CUVEX

CUVEX ACADEMY · 0.1

學習、理解，自己掌握。

循序學習比特幣與自我保管。課程、手冊、詞彙表和練習全部免費，無須註冊。從哪裡開始，由你決定。

免費 · 無須註冊

所有章節

1. 準備你的學習環境
2. 數位貨幣與信任問題
3. 比特幣的歷史與限制
4. 聰與正確的金額計算
5. 建立自己的威脅模型
6. 節點、挖礦與共識
7. UTXO 與交易找零
8. 記憶池、確認與鏈重組
9. 手續費、虛擬大小與交易替換
10. 網路、地址與付款請求
11. 雜湊、簽章與加密
12. 種子、密語與密碼
13. 金鑰衍生、xpub 與描述符
14. 選擇錢包與保管模式
15. 製作可實際復原的備份
16. 認識 Original 與 BIT
17. 使用實體熵建立種子
18. 使用 Cuvex 加密與解密祕密資料
19. 加密門檻與生物辨識
20. 複製、保存與驗證副本
21. 安裝與保護 Cuvex Desk
22. 連結密文與整理 WOW 帳戶
23. 將 Mirror 與 Desk 配對
24. 透過 Mirror 使用 NFC、USB-C 與讀取 QR 碼
25. 公共服務商與自有節點
26. 接收比特幣與核對地址
27. 標記、凍結與選擇 UTXO
28. 準備與核對付款
29. 使用 Original 與 BIT 簽署
30. 完成交易、廣播與排除問題
31. 比特幣上可觀察到什麼
32. 區分使用情境與管理找零
33. 網路隱私、Tor 與 VPN
34. CoinJoin、Payjoin 與目前限制
35. 從真實事件學到的教訓

36. 建立聊天身分與驗證聯絡人
37. 透過聊天請款與支付聰
38. 審慎分享密文
39. 復原聊天與理解其中繼資料
40. 日常設定與權限審查
41. 設計多重簽章錢包
42. 建立邀請與提供金鑰
43. 使用 Mirror 以任意順序核對政策
44. 協調簽章與發布多重簽章交易
45. 復原與變更多重簽章錢包
46. 按既定流程更新韌體
47. 遺失、故障與緊急復原
48. 網路釣魚、客服與語音詐騙
49. 隱私、法律與個人紀錄
50. 繼承、持續運作與年度演練
51. 價格、儲蓄與基本面分析
52. 選擇購買比特幣的管道
53. 帳戶、委託單與執行成本
54. K 線、指標與技術分析偏誤
55. 保證金、期貨與自動化
56. Lightning 與其他支付層
57. Taproot、MuSig2 與後量子未來
58. 互通性與脫離製造商後的使用
59. 使用 regtest 的技術實驗室
60. 期末專題與持續運作計畫
61. 學員手冊
62. 比特幣與自我保管詞彙表
63. 檢驗學習成果

M01

準備你的學習環境

學習目標

準備上課，分清三種設備，並約定哪些資料絕不能告知導師。

理解概念

你將學會自行判斷如何接收、保管、花費及復原比特幣，最終能在授權前說明自己的決定。課程可自行閱讀。語音導師提供解說、提問與陪伴，無須查看你的資產或控制你的裝置。

Cuvex 保護祕密資料，讓你在裝置螢幕上授權操作。Desk 在電腦上管理密文、觀察錢包、付款與協調作業。Mirror 為支援的操作提供本機傳輸橋接與資料比對功能，本身無法簽署，也不是獨立錢包。可用流程取決於版本與機型。

課程與 Desk 各用一個螢幕，手機與 Cuvex 放在手邊。若只有一個螢幕，輪流切換，輸入祕密資料時不要在視訊通話中分享畫面。通話可能在練習結束前中斷，暫停並非失敗。只記錄課程編號、完成的步驟和遇到的困難。

無論真人導師或 AI，都不應收到助記詞、BIP39 密語、密碼、聊天金鑰、PIN、私人檔案或完整購買代碼。導師也不需要你的 xpub、真實描述符或地址。後三者雖不能用來花費，卻會揭露活動。只描述錯誤訊息，使用實驗室的虛構資料。

練習

1. 找出電腦、手機及 Cuvex 機型，在私人筆記本記下各自版本。
2. 將無資金的學習環境與實際保管環境分開。練習時不要匯入正在使用的助記詞。
3. 開啟本課，找到暫停、說明與詞彙表。若有人索取祕密資料，立刻中止互動。

檢驗學習成果

說明誰簽署、誰查詢網路、誰傳輸資料。能獨立區分這些職責即可繼續。

常見問題

需要每天與導師交談嗎？不用。你可以自學、重複課程，只在特定操作時求助。課程使用權與語音服務餘額彼此獨立。

暫停點

已完成 L01，已辨識各設備，課程中未記錄任何祕密資料。

導師要求你說出助記詞，想確認你是否抄對。你會怎麼做？

1. 慢慢唸給導師聽。
2. 拒絕要求，只在自己的安全環境中核對助記詞。
3. 只傳送開頭幾個詞。

> **查看答案: 拒絕要求，只在自己的安全環境中核對助記詞。**
> 即使只是祕密資料的片段，也不屬於教學服務應接收的資訊。

M01

數位貨幣與信任問題

學習目標

開啟錢包之前，先了解比特幣想解決什麼問題。

理解概念

銀行餘額是由機構管理的帳面紀錄。銀行驗證客戶身分、決定處理哪些轉帳，並記帳。普通數位檔案很容易複製，寄出照片仍可保留一份。要讓數位單位充當貨幣，就得防止重複花費。

比特幣結合驗證規則、簽章與共享的交易歷史。參與者能獨立檢查交易是否符合規則，無須將完整紀錄交給單一機構。稀缺性取決於大家持續驗證並接受這些規則，硬幣圖案或交易所報價都無法創造稀缺性。

自我保管改變了責任分配。你無須保管人同意即可花費，但若銷毀所有備份或簽錯付款，也可能失去這項能力。操作自由仍需要安全措施、協調、用於廣播的網路連線，並須履行適用義務。

Bitcoin 是網路與協定，BTC 是其貨幣單位。其他網路也可能採用「區塊鏈」一詞，但特性不同。企業承諾交付名為「比特幣」的資產，並不等於你已持有由自己金鑰控制的比特幣交易輸出。

練習

1. 比較銀行餘額、交易所餘額和自己持有金鑰控制的 UTXO。
2. 分別寫出誰可以阻止你動用餘額，以及忘記存取方式時誰能幫你。
3. 描述複製照片的結果，以及嘗試花費同一筆輸出兩次的結果。

檢驗學習成果

用自己的話解釋帳面餘額與簽署能力的差別，無須背誦術語。

常見問題

自我保管代表所有中介均消失嗎？你仍可選擇購買、查詢或通訊服務。應關注的是服務方保有的權力和接收的資料。

暫停點

保存責任比較表，勿加入真實帳戶名稱。

單靠數位簽章無法解決哪個貨幣問題？

1. 防止有人試圖兩次花費同一筆輸出。
2. 證明某把金鑰已授權。
3. 偵測已簽署的訊息遭到更改。

> **查看答案: 防止有人試圖兩次花費同一筆輸出。**
> 簽章證明授權；規則與共識決定互相衝突的花費如何排序。

M01

比特幣的歷史與限制

學習目標

了解比特幣的起源，區分史實與商業敘事。

理解概念

中本聰的論文於 2008 年發表，網路於 2009 年啟動。它運用先前的密碼學、工作量證明與數位貨幣構想，提出點對點電子現金。驗證軟體或交易無須知道中本聰的真實身分。

規則的演變並非由某家公司片面決定。開發者提議與審查修改，節點營運者選擇軟體，礦工建立區塊，使用者與服務商決定接受什麼。分權可能帶來歧見。分叉與應用程式更新是兩件事。

即使投入大量工作，節點仍可拒絕違反自身規則的區塊。共識不是按電腦台數投票；執行數千份節點不會自動增加決策權。礦工占多數也無法因此取得使用者的私鑰。

比特幣刻意在區塊容量、驗證成本、變動的確認時間與公開帳本之間取捨。沒有由管理方撤回付款的機制，也不預設提供全面保密。其他層與應用為特定用途引入新的依賴。

練習

1. 在時間軸標出原始論文、網路啟動、採用 SegWit 和啟用 Taproot。公布日期前請查核來源。
2. 將「公司保證價格」、「節點負責驗證」與「礦工提出區塊」分成商業承諾與技術職能。
3. 說明缺少管理員撤銷付款能力的一項優點及一項代價。

檢驗學習成果

區分共識規則、本機政策與企業決策。你使用的應用程式並不代表整個網路。

常見問題

最新版軟體一定會改變貨幣規則嗎？不一定。版本更新也會修錯、提升效能或修改本機政策。請閱讀發行說明及相容性資訊。

暫停點

記下一項可核實的性質，以及一項仍需證據的說法。

某區塊內的花費欠缺有效授權。礦工多數支持就能使它有效嗎？

1. 可以，只要超過 51%。
2. 交易所公告時才可以。
3. 對執行拒絕該區塊之規則的節點而言，不行。

> **查看答案: 對執行拒絕該區塊之規則的節點而言，不行。**
> 節點只會在符合其規則的有效歷史之間比較累積工作量。

M01

聰與正確的金額計算

學習目標

換算 BTC 與聰，不依賴報價核對數量。

理解概念

1 BTC 等於 100,000,000 聰。sat 是單位，不是另一種貨幣。基礎鏈以整數聰記帳。0.001 BTC 等於 100,000 sat，0.00001000 BTC 等於 1,000 sat。介面的小數分隔符依語言而異，請勿憑感覺加零。

報價將 BTC 按當時價格換算為 EUR 或 USD 等貨幣，並不改變你控制的聰數。持有 100,000 sat，即使價格變動仍是 100,000 sat。Desk 的參考報價附來源與日期；即使 BTC 餘額正確，過期報價也可能導致錯誤決策。

付款時應分清收款額、網路手續費與總支出。若轉出 50,000 sat、手續費 600 sat，且無其他屬於自己的輸出，錢包支出為 50,600 sat。「傳送全部」通常會扣除手續費，收款淨額小於可用餘額。

課程數字僅供算術練習，並非市價或建議費率。簽署前在相應螢幕核對單位、網路、收款方與總成本。語音可以說「五萬聰」並同時顯示「50,000 sat」，不可根據不確定的轉錄決定金額。

練習

1. 將 250,000 sat 換算為 BTC，結果是 0.0025 BTC。將 0.00025000 BTC 換算為聰，結果是 25,000 sat。
2. 傳送 75,000 sat，手續費為 900 sat，總支出為 75,900 sat。
3. 模擬器以 120,000 sat 為輸入，傳送 70,000，手續費為 1,000。確認找零為 49,000 sat。

檢驗學習成果

用 BTC 和 sat 讀出同一金額，並說明哪個金額包含手續費。如有疑問，暫停操作。

常見問題

一定要買一整個比特幣嗎？不必。可購買一小部分，但須考慮服務商的最低金額及費用。

暫停點

只保留練習的計算結果。

可用餘額為 80,000 sat，選擇傳送全部，手續費為 1,200 sat。收款方會收到多少？

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

> **查看答案: 78,800 sat。**
> 這個例子沒有其他輸出，收款方取得可花費餘額減手續費。

M01

建立自己的威脅模型

學習目標

針對遺失、失竊、詐騙與資料外洩，採取與風險相稱的措施。

理解概念

安全是保有按自己意圖行動的能力。隱私是控制誰知道你的資料與關係。可用性是需要時可以存取。沒有人能打開的箱子，你自己也可能打不開；太方便的副本則可能暴露過多資訊。

列出資產、可能的對手與意外。資產包括金鑰、備份、歷史紀錄、備份所在地及聯絡人身分。風險包括惡意軟體、網路釣魚、火災、遺忘、脅迫、故障、死亡與自身失誤。單一工具無法降低所有風險。

用簡單表格寫下大致機率、影響與具體措施。長密碼可減少猜中的機會，但無法糾正你親自授權的詐騙收款人。兩份備份放在同一個袋子裡，袋子遺失時仍會一起丟失。若同一人控制多重簽章的所有裝置與備份，仍可能有共同失效點。

課程與導師也是模型的一部分。購買、通話、連線時間與學習進度都可能產生中繼資料。課程網站不應為個人化教學索取地址或餘額。Desk 或 Mirror 無須一般註冊，不代表商店、語音服務商或第三方查詢服務無法知悉你的活動。

練習

1. 列出三項最重要的風險，不要記錄資產金額或確切地點。
2. 依各風險選擇預防、偵測與復原方法。例如針對卡片遺失，分開存放兩份副本、建立清冊並測試還原。
3. 區分哪些人或系統可觀察購買、通話、餘額查詢與公開交易。

檢驗學習成果

說明下一項措施將如何處理特定風險。不要加入自己無法維護或向繼承人說明的複雜做法。

常見問題

裝置越多就越安全嗎？只有在減少共同依賴且能實際測試復原時才有幫助。新增裝置也會增加維護工作與混淆機會。

暫停點

將計畫存入私人文件，課程中只記錄「已檢視威脅模型」。

哪個做法最能降低同一場火災燒毀所有備份的風險？

1. 改變卡片顏色。
2. 把兩份備份放在同一個抽屜。
3. 將經過驗證的備份分放在風險互相獨立的地點。

> **查看答案: 將經過驗證的備份分放在風險互相獨立的地點。**
> 備援必須能挺過威脅原件的同一場事故。

M02

節點、挖礦與共識

學習目標

解釋什麼是節點和什麼是挖礦的有效性。

理解概念

完整節點 接收 區塊 和交易，檢查規則，並保持鏈條檢視。你不需要信任一個頁面向你宣佈的餘額。挖礦 是透過 工作量證明 提出 區塊 的過程。礦工 選擇有效的交易，並爭取找到一個可接受的 區塊。

工作量證明提高了改寫歷史的成本。若出現數條有效鏈，重要的是累積工作量，不能忽略難度只數區塊。區塊間隔會變，十分鐘是目標平均值，不是下一筆付款的保證時間。

礦業獎金結合補貼和手續費。補貼跟隨區塊的高度折扣日曆；手續費取決於包含的交易。一個付費的轉賬不會使一個錯誤的簽名有效。經濟安全和攻擊成本不會使最近的付款在數學上不可逆轉。

自有節點 降低了向外國供應商傳達查詢的必要性，並允許您驗證。你仍然需要保護你的作業系統,接入和連線。沒有同步的 節點 啟動，或者連線到另一個伺服器訪問的應用程式，不會自動提供這些優勢。

練習

1. 將這些任務分配到：檢查簽名，選擇區塊交易，保留你的種子並決定是否接受付款。
2. 解釋為什麼“礦工保留我的比特幣”是一個錯誤的描述。
3. 在實驗室網路中，觀察高度和同步；不要釋出RPC認證。

檢驗學習成果

它描述了檢查和建議之間的區別。您可以使用類似，但它以正確的技術功能結束。

常見問題

我需要挖礦才能使用比特幣嗎？不。你也不需要一個自有節點開始，但知道你的供應商的信任水平是必要的。

暫停點

按其型別註冊實驗室供應商，沒有私人URL。

正確設定的完整節點能為使用者做什麼？

1. 驗證所接受的鏈符合規則。
2. 復原所有遺失的金鑰。
3. 保證價格上漲。

> **查看答案: 驗證所接受的鏈符合規則。**
> 驗證與資產保管是不同職能。

M02

UTXO 與交易找零

學習目標

閱讀交易作為消費和建立輸出。

理解概念

UTXO 是一個未經過的交易的出口，並且仍然沒有花費。一個錢包透過識別可以控制的輸出來計算其餘額。沒有一個普遍的賬戶留在一個銀行表：一個輸入引用一個先前的輸出，透過交易和位置識別器。

一張UTXO時，全量消耗。如果你需要支付低於它的價值，通常你在你的控制下建立一個收款方輸出和另一個交換。有了 120.000 sat, 收款方 的 70.000 和 手續費 的 1.000 的輸入，更換為 49.000。輸入的總值應該相當於輸出的總值，加上手續費的總值。

一個地址不是一個UTXO。你可以得到多個輸出。他也不一定是個人。交易識別器可能是公開的，但將其與您的身份聯絡起來或解釋誰的每個輸出都新增了連結不單獨表達的資訊。

這個結構是為了隱私：結合輸入可能表明共享控制；變更可能涉及未來的支付。這個結論不是普遍的證據，因為有合作交易。硬幣控制是選擇什麼輸出花費，知道結合它們的後果。

練習

1. 畫出三個虛構輸入，金額分別為 40,000 sat、60,000 sat 與 200,000 sat。僅使用前兩個，支付 70,000 sat，手續費 1,000 sat。
2. 核對找零為 29,000 sat，第三個輸入未被使用。
3. 重複只使用 200.000:更改將是 129.000.比較潛在的成本和連結，不承擔相同的尺寸。

檢驗學習成果

在課程圖表中找到輸入、收款方、變更和手續費。如果您無法識別出路，則您不應該簽署實際交易。

常見問題

回到我的錢包的一切都是改變嗎？不。它可以是轉移到另一個自己的方向。排名要求瞭解政策和衍生,不要猜測的金額。

暫停點

保持虛構的計劃，永遠不要抓住你的遺產。

輸入為 100,000 sat，產生 30,000 和 69,200 兩個輸出。手續費是多少？

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

> **查看答案: 800 sat。**
> 100,000 減去 99,200 等於 800 sat。

M02

記憶池、確認與鏈重組

學習目標

區分已準備、釋出和確認的交易。

理解概念

記憶池 是 節點 所保留的非確認交易的本地集合。地球上沒有一個相同的記憶池。一個瀏覽器顯示付款意味著該服務知道它；它不保證所有節點都接受它，也不保證它會在一個特定的時間內得到確認。

建立 PSBT 不會發布交易。簽署產生授權，最終化則組成可廣播的交易；發布是嘗試將交易傳出。確認表示交易已納入驗證來源所接受之鏈的一個區塊。第二次確認表示該區塊上方又增加一個區塊，而非收款方第二次簽署。

可能會發生重組，其中一個鏈條的轉換和一個操作失去確認數或重新延遲。對於具有更高的曝光的支付，雙方通常需要更大的確認數。沒有一個數字可以消除任何風險的所有金額和情況。

如果 Desk 顯示儲存狀態，請參閱同步日期。“確認”根據一個古老的即時不一定描述當前狀態。如果發貨不出現，請保留您的本地識別符號，並在您重新準備之前檢視釋出和歷史記錄：無憂無慮地重複可以創造另一個有效的付款。

練習

1. 訂購這些卡：刪除器，PSBT,簽名，最終交易，傳播，包含在區塊。
2. 播放後進行分離。決定在重新支付之前檢查什麼。
3. 向交易者解釋為什麼一個聊天訊息說“付費”不會取代網路驗證。

檢驗學習成果

您可以表達交易的狀態以及這些資訊的來源和日期，而不會將其與保證混淆。

常見問題

關閉 Desk 取消釋出交易嗎？不。其他節點和參與者可以儲存它。取消本地排洩器有另一個範圍。

暫停點

指示模擬狀態；不要將真實的識別器新增到 導師。

按下發布後電腦立刻斷線，先做什麼？

1. 從頭重做相同付款。
2. 刪除錢包。
3. 重新連線，檢查交易及其輸入。

> **查看答案: 重新連線，檢查交易及其輸入。**
> 沒收到回應不能證明廣播失敗。

M02

手續費、虛擬大小與交易替換

學習目標

估計成本，解釋sat為vbyte並理解RBF和CPFP。

理解概念

網路手續費是輸入和輸出之間的區別。其競爭力通常以sat/vB:聰為虛擬位元表達。它不直接取決於傳送的經濟價值。很多輸入可以付出很小的付款；一個大付款，有很少的輸入可以佔用更少。

在200 vB到5 sat/vB的例子中，手續費是1.000 sat。在簽名之前，您只能有一個估計，因為最終尺寸可能取決於簽章和結構。Desk提供指向速度和手動價格；一個“快速”標籤不會承諾準時確認。

RBF 是一種不確認交易的替代政策，在某些條件下。該機制允許提出一個衝突的支出，以更大的手續費;節點的政策已經發展，並且不適合作為收費保證來處理非替代訊號。更換需要新的修訂和需要的簽章。

CPFP 是花費一份退出，以便父親和兒子的集合變得有吸引力。它需要控制可用的出口，遵守政策，並支付成本。這是一個比特幣的概念：在學生的Cuvex版本中，沒有一個CPFP按鈕。

“Dust”是根據適用的政策和估計的支出而過小的出口；它不是所有型別的指令碼的普遍邊緣。避免將固定數字作為共識的法則。如果更換不可行，請檢視值，輸入或折扣和手續費有效。

練習

1. 計算 180 vB 到 8 sat/vB: 1.440 sat。檢查是否超過您的實驗室預算。
2. 比較使用一個輸入與十個輸入的情況，解釋為何單看匯款金額不足以估算成本。
3. 模擬一筆交易，並決定等待，RBF或學習CPFP,而不承擔自動相容性。

檢驗學習成果

說明所選費率、手續費總額與其相對於付款金額的成本。若無法理解費用，請拒絕。

常見問題

RBF 是否肯定取消了以前的付款？不。版本一直在競爭，直到確認，傳播是重要的。不要以取消承諾為基礎交付貨物。

暫停點

保留實踐的決定和原因。

250 vB、費率 4 sat/vB，手續費是多少？

1. 1,000 sat。
2. 254 sat。
3. 轉出金額的 4%。

> **查看答案: 1,000 sat。**
> 虛擬大小乘以費率即為估計手續費。

M02

網路、地址與付款請求

學習目標

在複製或掃描之前，識別網路、地址格式和付款指示。

理解概念

Mainnet 移動 比特幣 以經濟價值。測試網路用於開發和學習，但它們不互相交換。Regtest是一個由實驗室組建者控制的本地網路；signet和testnet有自己的規則和生態系統。signet 中的單標函式並不意味著 Cuvex 的 多重簽章 個人資料支援該網路。

地址編碼接收條件。在 mainnet 中，您將找到從 1, 3, bc1q 或 bc1p 開始的格式。預告片 可以幫助識別一個家庭，但它不驗證收款方,不保證簽署者的相容性，也不會取代完整的格式驗證。

QR 是視覺容器。它可以攜帶一個地址，一個發票，一個描述符或惡意文字。掃描不真實的作者。連結 比特幣:可以新增值和訊息。BIP321 是代替 BIP21 的現代參考；Desk 保持了 BIP21 術語和相容性，並在其重新實施中進行修訂。標準的改進並不單獨擴充套件應用程式所理解的內容。

Lightning 發票 不是一個 On-chain 地址。它可能包括終止和其他欄位；如果應用程式不提供相容的流量，您不應該將其貼上到連結傳送中。一個稱為BTC的代幣在另一個網路上也不會自動成為比特幣的原產地。

練習

1. 列出未使用可支付地址的課程標籤樣本：地址，URI 比特幣:，發票Lightning和描述符.
2. 在實驗室中確定所選擇的網路。在 Cuvex 多重簽章 修訂，配置檔案的相容性為 mainnet/regtest.
3. 比較接收器要求的完整文字，在實際操作之前使用驗證的頻道。

檢驗學習成果

您可以拒絕一個您不知道的網路或模式的請求，並解釋您需要驗證的內容。

常見問題

我可以透過任何顯示交易所的網路傳送BTC嗎？不。退出網路必須與實際接收相匹配。不要選擇最低的手續費。

暫停點

它只記錄了學習網路的型別。

有 bc1 收款地址不代表就能經其他代幣網路提領 BTC。還要做什麼？

1. 更改收款方別名。
2. 確認使用比特幣鏈上提領，並核對全部資料。
3. 將種子輸入交易所。

> **查看答案: 確認使用比特幣鏈上提領，並核對全部資料。**
> 資產、網路與接收方式必須相容。

M03

雜湊、簽章與加密

學習目標

區分完整性、授權和保密性。

理解概念

雜湊值將資料轉化為固定長度的痕跡。比較已知的印記可以幫助檢測變更；它不會計算檔案，也不會單獨識別誰釋出了檔案。如果您從同一頁面下載檔案和雜湊值,攻擊者可能已經取代了兩者。

私鑰 可以建立 簽章;相應的 公鑰 可以檢查它們。簽名將許可證與特定資訊根據演算法和規則進行聯絡。它不隱藏簽名的內容。在 比特幣 中，有效的簽名是花費出門所需條件的一部分。

加密 只需要適當的容量才能閱讀內容。驗證式加密 顯示變異檢測在Cuvex生態系統中，有密文保護秘密、簽署交易、授權支出和傳輸訊息的加密渠道。它們不是相同的物件，儘管所有人都使用加密。

人類 密碼 通常透過 衍生 功能，然後將其作為加密 金鑰 使用。“AES-256”描述了金鑰的演算法和尺寸，但它不會使一個可預測的密碼成為一個強大的選擇。建立、實施、儲存、螢幕和恢復是整體安全的一部分。

也不能說QR是安全的，因為它看起來很複雜。需要知道它包含什麼，誰生產了它，以及應用程式將如何使用它。在接受行動之前，請求導師解釋其目的，而不要求隱私資料。

練習

1. 與“檢測檔案變更”，“隱藏一個種子”和“授權付款”與雜湊值,加密和簽名。
2. 改變一個虛構文字的字母，並注意到你的雜湊值正在改變；不要使用秘密來展示這個。
3. 解釋為什麼交易可以公開並同時簽署。

檢驗學習成果

您可以描述您正在尋找什麼保證，以及它提供什麼機制，而不使用“加密”作為所有安全的同義詞。

常見問題

雜湊值 韌體 是否證明沒有故障？不。確定如果參考是可靠的。一個審計，一個製造商簽名和一個物理測試回答不同的問題。

暫停點

保留三份工作日期。

何種機制可隱藏祕密資料的內容？

1. 公布檔名。
2. 只簽署而不加密。
3. 以受保護的金鑰正確加密。

> **查看答案: 以受保護的金鑰正確加密。**
> 簽章或指紋本身無法保密。

M03

種子、密語與密碼

學習目標

避免系統的不同訊號之間的混亂。

理解概念

BIP39 助記詞以字典中的詞表示熵與校驗碼。標準長度為 12、15、18、21 或 24 個詞。挑選好記的句子、歌詞或人為「隨機」選詞都無法重現安全的產生流程。校驗碼能偵測部分錯誤，不能證明是誰建立了種子，也不能證明沒有其他人知道它。

BIP39 密語參與二進位種子的衍生。不同密語可能開啟完全不同、看似空白的錢包，未必會出現「密語錯誤」。密語不必是字典中的詞，也不是字面意義上的第二十五個詞。

密碼 密文 Cuvex 保留的秘密。Desk 密碼 保護您的計算機的本地儲存庫。連結PIN允許一個通訊會議。金鑰 Chat 恢復了郵件身份。他們中沒有一個應該與種子混淆，並且認識一個並不意味著能夠重建所有其他人。

將 種子 和 密語 在 密文 中儲存在一起，可以幫助您恢復，但它會消除它們的分離，因為它可以被解密。把它們分開，對你和你的繼承人帶來了巨大的要求。該決策必須進行文件和驗證，而不是因為導師認為“更先進”的選擇。

練習

1. 製作五張沒有實際祕密值的紙卡，分別標示種子、密語、Cuvex 密碼、Desk 密碼與聊天金鑰。
2. 寫下你每個人都會得到什麼，當你忘記它時會失去什麼。
3. 設計一項使用空錢包的試驗。私下輸入助記詞與密語，只向導師回報結果。

檢驗學習成果

解釋為什麼課程永遠不應該要求密碼來“驗證”你的學習。找出你的恢復程式需要什麼秘密。

常見問題

可用電子郵件重設密語嗎？BIP39 沒有這種機制。保管服務商或許能復原帳戶，但那是另一種模式。

暫停點

記錄“分離訊號”，而不寫其值。

BIP39 密語改一個字母後餘額為零。何種解釋正確？

1. 可能是新密語衍生的另一個有效錢包。
2. 網路已刪除你的資金。
3. Desk 必須猜出原來的密語。

> **查看答案: 可能是新密語衍生的另一個有效錢包。**
> 另一個密語可能產生其他錢包，而不會回報錯誤。

M03

金鑰衍生、xpub 與描述符

學習目標

瞭解如何描述一個錢包沒有提供支出能力。

理解概念

一個錢包是由許多金鑰從一個根源產生的。一條路線指示哪個分支被使用。在 mainnet 中，BIP84 通常使用 m/84'/0'/0' 為第一個 SegWit 單位帳戶；BIP48 P2WSH 在第一個 多重簽章 帳戶中使用 m/48'/0'/0'/2'。指的是強化衍生。更改帳戶、網路或指令碼型別，可以從相同的 助記詞 中提供其他地址。

xpub 是一種延伸的 公鑰 可以產生某些 公鑰 後代。它不是一個密碼的支出，但它可以允許觀察一個地址家族。主金鑰指紋 是一個簡短的識別器，用於連線記錄；它不會自行保證身份，也不會避免碰撞。

一個描述符表達瞭如何構建指令碼和地址：指令碼型別，金鑰,起源和衍生物。描述符 唯讀觀察 與 公鑰 允許觀察，不簽名。“描述符”一詞不保證僅包含公共資訊：某些格式可能包括私鑰。永遠不要把一個真實的描述符上課。

要恢復一個多重簽章通常需要完整的政策，而不僅僅是簽署者的單詞。保持邊緣，參與者，xpubs，路線，網路，指令碼型別和發現資料。描述符的驗證總額有助於檢測過渡錯誤；不確認參與者。

練習

1. 閱讀一個虛構的路線，並解釋目的，貨幣，賬戶和分支。不要輸入真實的金鑰。
2. 區分收款地址、xpub的參與者和描述符的完整。
3. 準備一個私人恢復檔案，空域名稱和單獨的文件位置。

檢驗學習成果

你可以解釋為什麼一個空的錢包後恢復沒有失去測試：你必須檢查網路，密語,指令碼，帳戶，路線和發現。

常見問題

xpub 能否在沒有後果的情況下發布？它本身不會給出正常的支出能力，但它會揭示隱私，並且在特定加密組合中可能會增加其他風險。

暫停點

在課程中保留沒有敏感值的檔案。

只有一個種子，要復原多重簽章錢包時可能缺少什麼？

1. 裝置的顏色。
2. 政策與其他參與者的公鑰。
3. 社群帳號密碼。

> **查看答案: 政策與其他參與者的公鑰。**
> 除達到私鑰門檻外，重建腳本也需要完整政策。

M03

選擇錢包與保管模式

學習目標

比較工具的功能，信任和恢復。

理解概念

錢包是一組可描述、觀察並在適用時授權支出的工具。熱錢包在連網環境保有簽署能力，隔離的簽署裝置則盡量讓祕密遠離查詢網路的設備。觀察錢包持有足夠的公開資訊來查看及準備操作，但需其他系統簽署。

在第三方保管中，一個帳戶可以代表對企業的權利。在 自我保管 中，您保持個人或共享的技術支出能力。透過電子郵件恢復和阻止退出的力量通常反映了第一種模式。你不應該以相同的責任假設評估兩種選擇。

比較網路支援和指令碼，螢幕驗證，複製，更新，互動性，維護，供應商查詢和錯誤清晰度。一個貨幣列表或物理結尾不夠。簽名裝置也不會阻止您接受錯誤的地址，如果您不檢查。

Cuvex 將密文中的祕密與 Desk 的整理及查詢功能分開。此模式要求保存密文與解鎖手段。防範裝置遺失，不代表在所有副本或密碼都遺失時仍能復原。在移轉資產前先學會完整流程。

練習

1. 將 Cuvex 與 熱錢包 和 交易所 相比：誰簽名，誰看到查詢，誰可以恢復訪問，以及在公司關閉時發生什麼。
2. 選擇兩個標準，你必須透過證據來驗證，而不是透過廣告。
3. 請確保實習環境不會與您的實際儲蓄共享 金鑰。

檢驗學習成果

正當選擇一個具體的案例，而不宣佈一個不可逆轉的工具。

常見問題

硬體 錢包 會使所有交易都隱私嗎？不。它主要保護簽名能力和審查的一部分；鏈條，查詢和合作伙伴繼續產生資訊。

暫停點

保留您的基準記錄，沒有帳戶名稱。

使用公鑰正確設定的觀察錢包可以做什麼？

1. 觀察與準備操作，但無法單獨簽署。
2. 更換遺失的種子。
3. 保證匿名。

> **查看答案: 觀察與準備操作，但無法單獨簽署。**
> 觀察與授權是可分開的能力。

M03

製作可實際復原的備份

學習目標

設計完整的影印件，並在依賴它之前展示恢復。

理解概念

一個有用的 備份 恢復了一個容量，而不僅僅是一個檔案。單公司可能需要助記詞、密語和衍生資料。對於一個多重簽章,它還需要政策和足夠的簽署者。Desk 可能需要加密副本和 密碼。對於聊天，恢復身份不等於恢復歷史訊息。

回收保護於意外損失；分離保護於共同承諾。兩個副本在不同的支援和地點可以減少相關故障。每個額外的副本也需要訪問控制、儲存和審查。檔名和標籤不應披露遺產，也不應使所有元件的位置更容易。

一項測試必須確認已驗證的方向，並在學習環境中能夠簽署控制操作。看到檔案開啟並不表明它屬於正確的錢包。您也不會透過在任何計算機上輸入您的 種子 生產來檢查副本。

記錄什麼覆蓋和什麼刪除每個副本。更改現有 密碼 不會自動更改舊版本。如果前一個密碼被曝光，則這些備份仍然受到影響。刪除現代儲存中的檔案也不會保證刪除所有副本或版本。

練習

1. 填寫一個私人表：物件，內容，相關密碼,獨立位置，測試日期和負責。
2. 恢復一個學習副本在一個單獨的環境。檢查網路，第一地址和衍生。
3. 模擬計算機的損失，然後是裝置的損失。確定什麼樣的程式會改變。

檢驗學習成果

您可以在沒有 improvised 幫助的情況下恢復您的測試場景，並解釋其他場景會缺乏哪些資訊。

常見問題

Desk的全球副本是所有的一切的副本嗎？它不應該被接受。在審查基礎上，歷史和聊天會議不包括。政策多重簽章 和 私鑰 有不同的功能。

暫停點

記錄測試的日期和結果；從來沒有複製內容。

更改 Desk 密碼後，舊的備份會怎樣？

1. 自行更新。
2. 自動解除加密。
3. 維持建立時使用的保護方式與密碼。

> **查看答案: 維持建立時使用的保護方式與密碼。**
> 舊備份是獨立的物件。

M04

認識 Original 與 BIT

學習目標

根據裝置和版本選擇正確的路徑。

理解概念

Original 使用 NFC 卡運送 密文 和相容操作；Bluetooth 干預其更新。它的USB-C在文件模型中被用作供應。BIT 使用 USB-C 與檔案交換，並新增 生物辨識 為需要的 密文。不要將 NFC 或 Bluetooth 指示從 Original 轉移到 BIT.

在裝置上，您將找到 加密、解密 功能，建立 錢包 並簽名，以及設定。Original 包含卡克隆；BIT 與 USB 支援的檔案一起工作。標籤、語言和接入可能因版本而有所不同。BIT的新“檢視政策”訪問導致相容的流量，並且不會改變誰授權。

編輯參考是 Original 1.2.2 Final，BIT 1.2.3 Final，Desk beta.9.21 和 Mirror beta.12.12。它們是來源參考：每個組合的簽名、分發和物理接受必須與裝置進行驗證。不要將你的 韌體 替換為一個沒有簽名的二進位制包中包含的。

在使用裝置之前，檢查起源、字串、外觀和版本。可追蹤和更新簽名有助於具體威脅，但不取代所有檢查。如果您看到操作或意想不到的版本，請停止啟動並透過您確認的頻道查詢支援。

練習

1. 識別您的模型並記錄可見的版本，而無需拍攝秘密。
2. 查詢 加密, 解密,建立 錢包, PSBT 和設定。不要啟動刪除或更新來瀏覽選單。
3. 在課程中選擇Original或BIT分支。在實踐中保持這個選擇。

檢驗學習成果

解釋如何從您的模型中輸入和輸出操作，以及您應該保護哪些支援免受過度註冊。

常見問題

BIT 是自動更安全的任何人？模型提供不同的操作決策。答案取決於威脅，恢復和正確使用。

暫停點

保留模型和版本在您的本地記錄中；課程只需要您選擇的模型。

你持有 BIT，指南卻要求裝置直接寫入 NFC 卡。該怎麼做？

1. 核對指南是否適用於機型，並使用相容的 USB 流程。
2. 強制安裝 Original 更新。
3. 把種子傳到手機。

> **查看答案: 核對指南是否適用於機型，並使用相容的 USB 流程。**
> 說明必須符合機型實際使用的傳輸方式。

M04

使用實體熵建立種子

學習目標

瞭解生成和測試流量，而不會將課程資料轉換為自己的金鑰。

理解概念

熵是不可預測的。資料可以提供熵,如果它們是合適的，命令在發射之前固定，轉換演算法是正確的。拒絕一個程式的結果必須按照指定的方式重複；取代它們的最大數量或選擇另一個單詞會引入漏洞。

已審查的 Cuvex 流程結合一枚硬幣與四顆骰子。轉換函式以硬幣值 × 1,296，加上各骰值先減一後組成的六進位數，接受索引 0 到 2,047。若超出字典範圍，必須重擲硬幣及四顆骰子。保留硬幣結果只重擲骰子會造成偏差。這是已審查原始碼的行為；須針對每個發行韌體驗證螢幕及完整流程。

它不等於選擇最喜歡的詞語。不要把公共示範變成保留金錢的材料。任何在教學材料中出現的種子都被認為是已知的。最終單詞和其驗證必須透過裝置的完整演算法進行，而無需手動完成助記詞。

準備一個沒有攝像頭的空間，附近的活躍聲音助理，螢幕錄製或觀察者。導師必須在進入和審查秘密時停止。您可以先解釋，然後透過關於過程的問題來評估，而不會聽到發射結果或詞語。

建立後，您必須檢查 備份,根據模型編碼並測試一個空的 錢包 的恢復。一個驗證地址可以幫助確認一致性，而不會將 種子 曝光到計算機上。如果流量接受與指示相矛盾的值或顯示意想不到的單詞，則停止使用並僅記錄版本、螢幕和錯誤。

練習

1. 在測試中，跟隨裝置的步驟，無背景材料。設定資料的順序，不要改變結果。
2. 根據螢幕拒絕的 輸入 重複，而不會修復它們。
3. 將內容進行私人審查，建立影印件，並確認您可以重建相同的學習錢包。

檢驗學習成果

解釋為什麼熵物理，正確的轉換和結果的秘密是三個不同的要求。

常見問題

我能否在AI上計算我的拖動，以便我檢查演算法？不是你要使用的種子。助理用不同的合成例子工作。

暫停點

在安全的裝置狀態下完成，不要在休息期間看到種子。

韌體拒絕一次擲骰輸入時，怎樣做才符合流程？

1. 自行挑選一個詞。
2. 依裝置提示重做，不干預結果的隨機性。
3. 不斷縮小數字直到獲接受。

> **查看答案: 依裝置提示重做，不干預結果的隨機性。**
> 拒絕某些輸入是熵轉換的一部分，不能任意取代。

M04

使用 Cuvex 加密與解密祕密資料

學習目標

建立一個密文學習，並檢查它的恢復。

理解概念

選擇正確的內容型別：BIP39、SLIP39、Monero 或在流中可用的文字。它們是不同的格式。加密 文字 SLIP39 不將 Cuvex 變成所有可以使用該文字的網路的 簽署者。儲存秘密和執行簽名協議有不同的範圍。

直接輸入內容到裝置時，當您試圖將其保持在連線的裝置之外。從電話或PC的輸入方法可能已經揭示了原來的秘密，但後來仍然是加密。預覽螢幕是檢測錯誤的單詞、順序、大字和欄位的地方。

密碼的密文必須是長，獨特和可恢復的，根據你的計劃。修訂的建立鍵盤具有 40 字元的容量，並且驗證器要求至少 12，大和小 ASCII，認可的號碼和符號。不要自動使用 12 A 1.024 性格的 Desk 在鍵盤上 Cuvex：Desk 採取不同的政策。其他恢復欄位可能有不同的界限；檢查流和版本。

在Original上，寫在合適和空的卡上；保持位置，直到收到確認。BIT 保留由 USB 流產生的檔案，包括必要時的 生物辨識 元件。不要以直覺為名或組合檔案。接下來，它在裝置上進行閱讀和測試解密,而不會向導師傳達秘密。

練習

1. 編碼為此實踐建立的教學文字，沒有訊號或經濟價值。
2. 識別支援和結果的物件；隱私標記標誌和其功能。
3. 重新啟動 解密 過程，在可靠螢幕上檢查文字，並在完成時關閉檢視。

檢驗學習成果

你可以區分正確的內容，正確的寫作和正確的恢復。“複製檔案”的訊息不會測試所有三個。

常見問題

信用卡的標籤是密碼嗎？不。這是組織資訊。避免包含您的財產身份或描述。

暫停點

不要讓解密內容可見。只記錄試驗的成功或失敗。

怎樣最能證明練習密文確實可用於復原內容？

1. 名稱好看。
2. 兩個資料夾裡都有檔案。
3. 循正確流程讀取、解密，並私下核對內容。

> **查看答案: 循正確流程讀取、解密，並私下核對內容。**
> 有副本不等於副本可用，或確實對應正確資料。

M04

加密門檻與生物辨識

學習目標

將共享保護與秘密的分離多重簽章由比特幣。

理解概念

由多個 密碼 保護的 密文 控制誰可以 解密 內容。一 錢包 比特幣 多重簽章 規定什麼 金鑰 必須允許網路支出。您可以共享一個單一的 錢包 的 加密 秘密，或者每個 簽署者 的 多重簽章 與其自己的 密文 個別。

如果多個人共同開啟一個種子,而這個種子允許單獨花費，鏈條的邊緣仍然是金鑰。一旦被揭露，有人會保留它。不要把這個計劃描述為要為每個付款進行多個簽章的協調。

生物辨識 BIT 新增了使用它的格式的訪問條件。一隻手指不是種子或密碼的普遍替代品。計劃傷害，痕跡變化，故障，裝置可用性和遺產。在依賴於它之前，保留並測試該密文的記錄恢復路徑。

一項恢復出口可以揭示計算機上的秘密，正是為了解決緊急情況。這種功能的存在不會使PC變成與裝置相同的環境。正常的做法必須保持隔離；如果有曝光，當地的恢復會被有意識地研究，並透過後續移民計劃進行研究。

練習

1. 畫出兩項政策：「開啟一個種子需要兩個密碼」與「花費需要三把金鑰中的兩把」。
2. 在沒有資料的測試中，您可以確定需要生物學複製的檔案，並在哪裡檢查其恢復。
3. 假設一個人不存在。確定您的計劃的邊緣是否允許繼續。

檢驗學習成果

您可以解釋誰可以瞭解秘密，誰可以在解密後允許支出。

常見問題

我可以透過更改標籤取消一個參與者嗎？不。你必須區分組織變化，新的秘密保護和新的支出政策。

暫停點

保留沒有真實名稱或 生物辨識 資料的圖表。

三人以兩個密碼開啟含有單簽種子的密文。比特幣支出需要幾把金鑰？

1. 若錢包政策如此設定，只需一把。
2. 兩把，因檔案要求兩個密碼。
3. 三把，因有三人。

> **查看答案: 若錢包政策如此設定，只需一把。**
> 加密門檻不會改變控制資金的腳本。

M04

複製、保存與驗證副本

學習目標

建立 redundancy 而不會破壞唯一有效的副本。

理解概念

克隆一個密文複製加密資料；不會創造一個新的平衡，另一個種子或獨立與一個密碼暴露。相同的副本解決了支援損失，而不是原始秘密的承諾。因此，恢復和遷移到新的金鑰應對不同的情況。

Original 區分 密文 卡和 PSBT 運輸卡。操作支援可以根據流量重複使用；您的 備份 卡不應該成為該支援。如果交易拒絕包含密文的卡片，請不要試圖跳出保護或手動刪除頭部。

在 BIT 中，一個副本必須保留所需的集合和檔案之間的關係。檔案管理員可以顯示完整的傳輸，而不保證裝置已驗證內容或完成操作。等待指定的狀態，並透過控制恢復來檢查副本。

保留私人儲存庫，配有隱藏的識別器、格式版本、日期和最終測試結果。至少分兩份副本，面對您所定義的事件。避免上傳 備份 到支援渠道，以診斷問題；方便 中繼資料 清理和錯誤程式碼。

練習

1. 透過正確的流動，將您的 密文 教學影印件建立在另一個支援器上。
2. 關閉原始支援並從複製中恢復測試文字。
3. 記錄你會做什麼，因為丟失，檔案損壞和密碼的曝光。不是相同的程式。

檢驗學習成果

您可以識別您嘗試的副本，並解釋為什麼原件沒有被提前寫下。

常見問題

我可以看到第二個檔案後刪除原始檔案嗎？首先，檢查恢復和覆蓋。刪除必須符合一個計劃，而不是簡單的副本數量。

暫停點

在關閉會話之前保留支援；不要讓卡與付款測試混合。

若他人知道密碼並取得密文，再複製三份有何效果？

1. 撤銷攻擊者的副本。
2. 增加備援，但不撤銷其存取能力。
3. 自動更改比特幣種子。

> **查看答案: 增加備援，但不撤銷其存取能力。**
> 增加副本無法消除已發生的外洩。

M05

安裝與保護 Cuvex Desk

學習目標

開啟驗證的起源設施，並保護您的本地倉庫。

理解概念

依系統與架構選擇套件：macOS Intel 或 Apple Silicon、Windows x64 或 ARM64，以及依可用發行版本選擇 Linux x64 或 ARM64。原始碼 ZIP、Manager 套件與客戶端安裝程式是不同的交付物。課程不應引導學員取得私人簽署套件。

檢查系統的起源和檢查。Windows的工程公司本身並沒有給出版商帶來公共信任。在Mac上，應用簽名、註冊和評估是不同的控制。不要透過隨機支援電話關閉一般保護。如果版本發出意想不到的通知，則儲存文字並使用官方頻道。

Desk 建立 加密 與 密碼 的本地倉庫。在審查基礎上，新密碼可以從12到1.024字元；在確認的情況下，需要相匹配的欄位。這些限制並不是一個足夠的質量措施：使用一個單一的句子，避免重複使用。計算機的生物辨識,當它可用時，是一個方便的訪問，需要自己的設定。

設定阻止因不活躍而，如果有必要，則轉到背景。故障後延遲和可選刪除在手冊中進行研究：在示範過程中不要啟用自動刪除。該應用程式可能在沒有常規使用者帳戶的情況下執行，但其查詢、聊天或下載服務具有特定的要求和通訊。

練習

1. 檢視平臺、可見版本和包的起源，而無需向 導師 提供私人識別器。
2. 建立一個學習庫，並檢查鎖定和重新開啟。將密碼引入私人。
3. 程式設計一個加密副本，並根據您的計劃儲存 密碼。不要在現實環境中嘗試重複的封鎖。

檢驗學習成果

您可以區分密碼本地、商用賬戶和信件，以及您所提供的服務。

常見問題

換Desk 密碼會改變我的卡嗎？不。這是獨立的保護。舊版本也不能單獨改變。

暫停點

阻止 Desk 並保留教程識別器，沒有身份證。

安裝程式不適用於你的處理器架構，首先應怎麼做？

1. 關閉保護措施強行執行。
2. 取得正確的官方套件並核對系統需求。
3. 將種子匯入網站以繼續。

> **查看答案: 取得正確的官方套件並核對系統需求。**
> 接觸保管資料前應先確認相容性與來源。

M05

連結密文與整理 WOW 帳戶

學習目標

將加密影印件連線並將其與觀察帳戶區分。

理解概念

Desk 組織 密文 連線到 NFC, USB 或可複製的檔案。一個視覺設計和一個字串可以幫助你識別它們，但它們不是密碼身份證。在檔案中，您可以檢視應用程式所解釋的起源和屬性，如格式、尺寸和訪問功能。

連線輸入或組織相容的物件；並不意味著在PC中解密它，也不意味著檢查它的秘密。WOW 是一款 觀察錢包 由可接受的公共資訊相關聯。相同的秘密集可能有不同的帳戶或衍生：該協會必須符合您所管理的錢包。

啟用或進口與 描述符 帳戶或透過裝置流出口的公共資訊。檢視網路、指令碼型別、痕跡、路徑和控制地址。帳戶名稱是組織性的；由一個名稱產生的標識不應被視為強烈的匿名化，因為可以猜測一個可預測的名稱。

基於 Desk 的儲存會計和函式，以出口副本、克隆和刪除本地記錄。刪除 介面 卡不會破壞外部副本，也不會移動資金。“沒有備份”意味著應用程式不根據其標準認證副本，而不是世界上沒有備份存在。

練習

1. 透過選擇的運輸將密文教學連線並審查其檔案。
2. 輸入相容的學習帳戶，並檢查您的網路和驗證地址，而不會顯示 金鑰 到 導師.
3. 區分 密文 登記、 WOW 帳戶和物理支援。確定什麼會消失在一個地方的刪除。

檢驗學習成果

您可以解釋 Desk 需要哪些資料來觀察，以及在常用的使用期間應該追蹤哪些資料。

常見問題

否將 .bin 檔案轉換為我的 種子?不。你必須檢查它的起源和恢復。檔案擴充套件不證實內容。

暫停點

只保留“驗證的檢測漏洞”狀態。

在本機刪除 WOW 帳戶會移動其中的比特幣嗎？

1. 不會。流程刪除的是本機資訊，不會花費 UTXO。
2. 會，會傳給製造商。
3. 會取消他人保留的所有簽章。

> **查看答案: 不會。流程刪除的是本機資訊，不會花費 UTXO。**
> 本機狀態與鏈上狀態不同。

M05

將 Mirror 與 Desk 配對

學習目標

設定並完成一個授權的本地連結，而不會混淆您的程式碼。

理解概念

Mirror 可透過應用程式呈現的配對、PIN 及 QR 碼流程與 Desk 進行本機操作。六位數 PIN 僅屬於這次連線，不是 Desk 密碼、密文密碼或復原詞。確認在哪個螢幕產生代碼、應輸入何處。不要使用陌生人傳來的代碼。

從 Desk 的正確背景開始行動：連結、閱讀 QR、運輸 PSBT 或 韌體 是不同的用途。視窗提供搜尋、連線、發現、PIN、QR和卡或檔案上的行動。在搜尋中顯示一個裝置並不表明整個操作已經完成。

根據系統授予相關許可證：光學閱讀攝像頭和Bluetooth或NFC當流量要求時。一個沒有必要的物理能力的手機不會透過安裝軟體來獲得它。iOS 有介面卡和驗證的差異；不應該像已經在所有iPhone上分發和測試一樣提交一個可組合的專案。

如果錯誤，請確定確切的階段：不顯示，不顯示但不連線，PIN被拒絕，QR不可閱讀，未閱讀的卡或未收到的回覆。關閉舊會議，檢查相容和允許的版本，並以控制的方式重新嘗試。錯誤的 PIN 不允許更改 韌體 或在其他地方輸入 種子.

練習

1. 從 Desk 開始測試閱讀，並透過本地螢幕連線 Mirror。
2. 在提交QR或教學卡之前，請檢查目的。
3. 取消會議並確認此後不會從以前的背景中進行閱讀。重新啟動新會議。

檢驗學習成果

您可以描述失敗的階段和相關裝置，而無需傳輸活性程式碼或敏感內容。

常見問題

Mirror 是否需要始終保持連線？這取決於操作。不要把它視為一個永久服務，也不要假設一個會議在關閉或轉移到背景後仍然被允許。

暫停點

關閉連結會話並阻止您未使用的應用程式。

配對在顯示 PIN 前失敗，導師應怎麼做？

1. 索取種子。
2. 先檢查裝置探索、權限、連線階段與版本。
3. 認定已連線成功。

> **查看答案: 先檢查裝置探索、權限、連線階段與版本。**
> 診斷要以實際觀察到的階段為準，不能憑空宣告成功。

M05

透過 Mirror 使用 NFC、USB-C 與讀取 QR 碼

學習目標

依各傳輸方式的用途操作，並完成各自的查核。

理解概念

使用 Cuvex Desktop 的 NFC 流程時，必須在相容的智慧型手機上執行 Cuvex Mirror，並透過 Bluetooth 與電腦配對。Cuvex Desktop 不支援外接 USB NFC 讀卡機。卡片本身、格式與容量也必須相容。可存放密文的小容量卡片未必裝得下含有先前交易的 PSBT。實際限制取決於全部內容，不能只看收款方數量。不要把備份卡改當傳輸卡。

使用 Original 時，Mirror 可將請求寫入操作卡；裝置處理後將回應寫回卡中，再由 Mirror 傳回 Desk。寫入成功不代表 Desk 已收到。請保持卡片不動，直到設備顯示結果。如果系統為保護已識別的密文而拒絕寫入，應尊重此限制。

BIT 使用 USB 交換磁碟區或資料夾。過程中磁碟區可能卸載後重新出現。Desk 必須選對媒體、驗證回應，並執行預定的接收確認。將檔案複製到電腦上同名的資料夾，不等於已送達裝置。

相機讀不到 QR 碼，可能是對焦、反光、大小、晃動或資料密度所致。放大顯示並調整照明與距離。不要用長識別碼的前幾個字元代替完整識別碼，也不要接受不完整的轉錄。成功掃描後，還要驗證所讀資料的意義。

練習

1. 使用教材，在圖中分別指出 Original 和 BIT 的請求、媒體與回應。
2. 試著取消掃描 QR 碼，不保留取消後才出現的讀值。再換一種用途重試。
3. 模擬檔案過大，說明為什麼應簡化操作或選擇相容媒體，同時保留所有驗證。

檢驗學習成果

指出每個設備確認了哪個階段，例如讀取、寫入、驗證、接收或回覆收件確認。

常見問題

雜湊值或複製時的 OK 能證明比特幣收款方正確嗎？不能。必須在簽署裝置上核對交易及其輸出。

暫停點

取下並收好備份卡，清楚標明傳輸媒體。

Original 顯示已將回應寫入卡片。還要做什麼，才能說 Desk 已收到？

1. 把卡片塗成別的顏色。
2. 建立新種子。
3. 經相應流程讀取回應並在 Desk 中驗證。

> **查看答案: 經相應流程讀取回應並在 Desk 中驗證。**
> 成功寫入與成功接收是兩個不同事件。

公共服務商與自有節點

學習目標

選擇查詢來源，了解它可能洩露哪些資料以及它的限制。

理解概念

Desk 可查詢相容的公共服務商，或由使用者設定的 Bitcoin Core。服務商能看見收到的查詢、查詢順序與連線資料。不傳送完整 xpub 可減少一種暴露，但對方仍可能把不同腳本或其雜湊值關聯起來。

Desk 9.21 除 REST 選項及自有節點外，也能明確選擇經 TLS 使用 Blockstream Electrum。TLS 可防範部分網路觀察者，但服務商本身仍會收到查詢。沒有能保證匿名的背景自動輪替。選擇前應了解為方便而付出的隱私代價。

使用 Core 時，依相應指南設定端點、驗證及觀察錢包。不要公布 RPC 連接埠，也不要為了讓應用程式「找得到」就將連接埠開放至網際網路。僅允許受信任環境存取，使用適當的安全傳輸方式。不要向導師唸出 RPC 密碼。

初次同步及重新掃描可能耗時。進度表示工作正在進行，不代表已成功。Desk 會在背景繼續，關閉檢視不等於停止節點。文件所列的最小歷史掃描區間無法保證找到更早的活動。如果錢包更舊，請查看匯入日期與實際掃描範圍。

地址探索依據歷史紀錄，不以餘額是否大於零判斷。已全部花光的地址仍是使用過的地址。已審查的多重簽章流程會就每個分支和參與者，檢查連續 20 個沒有歷史紀錄的地址間隔，並受地址產生上限約束。不要將某個總上限套用至所有錢包。

練習

1. 為練習選擇查詢來源，並說明它能看到什麼。
2. 檢查上次同步日期、網路與進度。遇到 HTTP 429 時應等待，不要在未主動決定的情況下更換服務商。
3. 模擬一個餘額為零但有舊交易紀錄的錢包，確認「零餘額」與「未使用」有何不同。

檢驗學習成果

判斷資料來源能否滿足驗證與隱私需求，並識別尚未完成的狀態。

常見問題

使用自有節點就能匿名嗎？不能。它可減少對外部查詢的依賴，但仍須考慮連線、交易對方、廣播與其他中繼資料。

暫停點

只記錄服務商類型以及是否仍需完成掃描。

某地址曾收款且已花完，現在餘額為零。探索錢包時應如何處理？

1. 當作有歷史紀錄的地址。
2. 當作從未使用的地址。
3. 當作無效地址。

> **查看答案: 當作有歷史紀錄的地址。**
> 是否使用過取決於歷史紀錄，而非當前餘額。

M06

接收比特幣與核對地址

學習目標

建立接收請求，並在交付之前檢查。

理解概念

開啟正確的 WOW 帳戶，並確認網路和政策。建立或恢復接收請求。您可以為您的組織新增動機、觀察員和預期金額。這些欄位描述了您的本地資訊；預期的金額不會阻止任何人傳送其他金額。

透過裝置上的流量和 錢包 背景來檢查地址。如果這條路線在您的組合中尚未被物理證實，那麼實踐在收到重大資金之前將繼續進行模擬並擴充套件。比較兩個由相同的源源驅動的螢幕，不會帶來獨立性，它不存在。

使用新地址為新收費關係，當流量允許時。在修訂的多重簽章中，已顯示的地址不會重新簽名或終止，因為付款人可以隨後使用。到達未經歷史的新連續地址的邊界時，您可以恢復適當的預先請求，並瞭解邊界的理由；沒有折扣指數。

分享後，請在您的驗證來源中檢視輸入。電子郵件、交易所證書或支付者的捕獲不顯示清算。根據展覽，檢查網路、txid、輸出、值和確認數。不要為您的舒適度開設一個公共瀏覽器，如果您的計劃要求保持這些私人查詢。

練習

1. 它在實驗室中建立了一個請求，審查了帳戶和網路，並解釋瞭如何檢查地址。
2. 記錄一個虛擬標籤，並在關閉檢視後恢復相同的請求。
3. 它模擬了不同金額的收費，並決定如何將其平衡，而不會改變歷史。

檢驗學習成果

您可以區分所產生的地址、驗證的地址、共享請求和確認收費。

常見問題

一箇舊的地址在建立另一個時會停止執行嗎？通常不。保持發現和註冊申請，避免失去遲到的支付的可見性。

暫停點

保留實驗室請求的狀態，而不是導師中的內容。

付款人傳來一張寫著「提領完成」的截圖。接受收款前要查什麼？

1. 只看截圖畫質。
2. 在可靠網路來源查核對應輸出及所需的確認數。
3. 付款人的密碼。

> **查看答案: 在可靠網路來源查核對應輸出及所需的確認數。**
> 商業憑證或截圖無法取代付款驗證。

M06

標記、凍結與選擇 UTXO

學習目標

準備輸入不混合起源的意外。

理解概念

標籤可以保留鏈上不包含的背景：起源、對手、目的和使用限制。在 Desk 中，UTXO 標籤和地址標籤可能有不同的長度和功能。標記“客戶A”是有用的；使用您的檔案或全名可以建立一個不必要敏感的記錄。

冷凍UTXO在Desk將其排除在某些地方選擇中。它不會阻止您的 比特幣 支出，也不會改變指令碼，也不會阻止其他 金鑰 應用程式使用它。它還可以使總和可支付的平衡有所不同。檢查貨幣是否被凍結，被刪除機預訂或實際上被花費。

自動選擇根據演算法和背景最佳化；不一定知道您的私人關係。對於具體付款，檢查是否適合使用從同一背景中輸出，而不是結合儲蓄、工資和商業活動。有用的分離需要未來一致性，不僅僅是美麗的標籤。

以 BIP329 格式出口標籤，可以輕鬆儲存或遷移。格式不算單獨。Desk 提供 加密 包裝，以便出口；區分保護的檔案與相容的平板文字。在進口時，檢查與錢包和冷凍處理相匹配，然後提交資訊。

練習

1. 將三個虛構 UTXO 分別標為儲蓄、業務活動與捐款。
2. 冷卻一個，並檢查觀察和可選的平衡之間的差異。
3. 以 密碼 匯出實驗室標籤，以影印件匯入並審查結果，沒有真實的私人資料。

檢驗學習成果

根據成本和曝光，可以選擇輸入。冷凍是當地的優先事項。

常見問題

一張標籤在付款時乘坐收款方嗎？不是因為它只是一個地方標籤。您可以透過輸出、共享檔案、使用其他服務或將其新增到郵件中進行過濾。

暫停點

保留實踐標籤和凍結狀態。

在 Desk 凍結 UTXO 的效果為何？

1. 在網路上建立共識層級鎖定。
2. 將它轉移至特殊帳戶。
3. 依應用程式規則限制本機選擇該輸出。

> **查看答案: 依應用程式規則限制本機選擇該輸出。**
> 不會撤銷其他金鑰副本的花費能力。

準備與核對付款

學習目標

建立自己看得懂的 PSBT，辨明所有成本與輸出。

理解概念

選擇帳戶、可花費輸入、收款方及金額。核實請求來源。貼上或掃描後核對完整地址與網路，剪貼簿內容和圖片都有可能被替換。流程若允許完整核對，就不要只看頭尾字元。

選擇費率，核對手續費總額、估計大小、總額與找零。選「傳送全部」時，Desk 會從可用金額扣除手續費。若由聊天發起付款且淨額不足以支付請求金額，應明確決定是否部分付款；原請求不會被更改以隱藏差額。

查看找零是否過小，或是否沒有找零輸出。應依錢包政策核實標示為自己的輸出，不可只相信協調方給的名稱。找零無法成立時，請重新檢查全額轉出安排，或加入相容輸入；切勿讓剩餘金額在不知情的情況下變成過高手續費。

PSBT 是傳輸資訊及簽章的格式，本身不保證隱私或來源真實。它可能包含先前交易、公鑰、路徑及中繼資料。已審查的 Final 韌體多重簽章設定檔使用 PSBT v0/BIP174。「交易版本 2」不等於「PSBT 版本 2」。

練習

1. 在模擬器中建立一筆付款，輸入 120,000 sat，收款額 70,000 sat，手續費 1,000 sat。
2. 列出所有輸出，說明 49,000 sat 找零如何得出。再用全額轉出重做一次。
3. 取消草稿，說明在本機取消的是什麼。不得使用此模擬器簽署或廣播任何交易。

檢驗學習成果

匯出前，能說明輸入、輸出、收款方、成本以及仍缺少的授權。

常見問題

能傳送畫面上全部餘額嗎？只有應用程式能算出可行的實收金額並足以支付手續費時才可以。顯示餘額可能包含無法使用的資金。

暫停點

儲存練習草稿或將其取消，切勿把真實 PSBT 存入課程網站。

螢幕顯示「transaction version 2」。這能證明檔案格式是 PSBT v2 嗎？

1. 不能，這是不同的版本欄位。
2. 能，一定是。
3. 這能證明它使用 Taproot。

> **查看答案: 不能，這是不同的版本欄位。**
> BIP370 區分容器版本與交易版本。

使用 Original 與 BIT 簽署

學習目標

完成各機型的簽署流程，確認收到的回應對應正確操作。

理解概念

Original：使用 Cuvex Mirror 與相容流程所用的傳輸卡遞交 PSBT。在裝置上讀取請求，提供密文並私下解鎖。核對所有輸出、金額、找零與手續費。裝置將回應寫入卡片後，還須在 Desk 中讀取並驗證。寫卡成功不能取代傳回這一步。

BIT：選擇正確磁碟區，透過 USB-C 遞交請求。你操作裝置時，Desk 的本機服務會處理預定的資料交換。依螢幕指示提供密文，並在 BIT 上核對。「從 BIT 接收」會匯入回應；Desk 驗證並儲存後才確認收件。若斷線，應恢復同一筆操作，不可用外觀近似的另一筆代替。

使用 Final 韌體進行多重簽章時，必須核對摘要、必查的輸出、適用的警示，並完成「簽署 PSBT」的三次最終確認。選用的進階檢視可查看其他參數；選「否」不會略過必查項目。獨立驗證政策是另一個流程，其結論僅限於該次核對範圍。

簽署需要相容、且可驗證真實性的密文。舊備份即使仍可復原祕密，也不因此取得簽署資格。若裝置警告舊副本未通過真實性驗證，先依流程復原並核對祕密，建立新副本後再簽署。勿竄改標頭或繞過拒絕。

地址不一致、手續費非預期、資訊不足、出現其他網路或裝置拒絕政策時，請取消操作。不要因通話即將結束而勉強核准。AI 不會按鍵、不會完成最終確認，也不能將你尚未核實的操作宣告為已簽署。

練習

1. 用無資金的錢包或已通過實機驗收的實驗室環境，走過所用機型的流程。
2. 模擬在最終確認前停止，說明這與授權有何不同。
3. 檢查回傳是否成功、是否對應原始草稿；使用 BIT 時，也要檢查接收與收件確認狀態。

檢驗學習成果

在不揭露憑證的情況下敘述流程，並區分裝置上的核准、已匯入的回應與已發布的交易。

常見問題

離線裝置知道我的輸入是否仍未花費嗎？它無法獨立查看區塊鏈現況。應用程式必須透過其網路資料來源驗證最終交易。

暫停點

若中斷簽署，請依流程取消，或保留標識清楚的待處理操作，並避免顯示祕密資料。

BIT 已簽署，但 Desk 未確認收到。應將操作視為什麼狀態？

1. 付款確定已發布。
2. 回應待接收或待驗證，應恢復同一筆操作。
3. 錢包已遺失。

> **查看答案: 回應待接收或待驗證，應恢復同一筆操作。**
> 簽署、接收與發布是不同階段。

M06

完成交易、廣播與排除問題

學習目標

關閉支付週期，而不重複，並按步驟診斷故障。

理解概念

進口簽名後，Desk必須檢查它是否符合刪除器，並保留意圖。在多重簽章可能缺乏邊緣；在單一證據中，進口的簽名也不會免於審查。完成產生交易準備發行，當您的條件已經完成。

只有在最終審查後才釋出。伺服器或txid的答案顯示了該請求的結果，但跟蹤必須確認接受和連結。如果應用程式沒有收到回覆，請在重複之前查詢。不要發明新的付款來解決檢視問題。

對於即將付款，請檢視 RBF 的價格、有效性、衝突和實際可能性。如果有政策變化或收款方,新提案需要新的簽章適當。取消本地不會破壞其他人已經保留的簽名或交易；也不會取消確認的。

按階段診斷：準備、運輸、解鎖、審查、簽名、返回、驗證、完成、傳播和確認。記錄系統、版本、模型、階段、約時間和錯誤程式碼。該應用程式的診斷是為了刪除敏感資料，但在分享之前檢查它們，並避免新增副本，QR,金鑰聊天或認證。

練習

1. 訂購虛擬付款狀態，並確定您將安全休息的地方。
2. 解決了三個事件：不夠的平衡，USB回覆沒有收到，連線中斷的釋出。
3. 編寫一張票，使用合成資料和可驗證的預期結果。

檢驗學習成果

您可以決定是否缺乏學生、裝置、協調員或網路的行動，並避免第二次不必要支付。

常見問題

FIRMWARE_CAPABILITY_REQUIRED 錯誤是透過將 韌體 轉換為盲目的嗎？不。在 Desk 記錄的事件中，最終構建的認可需要修復 Desk 目錄。在更改裝置之前，請檢查版本和個人資料。

暫停點

保持狀態和下一個行動。如果您在實驗室外發布了實際操作，則將其記錄在您的私人檔案中。

以下哪個動作本身能撤銷已確認的交易？

1. 刪除本機草稿。
2. 關閉 Mirror。
3. 以上皆不能。

> **查看答案: 以上皆不能。**
> 刪除本機紀錄不會改寫區塊鏈或撤回已在流通的授權。

M07

比特幣上可觀察到什麼

學習目標

辨識公開資料、推論，以及你在鏈下額外提供的資訊。

理解概念

比特幣鏈上的資料是公開的。可分析腳本及可表示為地址的資料、金額、輸入與輸出的關係，以及交易在區塊中的位置。鏈上不一定有你的姓名，但經身分識別的購買紀錄、公開的發票或分享過的地址，都可能將你與這段歷史相連。

假名性表示使用不直接代表法定身分的識別碼。匿名則要求在某個群體和條件下無法區分個人，單純安裝應用程式無法達成。隱私取決於情境：商家知道你的付款，交易所可能知道你的提領，伺服器看見查詢，現場的人可能看見你的裝置。

區分事實與推論。「這筆輸出在該交易中被花費」可在鏈上驗證。「這些輸入全部屬於同一個人」只是可能失準的經驗法則。鏈下取得的身分資料能提高某個假設的可信度，但不會讓所有解讀都成為定論。

重複使用地址，讓活動更易彙整。合併不同情境的 UTXO 可能建立關聯。揭露 xpub 比提供單一地址讓他人看見更多。分享 txid 時，收件人也可能看到他原本不必知道的其他輸出與關係。

練習

1. 在虛構交易中標出哪些資料公開，哪些標籤屬於你自己。
2. 加入一張具名發票，描述新出現的關聯。
3. 寫一則足以處理錯誤的支援請求，不要附上地址、描述符或餘額。

檢驗學習成果

指出「這是可觀察的」或「這是推測的」，並解釋仍缺哪些證據。

常見問題

從不重複使用地址就能匿名嗎？不能。輸入選擇、找零、查詢、交易對方與其他中繼資料仍有影響。

暫停點

保存一份觀察者關係圖，不含真實身分或交易。

通常哪項資料可供觀察同一帳戶的一整組地址？

1. 圖示的顏色。
2. 該帳戶的 xpub 及足夠的衍生資訊。
3. 連接線的品牌。

> **查看答案: 該帳戶的 xpub 及足夠的衍生資訊。**
> 擴展公開資訊即使本身不能授權花費，仍屬於隱私敏感資料。

區分使用情境與管理找零

學習目標

做出與您的 UTXOs 的起源一致的支出決策。

理解概念

背景分離在付款之前開始。決定接收是否符合節約、職業活動、日常支出或具體關係。將此資訊保留在私人標籤中，以免未來的選擇因未知而刪除。

標籤不會加密分離輸出。如果您將兩個不同背景的UTXOs花在一起，交易將公佈其關係。固定將減少未來支付的輸入數量，但增加了固定輸出之間的聯絡。使用 手續費 低可以是有效的，同時反對您的隱私目標。

變革是由同一政策控制的新出口，而不是“看不見的錢”。其後續使用可能延長以前的關係。不要將地址標記為變更，因為它有一個奇怪的金額；在一個真實的審查中，裝置必須檢查它屬於錢包。

避免將隱私轉化為重複的數量、時間或轉換的機械模式。這些模式也可以識別，併產生更多的手續費。評估各方所知道的資料，以及建議行動將釋出哪些新資訊。沒有一個序列可以刪除已釋出的故事。

練習

1. 建立五個三個背景的UTXOs幻想，並準備一個支付，使用最少需要的背景。
2. 確定結果的變化，並決定如何標籤它。
3. 比較所有輸出的成本和曝光，以保持它們分開。

檢驗學習成果

您可以以某種具體的理由證明或拒絕一項鞏固，而不適用於任何情況的絕對規則。

常見問題

把一切轉向另一個方向打破了我的歷史嗎？不。轉賬釋出了額外的關係，並且可以新增成本，而不會解決您的威脅。

暫停點

保留實驗室的合理性和選擇的選擇政策。

將薪資與捐款的輸入併入一筆交易，可能造成什麼後果？

1. 讓人看見這些輸入之間的關聯。
2. 消除其公開來源。
3. 將其變成保證匿名的現金。

> **查看答案: 讓人看見這些輸入之間的關聯。**
> 減少 UTXO 數量可能增加外界可察覺的關聯。

M07

網路隱私、Tor 與 VPN

學習目標

將連線隱私與連結隱私分開。

理解概念

查詢伺服器可以將請求與連線相關聯。您的網際網路服務提供商可以根據運輸方式觀察目的地或模式。VPN 將某些信任轉移到 VPN 運營商身上；它不會刪除 比特幣 的公共資訊，也不會阻止已識別的帳戶識別您。

Tor 經其網路轉送流量，以減少來源與目的地之間的某些關聯。它不會使比特幣地址變成私人資料，應用程式的流量若未經 Tor，也得不到其保護。開啟 Tor Browser 不會自動設定 Desk、Bitcoin Core 或電腦上的所有服務。

在確認連線已被保護之前，您必須檢查路徑和設定。在此基礎上，沒有一個Tor整合的Desk交換機。使用節點 或 Proxy 的播放需要工程指南和真實流量驗證。沒有一個介面欄位被髮明，因為另一個錢包欄位有它。

還有DNS的漏洞，帳戶同步，瀏覽器連結和價格服務。一個圖表可以保護儲存查詢，並在開啟公共探測器時繼續披露活動。定義每個措施的範圍和連線故障行為；避免對一個不那麼私人供應商進行沉默的變化。

練習

1. 列印您的計算機路線，連線提供商，如果有，節點或服務和比特幣網路。
2. 說明誰接收查詢，誰看到你的商業身份。
3. 模擬，私人節點不響應。決定停止或明確地改變來源，瞭解曝光。

檢驗學習成果

您可以解釋哪些威脅會降低您的設定，以及哪些威脅仍然存在。

常見問題

Tor 是否保證沒有人可以與我聯絡付款？不。對方、商業識別、模式和操作錯誤可能會繼續連線它。

暫停點

記錄設計的範圍，沒有私人端點或密碼。

開啟 Tor Browser 會強制 Desk 透過 Tor 查詢嗎？

1. 會，因為兩者共用電腦。
2. 會，只要看得到圖示。
3. 不會。須分別設定、檢查每個應用程式的路徑。

> **查看答案: 不會。須分別設定、檢查每個應用程式的路徑。**
> 一個應用程式的保護不會自動延伸到其他程式。

CoinJoin、Payjoin 與目前限制

學習目標

理解合作工具，不給他們匿名或不存在的相容性。

理解概念

CoinJoin在交易中收集了多個人的貢獻，以便對輸入和輸出的某些結論變得困難。這並不意味著將貨幣交給保鏢服務，承諾將其他貨幣交回。不同的設計需要重新調整協調，保管,手續費,對惡意參與者的抵抗和後續治療。

Payjoin 將 輸入 的付款人和收件人納入合作付款，從而削弱了一些共同所有權的虛擬化。它需要在兩端相容的支援和一個具體的協議。它是技術理解材料：在審查的來源中沒有認可Payjoin或CoinJoin流，並在Cuvex Desk中進行整合和操作。

服務供應與法律背景會變動。Wasabi 文件記載 zkSNACKs 協調器於 2024 年 6 月 1 日關閉，不能用舊按鈕推斷今天仍保證提供服務。美國司法部在 2025 年公布 Samourai 創辦人認罪及其後判刑的消息，不能據此認定任何司法管轄區的所有隱私技術一律違法。

一個工具可以減少一個 inference 並留下另一個 intact。已識別的起源不會從對方的記錄中消失。隨後的重新組合、中繼資料和參與者組的故障可能會破壞隱私。此外，某些服務可以應用不同的交易政策，以換取具有特定歷史的貨幣。

練習

1. 比較一個流行的交易，一個合作伙伴和一個接收保管的服務，而無需進行實際交易。
2. 對於具體的工具，請在提議使用之前搜尋版本、維護器、服務狀態和當前檔案。
3. 保管的技術和法律風險分別識別。導師不應該設計逃避控制，也不應該承諾“無法追蹤的資金”。

檢驗學習成果

您可以解釋一個有限的優勢和至少兩個風險或隱私技術的要求。

常見問題

Cuvex需要一個混合器來服務於私人保管嗎？不。查詢控制、資料、金鑰和UTXOs的選擇已經解決了具體的風險，沒有承諾完全隱藏。

暫停點

它將一個工具列為“研究”，而不是沒有證據的“相容”。

哪一項說法站得住腳？

1. CoinJoin 保證永久匿名。
2. 協作技術可使某些推論更難，但有前提也有限制。
3. 凡稱為混幣器的服務都能維持自我保管。

> **查看答案: 協作技術可使某些推論更難，但有前提也有限制。**
> 特性取決於協定、實作、參與者與後續使用方式。

從真實事件學到的教訓

學習目標

從有記錄的事件中提出可核實的做法，不攻擊競爭品牌，也不誇大保護效果。

理解概念

Mt. Gox：美國司法部 2023 年的起訴書描述伺服器及金鑰遭未經授權存取，之後客戶資金消失。起訴書是指控，不是判決。保管人應能回答誰實際控制金鑰，以及公司倒閉會發生什麼事。

Ledger Connect Kit，2023 年 12 月：Ledger 記錄前員工存取權遭入侵後，供去中心化應用使用的程式庫被惡意發布。攻擊波及軟體供應鏈，使 EVM DApps 使用者受騙簽署。它不能證明 Ledger 硬體或比特幣共識遭破解。

Bybit，2025 年 2 月：FBI 將約 15 億美元虛擬資產失竊歸因於北韓。事件涉及交易所與其他網路的資產，並非比特幣密碼學遭破解。應核對簽署意圖，避免多人盲目信任同一螢幕。

Coinbase，2025 年 5 月：該公司表示客服人員被收買竊取資料，供社交工程使用，並表示密碼及私鑰未暴露。對方縱使知道真實資料，也可能仍是詐騙者。

Bitcoin Core 也會公布軟體缺陷。CVE-2024-35202 公告指出，早於 25.0 的版本可能被遠端觸發關閉。驗證規則不能取代軟體維護，該公告也不能證明金鑰遭竊。

2026 年 1 月，The Register 報導 Ledger 買家的訂單及聯絡資料經 Global-e 外洩，並引述兩家公司確認。依其聲明，復原金鑰未受影響。硬體即使未遭攻破，購買紀錄仍可能揭露你持有該裝置。

2026 年 4 月，The Record 報導 Drift 遇襲，平台宣布暫停存提款。Drift 是 Solana 上的去中心化金融協定，並非比特幣遭破解。初估損失及後續追回程序不能視為最終數字或退款保證。

練習

1. 依保管、介面或散布管道、個人資料、其他網路的協定及可用性，將各事件分類。
2. 為每個事件提出一項預防措施，以及該措施的一項限制。
3. 演練詐騙來電：「我知道你買了什麼，把資金轉到這個安全地址。」掛掉後，透過你自己主動聯繫的管道查證。

檢驗學習成果

解釋為什麼這些事件都不能證明另一品牌無懈可擊。證據只支持特定範圍的結論。

常見問題

這是最新全部駭客事件嗎？不是。這是為 2026 年 11 月 17 日版核實選錄的案例，並非完整清單或即時監測。

暫停點

寫下準備改變的習慣，以及日後如何確認自己持續實行。

對方知道你的購買紀錄，要求把錢轉到「救援錢包」。對方知道你曾購買能證明什麼？

1. 這可能是外洩資訊，不能驗證對方身分或地址。
2. 對方一定是合法客服。
3. 你應該分享種子。

> **查看答案: 這可能是外洩資訊，不能驗證對方身分或地址。**
> 真實資料也可能被用來營造可信的騙局。

M08

建立聊天身分與驗證聯絡人

學習目標

啟用一個聊天身份，而不顯示你的金鑰,並檢查對方。

理解概念

在 Desk 中，聊天將與 密文 連線到 金鑰 透過 Cuvex 建立的聊天。雖然它的代表性可能看起來像一個xpub,但它是秘密的，並且不應該被視為一個WOW帳戶的公鑰。導師 從來不需要在 QR 上閱讀或看到它。

流區分新 alias 和轉移或恢復一個現有。在審查的實施中，選擇相應的 iOS 或 Android 移動個人資料，因為歷史產生的身份不因直覺而可交換。DEV和生產是不同的環境：改變環境不會自動轉換對話或字串。

新增一個標籤不驗證身份。透過一個獨立和認證的頻道檢查印刷。如果應用程式提供認可問題，則使用不公開的資訊，並避免顯示 密碼 的答案。熟悉的聲音可以被模仿；在危險情況下，它結合了預先達成的方法。

如果您更改聯絡人的身份，請停止支付和協調，直到解決。它可以是合法的恢復或惡意替代。端到端的加密根據其協議和實施，保護一個頻道，但它並沒有證明誰正在使用另一邊的裝置。

練習

1. 在一個測試環境中，它解釋了建立或恢復的流動，而不提供金鑰聊天。
2. 新增一個實驗室聯絡，並透過另一個頻道進行痕跡驗證。
3. 模擬了身份變化。確定如何在付款之前確認交換。

檢驗學習成果

您可以區分名稱，公共印記，金鑰秘密聊天和人對一個人的信任。

常見問題

一個古老的 alias 保證它是相同的人嗎？不。金鑰的連續性和變化必須根據流量進行驗證。

暫停點

只註冊“驗證的測試聯絡人”和方法，沒有金鑰或私人問題。

某字串標為「聊天金鑰」，外觀與 xpub 相似。Desk 如何看待它？

1. 可貼到論壇的公開資料。
2. 用以復原身分的祕密。
3. 比特幣收款地址。

> **查看答案: 用以復原身分的祕密。**
> 外觀格式不決定資料的機密性或用途。

M08

透過聊天請款與支付聰

學習目標

從談話轉換到付款，而不會失去審查或背景。

理解概念

聊天可以要求地址，用收款地址回覆，請求付款，並從WOW帳戶開啟準備。在頻道中保持背景會減少在應用程式之間複製資訊的錯誤，但不會將每個訊息轉化為有效的支出順序。

在回覆或支付之前，請檢查已驗證的聯絡人、網路、金額和原始請求。共享表格保留 UTXOs 和 手續費 的選擇。如果郵件要求一筆錢，並選擇“傳送總額”，則手續費之後的淨值可能低；必須在適當情況下被確定為部分支付。

許可證仍然在Cuvex。聊天帶來意圖和協調；沒有自動簽名的許可。向聯絡人傳送的付款確認必須區分您已收到確認交易的資訊。接收者可以透過自己的賬戶或來源進行驗證。

外部連結、附件 QR 碼及地址在驗證前一律視為不可信。「在 Mempool 查看」可能開啟第三方服務並揭露查詢。若政策使用自有節點，優先在 WOW 以相容方式驗證，並評估每次連往公共服務的影響。

練習

1. 它代表兩個角色：接收器請求50.000 sat;付款人準備不釋出。
2. 模擬一個可用的淨平衡為48.000 sat.解釋是否缺乏部分付款的同意和和解。
3. 故意在測試訊息中更改網路，並停止流動。

檢驗學習成果

您可以跟蹤請求、地址、刪除、簽名和確認之間的關係，而不會將其縮小到“聊天說OK”。

常見問題

從聊天中傳送 sats 意味著使用 Lightning?不。文件的WOW流準備比特幣連鎖支付。“Sats”一詞是指一個單位，而不是一個運輸網路。

暫停點

取消實驗室刪除器或記錄狀態；不要釋出以證明介面。

聊天中收到確認訊息。要確認收款，決定性的查核是什麼？

1. 訊息圖示是綠色。
2. 對方說「已確認」。
3. 使用適當網路來源核對交易及其輸出。

> **查看答案: 使用適當網路來源核對交易及其輸出。**
> 訊息狀態不等同於交易狀態。

M08

審慎分享密文

學習目標

瞭解什麼意味著將加密副本交給另一個人。

理解概念

共享一個 密文 傳輸一個 加密 物件的副本。它不必傳送比特幣,也不必單獨插入新簽署者。如果接收器還獲得了足夠的開關，則可以按照計劃訪問內容；因此，您必須提前決定您正在轉移的容量。

聊天端到端的加密和檔案端的加密保護了不同的層。一旦下載，接收器可以將物件留在聊天室外。刪除您的郵件或本地登記不會保證您將取消所有副本。同一頻道共享的密碼可以將元件集中在一個路徑上。

在傳送之前，請檢查身份、格式和目的。如果應用程式允許將收到的 密文 連線，則組織一個影印件，不確認任何檔案是安全的 解密。不要使用需要在外部頁面上輸入 種子 或 密碼 的附件。

恢復需要一個操作協議：誰保留每個元件，誰可以開啟它，如何檢測到曝光，以及如何在關係結束時改變保管。通常只需有效的地址來支付，您不需要共享您的 密文。

練習

1. 設計從加密教學文字轉移到實驗室接觸。
2. 列出接收器在瞭解密碼之前和之後會做些什麼。
3. 她說，關係結束了。解釋為什麼刪除郵件不會取消複製或金鑰。

檢驗學習成果

您可以區分“我分享了資料”，“我共享了訪問一個秘密”和“我確認了支出”。

常見問題

加密 檔案是否可以流動，沒有任何後果？它可以揭示中繼資料,方便密碼的嘗試，並無限儲存。他們認為我們需要分享。

暫停點

不要在課堂上留下保管附件。只記錄了年度結論。

透過聊天分享密文等於發送比特幣嗎？

1. 不等於。傳送的是物件，其內容與存取權另有範圍。
2. 等於，只要檔名以 .bin 結尾。
3. 會自動啟用新的多重簽章錢包。

> **查看答案: 不等於。傳送的是物件，其內容與存取權另有範圍。**
> 傳送祕密資料與移動 UTXO 是不同操作。

M08

復原聊天與理解其中繼資料

學習目標

計劃更改裝置，並分開身份和訊息恢復。

理解概念

Desk 表示，歷史和會議被編碼為本地，並且不構成其全球副本的一部分。金鑰 聊天可以恢復身份；不保證恢復所有舊的聊天。該應用程式包括持續啟動狀態和操作，金鑰維護和當有相容材料時的本地恢復。

每個標籤必須按審查的基準同時在一個裝置上使用。不要同時在兩個裝置上啟動“測試同步”，如果使用不受支援。轉移必須遵循程式，並確保與聯絡的連續性。

“被拘留”，“伺服器接受”，“接收”和“無法解密”描述不同的階段。未經確認的發貨不會自動向盲人傳送：首先要解決是否到達。如果沒有一個金鑰的登入或更改身份，保持即將到來的訊息不等於閱讀。

加密 內容不一定隱藏時間、大小、交付關係、標籤或連線資料，而不是所有相關係統。在聲音中，發生了類似的事情：運輸的加密不會將傳統的通話變成一個適合秘密的頻道。使用所需的最小資料來學習和解決事件。

練習

1. 模擬失去PC,並解釋什麼恢復每個可用的材料。
2. 列出郵件狀態，並決定什麼時候不應該重新傳送付款請求。
3. 準備一個裝置更改通知，以便聯絡人可以透過獨立頻道進行驗證。

檢驗學習成果

你可以解釋什麼會談會失去，什麼身份可以恢復，而不會承諾備份不覆蓋的恢復。

常見問題

浪費當地聊天也會在另一端刪除郵件嗎？你不應該承認。接收器可以獨立儲存郵件和檔案。

暫停點

保留一個空域名稱的轉換計劃，沒有金鑰聊天。

依已審查的指南，單靠聊天金鑰可確保什麼？

1. 在任何電腦還原全部舊對話。
2. 可用相容流程復原身分，但不能保證找回所有舊訊息。
3. 自動取得聯絡人的比特幣金鑰。

> **查看答案: 可用相容流程復原身分，但不能保證找回所有舊訊息。**
> 身分復原與還原歷史檔案是不同能力。

M08

日常設定與權限審查

學習目標

控制 Desk 引數，而不會混淆舒適與保護。

理解概念

Desk提供主題夜晚，日或系統；自動同步和時間為3或5分鐘；交易聲音；聊天背景；語言和匯率。這些偏好會改變演示或查詢頻率。他們不會改變比特幣的簽名，也不會新增匿名。

修訂的安全設定允許因不活躍而阻止，在轉到背景時阻止，故障後最大延遲和可選刪除。因不活性計劃允許的間隔為 30 到 86.400 秒；介面 可以提供更合適的選項。預設值必須從您執行的版本中閱讀，而不是由錄製的類所假設。

比特幣 連結整合：開啟一個請求解鎖，選擇帳戶和審查。不允許自動支付。在Linux,指南區分整合安裝和AppImage記錄連結。Lightning 發票 需要不同的相容流量；它不會透過宣告 Desk 預定應用程式來解決。

報價,價格圖和資訊連結可以檢視外部服務。它的功能是資訊，而不是購買訊號。在使用資料之前，請檢查日期和來源來翻譯金額。黑暗模式或小視窗不應該隱藏終端按鈕，地址或手續費;如果發生，休息並報告地質問題。

練習

1. 在學習庫中調整外觀和封鎖。你可以再進去吧。
2. 檢視哪些動態自動化：韌體的同步、聲音和驗證並不相同。
3. 開啟一個虛構的連結請求 比特幣:並在準備任何實際操作之前取消。

檢驗學習成果

您可以解釋每個調整的效果，並找到涉及敏感查詢或行動的效果。

常見問題

生物辨識的PC是否取代了我的恢復副本？不。它可以依賴於系統的裝置和安全儲存。保持獨立的恢復。

暫停點

點選 Desk 並記錄您改變了哪些偏好。

選擇每三分鐘同步一次會改變什麼？

1. 該功能執行時的預定查詢頻率。
2. 鏈上簽章政策。
3. 裝置的種子。

> **查看答案: 該功能執行時的預定查詢頻率。**
> 這是操作偏好，不改變保管模式。

M09

設計多重簽章錢包

學習目標

選擇能抵禦合理預期的金鑰遺失與外洩情況的門檻。

理解概念

在 N 取 M 政策中，N 是持有不同金鑰的參與者人數，M 是所需簽章數。3 取 2 可容忍一把金鑰無法使用，但兩把金鑰遭入侵即可授權花費。三份種子若放在同處，或同時暴露，獨立性就會降低。

已審查的 Cuvex 多重簽章設定檔使用原生 P2WSH、sortedmulti 與 BIP48 衍生。Original 的政策結構最多容納六把金鑰，BIT 最多十五把。兩者同時參與時，流程須遵守較受限之參與者的限制與傳輸媒體的實際容量。結構上限不保證帶有很多金鑰與輸入的政策一定裝得下。

應用程式支援的門檻須符合政策中的數量關係。N 取 1 不需合作即可花費，韌體保留此項專門警示。提高門檻也會增加協調、成本、復原材料與無法存取的風險。

MuSig2 是不同的 Schnorr 簽章聚合方案，本身為 N 取 N，並非任意 5 取 3。所研究的 Final 韌體未實作 Taproot 輸入簽署、MuSig2 或 Miniscript。能付款至 P2TR 地址不代表能從 Taproot 錢包簽署支出。

練習

1. 設計一個虛構的 2 3 與每個參與者獨立的風險。
2. 模擬失去一個金鑰和承諾一個。解釋什麼可以和什麼不能做。
3. 在選擇更大的政策之前，請檢查模型限制。

檢驗學習成果

您可以表達對損失的寬容、攻擊邊緣和共享依賴於您的設計。

常見問題

多重簽章 是否要求人們瞭解其他人的 種子?不。目的在於，每個人都保持自己的私有能力，並共享必要的公共資訊來構建和恢復政策。

暫停點

保持設計與虛構參與者和他們的責任。

3 取 2 政策使用獨立金鑰，需要幾把私鑰才能授權一筆有效支出？

1. 一把。
2. 兩把。
3. 一定要三把。

> **查看答案: 兩把。**
> 門檻為兩把，其他條件及驗證也必須滿足。

建立邀請與提供金鑰

學習目標

建立一個與驗證的參與者的政策，而不共享 種子。

理解概念

建立者選擇名稱，網路，M，N，聯絡人，公共資訊本身和運營條件的邀請。在修訂的計劃中，接受mainnet和regtest網路為此流，從2到15參與者在應用裝置限制之前，並從1到720小時的運營期限。不要使用這些限制作為許可，跳出能力驗證。

每位參與者核對邀請，決定接受或拒絕，並依相容流程提供自己的擴展公鑰、指紋與 BIP48 路徑。不可提供種子、私鑰、孤立地址或另一錢包的整份描述符。即使外觀看似有效 xpub，來源資訊不正確仍可能產生不同政策。

建立者協調；不取代每個簽署者的驗證。在收到資金之前，每個人都應該能夠重建並檢查相同的引數和控制地址。在聊天中接受的聯絡人並不意味著您傳送的任何政策的自動批准。

邀請的終止是應用程式的協調規則。它不會單獨更改已資助的指令碼，不會刪除其他人儲存的簽章,也不會作為共識的時間表。取消提案和從現有政策中提取資金是不同的行動。

練習

1. 在準備的regtest實驗室中，建立一個3的2提議與測試接觸。
2. 它代表了一個接受，一個拒絕和一個不正確的網路的貢獻。請確保最後一站停下來。
3. 列出每個人都必須在融資之前儲存的資料：網路、邊緣、公鑰、起源、指令碼和驗證地址。

檢驗學習成果

您可以承認一個不完整的邀請，並解釋什麼批准缺乏，而不會因為聊天存在而承擔它。

常見問題

一個終止日期使不可能花費後？不是因為它是邀請場。比特幣的暫時限制需要具體的指令碼或交易條件和實際支援。

暫停點

保留建議和即將批准的教學標識。

要加入多重簽章，文件所述流程要求你提供什麼？

1. 全體參與者的種子。
2. 任意一個收款地址。
3. 你的擴展公鑰，以及相容的指紋與 BIP48 來源。

> **查看答案: 你的擴展公鑰，以及相容的指紋與 BIP48 來源。**
> 正確的公開資料可供建構政策，無須揭露私鑰。

使用 Mirror 以任意順序核對政策

學習目標

比對完整欄位，準確了解結果能證明什麼。

理解概念

獨立驗證會呈現門檻、網路、設定檔、SIGHASH、政策 ID、第一個地址、使用者位置，以及每位參與者的資料。用途是核對意圖與一致性，不能據此假設裝置永久登錄了某項政策。文件所載的驗證範圍僅限「這次核對」。

在 Mirror 12.12 中，可先讀取 Cuvex 或 Desk 的 QR 碼，再任選一項資料。無須從第 1 步開始、掃描全部資料或依固定順序操作。若手動核對文字而未掃描，Mirror 不會將該項標示為已驗證。

比較器會呈現完整原文。空格、換行、大小寫及 Unicode 差異都會計入。「一致」只表示這一對值相同，不會驗證來源、證明兩者屬於同一政策或啟用錢包。最終核准及對應回應仍循 Cuvex 與 Desk 的流程處理。

目前 Desk 的 QR 碼僅含數值或文字，不含序號或工作階段。Mirror 不一定能推斷步驟。「指定 Desk 步驟」會加入人工指定的背景資訊，應明確標示為人工輸入。有 N 位參與者時，文件所列共有 7 + 4N 個欄位：8+4k 為指紋、9+4k 為路徑、10+4k 為 xpub、11+4k 為金鑰 ID，k 從零起算。N=2 時，第 15 步是第二把金鑰的 ID，可最先比對。

練習

1. 使用虛構資料，先比較標示為第 15 步的 ID，再比較網路與門檻。
2. 改動一個字元，確認出現「不一致」。開始比較另一對資料時，不應沿用前一次結果。
3. 比較「2 / 3」，說明為什麼光看片段文字不一定能判斷是門檻還是使用者位置。

檢驗學習成果

說明核對了哪個欄位、如何確認其背景，以及還有哪些項目待核准。局部一致不能視為整體核准。

常見問題

一定要掃描所有 QR 碼才能繼續學習嗎？不用。可以自行選擇比對項目。簽署裝置要求的核對與授權仍須依其流程完成。

暫停點

關閉比較器。依已審查的設計，離開或切換至背景時應清除所讀資料。

Mirror 比對第 15 步的兩個 QR 碼，顯示「一致」。這能證明什麼？

1. 在已識別或人工指定的背景下，這一對資料的字面內容完全相同。
2. 整項政策已核准。
3. 兩個 QR 碼的來源均已驗真。

> **查看答案: 在已識別或人工指定的背景下，這一對資料的字面內容完全相同。**
> 比對不能取代來源驗證、整體核對或硬體回應。

協調簽章與發布多重簽章交易

學習目標

帶上一項提議在簽章的邊緣，而不會失去意圖或控制。

理解概念

交易 多重簽章 指定 輸入、收款方、進口、關稅、替換和運營筆記。創作者可以向相容的參與者申請簽章。每個 簽署者 透過其網路帳戶，政策，輸入 審查，所有 輸出 和 手續費 之前在您的裝置上授權。

一份部分簽名不會單獨移動資金，如果缺少邊緣。當它達到時，協調器可以根據流量結合和完成。其他參與者或協調員的報告是協調資訊，而不是您所做的本地驗證。該應用程式必須區分這些來源。

基地提供重新嘗試、簽名接收、起訴、拒絕和協調轉讓。一個轉換不會改變金鑰或鏈條的邊緣。儲存的答案必須與已使用的請求和實際配置檔案相匹配；不選擇其他政策，因為它類似或是目錄中的第一個。

如果有人修改收款方或相關條款，你必須審查一個新的建議，並獲得相應的簽章。不要用手“調整”一個 PSBT 透過刪除安全資料，以便它在 NFC 中出現。硬體需要相容的個人資料和驗證，限制為輸入、輸出和尺寸。

在釋出之前，請確保交易已達成協議，並且沒有已傳播的版本。接下來，確認數由所選擇的來源進行。在您的應用程式中拒絕不會自動取消其他人已經儲存的簽章,也不會阻止任何與剩餘的邊緣相容的操作。

練習

1. 以三個虛構角色模擬 3 取 2。第一人簽署，第二人拒絕，第三人要求說明。
2. 更改測試支付的地址，並解釋為什麼以前的口頭批准不被重新使用。
3. 模擬簽名後失敗的指控。恢復相同的工作，沒有翻倍付款或更改個人資料。

檢驗學習成果

你可以指明誰協調，誰簽名，誰結束，以及什麼測試存在於每個階段。

常見問題

聊天中兩則「OK」等於兩份簽章嗎？不等於。須依政策取得有效密碼學授權才能達到門檻，訊息不計入。

暫停點

登記狀態，簽章持久和下一個負責人沒有私人內容。

3 取 2 的交易已有一份有效簽章，另有兩則「同意」訊息。已達門檻嗎？

1. 有，因為已有三位參與者。
2. 沒有，還缺另一份有效的密碼學簽章。
3. 協調方宣布達成時就算。

> **查看答案: 沒有，還缺另一份有效的密碼學簽章。**
> 口頭或文字同意與有效簽章是不同證據。

復原與變更多重簽章錢包

學習目標

恢復政策，並計劃失去或取代參與者。

理解概念

恢復需要兩個類別：重建政策的資料和足夠的私人能力來花費。使用 xpubs 的政策副本可以透露歷史，而不包含 種子。加密副本將新增到檔案的保護，但需要儲存您的 密碼。.cuvexms 擴充套件本身並不表明它是加密的：具體的格式和出口必須檢查。

在 Desk 9.21 中，恢復要求參與者延伸的 公鑰 帶有痕跡和從裝置上出口的 BIP48 路線。允許透過 Webcam 或 Mirror 相容流的閱讀。不要用 收款地址 替換這份捐款，也不要將 種子 傳送給支援。

如果你失去一個金鑰在一個2的3,其他兩者可以保持支出能力。以前的政策仍然是相同的；為了有效地撤回一個參與者，並建立其他金鑰,通常建立一個新的政策，並將資金轉移到必要的許可。更改一個字元或刪除一個 錢包 的 Desk 不改變現有 UTXOs。

副本必須允許重建兩個分支，並發現歷史。保留指數、傳送的請求和必要的背景，以免重複使用地址或透過不完整的掃描來解釋一個空的 錢包。恢復和重新啟動即將到來的操作必須遵守建立時儲存的個人資料。

練習

1. 透過檔案函式，匯出和恢復實驗室政策。檢查網和已知地址。
2. 模擬一個參與者的損失，並制定一個旋轉計劃，而不移動真正的資金。
3. 模擬在底部的損失。承認支援或AI不能製造缺少的簽章。

檢驗學習成果

您可以恢復測試場景，並區分恢復資訊的貨幣控制的變化。

常見問題

刪除 多重簽章 在 Desk 關閉 錢包 為所有人？不。按流量排除當地狀態。其他人和副本可能繼續保持與政策相容的能力。

暫停點

保留已驗證的副本和私人計劃；在課程中只記錄結果。

要從已存有資金的政策移除一人，只在 Desk 刪除其姓名夠嗎？

1. 夠。
2. 若也刪除聊天就夠。
3. 不夠。應規劃新政策，並在適用時經授權移動資金。

> **查看答案: 不夠。應規劃新政策，並在適用時經授權移動資金。**
> 修改本機紀錄不會改變既有 UTXO 的腳本。

M10

按既定流程更新韌體

學習目標

準備一個相容的更新，並在裝置上檢查結果。

理解概念

一個更新改變軟體的可靠性。檢查製造商的模型、硬體審查、版本、起源和驗證機制。一個完整的下載或相同的雜湊值頁面不會取代簽名和相容性驗證。永遠不要安裝一個沒有簽名的 韌體 應用程式為工程師，就像它是客戶釋出一樣。

Original 更新為 Bluetooth 在文件流中。BIT 使用 USB-C。Mirror 包含相容的準備和運輸路線。PC、手機和裝置的具體組合不會在完成物理接受此組合之前執行。Original在Windows的歷史性更新頻率需要具體診斷；沒有解決，以達到99%的成功。

在開始之前，請檢查 備份 可恢復、穩定的供應和其他操作的缺乏。根據應用程式準備官方檔案或預先驗證的副本。在發貨期間，區分傳輸、驗證、安裝、重新啟動和版本檢查。這不是最終的測試。

完成後，檢查裝置上的可見版本並記錄日期和結果。Desk 相容性目錄不會遠端測量 韌體: firmwareAttestation 仍然是虛假的。選擇終端個人資料不確認哪些位元組實際上安裝。如果更新失敗，則繼續進行記錄的恢復，並保留階段和錯誤，而不會在關鍵階段將盲目分開。

練習

1. 在測試期間檢查準備列表，而不會開始實際更新。
2. 它命令國家，並解釋為什麼“轉移”和“安裝”是不同的。
3. 編寫一個虛構的 99% 故障報告，包含模型、版本、系統、階段和最終訊息。

檢驗學習成果

您可以確定合適的物品、運輸和最終成功標準。

常見問題

我只需要更新，以便Desk錯誤消失嗎？首先要確定起源。目錄不相容性可能需要修復 Desk 並保留 韌體 已驗證。

暫停點

實際更新只會在程式的明確安全狀態中停止，而不是透過打電話結束。

Desk 的明確相容性目錄單獨能說明什麼？

1. 列出所支援的相容性參考，不會遠端測量已安裝韌體。
2. 對所有已連接裝置做過實機證明。
3. 系統毫無弱點。

> **查看答案: 列出所支援的相容性參考，不會遠端測量已安裝韌體。**
> 相容性、簽章、測量與實機驗收是不同類型的證據。

M10

遺失、故障與緊急復原

學習目標

選擇與事故相比例的恢復，並保留有用的證據。

理解概念

在事故發生前，首先分類丟失或曝光的內容：計算機、裝置、卡、檔案、密碼、種子、密語 或政策。“我不能進去”並不一定意味著“我被偷了”。如果有疑惑的承諾，不要繼續在懷疑的團隊中引入秘密。

裝置損失可以透過相容的恢復支援和認證來解決。失去計算機可能需要恢復 Desk 儲存庫，並重建觀察。失去所有的解鎖手段或所有需要的金鑰在底層下可能沒有技術解決方案。沒有AI可以保證不存在的金鑰的救援。

Desk 包含可接受格式的本地恢復和相應的恢復材料的出口。解密在PC可以揭示秘密的作業系統或惡意軟體.這是一個很好的決定：使用一個準備好的環境，可容納的材料和轉換計劃到新金鑰,如果秘密可能被打破。不要把它描述為相當於常見的Cuvex隔離操作。

如果一個種子被過濾，更改Desk 密碼不會取消這個種子.您必須評估授權轉移到新 錢包,並保護它免受可靠的裝置。避免釋出幫助攻擊者或支付承諾恢復的服務，以換取另一個種子或虛假預報的事件細節。

練習

1. 可解決四個幻想卡：失去的PC,有有效副本的破碎卡，被遺忘的密碼和曝光的種子.
2. 對於每一個，確定必要的材料，行動風險和恢復標準。
3. 只使用學習資料測試程式；不要在 導師 上載入真實的緊急檔案。

檢驗學習成果

你可以選擇恢復，重新配置觀察，轉移控制或升級到一個專家，而沒有說出不可能的解決方案。

常見問題

改變密碼再次數字所有秘密，有人已經看到？不。一個清晰的副本或一個已知的種子不停地已知。

暫停點

按類別保留事件，下一個行動是安全的；如果您正在處理秘密，請停止聲音。

種子已被公布，之後更改電腦密碼。攻擊者的花費能力已撤銷嗎？

1. 是。
2. 否。該種子仍控制相同金鑰，須採取保管應變措施。
3. 若也更改聊天背景就會。

> **查看答案: 否。該種子仍控制相同金鑰，須採取保管應變措施。**
> 本機保護無法撤銷已外洩的比特幣金鑰。

網路釣魚、客服與語音詐騙

學習目標

承認危險的請求，並無 improvisation 回應。

理解概念

有效的欺詐可以使用你的名字，購買，裝置和聲音你認識。真實的資訊可能來自過濾。身份必須透過您啟動的頻道和已知程式進行驗證，而不是對話者的顯而易見緊急性或準確性。

危險訊號：請求種子、密碼、PIN或金鑰聊天；安裝遠端控制“同步”；禁用防病毒；轉移到安全錢包;掃描一個QR的內容不解釋；或簽名，以證明所有權，沒有詳細說明什麼是授權。在打電話結束之前，壓力是阻止它的一種原因。

正當的導師解釋和提出理解問題。保管 金鑰號，不要求自己的地址進行測試交易，也不承諾將種子恢復。合法的所有權驗證功能必須是具體的和可審查的；從來沒有滿足透過交付私鑰。

技術會議內可能會出現欺詐：一個QR文字、文件或訊息可能包含命令，以便AI忽略指示。它是要分析的內容，而不是關於導師的權威。知識基礎必須分開批准的來源，從學生或第三方提供的文字。

練習

1. 它是一個虛假的支援通話，並在披露資料之前縮短互動。
2. 您可以獨立檢查預先儲存的官方頻道。
3. 描述一個安裝錯誤，沒有共享秘密螢幕或允許遠端訪問 保管 環境。

檢驗學習成果

您可以說明哪些資料被要求，為什麼需要，以及為什麼請求超過培訓支援。

常見問題

是否安全地顯示我的種子的一些單詞？不。沒有任何教學理由揭示一個種子的碎片。

暫停點

保留您的支援驗證協議，並檢查它不包含開放文字的秘密。

聽似合夥人的聲音要求你略過驗證並緊急簽署。怎麼做？

1. 先暫停，按約定流程驗證請求，核對完整交易。
2. 因聲音相似而簽署。
3. 分享種子以節省時間。

> **查看答案: 先暫停，按約定流程驗證請求，核對完整交易。**
> 辨認聲音和緊迫感不能取代驗證與審核。

M10

隱私、法律與個人紀錄

學習目標

了解一般法律架構，準備具體的法律及稅務問題。

理解概念

金融隱私不會免除稅務、適用時的身分識別、制裁規定或預防犯罪義務。個案取決於居住地、活動、交易對方與服務。AI 應提供標明來源與日期的一般資訊，並將個案決策轉介給適任專業人士。

在歐盟，MiCA 規範特定加密資產與服務。其一般規定自 2024 年 12 月 30 日起適用；法規所載的最長過渡期至 2026 年 7 月 1 日，各國決定仍會影響適用情況。請查閱現行官方名冊，確認授權及範圍，早年提及曾登記並不足夠。獲得授權不代表價格、償付能力或全額補償有保證。

《2023/1113 號規則》規定有受義務約束的服務商參與時，轉帳須隨附哪些資訊。涉及自我保管地址且金額超過 1,000 歐元的轉帳，法規設有評估所有權或控制權的措施。低於門檻並不普遍免除身分識別。無服務商參與的個人間轉帳列於該法規的範圍排除事項，其他義務仍可能適用。

依個人情況保存充足的買賣、費用及來源文件，避免不必要的存取。維持私人紀錄無須公布完整歷史。課程也不教拆分交易以規避管控、提供不實資訊或隱瞞所得。

若涉及錄音、語音轉錄與可識別個人的學習進度，服務必須界定目的、法律依據、保存方式、存取、受託處理者及適用權利。商業服務的隱私設定應在銷售前驗證，不應在通話中臨時決定。

練習

1. 擬一份給顧問看的虛構案例，列出居住地、活動及交易，不含金鑰。
2. 確認從何處核實服務商的授權，以及資料的日期。
3. 設計一份私人資金流動紀錄，以及最低限度的學員資料政策。

檢驗學習成果

區分法律規則、交易所政策與比特幣技術能力。

常見問題

歐盟是否全面禁止自我保管？上述規定並不能得出這項結論。避免絕對化的標題，請核對具體條款與適用範圍。

暫停點

留下待請教顧問的問題，不要將私人文件輸入導師服務。

某些地址控制權查核措施提及 1,000 歐元門檻。低於門檻就免除所有義務嗎？

1. 是。
2. 只有拆分交易時才會。
3. 否。這並非身分識別或其他義務的普遍豁免。

> **查看答案: 否。這並非身分識別或其他義務的普遍豁免。**
> 解讀規定須看具體措施及範圍，不能將一項門檻視為通用豁免。

M10

繼承、持續運作與年度演練

學習目標

建立一個計劃，允許授權的人採取行動，而不會提前展示一切。

理解概念

遺產結合了法律合法性，材料的位置和技術能力。一個人可能有權繼承，而不知道如何重建錢包;另一個人可能有金鑰並且沒有使用它的許可。該計劃應以適當的建議解決兩個方面。

將公開的秘密訪問指示分開。存檔描述什麼是存在的，誰可以聯絡和哪些檢查，而不將所有金鑰和密碼一起放在一個廣泛可訪問的檔案中。請避免將 種子 釋出到可能在您的控制範圍之外的遺囑或檔案中。

在多重簽章中，設計誰保留了政策和副本，在損失後有哪些邊緣，如果一個金鑰的人死亡，會發生什麼。同一 保管人 儲存足夠的元件，可以成為一個單一的濫用點。過於複雜的分配可能會使財產不可收回。

包括 密碼 恢復 密文 和 密語 如果有，衍生 資料，裝置相容性和程式，如果製造商停止執行。不要假設所有者檔案或生物印記將無準備可用。可互動性必須用測試資料和文件格式進行測試。

經過家庭、住所、政策、軟體或參與者的變化，進行定期模擬。練習必須證明一個信任的人理解指示，而不透露財產或不必要移動資金。

練習

1. 填寫一個私人模板與負責人，元件，授權訪問和替代品。
2. 給另一個人實驗室指示，而不口頭解釋它們，並觀察它在哪裡被阻止。
3. 修正了雙重情況，並記錄了審查日期。課程不會自動建立回憶。

檢驗學習成果

你可以解釋發生了什麼，如果你不在，以及每個角色在每個階段需要什麼資訊。

常見問題

2的3是否會取代遺產計劃？不。這是一個技術工具。繼承人仍然需要背景、材料、協調和合法性。

暫停點

保持課程之外的計劃，並僅標記“審查模擬”。

評估繼承計畫時，哪項標準有用？

1. 獲授權的人能依文件演練，無須臨時摸索或提前取得祕密。
2. 計畫有很多頁。
3. 完全依賴記住一組密碼。

> **查看答案: 獲授權的人能依文件演練，無須臨時摸索或提前取得祕密。**
> 應實際測試可復原性與存取控制。

M11

價格、儲蓄與基本面分析

學習目標

分析投資論點，而不會將其與可驗證的技術特性混淆。

理解概念

價格是具體市場交易的結果，並且可能在平臺之間有所不同。流動性,硬幣報價,深度，銀行供應商時間和需求影響你可以執行的結果。螢幕上的報價不是你的容量保證的報價。

基本分析研究採用、需求、競爭、經濟安全、監管和供應等因素。一個已知的排放日曆並不單獨決定未來的價格。關於貨幣用途或“內在價值”的估計取決於假設；沒有一個客觀的數字，AI可以作為普遍的確定性。

定期購物策略分發了進入時刻，但不會保證利潤，也不會避免延長損失。長期儲蓄還需要流動性的債務，波動性寬容和保管計劃。該課程不要求你財產的一部分，也不會為你做出決定。

分三個問題：瞭解資產嗎？我能保守和恢復它嗎？我能否承擔經濟風險？主持金鑰不會自動響應第三個。培訓不會將價格預測或歷史圖表轉化為個性化建議。

練習

1. 她寫了一篇虛構論文，她的假設和事實，這將使她無效。
2. 模擬50%的下降和流動性的同時需求，而不會引入您的真實資產。
3. 確定論點的哪些資料可驗證，以及什麼是期望。

檢驗學習成果

你可以討論投資，而不會承諾盈利，也不會把信念與證據混淆。

常見問題

缺點會保證價格上漲嗎？不。需求和其他條件仍然對市場價格至關重要。

暫停點

保留實驗室假設，而不是自動購買指示。

定期購買可以保證什麼？

1. 長期獲利。
2. 不保證任何報酬，只依自選規則分散買入時點。
3. 防止遺失金鑰。

> **查看答案: 不保證任何報酬，只依自選規則分散買入時點。**
> 分散進場時間不會消除市場或作業風險。

M11

選擇購買比特幣的管道

學習目標

根據 保管 的許可、成本、撤銷、隱私和風險評估供應商。

理解概念

透過可驗證的標準比較供應商：法人和管轄權，授權服務，撤銷網路，手續費,價格差異，限制，支援，認證和資料處理。商標名稱或贊助商沒有證明特定服務的許可。

總成本可能包括存款，轉換，買賣價差,手續費交易，退款和銀行費用。交易“沒有手續費”可能有更大的差異。檢查淨值和參考貨幣。預算應該包括退出自我保管,當這是你的目標。

只要你保留保留的餘額，你就依賴供應商。預訂證並不單獨證明所有債務、資產所有權或未來的存款。檢查限制，並進行一個小退出，你可以在依賴新的流之前允許。

商業身份證可能會將您的身份與退出聯絡起來。此後保護這些資訊並不意味著刪除供應商所知道的資訊。不要假冒資料，也不要使用課程來避免義務。購買訓練程式碼也會產生您的 錢包 獨立的商業註冊。

練習

1. 填寫一個虛構的矩陣，兩個供應商：總成本，網路，最低退出，許可和要求的資料。
2. 計算一個學習操作的淨值，所有指定的職位。
3. 設計一個測試退出到預先驗證的地址，而不從這個迷你網站執行。

檢驗學習成果

您可以為您的案件做出選擇，並承認哪些資訊已被終止或未被驗證。

常見問題

該課程是否推薦一個交易所作為所有人最好的？不。許可證、關稅、受歡迎國家和條件正在變化。比較需要使用日期和案例。

暫停點

保留記錄，沒有身份證或身份證。

比起只比較交易手續費，更有用的是比較什麼？

1. 以所選網路、地址實際收到 BTC 的總成本。
2. 服務商的追蹤者數量。
3. 應用程式顏色。

> **查看答案: 以所選網路、地址實際收到 BTC 的總成本。**
> 最終價格可能還含有廣告手續費以外的成本。

M11

帳戶、委託單與執行成本

學習目標

瞭解基本訂單，並保護您的帳戶，而不會將課程轉換為交易終端。

理解概念

一個市場命令優先執行可用，風險為滑價。有限訂單設定購買最高或最低售價，但可能不會執行或部分完成。停止訂單根據供應商的規則啟用另一個行動；它本身不保證最終價格。

委託簿 顯示可用的報價，沒有承諾所有容量將保持。在 流動性 下跌或下跌時，結果可能不同於最後的 報價。停止市場和停止限制命令有不同的風險：執行最糟糕的價格，而可能的不執行。

使用獨特的 密碼 保護訪問，支援時可抵抗 網路釣魚 認證，審查會議和適當的撤銷控制。保持第二因素的恢復獨立。自動化 金鑰 API 可能比需要資料閱讀的人更危險的許可證；不要將其輸入到 導師 或迷你網站上。

在退出之前，請檢查 比特幣 資產和網路，您的 錢包 地址和淨數量。一個平臺可以使用相同的符號用於不同的產品。完成後，保留購買、執行、手續費和撤銷檔案，根據您的情況；不要將錢包撤銷與新購買混淆。

練習

1. 模擬一個委託簿，其中 1 單位售價為 100，另 1 單位為 102。說明以市價買入兩單位為何不能保證均價為 100。
2. 設計一個有限的順序，並描述沒有完成的場景。
3. 審查一個虛擬API的許可證，並刪除退出，如果你只需要諮詢。

檢驗學習成果

您可以描述每個訂單的優先事項、價格和不執行風險。

常見問題

停止失去總是限制損失嗎？不。Gaps、流動性、滑價 和供應商規則可能會阻止此事。

暫停點

保留沒有真實命令或金鑰 API的運動結果。

價格為 100 的限價買單仍有什麼風險？

1. 可能永不成交，或只部分成交。
2. 必須以任何價格成交。
3. 會自動建立備份。

> **查看答案: 可能永不成交，或只部分成交。**
> 控制價格的代價是可能無法成交。

M11

K 線、指標與技術分析偏誤

學習目標

閱讀影象作為歷史資料，並評估一個策略，而不會混淆模式與預測。

理解概念

一個K 線總結一個開放，最高，最低和關閉一個時期。量取決於來源。更改平臺、貨幣、時間段或時間段可能會改變你所看到的。K 線 不顯示在其範圍內移動的整個時間順序。

移動平均值緩慢過去的價格。一個時刻指標將觀察到的資料轉換為一個公式。沒有人知道未來。兩個來自同一系列的指標可以提供非常相關的資訊，儘管它們的顏色和名稱是不同的。

要評估一個規則，確定輸入、輸出、殘疾、成本、大小和資料，然後看看結果。避免只選擇獲勝的例子，調整引數，直到它們匹配或使用未來的資料在過去的決定。區分訓練和臨時驗證資料。

一個 backtest 必須考慮 買賣價差, 手續費, 滑價,資料可用性和可能的執行。總利潤率、準確率、最大損失和損失分配，回答了不同的問題。一個有許多錯誤的系統可能會失去資金，如果它的故障很大。沒有購買或銷售訊號作為確信。

練習

1. 閱讀一個K 線幻想，並解釋什麼時間資訊不包含。
2. 在評估10個合成結果之前，寫一個規則，包括成本和故障標準。
3. 比較 9 利潤 1 與 15 損失：總結果是 -6 儘管 90% 正確。

檢驗學習成果

您可以根據選擇、成本或風險來批評一個有吸引力的結果，而無需進行交易。

常見問題

多種指標的結合能保證更好的訊號嗎？不。它可以增加過度調整和複雜性，而不會提供獨立的資訊。

暫停點

保持規則和實驗室結果，而不是市場順序。

九筆交易各賺 1，一筆虧 15。扣除成本前的結果是什麼？

1. +90%。
2. +6。
3. -6。

> **查看答案: -6。**
> 賺九個單位、虧十五個單位，合計虧六個。

M11

保證金、期貨與自動化

學習目標

識別曝光，清算和自動化故障之前考慮複雜的產品。

理解概念

槓桿 增加了對投入資本的曝光。在一個簡化的例子中，1.000曝光的邊緣100意味著5%的底部不良運動相當於成本前的50:一半的初始邊緣。真正的維護規則，清算,側面和手續費可能會使結果惡化，並在預期之前啟用。

未來的和永久的可以包括終止，清算因差異，融資率和參考價格不同於最後的交換。它們不等於將 比特幣 帶回 Cuvex。保留一個 種子 不保護一個位置與 清算 或反對方故障。

一個機器人自動化規則，包括錯誤。需要位置限制、最低許可、命令能力、和解、損失控制、緊急中斷和監督。提交時間後複製請求可以複製曝光，如果未知的結果。

AI 可以解釋概念，並在虛構情況下檢測不一致性。您不應該收到 金鑰 API,啟用交易，也不應該承諾有利可圖的策略。對於本課程的主要目標，瞭解這些風險，可以決定不使用不理解的產品。

練習

1. 解決曝光和邊緣的例子，而不認為清算的水平是正確的10%。
2. 模擬一個API執行一個命令，但失去答案。解釋為什麼你必須在重複之前和解。
3. 設計一個停止按鈕，阻止新的訂單，並檢查已經開放的訂單，而不連線到經紀人。

檢驗學習成果

您可以描述一個在停止時生存的風險，另一個在機器人中生存的危險和另一個在外部基金自我保管中生存。

常見問題

自動化會消除情緒，從而保證結果嗎？不。它可以減少衝動的干預，並增加設計或執行錯誤。

暫停點

標記這種擴充套件如已理解，而不允許複雜產品。

曝險 1,000、保證金 100，按曝險虧損 5%，未扣成本為多少？

1. 虧 5。
2. 虧 50，等於保證金的 50%。
3. 若使用機器人就不會虧。

> **查看答案: 虧 50，等於保證金的 50%。**
> 槓桿與成本使保證金報酬率不同於資產價格變動幅度。

M12

Lightning 與其他支付層

學習目標

理解頻道支付，並識別哪些功能不提供修訂的Cuvex流。

理解概念

Lightning 透過通道與更新機制付款，不必將每次交換各自寫入基礎鏈。開關通道或某些復原情境仍可能需要鏈上交易。可用性、收付流動性及監控取決於錢包設計與所用服務。

付款請求可包含金額、說明及到期時間。依情境可使用聰或毫聰，後者不代表基礎鏈可產生不足一聰的輸出。付款需要相容功能與可用路徑，QR 碼不保證所有應用程式都可付款。

服務分為保管與非保管模式，特性差異甚大。通常付款很快，不代表沒有風險。Lightning 也並非完全匿名；觀察者、路徑、交易對方與中繼資料均須考慮。

Cuvex 聊天可協調以聰計價的請款，由 WOW 帳戶鏈上付款。本版並未將 Lightning 節點、通道管理或 Lightning 發票簽署列為 Desk 功能。請求若提供多種方式，請確認你理解哪一種，以及應用程式會執行哪一種。

練習

1. 列出一個線上地址，一個URI比特幣:和一個Lightning教學賬單。
2. 比較按鏈和頻道支付的確認，流動性,保管和恢復。
3. 解釋為什麼一個已關閉的發票必須與接收者進行審查，而不是作為地址重新解釋。

檢驗學習成果

您可以拒絕不相容的模式，而不會暴露金鑰或將錯誤歸咎於Cuvex.

常見問題

所有的支付是Lightning嗎？不。聰 表示值；模式取決於使用的協議。

暫停點

保留實費，沒有實際賬單。

如何判斷一個請求應透過 Lightning 付款？

1. 它寫有 sats。
2. 它透過聊天傳來。
3. 核對請求所用格式及支付方式符合 Lightning，不能只看單位或訊息管道。

> **查看答案: 核對請求所用格式及支付方式符合 Lightning，不能只看單位或訊息管道。**
> 計價單位與支付網路是不同資訊。

Taproot、MuSig2 與後量子未來

學習目標

區分實施的標準、建議和能力。

理解概念

Taproot 允許使用 金鑰 和指令碼路徑的支出條件。簽章 Schnorr 和整合可以改善某些結構，但隱私結果取決於它是如何配置和花費的。一個地址是 bc1p 不會證明沒有其他參與者，也不會揭示所有隱藏的條件。

MuSig2 允許一套 簽署者 新增 金鑰 並透過互動生產相容的 Schnorr 簽名。基準為 N 的 N。一個任意的 M 的 N 邊緣需要另一個建設或額外的協議。會議和會議管理是關鍵的，並且不透過非正式的資訊交換進行實施。

PSBT v2 相較於 v0 重新組織了資料。含有版本 2 交易的檔案不會自動升級。本版課程的 Final 韌體多重簽章設定檔仍採用 PSBT v0、P2WSH/sortedmulti 及 SIGHASH_ALL。未來新增能力須制定自己的介面契約並完成驗證。

NIST在2024上釋出了其第一批完成後標準。這不會改變簽章的比特幣。使用後方演算法來驗證 韌體 會保護這個層；不會自動將 ECDSA 或 Schnorr 從 UTXO 轉換為後方 簽章。此外，還沒有一個未來的攻擊日期，導師可以肯定地承諾。

練習

1. 它分為五個宣告，如標準，驗證的實施，建議或廣告。
2. 解釋為什麼“接受一個收款方 Taproot”不試圖“簽署一個Taproot輸入”。
3. 分開的層：韌體簽名，加密秘密，聊天和支出簽名比特幣。

檢驗學習成果

您可以要求一個層的具體證據，並避免在協議之間轉移保證。

常見問題

我是否需要透過量子計算的持有者轉移我的資金？一個真正的決定需要當前的技術證據，可驗證的支援，風險評估和安全的移民計劃；課程不命令持有者的動作。

暫停點

記錄技術問題，而不建立自動支出計劃。

假設開機載入程式已實作並驗證後量子簽章，這會改變既有 UTXO 的簽署條件嗎？

1. 不會，兩者位於不同層。
2. 會，整個網路都會改用另一演算法。
3. 會消除備份需要。

> **查看答案: 不會，兩者位於不同層。**
> 驗證軟體更新不會改寫比特幣的花費條件。

M12

互通性與脫離製造商後的使用

學習目標

如果您更改 軟體、裝置或供應商，則計劃連續性。

理解概念

可互動性不能透過字元列表進行驗證。它必須保留網路，指令碼，衍生,金鑰,政策，交易格式和簽章的序列。兩個應用程式可以理解 BIP174 並且不允許相同的欄位、尺寸或入口型別。

要擺脫介面依賴性，請保留記錄的恢復資訊，並使用錢包學習測試。標準 助記詞 可能允許 金鑰 衍生，但恢復 多重簽章 需要完整的政策。BIP329 標籤新增了隱私背景；聊天史具有不同的範圍。

不要將相容性測試轉化為真實種子的曝光。首先，檢查描述符的公共出口和唯讀觀察的恢復。如果緊急情況需要重建金鑰,請使用為此設計的環境，並考慮隨後遷移。顯示零的不相容的錢包並不單獨證明資金已經失去了。

保留可驗證的文件、課程版本和所需工具的副本。應用簽名、終止證書和系統變更可能會影響安裝。可用的開放程式碼並不保證任何人都可以在多年後編寫它，而不會保留依賴和知識。

練習

1. 設計一個空白帳戶的輸出測試：兩個相容的應用程式中的相同網路、政策和控制地址。
2. 列出哪些零件是標準的，以及哪些需要轉換器或Cuvex格式的檔案。
3. 確定什麼結果允許確認相容性，以及什麼是 硬體 或實際簽名。

檢驗學習成果

您可以描述一個恢復路線，而不需要公司繼續提供相同的服務。

常見問題

開源意味著製造商不再關心嗎？不。分銷、維護、物理元件和運營經驗仍在不斷增長。它提供了潛在的檢查和連續性，而不是自動保證。

暫停點

儲存實驗室結果與觀察的版本和限制。

哪項是較有力的互通性證據？

1. 兩個應用程式都寫著「Bitcoin」。
2. 在實驗室使用已記錄版本，重建並核對出相同政策與地址。
3. 圖示長得相像。

> **查看答案: 在實驗室使用已記錄版本，重建並核對出相同政策與地址。**
> 試驗須保留關鍵條件，且結果可供核實。

M12

使用 regtest 的技術實驗室

學習目標

了解可重現的實驗室，分清模擬資料測試與實機使用。

理解概念

Regtest 可建立受控的本機區塊鏈，產生區塊並演練沒有經濟價值的交易。須使用獨立的目錄與憑證，不得匯入真實材料。結果本身不能證明實體設備的 USB、NFC、Bluetooth 或相機相容性。

完整實驗會記錄版本、網路設定、政策、測試輸入、PSBT、簽章、最終交易及是否獲接受。可檢查金額加總、遭竄改簽章是否被拒絕，以及有效付款是否進入本機區塊。除了成功路徑，也應測試故障情境。

Desk 9.21 的驗證報告記載了 Bitcoin Core 31 regtest 測試，以及核心引擎與模擬 UI 的自動化測試。本版課程以報告為文件證據，並未聲稱重新執行這些測試或操作過實體裝置。檢查軟體套件也不能證明已在所有系統上安裝。

技術課開始前，工程師應交付已建置的實驗室，以及與學員版本相容的流程。不要將 RPC 開放到網際網路讓導師控制。AI 可協助解讀模擬結果，但不得取得憑證或管理權限。

練習

1. 在準備好的實驗室中觀察一筆有效交易，以及另一筆簽章被改動的交易。記下各自獲接受或拒絕。
2. 檢查找零錯誤及網路不相容兩種情境。
3. 在報告中區分「引擎測試」、「模擬介面」與「實體硬體」。

檢驗學習成果

精確說明測過什麼、還缺什麼，不將模擬結果當作認證。

常見問題

regtest 能正常運作，就可以宣稱課程已通過所有裝置的驗證並銷售嗎？不行。仍須測試實機流程、安裝、無障礙功能、復原及商業服務。

暫停點

依說明停止並儲存實驗室，只保留模擬資料。

引擎通過 regtest 測試，能證明某款手機真的讀得到 NFC 嗎？

1. 能，因為兩者都使用比特幣。
2. 能，只要 PSBT 夠小。
3. 不能，必須另做實機測試。

> **查看答案: 不能，必須另做實機測試。**
> 不同驗證環境有各自的範圍。

M12

期末專題與持續運作計畫

學習目標

從準備到恢復和隱私的獨立性。

理解概念

課程的結果不是記住選單：它是能夠解釋意圖，驗證結果，並阻止一個你不明白的操作。評估結合了概念，導向實踐和獨立案例。永遠不會依賴於向評估員披露種子,財產或個人地址。

案例A：設定學習環境，識別模型和版本，保護Desk,連線一個密文教學，並重建一個唯讀觀察帳戶。解釋什麼 備份 需要，以及您的供應商可以觀察哪些資料。

案例B：設計與不同背景的UTXOs虛構支付，正當選擇，檢查收款方,更換和手續費並描述您的裝置相關的簽名分支。解決一個退款中斷和另一個釋出中斷，而無需翻倍付款。如果沒有物理上接受的硬體,則該部分將被記錄為模擬，並保持延遲。

案例C：設計2的3,代表邀請和驗證，比較Mirror一個選定的欄位，並解釋OK的範圍。恢復學習政策，模擬參與者的損失，並準備連續性和遺產。

提議的超越需要至少80%的知識和所有正確的關鍵控制：不透露秘密，網路檢查和輸出,不混淆步驟，並保持恢復。一個關鍵的錯誤需要重新審查和新的實踐；它不被市場問題正確的補償。商業證書，如果發行，必須說明什麼被評估，是否有物理觀察或僅僅模擬。

練習

1. 填寫三個案例與合成資料和一個自己的解釋。
2. 完成附件的最終評估，並審查每個失敗的答案。
3. 只提供一張無秘密的結果表，包含範圍和延遲的證據。

檢驗學習成果

您可以自行停止，當交易缺乏足夠的證據時，並且知道您需要什麼才能繼續進行。

常見問題

關閉頁面是否等於準備好保留任何費用？不。能力必須被測試，風險必須根據你的情況進行評估。閱讀和測試不會保證未來的結果。

暫停點

保持您的審查計劃和即將到來的實踐。您可以回到所需的章節，而不重複整個課程。

完成實務訓練的一項關鍵要求是什麼？

1. 打開過所有頁面。
2. 在記錄清楚的範圍內證明能復原與核對交易，且不揭露祕密。
3. 預測下個月價格。

> **查看答案: 在記錄清楚的範圍內證明能復原與核對交易，且不揭露祕密。**
> 應以已驗證的能力與限制評量學習成果，不靠瀏覽頁面或預測。

學員手冊

Cuvex 操作手冊

本手冊配合課程使用。各項操作說明均依已審查之原始碼，列出流程、查核項目及停止點。本版是試行候選版本，並未證明編輯團隊以 Original、BIT、手機及各桌面平台完成實機測試。使用真實資金教學前，團隊須完成驗收矩陣，並修正與實機不符的介面標示或畫面。

參考版本為 Original 1.2.2 Final、BIT 1.2.3 Final、Desk 1.0.0-beta.9.21 和 Mirror 1.0.0-beta.12.12。在 Desk 選擇設定檔只代表已聲明的相容性，並非遠端測量韌體。手冊中的 Mirror 實際截圖來自 12.12 套件的 Android 模擬器。產品照片為公司素材，不能證明現有實機所顯示的版本。

P01 | 核對來源與版本 | Cuvex | L16,L21 | C01,C02

準備好購買憑據及可獨立查證的官方管道。此時不要輸入任何祕密。

1. 檢查包裝與封條。發現遭拆動跡象就停止啟用，保留不含敏感資料的證據。
2. 在與交付版本相容的應用程式中依完整性與封條查核流程操作。代碼只能在該處輸入，不得提供給導師。
3. 確認是 Original 或 BIT 及可辨識的修訂版。核對裝置與應用程式顯示的版本。
4. 對照團隊公布的相容性矩陣。目錄或雜湊值不能取代韌體真偽驗證或實機驗收。

結果：已辨識機型與版本，並在不揭露祕密的情況下檢查來源。代碼無效或介面不符時，不要硬套舊指南。

暫停點：載入保管資料之前。商業來源可追溯本身不能保證沒有進階竄改。

P02 | 透過 Bluetooth 更新 Original | Original | L46 | C01,C02,C03

準備可復原的備份、穩定電源、相容的官方套件，以及已對該系統驗收的流程。本課程未證明各平台都已完整通過實機測試。

1. 在應用程式的裝置或韌體頁選擇 Original，再選官方下載或對應的真實本機檔案。
2. 依裝置選單進入更新模式，再循應用程式的流程連線。讓設備彼此靠近，避免其他工作階段搶用連線。
3. 在指定欄位輸入 Original 螢幕顯示的代碼。不要把它與密文密碼混淆。
4. 依序觀察傳輸、驗證、安裝與重新啟動。進度百分比不能證明已成功安裝。
5. 在 Original 上核對最終版本。若應用程式有對應欄位，請記錄該版本。

結果：重新啟動後在裝置螢幕核對版本，確認流程完成。若在顯示 PIN 前、傳送封包期間或最後階段失敗，記下該階段及代碼。不要為了「超過 99%」臨時拔線或更換軟體。

P03 | 透過 USB 更新 BIT | BIT | L46 | C01,C02,C03

確認 BIT 的實際儲存媒體、電源與相容的官方套件。變更軟體前保留備份。

1. 在相容版本的 Desk 或 Mirror 韌體更新流程中選擇 BIT。
2. 使用合適的資料線與轉接器連接裝置。應用程式要求時，授權存取磁碟區或資料夾。
3. 選擇適用於該機型、經確認為真品的韌體，傳送前核對版本及相容性。
4. 等待裝置完成傳輸及驗證。依協定，磁碟區可能消失或重新掛載。
5. 重新啟動後，在 BIT 上核對版本，並查看應用程式的最終結果。

結果：已在實機上核實安裝。若磁碟區未出現，檢查裝置模式、資料線、權限、掛載狀態與其他進行中的連線。不要在電腦建立同名資料夾代替裝置。若更新失敗，須依該硬體的官方復原流程處理。

P04 | 使用硬幣與骰子建立錢包 | Cuvex | L17 | C01

準備私人空間、合適的骰子及硬幣，關閉導師麥克風，附近不可有相機。使用練習錢包。

1. 開啟建立錢包功能及韌體的熵輸入流程。擲骰前訂好四顆骰子的順序。
2. 依螢幕指示輸入硬幣和每顆骰子的結果，不得因個人偏好更改結果。
3. 已審查的原始碼計算：索引 = 硬幣值 × 1,296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1)。只接受從 0 到 2,047 的索引。
4. 若結果遭拒，重擲硬幣與全部骰子。提示訊息會保留先前的詞，並要求重擲整組。
5. 完成裝置的整套演算法，包括最終驗證。保護助記詞，並私下檢查復原能力。

結果：錢包由完整流程產生，並非自行選詞。螢幕與原始碼不符時，停止使用。勿使用已公開的擲骰結果、種子或金鑰作為自己的保管資料。

P05 | 加密祕密資料 | Cuvex | L18,L19 | C01

準備：選擇機型、內容格式與保護方式。即使最終儲存為密文，先在電腦或手機輸入仍會讓來源設備接觸明文。

1. 選擇加密，並選擇 BIP39、SLIP39、Monero 或相容的文字類型。不要混用字典。已審查的純文字鍵盤最多支援 500 個字元。可儲存另一種格式並不代表能為該網路簽署。
2. 直接在裝置上輸入內容以維持隔離，在裝置螢幕核對順序、字元與附加欄位。
3. 依流程選擇個人或共同保護，適用時可在 BIT 使用生物辨識。這個門檻與比特幣支出門檻不同。
4. 依韌體的密碼驗證規則私下輸入並確認密碼。不要直接套用 Desk 的規則。
5. Original 寫入相容的空白卡；BIT 則須保存 USB 流程匯出的物件。等候確認。
6. 進行一次測試復原來核對內容，完成後關閉祕密資料的顯示。

結果：已驗證密文可復原。遇讀寫失敗時保護原件，依螢幕提示重試，不要移除標頭或強行覆寫。

P06 | 在裝置上解密 | Cuvex | L18 | C01,C02

準備：確保周遭無人旁觀並備妥足夠的解鎖要素。祕密資料附近須關閉麥克風與螢幕擷取。

1. 在正確機型上啟動解密。Original 透過 NFC 提供密文，BIT 則使用其 USB 流程。
2. 輸入憑證前核對物件別名與身分識別資料。
3. 提供必要密碼，格式要求時也須提供生物辨識。出錯時不要機械地連續重試，系統設有存取控制與鎖定機制。
4. 只在指定螢幕核對內容。包含祕密的 QR 碼與明文同樣敏感。
5. 依裝置流程關閉或結束操作，並按照計畫分開保管媒體與憑證。

結果：已私下取回內容並結束工作階段。格式未識別、驗證失敗或出現非預期內容時，不要用不明應用程式「修正」。向客服描述版本、格式與錯誤，但勿附上祕密資料。

P07 | 準備復原以生物辨識保護的密文 | BIT | L19,L47 | C01,C02

準備：建立生物金鑰的金鑰，並記錄其格式。僅因為擁有 .bin 檔案，就不能假設可以恢復。

1. 在 Desk 介面中，確認是否有生物辨識元件，以及可用的恢復輸出格式。
2. 保留流程所關聯的所有檔案，以及一個獨立的副本，並使用隱藏的識別碼。
3. 在 BIT 上進行正常的解鎖測試，並記錄所需的密碼和條件。
4. 研究本地恢復的特殊途徑，以及其支援的格式。在使用之前，請先確認所需的資料是否存在。
5. 模擬在沒有資金的情況下，裝置故障或指紋不可用的情況。

結果：一個經過驗證的方案，具有其限制，適用於特定格式。宣告中沒有提到任何生物辨識資料可以被忽略，或指紋可以取代檔案。如果檔案在電腦上被恢復，請評估其暴露風險以及後續控制移轉的需求。

P08 | 建立並核對密文副本 | Cuvex 與 Desk | L20 | C01,C02

準備：一個已識別的原始副本，以及一個相容的目的地，且沒有需要保留的資料。

1. 對於 Original，可以使用裝置或 Desk 提供的相容功能進行複製，並按照指示提供來源和目的地。
2. 保持檔案穩定，並尊重已經包含金鑰的支援系統的拒絕。
3. 對於 BIT 或檔案，匯出流程的元件，並保留必要的名稱或關聯。
4. 將原件複製並從新版本中進行閱讀和測試恢復。
5. 隱私記錄日期、格式和結果；儲存具有獨立的物理風險的副本。

結果：這是第二份已驗證的副本。它不包括一個不同的錢包,密碼取消或對已過濾的種子的保護。如果命運失敗，保留原始，而不試圖“修復”，以便兩者都相匹配。

P09 | 建立、解鎖 Desk 及更改密碼 | Desk | L21,L40 | C02

準備：驗證的安裝器，適當的建築和倉庫的備份計劃。

1. 建立一個獨特的 密碼 儲存庫從 12 到 1.024 字元和相同的確認。
2. 點選並重新開啟，以確保您保留訪問。密碼 只在 Desk 中推出。
3. 在「安全性」及「存取與鎖定」檢查閒置與切換背景時的設定。示範時不要啟用選用的清除功能。
4. 更改密碼提供現行，並透過其流量確認新。
5. 如果您使用的是 生物辨識 的 PC,請按照指示重新設定。建立當前副本並保留與以前的副本的關係。

結果：已驗證的訪問。以前的副本保留了密碼和加密原始。生物辨識的PC和生物辨識的BIT是不同的機制。如果無法訪問，請停止重複的嘗試，並檢查恢復，而不要求導師儲存訊號。

P10 | 在 Desk 連結並檢查密文 | Desk | L22 | C02

準備：來源已知的測試密文，以及可用的傳輸方式。

1. 開啟密文或卡片頁，選擇透過 NFC、USB 或相容副本連結。
2. 選擇設計與來源。使用 NFC 時，須透過 Bluetooth 將 Cuvex Mirror 與電腦配對；另一種方式是使用經 USB-C 連接的 Cuvex BIT 磁碟區。Cuvex Desktop 不支援外接 USB NFC 讀卡機。
3. 檢查資料卡上的別名、來源、大小、格式與解析所得條件。這些是中繼資料，並非解密後的內容。
4. 查看是否有保留的帳戶尚待關聯，只連結已驗證的帳戶。
5. 若備份不足，匯出一份副本，並在獨立環境測試復原。

結果：物件已在本機整理。「已連結」不能證明種子真實或餘額正確。若無法識別物件，請查核格式與版本，不要為了讓應用程式接受而更改副檔名或刪除資料。

P11 | 啟用 WOW 唯讀觀察帳戶 | Desk 與 Cuvex | L13,L22 | C01,C02

準備：公共資訊從裝置的流動和私人控制其起源。

1. 開啟啟用 WOW 或從正確的 密文 新增帳戶。
2. 根據功能，將 描述符 或透過檔案、相機或 Mirror 允許的公共材料輸入。
3. 檢查網路、指令碼、起源、痕跡、路徑和 校驗碼 相應時。不要輸入 種子 或 xprv.
4. 請註冊您的帳戶，並以您的同意選擇查詢來源。
5. 檢查一個控制方向和發現的範圍，然後解釋平衡。

結果：觀察錢包已連結。若顯示零，先檢查網路、原密語、衍生路徑、帳戶、服務商及掃描，不要就此斷定資金消失。一般介面支援的網路不一定受多重簽章設定檔支援，須依各自情境判斷。

P12 | 設定節點與同步 | Desk | L25,L33 | C02

準備：先決定隱私需求。使用 Core 時，須可存取已同步且受保護的節點。

1. 在「安全性」的「隱私與節點」中，選擇 WOW 帳戶並查看其服務商。
2. 明確選擇相容的公共服務商或 Core。使用 Core 時，只在應用程式中輸入端點、錢包與憑證。
3. 了解每個服務會收到哪些資料，再授權查詢。TLS 不會對服務商隱藏查詢。
4. 同步後檢查日期、鏈尖、進度與完成狀態。重新掃描時，核對涵蓋的歷史範圍與工作是否持續執行。
5. 遇到 429 請遵守等待時間。發生錯誤時不要假定已切換到其他節點，設定不會在背景自動輪替。

結果：已知來源與狀態。不要將 RPC 暴露至網際網路、分享密碼，或只搜尋有餘額的地址。空白歷史可能是尚未完整掃描的結果。

P13 | 產生與找回收款請求 | Desk 與 Cuvex | L26 | C01,C02

準備：網和政策已驗證。

1. 開啟接收併產生或恢復適當的請求。
2. 新增觀察器，原因和預期金額，只要你需要這些 中繼資料 地方。
3. 在相關收費之前，檢查裝置的相容路徑的地址。如果缺乏物理接受，停止實踐模擬。
4. 僅透過接收器的驗證頻道共享所需的資料。
5. 在您的網路來源中檢視輸入、值和確認數。

結果：收費，而不僅僅是收費。在 多重簽章 中，顯示的地址保留為遲到的付款，而不會重新簽名。如果沒有歷史的新地址的限制達到，請恢復以前的請求；不要手動強化指數。

P14 | 標籤、凍結與 BIP329 | Desk | L27 | C02,B13

準備：實驗室賬戶與UTXOs和密碼的安全出口。

1. 標籤一個內容與您的背景，沒有不必要的個人資料。
2. 故意冷卻或解凍，並審查可用的平衡。限制是區域性的。
3. 透過保護功能輸出標籤。將 BIP329 分為檔案的 加密 格式。
4. 將其輸入到相容的影印件中；審查參考、標籤和凍結的相匹配。
5. 保持 備份 的 中繼資料 與 密碼 相結合，按照您的計劃。

結果：儲存和理解的選擇。進口不應用於自動解鎖未經審查的冷凍貨幣。不要將標籤檔案傳送到 導師:它可能會揭示對手和關係，即使它不包括 金鑰 支出。

P15 | 準備付款與傳送全部金額 | Desk | L28 | C02

準備：已驗證的申請，並有足夠的輸入可支付。

1. 開啟支付從WOW,UTXOs或聊天，並確認帳戶和網路。

2. 選擇 輸入、收款方 和值，並檢視相關背景。
3. 選擇價格和評論 手續費 絕對，變更和警告。如果有灰塵，請檢查不接受隱藏的手續費的替代品。
4. 要傳送全部，請檢查 手續費 後的淨。在聊天中，明確確認部分支付，如果不覆蓋申請。
5. 準備刪除器，並在出口到簽名之前檢視所有資料。

結果：可理解的意圖和PSBT這個操作。一般表格可以允許超過 輸入 或 收款方 比 硬體:應用 簽署者 的有效限制和運輸。如果 輸出 或條件更改，則將開始新的審查。

P16 | 使用 Original 簽署並傳回 PSBT | Original 與 Mirror | L29 | C01,C02,C03

準備正確草稿、相容的傳輸卡、可驗真且相容的密文，以及能私下解鎖的方式。來源未驗真的舊副本可能要先復原、核對並建立新副本才能簽署，不可編輯標頭規避限制。

1. 從 Desk/Mirror 的相容 NFC 流程匯出請求。
2. 將請求帶到 Original，依提示提供密文並私下解鎖，不要唸出憑證。
3. 核對網路、摘要、所有完整輸出、手續費、找零與必讀警示。
4. 使用 Final 多重簽章時可選擇是否檢查進階參數，只有全部一致才完成最後三次確認。
5. 等候將回應寫入卡片並從卡片重新讀取。
6. 使用 Cuvex Mirror 讀取回應，並在 Desk 的對應操作中驗證。

結果：已收到簽章且與草稿相符，尚未發布。若寫入失敗，保留狀態並依流程重試。不要把備份卡當作可隨意覆寫的付款媒體。

P17 | 使用 BIT 簽署、接收及確認收件 | BIT 與 Desk | L29 | C01,C02

準備正確草稿、可驗真且相容的密文，並選擇 BIT 真正的磁碟區。若舊副本被拒用於簽署，依提示復原並更新副本，不要強行改格式。

1. 經 Desk 服務使用 USB-C 遞交請求，再依裝置螢幕指示提供密文。
2. 私下解鎖，檢查摘要、每個輸出、費用與警示。
3. 使用 Final 多重簽章時，可檢視進階細節；授權必須完成最終確認。
4. 在 Desk 使用「從 BIT 接收」，匯入並驗證該筆作業的回應。
5. 檢查儲存與收件確認。若接收後收件確認失敗，重試同一操作，不要另選看似適合該機型的新操作。

結果：簽章已驗證，交換狀態一致。若在接收前或儲存後斷線，保留該請求的設定檔。不要為了配合待處理回應而改選目錄中的另一韌體。

P18 | 完成、發布及追蹤交易 | Desk | L30,L44 | C02

準備：簽章 已驗證並在適當情況下足夠的範圍。

1. 重新審查的意圖，輸入,輸出,手續費和網路。
2. 透過相應行動完成，並檢查沒有簽章或條件。
3. 允許傳播，並保留本地結果。如果網路響應丟失，請在重複之前查詢。
4. 跟隨 記憶池 和 確認數 在選擇的供應商與同步日期。
5. 如果提出RBF,請重新審查新的操作，並獲得所需的簽章。不要想起整合的CPFP功能。

結果：連鎖狀態與其來源驗證。取消刪除器不會取消已出口的簽章,也不會重新寫出確認的付款。聊天或捕捉的訊息不會取代跟蹤。

P19 | 自由比對兩個政策 QR 碼 | Mirror | L43 | C03,C02

準備：在 Desk 及 Cuvex 上顯示待核對欄位。練習僅用課程的虛構範例。

1. 開啟「比對政策」，任選一方先讀取。
2. 選擇要核對的資料。可從第 15 步開始，其他已人工核對的資料可略過掃描。
3. 讀取對應的另一方，核對兩段完整文字。步驟不明時選「指定 Desk 步驟」，並注意此背景資訊由人工提供。
4. 「一致」或「不一致」只針對這對文字。空格、大小寫與編碼都會影響結果。
5. 以任意順序開始下一對比對。依已審查的清除機制，離開或切換至背景即可結束。

結果：只完成一次本機比對，無法證明來源、工作階段、整體核准或啟用。有差異應向來源查清，不要正規化文字以硬湊出 OK。

P20 | 啟用、復原與移轉聊天 | Desk 與 Cuvex | L36,L39 | C02

準備：環境 DEV 或選擇的製作，一個標誌和 金鑰 聊天在裝置上，從來沒有在課程。

1. 開啟或恢復聊天從 密文 背景。
2. 選擇新的或現有轉換字母和應用程式所指定的相容的移動個人資料。
3. 輸入或閱讀 金鑰 聊天僅在私人流中。不要使用 種子、PIN 或 金鑰 的 WOW.
4. 檢查與服務的啟用；如果停止使用完成或檢查的行動，而不給它正確。
5. 檢查轉換後與聯絡的連續性，並避免在多個裝置上同時使用相同的標誌。

結果：在正確的環境中啟用或恢復的身份。歷史和以前的會議不會自動恢復，使用金鑰聊天或Desk的整體副本。保持可用的材料的限制。

P21 | 驗證聯絡人身分 | Desk | L36,L48 | C02

準備：與人事先前達成獨立通道。

1. 新增標籤並透過應用程式查詢您的公共身份。

2. 透過驗證的頻道比較痕跡，而不僅僅是在新建立的對話中。
3. 如果您使用識別，請避免在其他服務中重新使用的公共資訊或秘密。
4. 只有在解決差異後才會確認。在身份交換之前，支付和協調暫停到確認。
5. 文件驗證方法，沒有在課程中儲存敏感答案。

結果：背景信任聯絡人，而不是保證所有未來的請求。聲音可以被模仿和合法的團隊承諾。每個操作都進行審查。

P22 | 透過聊天索取地址、請款與付款 | Desk 與 Cuvex | L37 | C02,C01

準備：已驗證的聯絡人和相容的WOW帳戶。

1. 選擇請求地址，以地址回覆或根據意圖要求付款。
2. 在傳送之前，請檢查原始請求、網路、數量和筆記。
3. 要付款，從適當的賬戶開啟準備，選擇UTXOs和價格，並檢查淨金額。
4. Cuvex 透過模型程式授權。聊天不會自動簽名。
5. 繼續釋出和確認您的來源；與原始請求一致的部分支付。

結果：協調保持保管的審查。通訊狀態和交易狀態不等同。瀏覽器連結可以向第三方傳送資訊：在開啟它之前，您可以評估其使用。

P23 | 分享及連結收到的密文 | Desk | L38 | C02

準備：具體需要分享，確認的聯絡和接收的方式的定義。

1. 從聊天活動中選擇共享 密文 並檢視物件。
2. 不要新增 密碼, 種子 或 金鑰 聊天作為評論。
3. 接收者透過其接收行動驗證起源，並將相容的物件聯絡起來。
4. 評估您現在獲得的能力，如果您獲得了足夠的解鎖證據，您將獲得什麼。
5. 保持一個現實的撤銷計劃：刪除訊息不會刪除外部副本或已知的金鑰。

結果：一個加密物件的意識轉移。它不是付款，也不是單獨將金鑰納入多重簽章。如果附件要求訪問一個未知的頁面為解密,停止流。

P24 | 整體備份及還原 Desk | Desk | L15,L21 | C02

準備：供練習使用的資料庫與受自己控制的備份目的地。

1. 開啟資料庫備份功能，依提示設定密碼，並保存密碼與這份特定備份的對應關係。
2. 將副本儲存在唯一的工作設備以外，並依流程核對來源與完整性。
3. 在獨立測試環境還原，核對備份涵蓋的帳戶、設定與資料。
4. 檢查排除項目。不可假定聊天、相關工作階段與歷史紀錄已包含。多重簽章政策和私鑰不可互相取代。
5. 有重要變更後重做備份，並保存復原說明。

結果：已知備份範圍及密碼。舊備份仍使用原密碼。存取方式變更或資料外洩時，也要評估這些舊備份，不能只修改目前資料庫。

P25 | 建立與接受多重簽章錢包 | Desk 與 Cuvex | L41,L42 | C01,C02

準備：參與者彼此獨立，聯絡人已核實，已就網路及實際限制作出約定。

1. 建立者選擇名稱、M/N、網路、參與者及操作有效期。
2. 依相容流程提供正確的擴展公鑰，以及其指紋與 BIP48 路徑。
3. 每位參與者審核後接受或拒絕，並提供自己的公開資料。絕不分享種子。
4. 建立完整政策，並準備在每部裝置上驗證。
5. 存入資金之前先保存政策副本，核對作為檢查基準的地址，並確認有能力復原。

結果：提案完整且可驗證。接受邀請不代表完成實機核對。若 Original 參與，必須遵守其最多六把金鑰及 NFC 容量限制。BIT 不會擴大其他參與者的能力。

P26 | 驗證政策與接收確認 | Desk 與 Cuvex | L43 | C01,C02,C03

準備：各參與者持有相同的完整政策，使用正確韌體設定檔，裝置上沒有互相衝突的操作。

1. 在相容情境中啟動驗證政策。Original 須明確選擇已安裝的設定檔；BIT 則依其介面契約協商能力。
2. 依機型，透過 NFC/Mirror 或 USB-C 遞交請求。
3. 在裝置核對政策欄位。可選擇用 Mirror 比對任選資料對，不必依固定順序。
4. 完成裝置上的確認，經對應傳輸方式回傳回應。
5. 在 Desk 驗證與請求對應的回應。比對器顯示 OK 不能取代這一步。

結果：核對與請求相符，結論限本次核對。目錄不會遠端證明韌體版本，裝置也不是政策的永久儲存庫。遇到 FIRMWARE_CAPABILITY_REQUIRED，先檢查 Desk 版本與機型／建置組合。

P27 | 請求簽章、接收與移交協調職責 | Desk 與 Cuvex | L44 | C01,C02

準備：已驗證的政策，已識別的操作和收款方協議。

1. 準備 輸入、輸出、手續費 和筆記，並向相容的參與者請求 簽章。
2. 每位參與者都在他們的團隊中檢查和簽署他們的運輸分支。
3. 接收、驗證和保留每個簽名；解決即將到來的訴訟，而不會改變儲存的個人資料。
4. 如果協調被轉移，接收器接受流量並檢查狀態。因此，M/N 或 金鑰 的所有權不變。
5. 到達邊緣，審查並完成之前釋出。透過網路進行交易。

結果：與不同證據的協調。協調員的進展報告不是您的本地驗證。在應用程式中取消或拒絕不會必然破壞第三方已經儲存的簽章。

P28 | 匯出、還原與在本機移除多重簽章錢包 | Desk | L45 | C02

準備：已知的政策和加密複製與密碼單一。

1. 透過Desk的行動進行恢復。目前的流量使用一個驗證的CVXMSBK1容器來出口。
2. 保留副本和密碼與獨立風險。不要以歷史檔案擴充套件為 加密。
3. 恢復提供副本，密碼和公鑰的參與者正確的來源透過相機或Mirror如有。
4. 在運營之前，檢查政策、網路、方向和發現。
5. 要本地刪除，請閱讀範圍和確認，並儲存副本，如果您想要儲存恢復。恢復後是明確的。

結果：可恢復的政治或意識地消除的地方。刪除不會移動資金，不會從其他 簽署者 中刪除 金鑰 或單獨取消其他人儲存的交易。

P29 | 在電腦上執行例外復原 | Desk | L47 | C02

準備：可接受的格式材料，清潔的環境準備和備份。這項操作可以向PC揭示一個秘密；它在課程中使用學習資料。

1. 從正確的背景開始，並閱讀格式和通知的限制。
2. 意識地接受風險，並按流量要求關閉網路；視窗檢查狀態，然後允許繼續。
3. 只在私人視窗中輸入所需的身份證。他們不被指控，在課程中投票，也不與支援分享。
4. 只在沒有攝像頭或聽力助理的空間中啟用視覺；尊重臨時和關閉。
5. 結束，檢視可能存在的曝光，並計劃遷移到新金鑰,如果有必要。

結果：例外恢復，沒有法定刪除保證或與硬體隔離等值。如果您缺乏身份驗證、格式或訪問材料，請不要用真實的副本測試網際網路工具。

P30 | 檢查偏好設定、生物辨識與鎖定 | Desk | L40 | C02

準備：密碼 已知和 備份 已被測試，直到安全性更改。

1. 在 Access and Block 檢視 密碼, 生物辨識 可用，不活躍和鎖定，當轉到背景。
2. 它包括故障後延遲和更改之前設定的最大時間。
3. 保持可選刪除關閉，直到理解條件、邊緣和恢復。不要在生產中嘗試。
4. 在偏好中，調整語言、主題、貨幣、3或5分鐘的同步和聲音。
5. 如果您註冊比特幣連結，請確保開啟請求保持開鎖、選擇和審查；不單獨支付。

結果：理解的配置。作業系統 的 生物辨識 取決於裝置，並且不會取代 密碼 或 備份.視覺偏好不會改變 比特幣 政策。

P31 | 刪除紀錄並釐清影響範圍 | Desk | L22,L45 | C02

準備：確定您是否會刪除 密文 本地，帳戶，WOW,聊天或 多重簽章 以及您將儲存的副本。

1. 閱讀所選擇的物件和通知。當應用程式要求時，確認準確的代號或明確的條件。
2. 出口並測試副本，如果您需要恢復該狀態後。
3. 它僅刪除預定的物件，並檢查保留或撤回流的協會。
4. 檢查是否有外部參與者或活動。不要假設來自其他裝置的訊息、簽章或檔案會消失。
5. 記錄您的私人儲存中的變化，沒有敏感的課程資料。

結果：故意管理的地方。這些股票中的任何一項都不會單獨改變UTXOs的資助指令碼，破壞第三方所知的種子或轉換確認的交易。

P32 | 在不揭露祕密的情況下診斷問題 | Desk 與 Mirror | L23,L30,L48 | C02,C03

準備：記下大約時間、系統、架構、版本與步驟。敏感操作狀態未明時，不要不斷重試。

1. 辨別錯誤是在搜尋、配對、讀取、寫入、驗證、簽署、回傳、網路或顯示階段。
2. 複製錯誤代碼與訊息，勿包含 QR 碼或私人資料。適用時使用應用程式的診斷工具。
3. 分享前檢查檔案。勿附上資料庫備份、密文、種子、聊天金鑰、描述符或 RPC 憑證。
4. 遇到介面問題，使用虛構資料重現畫面，記錄視窗大小、縮放與被遮住的控制項。
5. 透過官方管道提供預期結果與可重現步驟。課程不會自動傳訊息給客服。

結果：以最低限度資料提供可供調查的報告。無證據的階段標為「待確認」，不標「已完成」。語音輔導不需遠端存取你的保管設備。

比特幣與自我保管詞彙表

比特幣

用於轉移價值並驗證其歷史的網路與規則，不需要單一帳本管理者。

BTC

比特幣的貨幣單位。1 BTC 等於一億聰。

聰（satoshi）

比特幣基礎鏈的單位，等於一億分之一 BTC。

區塊鏈

依一套規則串接、驗證的區塊歷史。光靠這個名稱無法說明某個網路的全部特性。

區塊

包含交易及可驗證標頭的一組資料。

完整節點

驗證其所接受的區塊與交易是否符合規則的軟體。

挖礦

依網路規則，透過工作量證明建構區塊。

工作量證明

提出區塊前必須完成可驗證運算工作的機制。

共識

參與者所接受的規則與有效歷史彼此相容。

記憶池政策

節點在本機決定是否接受、轉送交易的規則，不一定等同於共識規則。

記憶池

節點在本機保留的未確認交易集合。

確認

交易納入已接受鏈的區塊，以及該區塊隨後在鏈中的深度。

鏈重組

已接受的鏈有一部分被替換，可能改變交易確認情形。

UTXO

未花費的交易輸出，滿足其條件即可花費。

輸入

對先前輸出的參照，以及授權花費該筆輸出所需的資料。

輸出

交易所建立的金額及其花費條件。

找零

付款並扣除手續費後，將部分輸入價值轉回自己控制的輸出。

手續費

交易的輸入總值與輸出總值之差。

vbyte

虛擬大小單位，用來表示交易的相對成本。

每 vbyte 的聰數

以聰除以虛擬大小表示的手續費率。

零碎輸出（dust）

依節點政策和花費成本判定的小額輸出。門檻取決於情境與腳本。

RBF

依相容政策替換未確認交易的機制，不保證能取消交易。

CPFP

利用子交易提高礦工將它與父交易一起納入區塊的誘因。

雜湊值（hash）

可用於檢查資料完整性的指紋。它不會加密資料，也不能單獨識別作者。

私鑰

在對應密碼機制下產生有效授權的能力。

公鑰

可驗證簽章及建構特定條件的資料，不必揭露私鑰。

數位簽章

對特定訊息授權的密碼學證明，不會隱藏其內容。

加密

使用金鑰和演算法保護資料機密性。

驗證式加密

依設計兼具竄改檢查能力的加密方式。

AES GCM

本生態系部分格式使用的驗證式加密機制。特性取決於實作與金鑰管理。

助記詞

依特定格式，以詞語表達產生金鑰的材料及檢核資料。

種子

金鑰衍生的原始材料。口語上也用來指助記詞，須依上下文釐清。

熵

產生材料的不可預測性。刻意選擇易記的詞無法取得熵。

校驗碼（checksum）

用來偵測特定錯誤的校驗值，無法驗證作者身分。

BIP39

定義助記詞，以及使用可選密語衍生種子的規格。

BIP39 密語

衍生種子時的額外輸入。不同的密語可能產生另一個有效、但沒有餘額的錢包。

BIP32

定義金鑰階層式衍生的規格。

衍生路徑

自根金鑰取得子金鑰所經過的分支序列。

強化衍生

通常以撇號或 h 標示的衍生步驟，性質有別於普通的公開衍生。

xpub

附有衍生所需資訊的擴展公鑰，屬於隱私敏感資料。

xprv

擴展私鑰，不可分享或匯入課程。

主金鑰指紋

根金鑰的短識別碼，有助於核對關聯，但不足以單獨證明身分。

描述符

以金鑰及其衍生方式描述如何建立腳本的表示式，可僅含公開資料，也可能包含私密資料。

唯讀觀察錢包（watch only）

僅供觀察的錢包，本身不具備足以獨立簽署的私鑰能力。

WOW

Cuvex 生態系中，觀察帳戶與錢包管理所使用的名稱。

熱錢包

能在連網環境中簽署的工具。

自我保管

使用者依自己的政策，保有獨立或共同花費資產的技術能力。

保管人

代客戶控制花費能力，並施行其存取條件的機構。

Cuvex 密文

用於保護祕密的加密物件，其本身不是交易或餘額。

Desk 密碼

保護本機資料庫存取的密碼，有別於種子及密文密碼。

聊天金鑰

復原聊天身分的祕密。即使外觀像公開資料，也不可公開。

配對 PIN

某次連線階段的臨時代碼，不是保管資產的密碼。

實體隔離（air gap）

在操作上隔離不同環境。跨環境傳遞的資料仍須驗證。

NFC

透過相容卡片與讀取設備進行近距離通訊的技術。

USB Mass Storage

BIT 用來交換檔案的介面，須遵循其專用協定、驗證及收件確認流程。

PSBT

裝載資料及簽章的格式，供各方協同建構與授權交易。

PSBT v0

由 BIP174 定義的格式版本，已審查的 Final 多重簽章設定檔採用此版本。

PSBT v2

由 BIP370 定義的版本。交易本身版本號為 2，不代表採用此 PSBT 格式。

SIGHASH ALL

已審查設定檔所使用的簽章承諾模式。核對交易時，必須考慮簽章實際涵蓋的範圍。

P2WPKH

單一金鑰的 SegWit 支出條件，通常與 BIP84 帳戶搭配。

P2WSH

對腳本作出承諾的 SegWit 條件，已審查的 Final 多重簽章流程採用此格式。

P2TR

Taproot 輸出類型。能支付給這種輸出，並不表示能簽署花費這種輸出的交易。

sortedmulti

以固定規則排序金鑰，產生多重簽章腳本的結構。

N 取 M 的門檻

依具體政策，在 N 名參與者中必須取得 M 份授權。

MuSig2

Schnorr 簽章聚合協定，基本方案為 N 取 N，並非任意門檻。

Taproot

比特幣的一組花費與承諾機制，包含金鑰路徑與腳本路徑。

Miniscript

用來描述與分析特定腳本政策的語言。已審查的 Final 設定檔未實作它。

Regtest

由建置環境的人控制的本機實驗網路，沒有經濟價值。

Signet

有其特定屬性的測試網路，預設不能與 regtest 互換。

Mainnet

有真實經濟用途的比特幣主網。

地址間隔上限（gap limit）

探索地址時，以連續多少個地址沒有歷史紀錄作為停止依據。適用範圍依錢包而異。

輸入選擇（coin control）

有意識地選擇要花費哪些 UTXO。

整併

將多個輸出合併以減少零碎程度，會影響成本與隱私。

假名性

使用不直接等同於法定姓名的識別碼，並不會自動獲得匿名性。

匿名性

在特定情境中，指定的觀察者無法區分個人的性質。應用程式標示「匿名」並非保證。

中繼資料

通訊或活動的時間、大小及關聯等資訊，有別於內容本身。

CoinJoin

協同建構交易，使某些推論更困難，但不保證永久匿名。

Payjoin

依相容協定，由付款人和收款人共同提供輸入的協作付款。

Tor

用以保護連線的網路及工具。各應用程式須分別設定並驗證連線。

VPN

將部分連線信任轉移至其營運者的通道，無法隱藏鏈上紀錄。

Lightning

透過通道運作的支付系統，所需條件與風險有別於鏈上付款。

付款請求（invoice）

結構化的付款請求，須辨識其格式與支付方式。

RPC

呼叫 Bitcoin Core 等服務的介面，須驗證身分並妥善保護。

TLS

防範某些傳輸層威脅，接收端伺服器仍可看見請求內容。

SRTP

保護部分 VoIP 傳輸路段的音訊，但不代表營運者一定無法接觸內容。

冪等性

重複提交同一個已識別請求時，不會重複產生效果的性質。

Webhook

伺服器間傳送的事件通知，須驗證真實性並檢查是否重複送達。

RAG

檢索知識片段，利用其上下文與版本資訊作為回答依據。

回述檢核（teach back）

請學員用自己的話解釋所學，以確認理解程度。

網路釣魚

冒充他人並營造可信情境，以騙取存取權或誘導特定行動。

社交工程

操控他人的決定，可能利用真實資料與緊迫感施壓。

Apple 公證（notarization）

Apple 的發行管控機制，有別於產品稽核或各項流程的實機測試。

狀態證明（attestation）

特定機制提供的狀態證據。Desk 的相容性目錄不是遠端測量。

MiCA

歐洲針對特定加密資產和服務制定的架構，不保證獲利或全額補償。

Travel Rule

對適用範圍內資金移轉所要求的資訊義務，不會因自我保管而免除。

學習檢查點（checkpoint）

用最低限度資料記錄學習續接位置，不含錢包資訊。

檢驗學習成果

請勿使用真實資金練習。評量免費開放，無須帳戶。

一般使用 Cuvex 時，誰負責授權花費？

1. 使用者核對後，由裝置授權
2. 語音導師
3. 課程伺服器

> **查看答案: 使用者核對後，由裝置授權**
> 授權流程仍在 Cuvex 上完成。

0.001 BTC 是多少聰？

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

> **查看答案: 100,000**
> 1 BTC 等於 100,000,000 sat。

輸入為 120,000 sat，輸出為 119,000 sat。手續費是多少？

1. 1,000 sat
2. 119,000 sat
3. 無須其他資料，即可認定為 1 sat/vB

> **查看答案: 1,000 sat**
> 輸入與輸出總額的差額就是手續費總額。

一筆已簽署但尚未廣播的交易處於什麼狀態？

1. 已確認
2. 簽署後就不可逆
3. 已授權，但不一定已發布

> **查看答案: 已授權，但不一定已發布**
> 簽署與發布是不同階段。

交易大小 200 vB，費率 6 sat/vB，相當於多少費用？

1. 206 sat
2. 1,200 sat
3. 轉帳金額的 6%

> **查看答案: 1,200 sat**
> 虛擬大小乘以費率即為手續費。

從交易所提領前應核對什麼？

1. 只需查看最低手續費
2. 資產、網路、地址與實收金額是否相符
3. 交易對方的種子

> **查看答案: 資產、網路、地址與實收金額是否相符**
> 並非所有標示 BTC 的網路都是比特幣鏈上網路。

單靠數位簽章可以做什麼？

1. 隱藏整則訊息
2. 授權一則可依其簽章方案驗證的訊息
3. 刪除已發布的資料

> **查看答案: 授權一則可依其簽章方案驗證的訊息**
> 要達成保密還需其他機制。

更改 BIP39 密語可能會怎樣？

1. 產生另一個有效、看似空白的錢包
2. 總能透過電子郵件重設
3. 改變以往付款的公開紀錄

> **查看答案: 產生另一個有效、看似空白的錢包**
> 密語參與金鑰衍生。

應如何看待帳戶的 xpub？

1. 完全不會造成任何影響的資料
2. 等同於私密種子
3. 對隱私敏感的資訊

> **查看答案: 對隱私敏感的資訊**
> xpub 可能擴大他人觀察活動的範圍。

多重簽章錢包中，為何只有一份種子可能不足以復原？

1. 缺少政策與滿足門檻所需的授權
2. 比特幣不允許復原任何資料
3. 還需要應用程式原本的顏色

> **查看答案: 缺少政策與滿足門檻所需的授權**
> 留存政策與保有私鑰授權能力是不同的要求。

在已審查的 Final 演算法中，若擲骰結果遭拒，該怎麼做？

1. 只重擲硬幣，直到獲接受
2. 重新擲硬幣和全部四顆骰子
3. 挑選一個熟悉的詞

> **查看答案: 重新擲硬幣和全部四顆骰子**
> 只重做部分隨機輸入可能使映射結果產生偏差。

開啟單簽種子時須輸入兩個密碼，這代表什麼？

1. 鏈上必須使用兩把金鑰
2. 這是 Taproot 多重簽章
3. 存取祕密的門檻與比特幣支出的門檻各自獨立

> **查看答案: 存取祕密的門檻與比特幣支出的門檻各自獨立**
> 加密並不改變花費腳本。

評估 Desk 的整體備份時，應了解什麼？

1. 它一定包含所有聊天資料
2. 備份有範圍及排除項目，不能假定其中包含聊天資料
3. 它會更新所有舊備份

> **查看答案: 備份有範圍及排除項目，不能假定其中包含聊天資料**
> 復原身分與復原訊息是兩件事。

正確設定的自有節點可以做什麼？

1. 消除所有資料外洩途徑
2. 減少依賴第三方查詢，並讓你自行驗證
3. 復原遺失的金鑰

> **查看答案: 減少依賴第三方查詢，並讓你自行驗證**
> 自有節點不能保證匿名，也不能復原祕密資料。

在 Desk 凍結一個 UTXO 代表什麼？

1. 這是應用程式執行的本機限制
2. 它改變共識條件
3. 它撤銷其他種子副本的效力

> **查看答案: 這是應用程式執行的本機限制**
> 這不會在全網阻止該輸出被花費。

剛發布交易就失去連線，該怎麼做？

1. 立刻再付一次
2. 刪除錢包
3. 先確認付款是否已廣播

> **查看答案: 先確認付款是否已廣播**
> 逾時並不能證明操作未生效。

重複使用地址或合併不同情境的 UTXO 可能會怎樣？

1. 使外界更容易看出其關聯
2. 抹去歷史
3. 保證匿名

> **查看答案: 使外界更容易看出其關聯**
> 隱私取決於使用情境及後續操作。

開啟 Tor Browser 會自動設定 Desk 嗎？

1. 會
2. 不會
3. 只有使用深色主題才會

> **查看答案: 不會**
> 每個應用程式的連線路徑都需要核對。

外觀類似 xpub 的聊天金鑰是什麼？

1. 可公開的資料
2. 收款地址
3. 身分驗證祕密

> **查看答案: 身分驗證祕密**
> 敏感性取決於用途。

若聊天訊息顯示「已付款」，這代表什麼？

1. 可用聊天訊息取代交易確認
2. 仍需獨立在網路上核實付款
3. 訊息改變了請求的網路

> **查看答案: 仍需獨立在網路上核實付款**
> 訊息狀態與付款狀態不同。

已審查的 Final 多重簽章設定檔使用什麼？

1. MuSig2 與 PSBT v2
2. P2WSH、sortedmulti、BIP48、PSBT v0
3. 任何比特幣腳本

> **查看答案: P2WSH、sortedmulti、BIP48、PSBT v0**
> 期待或商業名稱不會擴大實際支援範圍。

在 Mirror 12.12，可從哪個項目開始比對？

1. 只能從第 1 項開始
2. 可任選一項，包括第 15 項
3. 只有完成所有項目後才能選最後一項

> **查看答案: 可任選一項，包括第 15 項**
> 每一對資料均可自由、獨立比對。

Mirror 顯示「一致」可以證明什麼？

1. 整體核准
2. 兩個 QR 碼來源都是真實的
3. 這一對資料的字面內容相同

> **查看答案: 這一對資料的字面內容相同**
> 其餘審核與回應仍有待完成。

若種子已經外洩，更改 Desk 密碼會怎樣？

1. 撤銷攻擊者的權限
2. 不會使該種子衍生的金鑰失效
3. 刪除所有副本

> **查看答案: 不會使該種子衍生的金鑰失效**
> 應評估如何安全轉移控制權。

實務訓練結束時應說明什麼？

1. 哪些是閱讀、模擬及實機測試，以及還有哪些項目待完成
2. 只報告已售時數
3. 保證保管方式絕不可能失守

> **查看答案: 哪些是閱讀、模擬及實機測試，以及還有哪些項目待完成**
> 不同證據所能證明的範圍各異。