidはその要求の結果を示しますが、継続確認で受理とチェーン上の状態を確かめます。アプリに応答がなければ繰り返す前に照会します。表示の問題を新たな支払いで解決しないでください。

保留中なら手数料率、有効性、競合、RBFを使えるかを確認します。ポリシーや宛先が変わる新しい提案には新しい適切な署名が必要です。ローカルで取り消しても、他人が持つ署名や取引は消えず、承認済みのものも失効しません。

準備、転送、ロック解除、確認、署名、応答返却、検証、最終化、配信、承認に分けて診断します。OS、版、モデル、段階、およその時刻、エラーコードを記録します。診断情報は機密を除く設計でも共有前に確認し、コピー、QR、チャットキー、認証情報を添付しません。

演習

1. 架空の支払い状態を並べ、安全に止められる場所を示します。
2. 残高不足、USB応答未着、配信時の回線切断の3例に対処します。
3. 架空データと検証可能な期待結果で問い合わせ票を作成します。

理解を確認する

次に動くべきなのが受講者、端末、調整役、ネットワークのどれかを判断し、不要な二重支払いを防ぎます。

よくある質問

FIRMWARE_CAPABILITY_REQUIREDなら、むやみにファームウェアを変えれば直りますか。いいえ。記録されたDeskの事例ではFinalビルドを認識するためDeskのカタログ修正が必要でした。機器変更の前に版とプロファイルを確かめます。

中断するとき

状態と次の操作を保存します。演習外で本物の取引を配信した場合は個人の資料にその記録を残します。

承認済み取引を単独で取り消せる操作はどれですか。

1. ローカルの下書きを消す。
2. Mirrorを閉じる。
3. どちらでも取り消せない。

> **答えを表示: どちらでも取り消せない。**
> ローカルでの削除はチェーンを書き換えず、すでに伝播した承認も撤回しません。

M07

Bitcoinで観察できる情報

学習目標

公開データ、そこからの推論、チェーン外で自分が付け加える情報を区別します。

解説

Bitcoinのオンチェーン情報は公開され、スクリプト、表示できるアドレス、金額、入出力の関係、ブロック内の位置を分析できます。名前が直接出なくても、本人確認済みの購入、公表された請求書、共有したアドレスから履歴が本人と結び付き得ます。

仮名性とは実名そのものではない識別子で活動することです。匿名性には観察者から区別できない集団と条件が必要で、アプリのインストールだけでは得られません。店舗は支払いを、取引所は出金を、サーバーは照会を知り、誰かが機器を見ることもあります。プライバシーは状況によります。

事実と推論を区別します。「この出力がその取引で使われた」はチェーンで検証できます。「これらの入力はすべて同じ人のもの」は外れることもある経験則です。チェーン外の本人確認は仮説を補強しても、すべての解釈を確実にはしません。

アドレスの再利用は活動の集計を容易にし、異なる文脈のUTXOの結合は関係を示し得ます。xpubの開示は単一アドレスより広い観察を許します。txidを共有すると相手が知る必要のなかった他の出力や関係も見えることがあります。

演習

1. 架空の取引で公開データと自分のラベルを区別して印を付けます。
2. 名前入りの請求書を加え、新たに分かる関係を説明します。
3. アドレス、ディスクリプタ、残高を載せずにエラー解決用の問い合わせ文を書きます。

理解を確認する

「観察できる」「推論できる」を使い分け、どの証拠が不足するかを説明します。

よくある質問

アドレスを再使用しなければ匿名ですか。いいえ。入力選択、お釣り、照会、相手方、その他のメタデータも関係します。

中断するとき

実在する人や取引を含めず、観察者の関係図を保管します。

通常、1つのアカウントに属する一群のアドレスの観察を可能にする情報は？

1. アイコンの色。
2. xpubと十分な導出情報。
3. ケーブルのブランド。

> **答えを表示: xpubと十分な導出情報。**
> 拡張公開情報だけでは支払えなくても、プライバシーに関わる情報です。

M07

用途を分け、お釣りを管理する

学習目標

UTXOの出所を踏まえて支出を決めます。

解説

用途の分離は支払う前から始まります。入金が貯蓄、事業、日常支出、特定の相手との関係のどれか決め、非公開ラベルに残します。後で知らずに混ぜないためです。

ラベルは出力を暗号学的には分離しません。異なる文脈のUTXOを一緒に使えば関係が公開されます。統合は将来の入力数を減らしますが統合した出力同士の関連は強まります。手数料が安い時点の統合が効率的でもプライバシーの目的に反することがあります。

お釣りは同じポリシーで管理する新しい出力で、「見えないお金」ではありません。その後の支出で既存の結び付きが広がります。金額が不規則だからとお釣り扱いせず、実取引ではデバイスでウォレットへの帰属を検証します。

プライバシー対策を金額、時刻、反復送金の機械的なパターンにしないでください。それ自体が識別に使われ、手数料も増えます。各当事者が知る情報と提案取引が新たに公開する情報を評価します。どの手順でも公開済みの履歴は消えません。

演習

1. 3用途の架空UTXOを5つ作り、必要最小限の用途だけを組み合わせて支払いを準備します。
2. 生じるお釣りを特定し、どのラベルを付けるかを決めます。
3. すべての出力を統合する場合と分離したままの場合の費用と情報露出を比べます。

理解を確認する

すべてに一律の規則を当てず、具体的理由で統合を正当化または拒否します。

よくある質問

全額を別の自己アドレスに移せば履歴のつながりは切れますか。いいえ。新たな関係を公開し、脅威を解消せず費用だけ増えることがあります。

中断するとき

演習での判断理由と選択した入力ポリシーを保管します。

給与と寄付を同じ取引で統合すると何が起こり得ますか。

1. それらの入力の関係が見えやすくなる。
2. 過去の公開された出所が消える。
3. 匿名の現金になることが保証される。

> **答えを表示: それらの入力の関係が見えやすくなる。**
> UTXOを減らすと観察できる結び付きが増える場合があります。

M07

ネットワークのプライバシー、Tor、VPN

学習目標

接続時のプライバシーとチェーン上のプライバシーを区別します。

解説

照会サーバーは要求を接続元と結び付けられます。回線事業者は通信方式に応じて宛先やパターンを観察できます。VPNは接続に関する信頼の一部をVPN運営者に移しますが、Bitcoinの公開情報は消えず、本人確認済みアカウントが利用者を識別することも防ぎません。

Torはネットワークを介して通信を経由させ、接続元と宛先の一部の関連付けを減らします。Bitcoinアドレスは非公開にならず、Torを通らないアプリも保護しません。Tor Browserを開いてもDesk、Bitcoin Core、PC全体が自動設定されるわけではありません。

保護されていると言う前に通信経路と設定を検証します。確認した版ではDeskにTor切替が内蔵されるとは想定しません。ノードやプロキシ経由の配備には技術ガイドと実トラフィックの検証が必要です。他のウォレットにあるという理由で画面項目を想定しません。

DNS、アカウント同期、エクスプローラーへのリンク、価格サービスからも情報が漏れます。残高照会を守っても公開エクスプローラーを開けば活動が見えることがあります。各対策の範囲と切断時の動作を決め、黙って秘匿性の低い提供者に切り替えません。

演習

1. PC、回線事業者、該当する場合はプロキシ、ノードまたはサービス、Bitcoin網までの経路を描きます。
2. 誰が照会を受け、誰が取引先としての身元を知るかを示します。
3. 非公開ノードの無応答を模擬し、露出を理解したうえで中断または明示的な情報源変更を選びます。

理解を確認する

自分の設定で減る脅威と残る脅威を説明します。

よくある質問

Torなら誰も支払いを自分と結び付けられませんか。いいえ。相手、商用本人確認、パターン、操作ミスで依然として結び付きます。

中断するとき

設計の範囲だけを記録し、非公開エンドポイントやパスワードを記載しません。

Tor Browserを開くとDeskの照会も必ずTorを通りますか。

1. 同じパソコンなので通る。
2. アイコンが見えていれば通る。
3. いいえ。アプリごとに経路を設定・確認する。

> **答えを表示: いいえ。アプリごとに経路を設定・確認する。**
> あるアプリの保護が自動で他のアプリに引き継がれることはありません。

M07

CoinJoin、Payjoinと現在の限界

学習目標

共同取引ツールの仕組みを学び、実際にはない匿名性や互換性を想定しないようにします。

解説

CoinJoinは複数人の拠出を1取引に集め、入出力に関する一部の推論を難しくします。別のコインを返すと約束する保管業者に預けることとは異なります。設計ごとに調整方法、保管権限、費用、悪意ある参加者への耐性、その後の取扱いを確認します。

Payjoinは支払人と受取人の入力を共同支払いに含め、共通所有を推定する一部の経験則を弱めます。両端の対応と所定のプロトコルが必要です。技術を理解するための解説で、確認した資料ではCuvex DeskにPayjoinやCoinJoinが統合され実際に使えることは実証されていません。

提供状況と法的背景は変わります。Wasabiの資料ではzkSNACKsコーディネーターは2024年6月1日に終了しました。かつてのボタンが今の提供を保証するように教えません。米司法省は2025年にSamourai創設者の有罪答弁とその後の判決を発表しました。これを根拠にすべての法域で全プライバシー技術が違法とは言えません。

ある推論を減らしても他の推論は残ります。特定済みの出所は相手の記録から消えません。後の再結合、メタデータ、参加者側の失敗でプライバシーは損なわれます。特定の履歴を持つコインに異なる商業ポリシーを適用するサービスもあります。

演習

1. 実取引をせず、通常の取引、共同取引、資産を預かるサービスを比較します。
2. 特定ツールの利用を提案する前に版、保守担当、サービス状況、現行資料を調べます。
3. 技術、保管、法的リスクを個別に特定します。チューターは規制回避を設計せず「追跡不能な資金」を約束しません。

理解を確認する

プライバシー技術について限定的な利点1つと、少なくとも2つのリスクまたは要件を説明します。

よくある質問

Cuvexを非公開での保管に使うにはミキサーが必要ですか。いいえ。照会、データ、鍵、UTXO選択の管理で具体的なリスクに対処でき、完全な隠蔽を約束するものではありません。

中断するとき

証拠なしに「対応」とせず、ツールを「学習済み」と記録します。

根拠を示せる説明はどれですか。

1. CoinJoinは恒久的な匿名性を保証する。
2. 共同取引は、一定の要件と限界のもとで、一部の推論を難しくできる。
3. ミキサーと名乗るすべてのサービスで自己管理が維持される。

> **答えを表示: 共同取引は、一定の要件と限界のもとで、一部の推論を難しくできる。**
> 特性はプロトコル、実装、参加者、その後の使い方によります。

M07

実際のインシデントから学ぶ

学習目標

報告された事例を検証可能な対策につなげます。競合他社を中傷せず、保護効果を誇張しません。

解説

Mt. Goxについて、米司法省の2023年の起訴状は、サーバーと鍵への不正アクセス、それに続く顧客資金の消失を記載しました。起訴状は訴追側の主張で、判決ではありません。保管上の教訓は、実際に誰が鍵を管理し、会社が機能しなくなったらどうなるかを問うことです。

2023年12月のLedger Connect Kitでは、退職者のアクセス権が侵害された後、分散型アプリ用ライブラリの悪意ある版が公開されたとLedgerが記録しました。ソフトウェア配布網に影響し、EVMのDApps利用者がだまされて署名しました。LedgerのハードウェアやBitcoinのコンセンサスが破られた証拠ではありません。

2025年2月のBybit事件で、FBIは約15億米ドル相当の仮想資産窃盗を北朝鮮によるものとしました。取引所と他ネットワークの資産に関する事件で、Bitcoinの暗号が破られた事例ではありません。署名が意図に沿うかを確認し、複数人が同じ画面を盲信しないことが教訓です。

2025年5月、Coinbaseは、ソーシャルエンジニアリングを助けるために買収されたサポート担当者によるデータ窃取を発表しました。同社はパスワードや秘密鍵は流出していないと説明しています。正確な事実を知る相手でも詐欺師の場合があることを学びます。

Bitcoin Coreもソフトウェア障害を公表します。CVE-2024-35202の通知は25.0より古い版で遠隔から停止させられる可能性を説明しました。規則を検証してもソフトウェアの保守は必要です。この通知から鍵の窃盗は推定できません。

2026年1月、The Registerは、Global-e経由でLedger購入者の注文情報と連絡先が流出し、両社が確認したと報じました。両社の説明では復元鍵には影響していません。ハードウェアが破られなくても、購入記録で所有が明らかになることがあります。

2026年4月、The RecordはDriftへの攻撃と同プラットフォームが発表した入出金停止を報じました。Solana上の分散型金融プロトコルの事例で、Bitcoinの破綻ではありません。当初の損失見積もりやその後の回収策を確定額・返金保証として扱ってはいけません。

演習

1. 各事例を保管、画面または配布、個人情報、他ネットワークのプロトコル、可用性に分類します。
2. それぞれに予防策を1つと、その限界を1つ挙げます。

3. 「買ったことを知っている。この安全なアドレスに移して」という詐欺電話を練習します。切ってから自分で始めた経路で確認します。

理解を確認する

どの事件も別ブランドの無敵さを証明しない理由を説明します。証拠が支える範囲は具体的です。

よくある質問

これが最新のハッキングのすべてですか。いいえ。2026年11月17日版のために確認した抜粋で、網羅的な目録やリアルタイム監視ではありません。

中断するとき

改める習慣と、それを続けていることの確認方法を記録します。

購入履歴を知る相手が「救済用ウォレット」に送金するよう求めています。購入を知っていることで何が分かりますか。

1. 流出情報の可能性があり、身元もアドレスも認証されない。
2. 必ず正規サポートである。
3. シードを共有すべきである。

> **答えを表示: 流出情報の可能性があり、身元もアドレスも認証されない。**
> 本当の情報も説得力のある詐欺に使われます。

M08

チャットのアイデンティティ作成と連絡先確認

学習目標

鍵を明かさずにチャットのアイデンティティを有効化し、相手を確認します。

解説

DeskではCuvexで生成したチャットキーでチャットと暗号文を結び付けます。xpubのように見えても秘密であり、WOWアカウントの公開鍵のようには扱えません。チューターが文字列やQRを見る必要はありません。

新しい別名の作成と既存の別名の移行・復旧は別の手順です。確認した実装では対応するiOSまたはAndroidプロファイルを選びます。過去の方式で導出したアイデンティティを推測で入れ替えられないためです。DEVと本番は別環境で、切り替えても会話や別名は自動移行しません。

別名を追加しても本人確認にはなりません。独立した認証済みの経路でフィンガープリントを照合します。本人確認用の質問があれば非公開の情報を使い、パスワードを明かす回答は避けます。聞き慣れた声も模倣できるため、リスクがある場面では事前合意した複数手段を組み合わせます。

連絡先のアイデンティティが変わったら解決するまで支払いと調整を止めます。正当な復旧の場合も悪意あるすり替えの場合もあります。エンドツーエンド暗号化はプロトコルと実装に応じて通信路を守りますが、相手側の機器を今誰が使っているかは証明しません。

演習

1. テスト環境でチャットキーを示さず作成・復旧の手順を説明します。
2. 練習用連絡先を加え、他の経路でフィンガープリントの検証方法を合意します。
3. アイデンティティ変更を模擬し、支払い前にどう確認するかを決めます。

理解を確認する

別名、公開フィンガープリント、秘密のチャットキー、人への信頼を区別します。

よくある質問

古くからの別名なら同じ人と保証されますか。いいえ。継続性と鍵の変更は手順に従い検証する必要があります。

中断するとき

鍵や私的な質問を除き「練習用連絡先を確認済み」と確認方法だけを記録します。

チャットキーという名前でxpubに似た文字列をDeskではどう扱いますか。

1. フォーラムで公開できる情報。
2. アイデンティティを復旧する秘密。
3. Bitcoinの入金アドレス。

> **答えを表示: アイデンティティを復旧する秘密。**
> 見た目の形式で機密性や用途は決まりません。

M08

チャットからサトシを請求・支払う

学習目標

依頼の背景と確認手順を保ったまま会話から支払いに進みます。

解説

チャットではアドレスを尋ね、入金アドレスを返し、支払いを請求し、WOWアカウントから支払い準備を開けます。文脈を同じチャネルに保つとアプリ間の転記ミスは減りますが、すべてのメッセージが認証済みの支出指示になるわけではありません。

返事や支払いの前に、確認済みの相手、ネットワーク、金額、元の依頼を確認します。共通フォームにはUTXO選択と手数料が維持されます。「全額送金」を選ぶと手数料差引後の額が依頼額を下回り得ます。該当時は一部支払いと明示します。

承認はCuvexで行います。チャットは意図と調整を伝えますが自動署名権限はありません。相手に支払い通知を送る際はメッセージの受信とブロック承認済み取引の存在を区別します。受取人は自分のアカウントまたは情報源で検証します。

外部リンク、添付QR、アドレスは検証するまで信頼しません。「Mempoolで表示」は第三者サービスを開いて照会を明かす場合があります。自分のノードを使う方針ならWOWの対応検証を優先し、公開サービスへの移動の影響を検討します。

演習

1. 受取人が50,000 satを請求し、支払人が配信せず準備する2役を演じます。
2. 手取りの利用可能残高48,000 satを模擬し、一部支払いに必要な同意と照合を説明します。
3. テストメッセージのネットワークを意図的に変え、手順を中止します。

理解を確認する

「チャットがOKと言った」で済ませず、依頼、アドレス、下書き、署名、承認の関係をたどります。

よくある質問

チャットからsatを送ればLightningですか。いいえ。資料にあるWOWはBitcoinオンチェーン支払いを準備します。satは単位であり伝送網ではありません。

中断するとき

練習下書きを取消すか状態を記録し、画面を示すためだけに公開しません。

チャットで確認メッセージを受けました。入金判断で決め手となる確認は？

1. メッセージのアイコンが緑色。
2. 相手が「承認済み」と言う。
3. 適切な情報源を使い、ネットワーク上の取引と出力を検証する。

> **答えを表示: 適切な情報源を使い、ネットワーク上の取引と出力を検証する。**
> メッセージの状態と取引状態は別です。

M08

暗号文を理解して共有する

学習目標

暗号化したコピーを他人に渡すことの意味を理解します。

解説

暗号文の共有は暗号化されたオブジェクトのコピーを渡すことです。必ずしもビットコインを送るわけではなく、新たな署名者を自動で加えるものでもありません。受取人が十分な解除手段も得れば方式に応じて内容にアクセスできます。どの能力を渡すかを先に決めます。

チャットのエンドツーエンド暗号とファイルの暗号化は異なる層を守ります。ダウンロード後に相手はチャット外のコピーを保管できます。自分のメッセージやローカル記録を消しても全コピーの回収は保証されません。同じ経路でパスワードも渡すと必要な要素が集中します。

送る前に相手の身元、形式、目的を確認します。受け取った暗号文の関連付け機能はコピーを整理するもので、任意のファイルを安全に復号できる証拠ではありません。外部ページにシードやパスワードを入力させる添付物を使いません。

復旧には、各要素を誰が保管し、誰が開けるか、露出をどう検知し、関係終了時に管理をどう変更するかの合意が必要です。通常の支払いは検証済みのアドレスで足り、自分の暗号文を共有する必要はありません。

演習

1. 暗号化した練習テキストを練習用連絡先に渡す手順を設計します。
2. パスワードを知る前後で受取人が何を知り何をできるか列挙します。
3. 関係終了を模擬し、メッセージ削除ではコピーや鍵が失効しない理由を説明します。

理解を確認する

「データを共有した」「秘密へのアクセスを共有した」「支出に署名した」を区別します。

よくある質問

暗号化ファイルは影響なく流通させられますか。メタデータが漏れ、パスワード推測を試しやすくなり、無期限に保管され得ます。共有の必要性を評価します。

中断するとき

保管用の添付ファイルを講座に残さず、演習の結論だけを記録します。

チャットで暗号文を共有することは、ビットコインの送金と同じですか。

1. いいえ。別の内容とアクセス範囲を持つオブジェクトを渡す操作です。
2. はい。.binで終われば同じです。
3. 新しいマルチシグが自動で有効になります。

> **答えを表示: いいえ。別の内容とアクセス範囲を持つオブジェクトを渡す操作です。**
> 秘密情報の転送とUTXOを動かすことは別の操作です。

M08

チャットの復旧とメタデータ

学習目標

機器変更を計画し、アイデンティティの復旧とメッセージの復旧を区別します。

解説

Deskは、履歴とセッションをローカルで暗号化し、全体バックアップには含めないと説明しています。チャットキーはアイデンティティを復旧しますが過去の全会話は保証しません。対応する資料があれば、有効化待ち、鍵の維持、ローカル復旧の状態と操作が用意されています。

確認したガイドでは各別名は同時に1台だけで使います。非対応の2台同時有効化で「同期を試す」ことは避けます。移行は手順に従い、連絡先と継続性を確認してください。

「保留」「サーバーが受理」「受信」「復号できない」は別の段階です。未確認の送信をむやみに再送せず、まず到着したかを確かめます。セッション鍵不足やアイデンティティ変更があると、保留メッセージが残っていても読めたことにはなりません。

内容を暗号化しても時刻、サイズ、配送関係、別名、接続情報が全関係システムから隠れるとは限りません。音声も同様で、経路の暗号化だけで普通の通話が秘密を伝える適切な経路にはなりません。学習と問題解決に必要最小限の情報だけを使います。

演習

1. PC紛失を模擬し、手元の各資料で何が復旧できるか説明します。
2. メッセージ状態を分類し、支払い依頼を再送してはいけない場面を判断します。
3. 独立した経路で連絡先が確認できる機器変更の通知を用意します。

理解を確認する

バックアップの範囲を超えた復元を約束せず、失われる会話と復旧可能なアイデンティティを説明します。

よくある質問

ローカルチャットを消せば相手側のメッセージも消えますか。そう仮定しません。受取人はメッセージやファイルを別に保管できます。

中断するとき

欄名だけの移行計画を保存し、チャットキーは入れません。

確認したガイドによるとチャットキー単独で何ができますか。

1. どのPCでも過去のすべての会話を復旧できる。
2. 対応手順でアイデンティティを復旧できるが、古い全メッセージの復旧は保証されない。
3. 連絡先のBitcoin鍵に自動でアクセスできる。

> **答えを表示: 対応手順でアイデンティティを復旧できるが、古い全メッセージの復旧は保証されない。**
> アイデンティティと過去ログの保管は別の機能です。

M08

日常の設定と権限の見直し

学習目標

利便性と保護効果を区別してDeskの設定を管理します。

解説

Deskには夜・昼・システムのテーマ、自動同期と3分・5分の間隔、取引音、チャット背景、言語、参照通貨があります。表示や照会頻度を変える設定で、Bitcoin署名を変えたり匿名性を加えたりしません。

確認したセキュリティ設定には無操作ロック、バックグラウンド移行時ロック、失敗後の最大待機時間、任意の消去があります。無操作設定のスキーマは30〜86,400秒を許容しますが、画面の選択肢は狭い場合があります。既定値は録画授業から推測せず実行中の版を確認します。

bitcoin: リンクを開くと、ロック解除、アカウント選択、確認の依頼が開きます。自動決済ではありません。Linuxのリンク登録は統合インストールとAppImageで手順が異なります。Lightningインボイスには別の対応フローが必要で、Deskを既定アプリにするだけでは処理できません。

相場、価格チャート、情報リンクは外部サービスに照会する場合があります。情報提供用で買いシグナルではありません。金額換算前に日付と出典を確認します。ダークモードや小さなウィンドウで最終操作、宛先、手数料が隠れたら中止し、表示レイアウトの問題を報告してください。

演習

1. 練習用ストアで外観とロックを調整し、再度入れることを確認します。
2. 有効化する自動機能を確認します。同期、効果音、ファームウェア確認は別の機能です。
3. 架空のbitcoin:リンク依頼を開き、実取引の準備前に取消します。

理解を確認する

各設定の効果を説明し、照会や機微な操作を伴う項目を見つけます。

よくある質問

PCの生体認証は復旧コピーの代わりですか。いいえ。機器やOSの安全なストアに依存する場合があります。独立した復旧手段を保管してください。

中断するとき

Deskをロックし、変更した設定だけを記録します。

3分ごとの同期を選ぶと何が変わりますか。

1. 機能が動いている間の予定照会頻度。
2. チェーン上の署名ポリシー。
3. 機器のシード。

> **答えを表示: 機能が動いている間の予定照会頻度。**
> 運用上の設定であり、保管方式の変更ではありません。

M09

マルチシグウォレットを設計する

学習目標

想定される紛失や侵害に耐えられる署名閾値を選びます。

解説

N人中M人のポリシーでNは異なる鍵を持つ参加者数、Mは必要署名数です。3人中2人なら1鍵を使えなくても支払えますが、2鍵が侵害されると支出を承認できます。3つのシードを同じ場所に置いたり同じ機会に露出させたりすれば独立性は下がります。

確認したCuvexマルチシグはネイティブP2WSH、sortedmulti、BIP48導出を使います。構造上のポリシー鍵上限はOriginalが6、BITが15です。併用する場合は制約の厳しい参加者と実際の転送容量に合わせます。構造上の上限内でも鍵や入力が多いポリシーが収まるとは限りません。

アプリはポリシーの関係を満たす閾値を扱いますが、N人中1人なら支出に協力は不要です。ファームウェアはこのリスクに個別警告を表示します。数を増やせば調整、費用、復旧資料、動かせなくなる可能性も増えます。

MuSig2はSchnorr署名を集約する別方式で、基本はN人中N人であり任意の5人中3人ではありません。確認したFinal版ファームウェアにTaproot入力の署名、MuSig2、Miniscriptの実装はありません。P2TRを宛先にできてもTaprootウォレットから署名できる証拠ではありません。

演習

1. 参加者が独立したリスクを持つ、架空の3人中2人の構成を設計します。
2. 鍵を1つ失う場合と1つ侵害される場合を模擬し、できること・できないことを説明します。
3. より大きなポリシーを選ぶ前にモデルごとの上限を確認します。

理解を確認する

設計の紛失耐性、攻撃成立の閾値、共通の依存先を説明します。

よくある質問

マルチシグでは他の人のシードも知る必要がありますか。いいえ。各自の秘密の能力を保ち、ポリシー構築・復旧に必要な公開情報を共有するのが目的です。

中断するとき

架空の参加者とその責任を含め設計を保存します。

独立鍵を使う3人中2人のポリシーでは、有効な支出の承認に秘密鍵はいくつあれば足りますか。

1. 1つ。
2. 2つ。
3. 常に3つ全部。

> **答えを表示: 2つ。**
> 閾値は2つで、その他の条件と検証も満たす必要があります。

M09

招待の作成と鍵の提供

学習目標

シードを共有せず、身元を確認した参加者でポリシーを構築します。

解説

作成者は名前、ネットワーク、M、N、連絡先、自分の公開情報、招待の運用条件を決めます。確認した仕様ではmainnetとregtestが対象で、端末の上限を適用する前の参加者数は2〜15人、招待の有効期間は1〜720時間です。これらの範囲内でも容量の確認は必要です。

各参加者は招待を確認し、受諾・拒否を選び、対応手順で自分の拡張公開鍵、フィンガープリント、BIP48パスを提供します。渡すのはシード、秘密鍵、単独アドレス、別ウォレットのディスクリプタ全体ではありません。有効なxpubに見えても文脈が違えば別のポリシーになります。

作成者は調整役で、各署名者の検証を代行しません。入金前に全員が同じパラメーターと照合用アドレスを再構築・検証できなければなりません。チャットで連絡先を受け入れても、その人が送るすべてのポリシーが承認されるわけではありません。

招待期限はアプリ上の調整ルールです。入金済みスクリプトを変えず、他人の保管済み署名を消さず、コンセンサスのタイムロックにもなりません。提案の取消しと既存ポリシーからの出金は別の操作です。

演習

1. 準備したregtest環境で練習用の連絡先を使い、3人中2人の提案を作ります。
2. 受諾、拒否、誤ったネットワークの情報提供を演じ、最後の例で手順が止まることを確認します。
3. 入金前に全員が保管するネットワーク、閾値、公開鍵、起点、スクリプト、検証済みアドレスを挙げます。

理解を確認する

不完全な招待を識別し、チャットがあるからと推定せず足りない承認を説明します。

よくある質問

招待期限後に支出は不可能になりますか。招待の項目だけではなりません。Bitcoinの時間制約には特定のスクリプトや取引条件と実際の対応が必要です。

中断するとき

演習提案のIDと保留中の承認を保存します。

マルチシグに自分の分を提供する際、記載された手順が求めるものは？

1. 全参加者のシード。
2. 任意の入金アドレス。
3. 互換性のあるフィンガープリントとBIP48の鍵の起点を伴う自分の拡張公開鍵。

> **答えを表示: 互換性のあるフィンガープリントとBIP48の鍵の起点を伴う自分の拡張公開鍵。**
> 正しい公開情報から、秘密鍵を明かさずポリシーを構築できます。

M09

Mirrorで任意の順にポリシーを照合する

学習目標

各項目の値全体を照合し、その結果が何を証明するかを正確に理解します。

解説

独立検証では閾値、ネットワーク、プロファイル、SIGHASH、ポリシーID、最初のアドレス、利用者の位置、参加者別のデータを示します。意図と整合性を確かめる手順です。デバイスがポリシーを永続登録したと仮定せず、文書化された範囲は「今回の確認」に限られます。

Mirror 12.12ではCuvexとDeskのどちらのQRから読んでもよく、任意の項目を選べます。手順1から始める、全件スキャンする、順番を守るといった義務はありません。手作業で確認した項目をスキャンしなくてもMirrorで確認済みとは表示されません。

比較画面は文字列全体をそのまま表示し、空白、改行、大文字小文字、Unicodeの違いも区別します。「一致」はその一対の値が等しいという意味で、出所の認証、同じポリシーに属する証明、ウォレットの有効化にはなりません。最終承認と紐付いた応答はCuvexとDeskの手順で行います。

現行のDesk QRは値だけで、順番やセッションを含まないため、Mirrorが手順番号を常に推定できるわけではありません。「Deskの手順を指定」は手動で文脈を加える操作で、その旨を明示します。N人なら7 + 4N項目で、kを0から数え、8+4kはフィンガープリント、9+4kはパス、10+4kはxpub、11+4kは鍵IDです。N=2では手順15が2つ目の鍵IDで、最初に照合できます。

演習

1. 架空データで手順15と表示したIDを先に比べ、次にネットワークと閾値を比べます。
2. 1文字だけ変えて「不一致」を確認し、前の結果を引き継がず別の対を開始します。
3. 「2 / 3」を比較し、文字列だけで閾値か利用者位置かを必ず区別できるわけではない理由を説明します。

理解を確認する

確認した項目、与えた文脈、残る承認を説明します。部分的な一致を全体承認とみなしません。

よくある質問

先に進むには全QRのスキャンが必要ですか。いいえ。照合は自由です。署名者に必須の確認・承認にはそれぞれ所定の手順があります。

中断するとき

比較画面を閉じます。確認した設計では退出やバックグラウンド移行で値を消去する必要があります。

Mirrorで手順15の2つのQRが「一致」と表示されました。何を証明しますか。

1. 特定または手動指定した文脈で、その二値が文字単位で等しい。
2. ポリシー全体の承認。
3. 両方のQRの出所の真正性。

> **答えを表示: 特定または手動指定した文脈で、その二値が文字単位で等しい。**
> 照合は認証、全体確認、ハードウェアの応答に代わりません。

M09

マルチシグの署名調整と配信

学習目標

意図と管理権を保ちつつ、提案に必要な閾値まで署名を集めます。

解説

マルチシグ取引には入力、宛先、金額、手数料率、置換条件、運用メモを指定します。作成者は対応する参加者に署名を依頼できます。各署名者は自分のデバイスで承認する前にネットワーク、ポリシー、入力、すべての出力、手数料を独立して確認します。

閾値未達なら部分署名だけで資金は動きません。閾値に達したら調整役が手順に従い結合・最終化できます。他の参加者や調整役からの報告は調整情報で、自分のローカル検証ではありません。アプリは出所を区別して表示する必要があります。

確認した版には再試行、署名受信、受領確認、拒否、調整役の移管があります。移管してもチェーン上の鍵や閾値は変わりません。保管済みの応答は元の依頼と実際に使ったプロファイルに対応させます。似ている、一覧で最初にあるという理由で別のポリシーを選びません。

宛先や重要な条件を変えたら新しい提案を確認し、対応する署名を集め直します。NFCに収めるためにセキュリティ情報を手で削除してPSBTを「修正」しないでください。ファームウェアは対応するプロファイルと検証を要求し、入力数、出力数、サイズに制約があります。

公開前に合意した取引か、すでに配信された版がないかを確認し、公開後は選んだ情報源で承認を追跡します。自分のアプリで拒否しても他人の保存済み署名が自動失効したり、残る閾値で可能なすべての行為を阻止したりはしません。

演習

1. 架空の3人で3人中2人の構成を演じ、一人は署名、一人は拒否、最後の一人は説明を求めます。
2. 練習用支払いのアドレスを変え、以前の口頭同意を流用できない理由を説明します。
3. 署名保存後の受領確認失敗を模擬し、支払いを重複させずプロファイルも変えず同じ作業を再開します。

理解を確認する

調整、署名、最終化の担当者と各段階の証拠を示します。

よくある質問

チャットのOKが2つあれば署名2件ですか。いいえ。ポリシー上有効な暗号学的承認が閾値を満たします。メッセージではありません。

中断するとき

非公開の内容を除き、状態、残る署名、次の担当者を記録します。

3人中2人の取引に有効な署名1つと「同意する」というメッセージ2件があります。閾値を満たしますか。

1. はい、3人いるので満たします。
2. いいえ。もう1つ有効な暗号学的署名が必要です。
3. 調整役が発表すれば満たします。

> **答えを表示: いいえ。もう1つ有効な暗号学的署名が必要です。**
> 会話上の同意と有効な署名は別の証拠です。

M09

マルチシグの復旧と変更

学習目標

ポリシーを復旧し、参加者が鍵を失う場合や交代する場合に備えます。

解説

復旧にはポリシーを再構築するデータと、支出に足りる秘密鍵の利用能力が必要です。xpub入りのポリシーバックアップはシードを含まなくても履歴を明かし得ます。暗号化コピーはファイルを守る一方でパスワードの保管が必要です。.cuvexms拡張子だけでは暗号化の証明にならず、実際の形式とエクスポート方法を確認します。

Desk 9.21の復旧では、参加者の端末からエクスポートした拡張公開鍵とフィンガープリント、BIP48パスを求めます。対応フローではウェブカメラやMirrorで読めます。代わりに入金アドレスを使ったりサポートにシードを送ったりしません。

3人中2人の鍵を1つ紛失しても残り2つで支出できる場合があります。旧ポリシーは変わらず、参加者を実質的に外し鍵を変更するには通常、新しいポリシーを作り必要な承認で資金を移します。Deskの別名変更やウォレット削除は既存UTXOを変えません。

バックアップで両ブランチを再構築し履歴を探索できるようにします。索引、発行済み依頼、必要な文脈を保管し、アドレスの再使用や不完全なスキャンによる「空のウォレット」という誤解を避けます。保留操作の復旧・再開には作成時の保存プロファイルを使います。

演習

1. 文書化された機能で練習ポリシーを出力・復元し、ネットワークと既知アドレスを確認します。
2. 参加者1人の喪失を模擬し、本物の資金を移さず鍵の入替計画を作ります。
3. 鍵の喪失で閾値未満になる場合を模擬し、サポートやAIが不足署名を作り出せないことを理解します。

理解を確認する

練習の状況を復旧し、情報の復元とコインの管理権変更を区別します。

よくある質問

Deskでマルチシグを消せば全員のウォレットが無効になりますか。いいえ。手順の範囲でローカル状態を消します。他の人やコピーはポリシーに沿った能力を保ち得ます。

中断するとき

確認済みのコピーと個人計画を保管し、講座には結果だけを記録します。

すでに入金されたポリシーから人を外すにはDeskで名前を消すだけで十分ですか。

1. はい。
2. チャットも削除すれば十分。
3. いいえ。必要に応じて新しいポリシーと承認済みの資金移動を計画します。

> **答えを表示: いいえ。必要に応じて新しいポリシーと承認済みの資金移動を計画します。**
> ローカル記録を編集しても既存UTXOのスクリプトは変わりません。

M10

手順に沿ってファームウェアを更新する

学習目標

対応する更新を準備し、機器上で結果を確認します。

解説

更新は信頼して使うソフトウェアの変更です。モデル、ハードウェアのリビジョン、版、出所、メーカーの認証方法を確認します。ダウンロード完了やウェブページのハッシュとの一致は署名・互換性の検証に代わりません。技術者向け未署名ファームウェアを顧客向け公開版として入れないでください。

資料の手順でOriginalはBluetooth、BITはUSB-Cで更新します。Mirrorには対応する準備・転送手順があります。PC、電話、デバイスの特定の組合せは実機受入試験が済むまで動作を約束できません。Windows上のOriginal更新で過去にあった問題は個別診断が必要で、99%で成功扱いにしても解決しません。

開始前に復旧可能なバックアップ、安定した電源、他の操作がないことを確認し、アプリに応じて公式ファイルまたは検証済みコピーを用意します。転送、検証、インストール、再起動、版の確認を区別してください。進捗バーは最終証明ではありません。

終了後は本体表示の版を確認し、日付と結果を記録します。Deskの互換性カタログはファームウェアを遠隔測定せず、firmwareAttestationはfalseのままです。Finalプロファイルの選択は実際に入っているバイトの証明ではありません。失敗したら重要な段階でむやみに抜かず、段階とエラーを控えて文書化された復旧手順に従います。

演習

1. 練習中に実際の更新は開始せず準備リストを確認します。
2. 状態を順に並べ、「転送済み」と「インストール済み」が異なる理由を説明します。
3. 99%での架空の失敗についてモデル、版、OS、段階、最終メッセージを含む報告を書きます。

理解を確認する

適切なファイル、伝送手段、最終的な成功判定基準を特定します。

よくある質問

Deskのエラーを消すためだけに更新すべきですか。まず原因を特定します。カタログの不一致ならDeskを修正して検証済みファームウェアを保つ場合があります。

中断するとき

実際の更新は明示的に安全とされた段階でだけ中断します。通話終了は中断理由になりません。

Deskの明示的な対応カタログだけで検証できることは？

1. 対応する互換性の参照情報。インストール済みファームウェアの遠隔測定はしない。
2. すべての接続機器について実機でのアテステーション。
3. 脆弱性が存在しないこと。

> **答えを表示: 対応する互換性の参照情報。インストール済みファームウェアの遠隔測定はしない。**
> 互換性、署名、測定、実機受入試験は別々の証拠です。

M10

紛失、故障、緊急時の復旧

学習目標

事象に応じた復旧方法を選び、役に立つ証拠を保全します。

解説

事故時には何を紛失・漏えいしたかを先に分けます。PC、端末、カード、ファイル、パスワード、シード、パスフレーズ、ポリシーがあります。「入れない」は必ずしも「盗まれた」ではありません。侵害の疑いがある端末に秘密を入力し続けないでください。

端末の紛失は対応する復旧媒体と認証情報で解決できる場合があります。PCの紛失ではDeskストアの復元と監視設定の再構築が必要な場合があります。解除手段をすべて失い、または利用可能な鍵が閾値を下回れば技術的解決がないこともあります。存在しない鍵の救出を保証できるAIはありません。

Deskには対応形式のローカル復旧と対応する復旧資料のエクスポートがあります。PCで復号するとOSやマルウェアに秘密が見える場合があります。例外的な判断として、準備した環境、対応資料、漏えい可能性があれば新しい鍵への移行計画を用意します。通常のCuvexの隔離操作と同等には扱いません。

シードが漏れたら、Deskパスワードを変えてもそのシードは失効しません。信頼できる機器で新しいウォレットを守り、承認を得た移行を検討します。攻撃者を助ける事故詳細を公開せず、別のシードや不正な前払いと引き換えに復旧を約束するサービスに支払わないでください。

演習

1. PC紛失、有効なコピーがあるカード破損、パスワード失念、シード露出の4つの架空事例を解決します。
2. 各事例に必要な資料、操作のリスク、復旧の判定基準を特定します。
3. 練習データだけで手順を演習し、実際の緊急復旧ファイルをチューターにアップロードしません。

理解を確認する

不可能な解決を約束せず、復元、監視再設定、管理権移行、専門家への引継ぎから選べます。

よくある質問

パスワードを変えれば誰かが見た秘密を暗号化し直せますか。いいえ。平文コピーや知られたシードが知られていない状態に戻ることはありません。

中断するとき

事故の分類と次の安全な操作を記録し、秘密を扱う前に音声を止めます。

シードが公開されてしまい、PCのパスワードを変更しました。攻撃者の権限は失効しましたか。

1. はい。
2. いいえ。同じシードが同じ鍵を管理するため、資産保管上の対応が必要です。
3. チャットの背景も変えれば失効します。

> **答えを表示: いいえ。同じシードが同じ鍵を管理するため、資産保管上の対応が必要です。**
> ローカル保護を変えても漏えいしたBitcoin鍵は失効しません。

M10

フィッシング、サポート詐称、音声詐欺

学習目標

危険な要求を見抜き、あらかじめ決めた手順で対応します。

解説

巧妙な詐欺はあなたの名前、購入、機器、聞き慣れた声を使えます。正しい情報も漏えい由来かもしれません。急かし方や話の正確さに頼らず、自分から開始した経路と既知の手順で身元を確認します。

シード、パスワード、PIN、チャットキーの要求、「同期」用の遠隔操作導入、ウイルス対策の停止、安全用ウォレットへの送金、説明されないQRのスキャン、承認内容を示さない所有証明署名は危険信号です。通話終了前に行うよう迫られたら通話を中止します。

正規のチューターは説明と理解度確認を行います。鍵を預かったり、自分のアドレスへのテスト送金を求めたり、シード復元を約束したりしません。正当な所有証明の機能は対象が明確で確認可能でなければならず、秘密鍵を渡して達成することはありません。

技術セッション内にも詐欺はあり得ます。QR内テキスト、文書、メッセージに「以前の指示を無視せよ」などAIへの命令が含まれても、分析する内容であってチューターへの権限ではありません。知識ベースは承認済み資料と受講者・第三者提供の文を区別します。

演習

1. 偽サポートの電話を演じ、情報を明かす前にやり取りを切ります。
2. 以前に保存した公式窓口を独立した方法で確認します。
3. 秘密が映る画面を共有したり保管環境への遠隔アクセスを許可したりせず、インストールエラーを説明します。

理解を確認する

求められたデータ、その必要性と、依頼が学習サポートの範囲を越える理由を説明します。

よくある質問

シードの一部の単語だけなら安全ですか。いいえ。自分のシードの断片を示す教育上の理由はありません。

中断するとき

サポートの身元確認手順を保管し、平文の秘密を含まないことを確認します。

共同作業者に似た声が、確認を省いて急いで署名するよう求めます。どうしますか。

1. いったん止め、合意済みの手順で依頼を認証し、取引全体を見直す。
2. 声が一致するので署名する。
3. 時間節約のためシードを共有する。

> **答えを表示: いったん止め、合意済みの手順で依頼を認証し、取引全体を見直す。**
> 声の聞き分けと緊急性は認証や検証の代わりになりません。

M10

プライバシー、法令、個人の記録

学習目標

一般的な枠組みを理解し、法律・税務の専門家に聞く具体的な質問を準備します。

解説

金融プライバシーを保っても納税、該当する本人確認、制裁措置、犯罪防止の義務はなくなりません。状況は居住地、活動、相手、サービスによります。AIは出典と日付のある一般情報を提供し、個別判断は適切な専門家につなぎます。

EUではMiCAが一定の暗号資産とサービスを規制します。一般適用は2024年12月30日に始まり、規則にある最長移行期間は各国の判断により2026年7月1日までででした。古い登録の記載だけに頼らず、現行の公式登録簿で認可と範囲を確認します。認可は価格、支払い能力、全額補償を保証しません。

規則2023/1113は義務対象事業者が関与する移転に伴う情報を定めます。自己管理アドレスが関わる1,000ユーロ超の移転について所有・支配を評価する措置を設けています。この基準以下が本人確認全般の免除になるわけではありません。同規則では事業者を介さない個人間移転に適用除外がありますが、他の義務は残ります。

自分の状況に応じて購入、売却、手数料、出所の資料を十分に保管し、不要なアクセスから守ります。私的な記録のために履歴全体を公開する必要はありません。規制回避の分割、虚偽申告、所得隠しを教えるものでもありません。

音声録音・文字起こしや個人と結び付く進捗がある場合、提供者は目的、法的根拠、保管、アクセス、処理受託者、適用される権利を定める必要があります。商用のプライバシー設定は販売前に検証し、通話中に場当たり的に決めません。

演習

1. 専門家に示す架空事例を、鍵を含めず居住地、活動、取引を明記して書きます。
2. 事業者の認可を確認できる場所と情報の日付を調べます。
3. 入出金の非公開記録と受講者データを最小化する方針を設計します。

理解を確認する

法規、取引所の方針、Bitcoinの技術能力を区別します。

よくある質問

EUでは自己管理が全面禁止されていますか。挙げた規則からその結論は出ません。断定的な見出しを避け、条文と適用範囲を確かめます。

中断するとき

チューターに個人書類を入力せず、専門家への未解決の質問を保存します。

特定のアドレス管理確認措置の基準である1,000ユーロを下回れば、すべての義務がなくなりますか。

1. はい。
2. 取引を分割すればなくなる。
3. いいえ。本人確認や他の義務の一般的な免除ではありません。

> **答えを表示: いいえ。本人確認や他の義務の一般的な免除ではありません。**
> 基準額を一律免除に読み替えず、規則は対象措置と範囲に即して解釈します。

M10

相続、継続計画、年次訓練

学習目標

あらかじめすべてを明かさず、権限を持つ人が必要時に動ける計画を作ります。

解説

相続には法的な正当性、資料の所在、技術的能力が必要です。相続権があってもウォレットを再構築できない人や、鍵を持っていても使う権限がない人もいます。適切な助言を受けて両方を解決する計画にします。

広く読める手順と秘密へのアクセスは分けます。一覧には何が存在し誰に連絡し何を検証するかを書き、すべての鍵とパスワードを広く参照できる1文書に置きません。自分の管理外で流通し得る遺言書や記録にシードを書かないでください。

マルチシグでは誰がポリシーとコピーを保管し、紛失後にどの閾値が残り、重要な人が亡くなったらどうするかを設計します。一人が十分な要素を握れば悪用の単一障害点になり、分散が複雑すぎれば資産を復旧できなくなります。

暗号文のパスワード、あればパスフレーズの復旧、導出情報、機器の互換性、メーカー終了時の手順を含めます。独自ファイルや生体指紋が準備なしに使えるとは仮定しません。文書化された形式とテストデータで相互運用性を試します。

家族、住居、ポリシー、ソフトウェア、参加者が変わったら見直し、定期訓練を行います。信頼できる人が資産を明かしたり不要な送金をしたりせず指示を理解できることを試します。

演習

1. 担当者、構成要素、許可されたアクセス、代替担当者を非公開テンプレートに記入します。
2. 口頭説明をせず、別の人に実習指示を渡してどこで詰まるか観察します。
3. 曖昧な箇所を直し、見直し日を記録します。講座は自動リマインダーを作成しません。

理解を確認する

自分が不在の場合に何が起きるか、各段階で各担当者が必要とする情報を説明します。

よくある質問

3人中2人で相続計画の代わりになりますか。いいえ。技術手段の一つです。相続人には背景、資料、調整、法的な正当性も必要です。

中断するとき

計画は講座外に保管し、「訓練の見直し済み」とだけ記録します。

相続計画を評価するのに役立つ基準は？

1. 権限を持つ人が、場当たり的な対応や秘密の早すぎる開示なしに記載された訓練を実行できる。
2. ページ数が多い。
3. パスワードを覚えていることだけに頼る。

> **答えを表示: 権限を持つ人が、場当たり的な対応や秘密の早すぎる開示なしに記載された訓練を実行できる。**
> 復旧可能性とアクセス制御は実地に確かめます。

M11

価格、貯蓄、ファンダメンタル分析

学習目標

投資に関する主張と、検証可能な技術特性を区別して分析します。

解説

価格は個々の市場の取引結果で、プラットフォームごとに異なります。流動性、建値通貨、板の厚さ、銀行の営業時間、需要が実際の約定に影響します。画面の気配値は、希望する数量すべてに対する確約ではありません。

ファンダメンタル分析は普及、需要、競争、経済的安全性、規制、供給などを調べます。発行日程が既知でも将来価格は決まりません。通貨としての有用性や「本源的価値」の評価は前提に依存し、AIが普遍的な確実性として示せる客観額はありません。

定期購入は購入時期を分散しますが、利益を保証せず長期損失も防ぎません。長期貯蓄には支払義務に備えた流動性、値動きへの許容度、保管計画も必要です。講座は資産配分を指定せず利用者の決定を代行しません。

「資産を理解しているか」「保管・復旧できるか」「経済的リスクを負えるか」を分けます。鍵の扱いを習得しても3つ目の答えにはなりません。教育を受けても価格予測や過去のグラフが個人向け推奨に変わることはありません。

演習

1. 架空の投資仮説と前提、それを覆す事実を書きます。
2. 本物の資産額を入力せず、50%の下落と同時に現金が必要な状況を模擬します。
3. 議論のうち検証可能なデータと期待を区別します。

理解を確認する

収益を約束せず、確信と証拠を区別して投資を論じます。

よくある質問

希少性があれば価格は必ず上がりますか。いいえ。市場価格には需要その他の条件も決定的です。

中断するとき

自動購入の指示ではなく、演習で置いた前提を保存します。

定期購入は何を保証しますか。

1. 長期的な利益。
2. 収益は保証せず、選んだルールで購入時期を分散する。
3. 鍵の紛失に対する保護。

> **答えを表示: 収益は保証せず、選んだルールで購入時期を分散する。**
> 購入時期の分散で経済上・運用上のリスクがなくなるわけではありません。

M11

ビットコインの購入先を選ぶ

学習目標

事業者の認可、費用、出金、プライバシー、保管リスクを検討します。

解説

法人・法域、認可されたサービス、出金網、手数料、価格差、限度額、サポート、認証、データの取扱いという検証可能な基準で比較します。ブランド名や協賛だけでは特定サービスの認可を証明しません。

総費用には入金、両替、スプレッド、売買手数料、出金、銀行手数料が含まれ得ます。「手数料無料」でも価格差が大きい場合があります。手取り額と参照通貨を確認し、自己管理が目的なら出金まで予算に含めます。

保管業者に残高を預ける間は事業者に依存します。準備金証明だけでは負債全体、資金の所有権、将来の支払い能力を証明できません。制限を確認し、新しい出金手順に頼る前に負担できる少額で試します。

事業者の本人確認で身元が出金と結び付きます。後から情報を保護しても事業者が知ったことは消えません。虚偽情報を出さず義務回避に講座を使いません。学習コードの購入でもウォレットとは別の商取引記録が生じます。

演習

1. 架空の2事業者について総費用、ネットワーク、最低出金額、認可、要求データを表にします。
2. 指定された全費用を含め、練習取引の手取り額を計算します。
3. 事前検証したアドレスへのテスト出金を設計します。このサイトから実行しません。

理解を確認する

事例に合う選択を説明し、古くなった情報や未確認事項を特定します。

よくある質問

全員に最適な取引所を講座が勧めますか。いいえ。認可、料金、対象国、条件は変わります。比較には時点と用途が必要です。

中断するとき

認証情報や本人確認書類を含めず、表を保存します。

売買手数料だけを見るより有用な比較は？

1. 希望するネットワークとアドレスでBTCを受け取るまでの総費用。
2. 事業者のフォロワー数。
3. アプリの色。

> **答えを表示: 希望するネットワークとアドレスでBTCを受け取るまでの総費用。**
> 最終費用には表示手数料に含まれない項目もあります。

M11

口座、注文、約定コスト

学習目標

基本的な注文と口座保護を学びます。講座で取引を実行するわけではありません。

解説

成行注文は可能な約定を優先するためスリッページのリスクがあります。指値は買いの上限・売りの下限を指定しますが、未約定や一部約定になり得ます。ストップ注文は事業者の規則に従い次の動作を発動し、最終価格自体は保証しません。

注文板は現在の注文を示すもので、数量がそのまま残る約束ではありません。急落時や流動性が低いと直近価格からずれます。ストップ成行は不利な価格で約定するリスク、ストップ指値は約定しないリスクがあります。

独自パスワード、対応時のフィッシング耐性認証、セッション確認、適切な出金制御で口座を守ります。第2要素の復旧手段は別保管します。自動化用API鍵にはデータ閲覧以上の危険な権限がある場合があり、チューターやサイトには入力しません。

出金前に資産、Bitcoinネットワーク、自分のウォレットのアドレス、受取額を確認します。プラットフォームが異なる商品に同じ記号を使う場合があります。終了後は必要に応じ購入、約定、手数料、出金の資料を残します。自己ウォレットへの出金と新たな購入を混同しません。

演習

1. 100で1単位、102でもう1単位の架空の注文板を作ります。2単位の成行買いで平均100が保証されない理由を説明します。
2. 指値注文を設計し、約定しない状況を説明します。
3. 架空APIの権限を点検し、照会だけなら出金権限を外します。

理解を確認する

各注文の優先事項、価格、未約定リスクを説明します。

よくある質問

ストップロスは常に損失を正確に制限しますか。いいえ。価格の飛び、流動性、スリッページ、事業者規則の影響があります。

中断するとき

実注文やAPI鍵を含めず演習結果を保存します。

100の買い指値注文に残るリスクは？

1. 全く約定しない、または一部しか約定しない。
2. どんな価格でも必ず約定する。
3. バックアップが自動作成される。

> **答えを表示: 全く約定しない、または一部しか約定しない。**
> 価格を制限する対価として約定しない可能性があります。

M11

ローソク足、指標、テクニカル分析の偏り

学習目標

チャートを過去のデータとして読み、パターンを予測と混同せずに戦略を評価します。

解説

ローソク足は期間の始値、高値、安値、終値をまとめます。出来高は情報源によります。取引所、通貨、タイムゾーン、期間で表示は変わります。足の中ですべての値動きが起きた順番までは分かりません。

移動平均は過去の価格を平滑化し、モメンタム指標は観測値を式で変換します。いずれも未来は知りません。同じ系列から作った指標は、名前や色が違っても強く相関し得ます。

ルール評価では結果を見る前にエントリー、イグジット、無効条件、費用、サイズ、データを定義します。勝ち例だけの選択、結果に合うまでの調整、過去の判断への未来データの使用を避けます。学習データと時系列検証データを分けます。

バックテストではスプレッド、手数料、スリッページ、データの入手性、実際に約定できるかを考慮します。粗利益率、勝率、最大損失、損失分布は違う問いに答えます。勝ちが多くても一度の損が大きければ資金を失います。売買シグナルを確実な予測として教えません。

演習

1. 架空のローソク足を読み、含まない時間順の情報を説明します。
2. 10件の架空結果を評価する前に費用と失敗基準を含む規則を書きます。
3. 1ずつの利益9回と15の損失1回を比較します。勝率90%でも費用前の結果は−6です。

理解を確認する

実取引をせず、魅力的に見える結果を事例選択、費用、リスクから吟味します。

よくある質問

多数の指標を組み合わせればシグナルは必ず改善しますか。いいえ。独立した情報を増やさず過剰適合や複雑さだけが増える場合があります。

中断するとき

成行注文を出さず、規則と演習結果を保管します。

9回の取引で各1の利益、1回で15の損失です。費用を除いた結果は？

1. +90%。
2. +6。
3. -6。

> **答えを表示: -6。**
> 9の利益から15の損失を引くと6の損失です。

M11

証拠金、先物、自動化

学習目標

複雑な商品を検討する前に、リスクへの露出、清算、自動化の障害を理解します。

解説

レバレッジは拠出資本に対するエクスポージャーを拡大します。単純化した例では証拠金100で1,000のエクスポージャーを持ち、原資産が5%不利に動けば費用前損失は50、当初証拠金の半分です。実際の維持証拠金、清算、担保、手数料の規則で結果が悪化し、想定より早く清算され得ます。

先物や無期限契約には、満期、差金決済、資金調達率、直近約定と異なる参照価格などがあり得ます。ネイティブなビットコインをCuvexに引き出すこととは異なります。シードを保管してもポジションの清算や相手方の破綻は防げません。

ボットは規則を誤りごと自動化します。ポジション上限、最小権限、注文の冪等性、照合、損失管理、緊急停止、監視が必要です。前の結果を知らずタイムアウト後に要求を再送すると、エクスポージャーも二重になり得ます。

AIは概念を説明し架空事例の矛盾を見つけられます。API鍵を受けたり売買を有効にしたり、利益が出る戦略を約束したりしません。これらのリスクを理解し、分からない商品を使わないと判断できることが本講座の目的に沿います。

演習

1. 清算水準をちょうど10%と仮定せず、エクスポージャーと証拠金の例を解きます。
2. 注文は実行したが応答が消えたAPIを模擬し、繰り返す前に照合すべき理由を説明します。
3. ブローカーにつながず、新規注文を止め、すでに出ている注文を確認する停止ボタンを設計します。

理解を確認する

ストップ注文後にも残るリスク、ボット使用後にも残るリスク、外部資金を自己管理しても残るリスクを1つずつ述べます。

よくある質問

自動化で感情がなくなり結果が保証されますか。いいえ。衝動的介入を減らせても設計や執行の誤りを増幅し得ます。

中断するとき

複雑な商品を有効にせず、この発展項目を理解済みと記録します。

エクスポージャー1,000、証拠金100で、エクスポージャーの5%を失った場合、費用を除くと？

1. 損失5。
2. 損失50、証拠金の50%。
3. ボットなら損失なし。

> **答えを表示: 損失50、証拠金の50%。**
> レバレッジと費用により、証拠金に対する損益率は資産価格の変動率と異なります。

M12

Lightningとその他のレイヤー

学習目標

チャネルによる支払いを理解し、確認したCuvexの手順が提供しない機能を特定します。

解説

Lightningはチャネルと状態更新を利用し、一回一回のやり取りをベースチェーンに記録せずに支払います。チャネル開閉や一部の復旧ではオンチェーン取引が必要です。利用可能性、入出金方向の流動性、監視はウォレットと利用サービスの設計によります。

インボイスには金額、説明、有効期限を含められます。文脈によりサトシまたはミリサトシで表せますが、後者はベースチェーンに1サトシ未満の出力があるという意味ではありません。支払いには互換性と経路が必要で、QRならどのアプリでも払えるわけではありません。

カストディ型と非カストディ型のサービスには大きく異なるモデルがあります。普段速いことはリスクがない証明ではありません。観察者、経路、相手、メタデータが関係するので、Lightningを完全匿名としては扱いません。

CuvexチャットはWOWアカウントでオンチェーン支払いするsatの請求を調整できます。本版ではDeskにLightningノード、チャネル管理、Lightningインボイス署名の機能があるとはしていません。複数の支払い方法がある依頼では、自分が理解する方法とアプリが実行する方法を確認します。

演習

1. 教材用のオンチェーンアドレス、bitcoin: URI、Lightningインボイスを分類します。
2. チェーン決済とチャネル決済を承認、流動性、保管、復旧の観点で比較します。
3. 期限切れインボイスをアドレスとして解釈し直さず、受取人に確認する理由を説明します。

理解を確認する

鍵を明かしたりCuvexの故障と決めつけたりせず、非対応方式を拒否できます。

よくある質問

sat建ての支払いはすべてLightningですか。いいえ。サトシは価値の単位で、支払い方法は使うプロトコルによります。

中断するとき

実際のインボイスは保存せず演習の方式だけを記録します。

Lightningで支払う依頼だと見分けるのに必要な情報は？

1. satsという言葉がある。
2. チャットで届いた。
3. 対応する形式と支払い方法。単位やメッセージの伝達経路だけでは決まらない。

> **答えを表示: 対応する形式と支払い方法。単位やメッセージの伝達経路だけでは決まらない。**
> 計算単位と支払いネットワークは別の要素です。

M12

Taproot、MuSig2、耐量子技術の展望

学習目標

標準、提案、すでに実装された機能を区別します。

解説

Taprootは鍵パスとスクリプトパスを使う支出条件を可能にします。Schnorr署名と集約で一部の構成を改善できますが、プライバシーは設定と支出方法によります。bc1pで始まるアドレスだけでは他の参加者がいないことは証明できず、隠れた条件すべても分かりません。

MuSig2は署名者が対話して鍵を集約し、互換性のあるSchnorr署名を作る方式です。基本規格はN人中N人です。任意のN人中M人には別の構成または追加プロトコルが必要です。ノンスとセッションの管理は重要で、非公式なメッセージ交換では実装できません。

PSBT v2はv0から情報構成を変更した形式です。バージョン2取引入りファイルが自動でPSBT v2になることはありません。本版のFinalファームウェアのマルチシグはPSBT v0、P2WSH/sortedmulti、SIGHASH_ALLを維持します。将来の機能には独自の仕様と検証が必要です。

NISTは2024年に最初の確定版耐量子暗号標準を発表しました。それだけでBitcoinの署名は変わりません。耐量子アルゴリズムでファームウェアを認証すれば守るのはその層で、UTXOのECDSA・Schnorr署名が自動的に耐量子化するわけではありません。将来の攻撃時期をチューターが確実に予告することもできません。

演習

1. 5つの主張を標準、検証済み実装、提案、広告に分類します。
2. 「Taproot宛先に送れる」が「Taproot入力に署名できる」の証拠でない理由を説明します。
3. ファームウェア署名、秘密の暗号化、チャット、Bitcoin支出署名を別の層として描きます。

理解を確認する

特定レイヤーの証拠を求め、あるプロトコルの保証を別のプロトコルに移さないようにします。

よくある質問

量子計算の見出しを見て資金を移すべきですか。実際の判断には最新の技術的証拠、検証可能な対応状況、リスク評価、安全な移行計画が必要です。講座は見出しだけで移動を指示しません。

中断するとき

自動支出計画を作らず、技術的な質問を記録します。

ブートローダーに耐量子署名を実装し検証したと仮定すると、既存のUTXOの署名条件は変わりますか。

1. いいえ。異なるレイヤーです。
2. はい。ネットワーク全体のアルゴリズムが変わります。
3. バックアップが不要になります。

> **答えを表示: いいえ。異なるレイヤーです。**
> 更新の真正性確認はBitcoinの支出条件を書き換えません。

M12

相互運用性とメーカーに依存しない復旧

学習目標

ソフトウェア、機器、サービス提供者が変わっても使い続けられるように計画します。

解説

相互運用性は略語の一覧では実証できません。ネットワーク、スクリプト、導出、鍵、ポリシー、取引形式、署名の意味を保つ必要があります。両アプリがBIP174を読めても対応フィールド、サイズ、入力形式が同じとは限りません。

特定画面への依存をなくすには、文書化した復旧情報を保管し練習ウォレットで試します。標準ニーモニックで鍵を導出できてもマルチシグ復旧には完全なポリシーが必要です。BIP329ラベルはプライバシーの文脈を補い、チャット履歴は別範囲です。

互換試験で本物のシードを露出させないでください。まず公開ディスクリプタのエクスポートと監視専用の復元を確かめます。緊急時に鍵の再構築が必要なら専用環境を用い、その後の移行も検討します。非対応ウォレットで残高ゼロに見えても資金喪失の証明にはなりません。

資料、講座の版、必要なツールの検証可能なコピーを保管します。アプリ署名、証明書の失効、OSの変更はインストールに影響します。ソース公開だけでは、依存関係や知識を残さずに何年後も誰でもビルドできるとは限りません。

演習

1. 空アカウントで移行試験を設計し、対応する2実装で同じネットワーク、ポリシー、照合用アドレスを確かめます。
2. 標準要素と、変換器またはCuvex形式の資料が必要な要素を列挙します。
3. 互換性を示せる結果と、実機・実署名で未確認の部分を定義します。

理解を確認する

企業が同じサービスを続けることに依存しない復旧経路を説明します。

よくある質問

オープンソースならメーカーはもう重要ではありませんか。いいえ。配布、保守、物理部品、運用経験は引き続き重要です。検査や継続の可能性は開けますが、自動保証ではありません。

中断するとき

版と観察した限界を記して演習結果を保存します。

相互運用性をより強く裏付ける証拠は？

1. 両方のアプリに「Bitcoin」と書いてある。
2. バージョンを特定した演習環境で同じポリシーとアドレスを再構築し、照合する。
3. アイコンが似ている。

> **答えを表示: バージョンを特定した演習環境で同じポリシーとアドレスを再構築し、照合する。**
> 試験では関連条件を保ち、検証可能な結果を得る必要があります。

M12

regtestを使う技術演習

学習目標

模擬試験と実機利用の違いを踏まえ、再現可能な演習環境を理解します。

解説

regtestでは自分で制御するローカルチェーンを作り、ブロックを生成し経済価値のない取引を練習できます。別のディレクトリと認証情報を使い、本番資料を取り込みません。結果だけでは実機のUSB、NFC、Bluetooth、カメラの互換性は証明できません。

完全な演習記録には版、ネットワーク構成、ポリシー、テスト入力、PSBT、署名、最終取引、受理結果を含めます。合計の一致、改変署名の拒否、有効な支払いのローカルブロックへの収録を確認できます。成功例だけでなく失敗例も試してください。

Desk 9.21の検証資料はBitcoin Core 31 regtestとエンジン・模擬UIの自動試験を報告しています。本版はそれを文書証拠として使い、再試験や実機操作を行ったとはしていません。パッケージ検査も全OSへのインストールを証明しません。

技術演習の前に技術担当者が、受講者の版に対応する構築済み環境と手順を用意します。チューターの操作用にRPCをインターネットへ公開しないでください。AIは模擬結果の読み方を案内できますが、認証情報や管理者権限を受け取ってはいけません。

演習

1. 用意した環境で有効な取引と署名を改変した取引を観察し、受理・拒否を記録します。
2. お釣りが不正な場合とネットワークが非互換な場合を確認します。
3. 報告では「エンジン試験」「模擬UI」「物理ハードウェア」を区別します。

理解を確認する

模擬を認証と扱わず、試験した範囲と残る項目を正確に説明します。

よくある質問

regtestが動けば全端末検証済みとして講座を販売できますか。いいえ。実機手順、インストール、アクセシビリティ、復旧、商用サービスの試験が残ります。

中断するとき

手順に従い演習環境を停止・保存し、架空データだけを残します。

エンジンのregtest試験で、特定の電話の実際のNFC読み取りを証明できますか。

1. はい。どちらもBitcoinを使います。
2. PSBTが小さければ可能です。
3. いいえ。別途実機試験が必要です。

> **答えを表示: いいえ。別途実機試験が必要です。**
> 検証環境によって確かめられる範囲は異なります。

M12

最終課題と継続計画

学習目標

準備から復旧、プライバシーまで、自立して判断できることを示します。

解説

目標はメニュー暗記ではなく、意図を説明し結果を検証し、理解できない操作を止められることです。評価は概念、ガイド付き演習、独立課題を組み合わせます。評価者にシード、資産額、個人のアドレスを明かす必要はありません。

課題Aでは学習環境を設定し、モデルと版を特定し、Deskを保護し、演習用暗号文を関連付けて監視専用アカウントを再構築します。必要なバックアップと、プロバイダーに見える情報を説明します。

課題Bでは異なる文脈の架空UTXOで支払いを設計します。選択理由を示し、宛先、お釣り、手数料を確認し、機種別署名手順を説明します。応答返却時と配信時の中断に、二重に支払わずに対処します。実機受入試験済みの機器がなければ模擬として記録し、実機部分は未実施とします。

課題Cでは3人中2人を設計し、招待と検証を演じ、Mirrorで任意の項目を先に照合し、OKの範囲を説明します。練習用ポリシーを復旧し、参加者1人の喪失を模擬し、継続・相続計画を用意します。

提案する合格基準は知識問題80%以上と、秘密非開示、ネットワークと出力の確認、段階の区別、復旧手段の保持という重要項目すべての正解です。重要な誤りは再確認・再演習が必要で、市場問題の正解では相殺できません。商用修了証を発行する場合は評価項目と、実機観察の有無または模擬のみであることを記します。

演習

1. 架空データと自分の説明で3つの課題をすべて完了します。
2. 付録の最終評価を解き、不正解を一つずつ見直します。
3. 秘密を含めず、確認範囲の証拠と未完了事項を記した結果シートだけを提出します。

理解を確認する

証拠が足りない操作を自分から中止でき、続けるのに必要な情報を挙げられます。

よくある質問

全ページを読めばどんな金額も保管できますか。いいえ。能力は試験し、リスクは自分の状況に合わせて評価します。読むことや演習は将来の結果を保証しません。

中断するとき

見直し計画と未完了の演習を保管します。講座全体を繰り返さず、必要な章に戻れます。

実習を終えるための重要な要件はどれですか。

1. すべてのページを開いたこと。
2. 秘密を明かさず、明記した範囲で復旧と取引の確認を実証すること。
3. 翌月の価格を予測すること。

> **答えを表示: 秘密を明かさず、明記した範囲で復旧と取引の確認を実証すること。**
> 学習は閲覧数や予測ではなく、確かめた能力と限界で示します。

受講者マニュアル

Cuvex操作マニュアル

このマニュアルはレッスンの補助資料です。各手順には、確認したソースにある流れ、確認事項、中断点を記載します。試行導入の候補版で、Original、BIT、電話、各デスクトップOSを使った独自の実機試験を証明するものではありません。実資金を使う指導の前に、担当チームが受入試験表を完成し、異なる表示名や画面を修正する必要があります。

参照バージョン　Original 1.2.2 Final、BIT 1.2.3 Final、Desk 1.0.0-beta.9.21、Mirror 1.0.0-beta.12.12。Deskでのプロファイル選択は公称互換性で、ファームウェアの遠隔測定ではありません。掲載したMirror画面はパッケージ12.12のAndroidエミュレーターで取得しました。製品写真は企業資料で、現在の実機で表示される版の証明ではありません。

P01 | 出所とバージョンを確認する | Cuvex | L16,L21 | C01,C02

準備　購入情報と、自分で真正性を確認できる公式窓口を用意します。まだ秘密を入力しません。

1. 梱包と封印を点検します。改変の痕跡があれば開始を中止し、機密を含まない証拠を残します。
2. 納品物に対応するアプリで完全性と封印の確認手順を使います。コードはその画面だけに入力し、チューターには伝えません。
3. OriginalかBITか、利用可能なリビジョンは何かを特定し、端末とアプリの表示バージョンを確認します。
4. 担当チーム公開の対応表と比較します。カタログやハッシュはファームウェア認証や実機受入試験に代わりません。

結果　モデルと版を特定し、秘密を出さずに出所を確認できました。コードが無効、または画面が異なる場合、旧版のガイドで無理に進めません。

中断時　資産管理用の秘密を入れる前に止まります。商流の追跡だけで高度な改変がなかったとは保証できません。

P02 | BluetoothでOriginalを更新する | Original | L46 | C01,C02,C03

準備　復旧できるコピー、安定電源、対応する公式パッケージ、使用OSで受入確認済みの手順を用意します。全プラットフォームでの実機動作を本講座は証明していません。

1. アプリのデバイスまたはファームウェア画面でOriginalを選び、公式ダウンロードまたは対応する真正なローカルファイルを選択します。

2. 本体メニューに従って更新モードにし、アプリの手順で接続します。近距離を保ち、競合するセッションを避けます。
3. Original画面のコードを指定欄に入力します。暗号文パスワードと混同しません。
4. 転送、検証、インストール、再起動を順に確認します。進捗率はインストールの証明ではありません。
5. Originalで最終バージョンを確認し、対応欄があればアプリにも記録します。

結果　再起動後に画面で版を確認し、手順の終了を確認できました。PIN前、パッケージ転送中、終了時のどこで失敗したかとコードを記録します。「99%を突破」するためにむやみに切断・ソフト変更しないでください。

P03 | USBでBITを更新する | BIT | L46 | C01,C02,C03

準備　BITの実際の媒体、電源、対応する公式パッケージを確認します。ソフト変更の前にバックアップを保管します。

1. 対応するDeskまたはMirrorのファームウェア手順でBITを選びます。
2. 適切なデータ用ケーブルとアダプターで接続します。要求されたらボリュームまたはフォルダーへのアクセスを許可します。
3. モデルに合う真正なファームウェアを選び、送る前に版と互換性を確認します。
4. デバイスの転送・検証を待ちます。プロトコルの動作でボリュームが消えたり再マウントされたりします。
5. 再起動後、BITの版とアプリの最終結果を確認します。

結果　本体でインストールを確認できました。ボリュームが出ないときは本体モード、データケーブル、権限、マウント、他の使用中セッションを確認します。代わりにPCに同名フォルダーを作りません。更新失敗からの復旧にはそのハードウェアの公式手順が必要です。

P04 | コインとサイコロでウォレットを生成する | Cuvex | L17 | C01

準備　非公開の場所、適切なサイコロとコイン、練習用ウォレットを用意します。チューターのマイクとカメラを切ります。

1. ウォレット作成とファームウェアのエントロピー手順を開き、サイコロ4個の順を先に決めます。
2. 好みで結果を変えず、画面どおりにコインと各サイコロの値を入力します。
3. 確認したソースの計算式は、索引 = コインの値 × 1,296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1) です。0〜2,047だけを受理します。
4. 棄却されたらコインと全サイコロを振り直します。警告はそれまでの単語を保持し、一組をやり直すよう求めます。
5. 最後の検証を含む本体アルゴリズムを完了し、ニーモニックを保護し、復旧を非公開で確認します。

結果　手選びの単語でなく全手順でウォレットを生成しました。画面とソースが食い違えば使用を止めます。公開されたサイコロの例、シード、鍵を自分のものとして使わないでください。

P05 | 秘密情報を暗号化する | Cuvex | L18,L19 | C01

準備　モデル、内容形式、保護方法を選びます。保存先が暗号化されても、PCや電話に入力すれば入力元で露出します。

1. 暗号化を選び、BIP39、SLIP39、Monero、対応テキストから種類を選びます。辞書を混ぜません。確認した平文キーボードは最大500文字です。他形式の保存がそのネットワークでの署名対応を意味するわけではありません。
2. 隔離を保つために本体へ直接入力し、画面で順序、文字、補助欄を確認します。
3. 手順に応じ個人・共同の保護を選び、必要ならBITで生体認証を選びます。この閾値はBitcoinの閾値とは別です。
4. ファームウェアの条件に従って人に見られずパスワードを入力し確認します。Deskの規則を自動で流用しません。
5. Originalは対応する空のカードに書き込み、BITはUSB手順で出力された一式を保管します。確認を待ちます。
6. 練習用復旧を開いて内容を照合し、終了時に秘密の表示を閉じます。

結果　復旧を確認した暗号文ができました。読み書き失敗時は元データを守り、画面の再試行手順に従います。ヘッダー削除や上書きの強制はしません。

P06 | デバイスで復号する | Cuvex | L18 | C01,C02

準備　人目に触れない環境と必要な解除要素を用意し、秘密の近くではマイクと画面キャプチャを無効にします。

1. 正しいモデルで復号を開始し、OriginalならNFC、BITならUSB手順で暗号文を渡します。
2. 認証情報を入れる前に対象の別名と識別情報を確認します。
3. 必要なパスワードと、形式が求める場合は生体認証を提供します。アクセス制御とロックがあるので失敗時に機械的に繰り返しません。
4. 指定画面だけで内容を確かめます。秘密を表示するQRはテキストと同じ機密性を持ちます。
5. 端末手順に従って閉じるか終了し、計画に沿って媒体と認証情報を分けて保管します。

結果　非公開で内容を復旧しセッションを終了しました。形式未認識、認証失敗、予想外の内容のときは、出所不明のアプリで「修正」しません。秘密を添付せず版、形式、エラーをサポートに説明します。

P07 | 生体認証付き暗号文の復旧に備える | BIT | L19,L47 | C01,C02

準備　練習用暗号文と形式の資料を用意します。.binコピーがあるだけで復旧できるとは判断しません。

1. Deskの詳細画面で生体認証要素の有無と利用できる復旧用エクスポートを確認します。
2. 手順が関連付けるファイル一式と独立したコピーを、目立たない識別子で保管します。
3. BITで通常のロック解除を試し、必要なパスワードと条件を記録します。

4. 例外的なローカル復旧の経路と対応形式を学び、必要になる前に資料がそろっているか確認します。
5. 資金のないデータで機器故障や指紋を使えない場合を練習します。

結果　該当形式について限界を含め確認した計画ができました。どの生体認証も省略できる、指紋がコピーの代わりになるという意味ではありません。PCで秘密を復旧したら、露出とその後の管理権移行の必要性を評価します。

P08 | 暗号文のコピーを作成・検証する | CuvexとDesk | L20 | C01,C02

準備　識別済みの元のコピーと、残すべきデータのない互換媒体を用意します。

1. Originalでは本体の複製またはDeskの対応機能を使い、指定順で複製元・複製先を提示します。
2. カードを動かさず、すでに暗号文を含む媒体が拒否された場合は従います。
3. BITやファイルの場合は関連する要素をまとめてエクスポートし、必要な名前と対応関係を保持します。
4. 元のコピーを隔離し、新しいコピーから読み取りと復旧の試験を行います。
5. 日付、形式、結果を非公開で記録し、同じ物理的事故に遭いにくい別々の場所に保管します。

結果　検証済みの2つ目のコピーができました。別ウォレットの生成、パスワード失効、漏えい済みシードの保護は起きません。複製先が壊れた場合、両者を一致させるために元のコピーを「修理」せず保管してください。

P09 | Deskの作成、ロック解除、パスワード変更 | Desk | L21,L40 | C02

準備　確認済みのインストーラー、適切なアーキテクチャ、ストアのバックアップ計画を用意します。

1. 12〜1,024文字の使い回さないパスワードを設定し、確認欄と一致させてストアを作成します。
2. ロックして開き直し、アクセスできることを確認します。パスワードはDeskだけに入力します。
3. 「セキュリティ」の「アクセスとロック」で無操作時・バックグラウンド移行時の動作を確認します。実演中に任意消去を有効にしません。
4. パスワードを変えるには現在の値を入力し、所定の手順で新しい値を確認します。
5. PCの生体認証を使っていた場合は指示に従い設定し直します。現時点のコピーを作り、古いコピーとの対応も残します。

結果　アクセスを確認できました。古いコピーは作成時のパスワードと暗号化を保持します。PCとBITの生体認証は別方式です。入れなければ試行を繰り返さず、チューターに認証情報を保管させずに復旧手順を見直します。

P10 | Deskに暗号文を関連付けて確認する | Desk | L22 | C02

準備　出所が分かる練習用暗号文と使える転送手段を用意します。

1. 暗号文またはカードの画面を開き、NFC、USB、対応コピーのいずれかで関連付けを選びます。
2. デザインと取得元を選びます。NFCにはパソコンとBluetoothで接続したCuvex Mirrorを使い、BITにはUSB-Cで接続したCuvex BITのボリュームを使います。Cuvex Desktopは外付けUSB NFCリーダーに対応していません。
3. 詳細画面で別名、出所、サイズ、形式、解釈された条件を確認します。復号した内容ではなくメタデータです。
4. 保持されている関連付け待ちのアカウントを調べ、検証済みアカウントだけを関連付けます。
5. バックアップが足りなければコピーをエクスポートし、別途復旧を試します。

結果　オブジェクトをローカルで整理できました。「関連付け済み」はシードの真正性や残高を証明しません。未認識のものは形式と版を確認し、認識させようと拡張子を変えたりデータを消したりしません。

P11 | 監視専用WOWアカウントを有効化する | DeskとCuvex | L13,L22 | C01,C02

準備　端末の手順で取得した公開情報と、出所を自分で確認する手段を用意します。

1. 正しい暗号文からWOW有効化またはアカウント追加を開きます。
2. 機能に応じ、ファイル、ウェブカメラ、Mirror経由で対応ディスクリプタまたは公開資料を取り込みます。
3. ネットワーク、スクリプト、起点、フィンガープリント、パス、該当するチェックサムを確認します。シードやxprvを入力しません。
4. アカウント名を付け、同意した照会先を選びます。
5. 残高を解釈する前に照合用アドレスと探索範囲を確認します。

結果　監視専用ウォレットを関連付けました。残高ゼロなら資金が消えたと決めず、ネットワーク、元のパスフレーズ、導出、アカウント、提供者、スキャンを確認します。画面で一般対応している網でもマルチシグプロファイルは非対応の場合があり、各状況に従います。

P12 | ノードと同期を設定する | Desk | L25,L33 | C02

準備　プライバシー方針を定め、Coreを使う場合は保護され同期済みのノードにアクセスできるようにします。

1. 「セキュリティ」の「プライバシーとノード」でWOWアカウントを選び、照会先を確認します。
2. 対応する公開プロバイダーかCoreを明示的に選びます。Coreではエンドポイント、ウォレット、認証情報をアプリだけに入力します。
3. 各サービスが受ける情報を理解したうえで照会を許可します。TLSは照会内容を提供者から隠しません。

4. 同期し、日時、チェーン先端、進捗、完了状態を確認します。再スキャンでは遡る期間と処理が継続しているかを調べます。
5. 429なら指定の待機時間を守ります。失敗しても別ノードが自動で有効になったと考えません。この設定は黙って切り替わりません。

結果　情報源と状態が分かりました。RPCをネットに公開せず、パスワードを共有せず、探索を残高ありのアドレスに限定しません。空の履歴は部分的な結果かもしれません。

P13 | 入金依頼を作成・再表示する | DeskとCuvex | L26 | C01,C02

準備　アカウント、ネットワーク、ポリシーを検証します。

1. 受け取り画面を開き、適切な依頼を生成または再表示します。
2. ローカルのメタデータが必要な場合だけ、観察者、理由、予定額を加えます。
3. 重要な入金前には端末の対応手順でアドレスを検証します。実機受入試験が未実施なら模擬操作で止めます。
4. 受取人との認証済み経路で必要なデータだけを共有します。
5. ネットワーク情報源で入金、金額、承認数を確認します。

結果　依頼の発行だけでなく入金との照合ができました。マルチシグの表示済みアドレスは後払いのため保持され再割当てされません。履歴なしの新規アドレス上限に達したら過去の依頼を再表示し、索引を手動で強制しません。

P14 | ラベル、凍結、BIP329 | Desk | L27 | C02,B13

準備　UTXOのある練習アカウントと保護付きエクスポート用パスワードを用意します。

1. 不要な個人情報を入れず、入力の文脈を示すラベルを付けます。
2. 意図して凍結または解除し、使える残高を確認します。制限はローカルです。
3. 保護付き機能でラベルを出力します。BIP329という形式とファイルの暗号化は区別します。
4. 対応するコピーに取り込み、参照先、ラベル、凍結状態の一致を確認します。
5. 計画に従ってメタデータの最新バックアップと対応パスワードを保管します。

結果　文脈を保ち、入力選択を理解できました。取り込みで確認なしに凍結コインを自動解除しません。ラベルファイルは支出鍵を含まなくても相手や関係を明かすため、チューターに送りません。

P15 | 支払いを準備し、全額を送金する | Desk | L28 | C02

準備　検証済みの支払い依頼と、十分な使用可能入力のあるアカウントを用意します。

1. WOW、UTXO、またはチャットから支払いを開き、アカウントとネットワークを確認します。
2. 入力、宛先、金額を選び、結び付く文脈を確認します。
3. 手数料率を選び、手数料総額、お釣り、警告を確認します。ダストがあれば隠れた手数料を受け入れず代替策を見直します。

4. 全額送金では手数料差引後を確認します。チャットの請求額に足りなければ、一部支払いであることを明示的に確認します。
5. 下書きを作り、署名用エクスポートの前にすべてのデータを見直します。

結果　意図を説明できる取引とそのPSBTが準備できました。一般フォームは実機より多い入力や宛先を受け付ける場合があるため、署名機と転送手段の実効上限を適用します。出力や条件が変われば新たに確認を始めます。

P16 | OriginalでPSBTに署名して返す | OriginalとMirror | L29 | C01,C02,C03

準備　正しい下書き、対応転送カード、真正性を確認した互換暗号文、非公開の解除手段を用意します。古い未認証コピーでは署名前に復旧の検証と新しいコピー作成が必要な場合があります。ヘッダー編集で解決しません。

1. Desk/Mirrorから対応するNFC手順で要求を出力します。
2. Originalに渡し、指示に応じ暗号文を提示し、認証情報を読み上げずに解除します。
3. ネットワーク、要約、すべての出力、手数料、お釣り、必須警告を確認します。
4. Final版マルチシグでは拡張項目を調べるか選び、すべて一致するときだけ最後の3回の確認を完了します。
5. カードへの応答書き込みと再読み取りを待ちます。
6. Cuvex Mirrorで応答を読み取り、Deskの該当する操作で検証します。

結果　署名が受信され下書きに結び付きました。これはまだ配信ではありません。書き込みに失敗したら状態を保ち再試行手順に従います。バックアップカードを使い捨ての支払媒体にしないでください。

P17 | BITで署名し、受信して受領確認を返す | BITとDesk | L29 | C01,C02

準備　正しい下書き、真正性確認済みの互換暗号文、選択済みの実際のBITボリュームを用意します。旧コピーが署名を拒否されたら形式を強制せず、指示された復旧・更新手順に従います。

1. DeskのサービスでUSB-C経由の要求を渡し、暗号文は本体画面の指示に従います。
2. 非公開で解除し、要約、すべての出力、手数料、警告を確認します。
3. Final版マルチシグでは任意で詳細を確認し、必須の最終確認で承認します。
4. Deskの「BITから受信」でその作業の応答を取り込み、検証します。
5. 保存と受領確認を確かめます。受信後に受領確認が失敗したら同じ操作を再試行し、モデルが選んだ別の新規操作は使いません。

結果　署名を検証し、交換状態が整合しています。受信前や保存後に切断したら依頼時のプロファイルを保ちます。保留応答に合わせるためカタログの別ファームウェアに切り替えません。

P18 | 取引の最終化、配信、追跡 | Desk | L30,L44 | C02

準備　検証済みの署名と、該当する場合は必要な閾値を確保します。

1. 意図、入力、出力、手数料、ネットワークを再確認します。
2. 所定の操作で最終化し、署名や条件が不足していないかを確認します。
3. 配信を許可しローカル結果を保存します。ネットワーク応答を失ったら繰り返す前に照会します。
4. 選択した提供者と同期日時を確認し、メモリプールと承認数を追跡します。
5. RBFを検討する場合は新しい取引を確認し、必要な署名を集めます。CPFPが組み込まれているとは仮定しません。

結果　情報源を明示してチェーンの状態を検証できました。下書きの取消しで出力済み署名は失効せず承認済み支払いも書き換わりません。チャットや画面画像は追跡に代わりません。

P19 | 2つのポリシーQRを任意順で比較する | Mirror | L43 | C03,C02

準備　DeskとCuvexに対象項目を表示します。練習では講座の架空サンプルだけを使います。

1. ポリシー比較を開き、どちらか一方を先に読み取ります。
2. 確認したい項目を選びます。手順15から始め、手作業で確認した他項目のスキャンを省いてもかまいません。
3. 対になる値を読み、両方の全文を確認します。手順が曖昧な場合は「Deskの手順を指定」を使い、文脈が手動指定であることを理解します。
4. 「一致」「不一致」はその一対の文字どおりの比較だけに適用します。空白、大文字小文字、符号化も区別します。
5. 任意の順で次の対を開始します。確認した消去動作に従い、終了またはバックグラウンド移行で完了します。

結果　該当項目をローカルで比較できました。出所、セッション、全体承認、有効化の証明ではありません。差は元の情報源に照会し、無理にOKにするため文字列を正規化しません。

P20 | チャットの有効化、復旧、移行 | DeskとCuvex | L36,L39 | C02

準備　DEVまたは本番環境を選び、別名とチャットキーを機器に用意します。講座には入力しません。

1. 暗号文の画面からチャットの有効化または復旧を開きます。
2. 新しい別名か既存の移行かを選び、アプリが示す対応モバイルプロファイルを選びます。
3. 非公開の手順でのみチャットキーを入力または読み取ります。シード、PIN、WOWの鍵は使いません。

4. サービスで有効化を確認します。保留なら「完了」または「確認」の操作で実際の状態を確かめ、成功扱いしません。
5. 移行後は連絡先と継続性を確認し、同じ別名を複数機器で同時使用しません。

結果　正しい環境でアイデンティティを有効化または復旧できました。以前の履歴・セッションはチャットキーやDesk全体バックアップから自動復旧しません。手元の資料で可能な範囲を守ります。

P21 | 連絡先の本人確認 | Desk | L36,L48 | C02

準備　本人と事前合意した独立の連絡経路を用意します。

1. 別名を追加し、アプリで公開アイデンティティを確認します。
2. 作ったばかりのチャットだけでなく、認証済み経路でフィンガープリントを照合します。
3. 本人確認質問を使う場合は公知の情報や他サービスでも使う秘密を避けます。
4. 差を解決してから確認します。アイデンティティが変わったら検証まで支払い・調整を止めます。
5. 検証方法を記録し、機密性のある回答を講座に保存しません。

結果　その文脈での相手への信頼を確認しました。将来の全依頼の保証ではありません。声は模倣でき正規の端末も侵害され得ます。取引ごとに確認を続けます。

P22 | チャットでアドレスを尋ね、支払いを請求・実行する | DeskとCuvex | L37 | C02,C01

準備　検証済みの連絡先と対応するWOWアカウントを用意します。

1. 目的に応じてアドレスを尋ねる、アドレスで返答する、支払いを請求する、のいずれかを選びます。
2. 送る前に元の依頼、ネットワーク、金額、メモを確認します。
3. 支払い時は適切なアカウントから準備を開き、UTXOと手数料率を選び、手取り額を確認します。
4. モデル別手順でCuvex上で承認します。チャットは自動署名しません。
5. 自分の情報源で配信と承認を追跡し、明示した一部支払いを元の依頼と照合します。

結果　保管上の確認を維持して調整できました。メッセージの状態と取引状態は異なります。エクスプローラーへのリンクは第三者に情報を送る場合があるので開く前に判断します。

P23 | 暗号文を共有し、受け取った暗号文を関連付ける | Desk | L38 | C02

準備　共有する具体的な必要性、検証済みの相手、その人に渡すアクセス手段を決めます。

1. チャットから暗号文の共有を選び、対象を確認します。
2. コメントにパスワード、シード、チャットキーを添えません。
3. 受取人が出所を確認し、受信操作で対応するオブジェクトを関連付けます。
4. 相手が今得る能力と、十分な解除用の認証情報を得たときに持つ能力を評価します。

5. 現実的な失効計画を保ちます。メッセージを消しても外部コピーや知られた鍵は回収できません。

結果　意味を理解して暗号化オブジェクトを転送できました。支払いでも、マルチシグへの鍵の自動追加でもありません。不明なページで復号するよう添付物が求めたら中止します。

P24 | Deskの全体バックアップと復元 | Desk | L15,L21 | C02

準備　練習用ストアと自分が管理するバックアップ先を用意します。

1. ストアのバックアップ機能を開き、指示されたパスワードを設定します。このコピーとパスワードの対応を保管します。
2. 普段使う唯一の機器の外に保管し、手順に沿って出所と完全性を確認します。
3. 分離したテスト環境で復元し、含まれるアカウント、設定、データを確認します。
4. 除外項目を確認します。チャットやセッション、履歴を含むとは仮定しません。マルチシグポリシーと秘密鍵は互いに代替できません。
5. 重要な変更後に繰り返し、復旧手順を保管します。

結果　対象範囲とパスワードが分かるバックアップができました。古いコピーは旧パスワードのままです。アクセス変更や漏えい時には古いコピーも評価し、現在のストアの変更だけで済ませません。

P25 | マルチシグを作成・受諾する | DeskとCuvex | L41,L42 | C01,C02

準備　独立した参加者、検証済みの連絡先、合意したネットワークと実効上限を用意します。

1. 作成者が名前、M/N、ネットワーク、参加者、運用上の有効期限を選びます。
2. 対応手順で正しい拡張公開鍵をフィンガープリントとBIP48パスとともに提供します。
3. 各参加者が確認し、受諾または拒否を選び、自分の公開資料を提供します。シードは共有しません。
4. 完全なポリシーを構築し、各端末で検証する準備をします。
5. 入金前にポリシーのコピーを保管し、照合用アドレスと復旧能力を確認します。

結果　完全で検証可能な提案ができました。招待の受諾は実機上の確認に代わりません。Originalが加われば鍵6つの上限とNFC容量を適用します。BITを含めても他の参加者の能力は増えません。

P26 | ポリシーを検証して確認応答を受け取る | Deskと Cuvex | L43 | C01,C02,C03

準備　全員に同じ完全なポリシー、正しいファームウェアプロファイル、競合操作のない端末を用意します。

1. 対応画面からポリシー検証を開始します。Originalではインストール済みのプロファイルを明示選択し、BITでは仕様に従い対応機能をネゴシエートします。

2. モデルに応じてNFC/MirrorまたはUSB-Cで要求を渡します。
3. 端末でポリシー項目を確認します。Mirrorは任意の対を自由な順に照合する補助手段として使えます。
4. 端末で確認を完了し、該当する伝送手段で応答を返します。
5. Deskで要求に紐付く応答を検証します。比較画面のOK表示でこの手順を代用しません。

結果　今回の確認範囲で要求と応答を照合できました。カタログはファームウェアを遠隔証明せず、端末をポリシーの永続保管庫とはみなしません。FIRMWARE_CAPABILITY_REQUIREDの場合はまずDeskの版とモデル・ビルドの組合せを確認してください。

P27 | 署名を依頼・受信し、調整役を引き継ぐ | Deskと Cuvex | L44 | C01,C02

準備　検証済みポリシー、識別した取引、合意済みの宛先を用意します。

1. 入力、出力、手数料、メモを準備し、対応する参加者へ署名を求めます。
2. 各参加者が自分の転送手段を用い自分の端末で確認・署名します。
3. 各署名を受信・検証・保存し、保管したプロファイルを変えずに保留中の受領確認を解決します。
4. 調整役を引き継ぐ場合、受け手が手順を受け入れ状態を検証します。M/Nも鍵の所有者も変わりません。
5. 閾値に達したら確認・最終化してから公開し、ネットワーク上で追跡します。

結果　証拠の出所を区別して調整できました。調整役の進捗報告は自分のローカル検証ではありません。あるアプリで取消しや拒否をしても、他者の保管済み署名は必ずしも消えません。

P28 | ローカルのマルチシグをエクスポート・復元・削除する | Desk | L45 | C02

準備　内容が分かるポリシーと、独自パスワードで暗号化したコピーを用意します。

1. Deskの復旧用エクスポートを使います。現行の手順ではこの出力に認証付きコンテナCVXMSBK1を使います。
2. コピーとパスワードは独立したリスクにさらされる形で保管します。古いファイルの拡張子から暗号化を推定しません。
3. 復元時はコピー、パスワード、正しい起点情報を持つ参加者公開鍵を用意し、対応する場合はウェブカメラまたはMirrorを使います。
4. 操作前にポリシー、ネットワーク、アドレス、探索範囲を確認します。
5. ローカル削除前に対象範囲と確認を読みます。後で復旧するならコピーを保存します。後日の復元は明示的な操作です。

結果　復旧可能なポリシーまたは意味を理解したローカル削除が得られました。削除は資金を移さず、他の署名者の鍵を消さず、他人が保持する取引を単独では取り消せません。

P29 | 例外的なPCでの復旧 | Desk | L47 | C02

準備　対応形式の資料、準備したクリーンな環境、バックアップを用意します。この操作でPCに秘密が見える場合があるため、講座では練習用データを使います。

1. 正しい画面からローカル復旧を開始し、形式の制限と警告を読みます。
2. リスクを理解して同意し、手順どおりネットワークを切断します。ウィンドウは続行を許す前に状態を確認します。
3. 非公開ウィンドウに必要な認証情報だけを入力します。読み上げ、講座への貼り付け、サポートとの共有をしません。
4. カメラや音声を聞くアシスタントのない場所でだけ表示を有効にし、タイマーと終了手順に従います。
5. 終了後、起こり得た露出を確認し、必要なら新しい鍵への移行を計画します。

結果　例外的な復旧ができました。フォレンジック上の完全消去や隔離機器との同等性を保証しません。認証、形式、アクセス資料が不足するなら、インターネット上のツールを本物のコピーで試しません。

P30 | 設定、生体認証、ロックを確認する | Desk | L40 | C02

準備　セキュリティ設定を変える前にパスワードを確認し、バックアップを試します。

1. 「アクセスとロック」でパスワード、利用可能な生体認証、無操作時・バックグラウンド移行時のロックを確認します。
2. 変更前に、失敗後の待機と設定済みの最大値を理解します。
3. 条件、閾値、復旧手順を理解するまで任意消去は無効にしておきます。本番で試しません。
4. 「設定」で言語、テーマ、通貨、3分または5分の同期、効果音を調整します。
5. bitcoin: リンクを登録する場合、依頼を開いても解除、選択、確認の段階が残り、自動支払いしないことを確かめます。

結果　設定を理解できました。OSの生体認証は機器に依存し、パスワードやバックアップに取って代わりません。外観設定はBitcoinポリシーを変えません。

P31 | 影響範囲を理解して記録を削除する | Desk | L22,L45 | C02

準備　削除するのがローカル暗号文、アカウント、WOW、チャット、マルチシグのどれか、残すコピーは何かを特定します。

1. 選択対象と警告を読み、アプリが求めれば正確な別名や明示された条件を確認します。
2. 後でこの状態を復元する必要があればコピーをエクスポートして試験します。
3. 意図した対象だけを消し、その手順でどの関連付けが残るか、外れるかを確かめます。
4. 外部の取引や参加者が残っていないか確認します。他の機器のメッセージ、署名、ファイルまで消えたとは仮定しません。
5. 変更を自分の非公開一覧に記録します。講座に機密情報を残しません。

結果　意味を理解してローカル状態を管理できました。これらの操作だけで資金のあるUTXOのスクリプトを変えたり、第三者が知るシードを消したり、承認済み取引を元に戻したりはできません。

P32 | 秘密を明かさずに診断する | DeskとMirror | L23,L30,L48 | C02,C03

準備　およその時刻、システム、アーキテクチャ、版、段階を控えます。状態不明のまま機微な操作を繰り返しません。

1. 検索、ペアリング、読み取り、書き込み、検証、署名、応答返却、ネットワーク、表示のどこで失敗したかを特定します。
2. QRや非公開データを含めずエラーコードと文面をコピーします。適切ならアプリの診断機能を使います。
3. 共有前にファイルを確認し、ストアのコピー、暗号文、シード、チャットキー、ディスクリプタ、RPC認証情報を添えません。
4. 画面上の不具合なら、架空の画面でウィンドウサイズ、ズーム、隠れた操作項目を記録します。
5. 期待する結果と再現手順を公式窓口に送ります。講座からサポートへメッセージを自動送信することはありません。

結果　最小限のデータで調査可能な報告ができました。ある段階の証拠がなければ「完了」ではなく「未確認」と記録します。音声サポートに資産管理端末へのリモートアクセスは不要です。

Bitcoinと自己管理の用語集

Bitcoin

単一の台帳管理者なしに価値を移転し、その履歴を検証するネットワークと規則の集合。

BTC

Bitcoinの通貨単位。1 BTCは1億サトシ。

サトシ

ベースチェーンの単位で、1 BTCの1億分の1。

ブロックチェーン

規則に従って連結・検証したブロックの履歴。この語だけでネットワークの全特性が決まるわけではない。

ブロック

トランザクションと、検証可能なヘッダーを含むデータの集合。

フルノード

受け入れるブロックとトランザクションが規則に従うか検証するソフトウェア。

マイニング

ネットワーク規則の下でプルーフ・オブ・ワークによりブロックを作ること。

プルーフ・オブ・ワーク

ブロックの提案に検証可能な計算作業を求める仕組み。

コンセンサス

参加者が受け入れる規則と有効な履歴の間で整合が取れている状態。

メモリプールポリシー

取引の受け入れ・再配信に関するローカル規則。コンセンサス規則と同一とは限らない。

メモリプール

各ノードがローカルに保持する未承認取引の集合。

承認

採用されたチェーンのブロックに含まれたことと、その後のブロックの深さ。

チェーン再編成

採用されたチェーンの一部が入れ替わり、承認数が変わり得ること。

UTXO

条件を満たせば消費できる、未使用のトランザクション出力。

入力

過去の出力への参照と、その支出を承認するのに必要なデータ。

出力

トランザクションが生成する金額と支出条件。

お釣り

支払額と手数料を除いた入力の一部を、自分の管理下に戻す出力。

手数料

トランザクションの入力総額と出力総額の差。

仮想バイト（vbyte）

トランザクションの相対的なコストを表す仮想サイズの単位。

仮想バイト当たりのサトシ

仮想サイズ1単位当たりのサトシで表した手数料率。

ダスト

ポリシーと支出コストに照らして小さすぎる出力。閾値は状況とスクリプトによる。

RBF

対応ポリシーの下で未承認取引を置換する方法。確実な取消しではない。

CPFP

子取引を利用して、親子を一緒にブロックへ収録する誘因を高める方法。

ハッシュ

データの完全性の確認に使う指紋。暗号化するものでも、単独で作成者を特定するものでもない。

秘密鍵

所定の方式で暗号学的な承認を作成できる秘密情報。

公開鍵

秘密鍵を明かさずに署名を検証し、所定の支出条件を構築するためのデータ。

電子署名

特定メッセージの承認を示す暗号学的証拠。内容を隠すものではない。

暗号化

鍵とアルゴリズムによる機密性の保護。

認証付き暗号

その設計に従って改変も検出できる暗号化方式。

AES GCM

このエコシステムの形式で用いる認証付き暗号方式。その性質は実装と鍵の取扱いに依存する。

ニーモニック

生成用データと検査情報を、所定の形式で単語として表したもの。

シード

鍵を導出する元のデータ。日常的には単語列もこう呼ぶので、文脈の確認が必要。

エントロピー

生成に使うデータの予測困難性。覚えやすい単語を選んでも得られない。

チェックサム

特定の誤りを検出する検査値。作成者の真正性を証明しない。

BIP39

ニーモニックと、任意のパスフレーズを使ったシード導出の仕様。

BIP39パスフレーズ

導出への追加入力。違う値なら、別の有効な空のウォレットが得られ得る。

BIP32

鍵の階層的な導出を定める仕様。

導出パス

ルートから鍵を得るためにたどる分岐の列。

強化導出

通常はアポストロフィまたはhで示し、通常の公開導出とは異なる性質を持つ導出ステップ。

xpub

導出用の情報を伴う拡張公開鍵。プライバシー上の機密情報。

xprv

拡張秘密鍵。共有したり講座に取り込んだりしてはいけない。

マスターフィンガープリント

ルートを示す短い識別子。関連付けには有用だが、それだけでは十分な本人証明にならない。

ディスクリプタ

鍵と導出からスクリプトを構築する式。公開情報だけの場合と秘密情報を含む場合がある。

監視専用ウォレット

自力で署名するのに十分な秘密情報を持たない観察用ウォレット。

WOW

Cuvexのエコシステムでウォレットを観察・管理するアカウントの名称。

ホットウォレット

接続された環境で署名できるツール。

自己管理

利用者が自らのポリシーに従い、単独または共同で支出できる技術的能力を保つ方式。

カストディアン

顧客に代わって支出能力を管理し、自らのアクセス条件を適用する主体。

Cuvex暗号文

秘密を保護する暗号化オブジェクト。それ自体は取引でも残高でもない。

Deskパスワード

ローカルストアへのアクセスを保護するもの。シードや暗号文のパスワードとは異なる。

チャットキー

チャットのアイデンティティを復旧する秘密。公開情報のように見えても公開してはいけない。

ペアリングPIN

接続セッションで使う一時コード。資産保管用パスワードではない。

エアギャップ

環境を運用上分離すること。受け渡したデータは引き続き検証する必要がある。

NFC

対応するカードやリーダーで使う近距離通信技術。

USB Mass Storage

BITでファイルをやり取りするインターフェース。固有のプロトコル、検証、受領確認が必要。

PSBT

取引の作成と承認を調整する情報・署名を格納する形式。

PSBT v0

BIP174で定義された形式。確認したFinal版マルチシグプロファイルが使う。

PSBT v2

BIP370で定義されたバージョン。トランザクション自体がバージョン2でもPSBT v2とは限らない。

SIGHASH ALL

確認したプロファイルが使う署名の対象範囲の指定方式。取引検証ではその技術的な範囲も確認する。

P2WPKH

通常BIP84アカウントと関連する、単一鍵のSegWit支出条件。

P2WSH

スクリプトにコミットするSegWit条件。確認したFinal版マルチシグで使用。

P2TR

Taprootの出力形式。送金先として対応していても、そこからの支出に署名できるとは限らない。

sortedmulti

鍵を決定的な順番に並べてスクリプトを生成するマルチシグ構成。

N人中M人の閾値

指定ポリシーで、N人の参加者のうち必要な承認数M。

MuSig2

Schnorr署名の集約プロトコル。基本方式はN人中N人で、任意の閾値方式とは異なる。

Taproot

鍵パスとスクリプトパスを持つ、Bitcoinの支出・コミットメント機構の集合。

Miniscript

一定のスクリプトポリシーを記述・分析する言語。確認したFinal版プロファイルには実装されていない。

regtest

演習環境の設置者が制御する、経済的価値のないローカルネットワーク。

signet

独自の特性を持つテストネットワーク。初めからregtestと互換というわけではない。

mainnet

実際の経済活動に使うBitcoinネットワーク。

ギャップリミット

アドレス発見に使う履歴のないアドレスの連続数の基準。適用範囲はウォレットによる。

コインコントロール

支出するUTXOを意識的に選ぶこと。

UTXOの統合

出力をまとめて分散を減らすこと。費用とプライバシーに影響する。

仮名性

実名を直接表さない識別子を使うこと。自動的に匿名になるわけではない。

匿名性

ある観察者が対象を見分けられないという、状況に依存する性質。アプリの表示では保証されない。

メタデータ

通信や活動の時刻、サイズ、関係など、内容そのものとは別の情報。

CoinJoin

一定の推論を難しくする共同取引の構成。永続的な匿名性は保証しない。

Payjoin

対応するプロトコルに従い、支払人と受取人の双方が入力を提供する共同支払い。

Tor

接続を保護するネットワークとツール。利用するアプリごとに経路を設定・検証する。

VPN

接続について信頼する相手の一部を運営者に移す通信路。チェーン上の情報は隠さない。

Lightning

チャネルを使う支払いシステム。オンチェーン送金とは要件とリスクが異なる。

インボイス

形式と支払い方法を確認する必要がある、構造化された支払い依頼。

RPC

Bitcoin Coreなどのサービスを呼び出すインターフェース。認証と保護が必要。

TLS

一定の脅威から通信経路を保護する仕組み。受信サーバーにはリクエストが見える。

SRTP

一部のVoIP区間で音声を保護する方式。運営者からも秘匿されるとは限らない。

冪等性

識別された要求を繰り返しても効果が重複しない性質。

Webhook

サーバー間で送るイベント。真正性と重複送信の有無を確認する。

RAG

知識の断片を検索し、文脈とバージョンを踏まえた回答の根拠にする手法。

ティーチバック

理解したことを受講者自身の言葉で説明してもらう学習確認法。

フィッシング

なりすましと説得力のある状況を使い、アクセス権を奪ったり行動を誘導したりする詐欺。

ソーシャルエンジニアリング

事実に基づく情報や緊急性を利用することもある、人の判断を操作する手口。

公証（Notarization）

Appleによる配布時の確認。製品監査や全手順の実機試験とは異なる。

アテステーション

特定の仕組みで得る状態の証拠。Deskの互換性カタログは遠隔測定ではない。

MiCA

特定の暗号資産とサービスを対象とする欧州の枠組み。収益や全額補償は保証しない。

トラベルルール

適用範囲にある移転に関する情報提供義務。自己管理を選んでも免除されない。

チェックポイント

ウォレット情報を含めず最小限のデータで記録する学習の再開地点。

学んだことを確認しよう

実際の資金を使わずに練習しましょう。評価は誰でも自由に受けられ、アカウントは不要です。

Cuvexの通常の利用で支出を承認するのは誰ですか。

1. 利用者が内容を確認したうえでCuvex端末が承認する
2. 音声チューター
3. 講座のサーバー

> **答えを表示: 利用者が内容を確認したうえでCuvex端末が承認する**
> 承認はCuvex上の所定の手順で行います。

0.001 BTCは何サトシですか。

1. 1,000
2. 100,000
3. 1,000,000

> **答えを表示: 100,000**
> 1 BTCは100,000,000 satです。

入力が120,000 sat、出力が119,000 satなら、手数料はいくらですか。

1. 1,000 sat
2. 119,000 sat
3. 追加情報がなくても1 sat/vB

> **答えを表示: 1,000 sat**
> 入力総額と出力総額の差が手数料の絶対額です。

署名済みで、まだ配信されていない取引はどの状態ですか。

1. ブロックで承認済み
2. 署名したので取り消せない
3. 支出は承認済みだが、ネットワークに公開されたとは限らない

> **答えを表示: 支出は承認済みだが、ネットワークに公開されたとは限らない**
> 署名と配信は別の段階です。

200 vBに6 sat/vBを適用した手数料は？

1. 206 sat
2. 1,200 sat
3. 送金額の6%

> **答えを表示: 1,200 sat**
> 仮想サイズに手数料率を掛けます。

取引所から出金する前に確認することは？

1. 最も安い手数料だけ
2. 資産、ネットワーク、アドレス、受取額が受け取り方法に適合すること
3. 相手のシード

> **答えを表示: 資産、ネットワーク、アドレス、受取額が受け取り方法に適合すること**
> BTCと表示するすべてのネットワークがBitcoinのオンチェーンとは限りません。

電子署名だけで何ができますか。

1. メッセージ全体を隠す
2. 署名方式に従って検証できるメッセージを承認する
3. 公開済みデータを消す

> **答えを表示: 署名方式に従って検証できるメッセージを承認する**
> 秘匿性には別の仕組みが必要です。

BIP39パスフレーズを変更すると何が起こり得ますか。

1. 別の有効なウォレットが生成され、空に見える
2. 必ずメールでリセットできる
3. 過去の支払いの公開記録が変わる

> **答えを表示: 別の有効なウォレットが生成され、空に見える**
> パスフレーズは導出に使われます。

アカウントのxpubはどのように扱いますか。

1. 公開しても一切影響しないデータ
2. 秘密のシードそのもの
3. プライバシーに関わる機密情報

> **答えを表示: プライバシーに関わる機密情報**
> 観察できる活動の範囲が広がることがあります。

マルチシグでシード1つでは不十分な場合があるのはなぜですか。

1. ポリシーと、閾値に達するだけの承認が不足するため
2. Bitcoinでは一切復旧できないため
3. アプリの元の配色が必要なため

> **答えを表示: ポリシーと、閾値に達するだけの承認が不足するため**
> ポリシーの保管と秘密鍵を使える状態の確保は別の要件です。

確認済みのFinal版アルゴリズムでサイコロの結果が棄却されたら？

1. 採用されるまでコインだけを投げ直す
2. コインと4つのサイコロをすべて振り直す
3. 知っている単語を選ぶ

> **答えを表示: コインと4つのサイコロをすべて振り直す**
> 一部だけをやり直すと値の対応付けに偏りが生じ得ます。

単一署名のシードを開くのにパスワード2つが必要な場合、何を意味しますか。

1. オンチェーン支払いに鍵が2つ必要
2. Taprootマルチシグ
3. 秘密へアクセスする閾値とBitcoinの支出閾値は別

> **答えを表示: 秘密へアクセスする閾値とBitcoinの支出閾値は別**
> 暗号化してもスクリプトは変わりません。

Deskの全体バックアップを評価する際に考慮すべきことは？

1. チャット全体が必ず入る
2. 対象範囲と除外項目があり、チャットが含まれるとは限らない
3. 古いコピーをすべて更新する

> **答えを表示: 対象範囲と除外項目があり、チャットが含まれるとは限らない**
> アイデンティティの復旧とメッセージの復旧は別です。

正しく設定した自分のノードで可能になることは？

1. すべての情報漏えいを防ぐ
2. 第三者への照会依存を減らし、自分で検証する
3. 紛失した鍵を復元する

> **答えを表示: 第三者への照会依存を減らし、自分で検証する**
> 匿名性や秘密の復旧を保証するものではありません。

DeskでUTXOを凍結する操作とは？

1. アプリ内でのローカルな制限
2. コンセンサス条件の変更
3. 同じシードのほかのコピーの失効

> **答えを表示: アプリ内でのローカルな制限**
> ネットワーク全体での支出禁止ではありません。

配信操作の直後に接続が切れたら？

1. 直ちにもう一度支払う
2. ウォレットを削除する
3. まず支払いがすでに配信されたか確認する

> **答えを表示: まず支払いがすでに配信されたか確認する**
> タイムアウトだけで処理が行われなかったとは断定できません。

アドレスの再利用や、異なる用途のUTXOの結合で何が起こり得ますか。

1. 関連性を観察しやすくなる
2. 履歴が消える
3. 匿名性が保証される

> **答えを表示: 関連性を観察しやすくなる**
> プライバシーは利用状況とその後の使い方に左右されます。

Tor Browserを開くだけでDeskも自動設定されますか。

1. はい
2. いいえ
3. ダークテーマの場合のみ

> **答えを表示: いいえ**
> アプリごとに通信経路を確認する必要があります。

xpubに似た外観のチャットキーは何ですか。

1. 公開してよい情報
2. 入金アドレス
3. アイデンティティを保護する秘密情報

> **答えを表示: アイデンティティを保護する秘密情報**
> 機密性はその用途で決まります。

チャットに「支払済み」と表示されたら？

1. ネットワークの承認に代わる
2. 実際の支払いをネットワークで別途検証する
3. 請求で指定されたネットワークが変わる

> **答えを表示: 実際の支払いをネットワークで別途検証する**
> メッセージの状態と支払いの状態は別です。

確認済みのFinal版マルチシグプロファイルが使うものは？

1. MuSig2とPSBT v2
2. P2WSH、sortedmulti、BIP48、PSBT v0
3. あらゆるBitcoinスクリプト

> **答えを表示: P2WSH、sortedmulti、BIP48、PSBT v0**
> 希望や商品名によって対応範囲が広がるわけではありません。

Mirror 12.12ではどこから照合を始められますか。

1. 手順1からのみ
2. 15番目を含む、任意の項目から
3. すべてを終えて最後の項目からのみ

> **答えを表示: 15番目を含む、任意の項目から**
> 項目の対ごとに独立して任意順で照合できます。

Mirrorの「一致」が証明するのは？

1. 全項目の承認
2. 両方のQRの出所が真正であること
3. 比較した一対の値が文字どおり一致すること

> **答えを表示: 比較した一対の値が文字どおり一致すること**
> 残りの確認と応答はまだ必要です。

シードが漏えいしたとき、Deskのパスワードを変更すると？

1. 攻撃者の権限が取り消される
2. そのシードから導出される鍵は失効しない
3. すべてのコピーが削除される

> **答えを表示: そのシードから導出される鍵は失効しない**
> 資産の管理権を安全に移す方法を検討する必要があります。

実習の終了時に何を記録しますか。

1. 読んだ内容、模擬操作、実機テスト、未確認事項
2. 販売した時間だけ
3. 侵害されない保管方法であるという約束

> **答えを表示: 読んだ内容、模擬操作、実機テスト、未確認事項**
> 証拠の種類によって確認できる範囲が異なります。