CUVEX

CUVEX ACADEMY · 0.1

Học hỏi. Thấu hiểu. Tự nắm quyền kiểm soát.

Tìm hiểu Bitcoin và cách tự lưu ký theo từng bước. Khóa học, sổ tay, bảng thuật ngữ và bài thực hành đều miễn phí, không cần đăng ký. Bạn tự chọn điểm bắt đầu.

Miễn phí · không cần đăng ký

Tất cả các phần

1. Chuẩn bị không gian học
2. Tiền kỹ thuật số và bài toán niềm tin
3. Lịch sử và giới hạn của Bitcoin
4. Satoshi và cách tính chính xác
5. Xây dựng mô hình mối đe dọa của bạn
6. Nút, khai thác và đồng thuận
7. UTXO và tiền thừa trong giao dịch
8. Mempool, xác nhận và tái tổ chức chuỗi
9. Phí, kích thước ảo và thay thế giao dịch
10. Mạng, địa chỉ và yêu cầu thanh toán
11. Hàm băm, chữ ký và mã hóa
12. Hạt giống, cụm mật khẩu và mật khẩu
13. Dẫn xuất khóa, xpub và descriptor
14. Chọn ví và mô hình lưu ký
15. Tạo bản sao lưu có thể khôi phục
16. Làm quen với Original và BIT
17. Tạo hạt giống bằng entropy vật lý
18. Mã hóa và giải mã bí mật bằng Cuvex
19. Ngưỡng mã hóa và sinh trắc học
20. Nhân bản, lưu giữ và kiểm tra các bản sao
21. Cài đặt và bảo vệ Cuvex Desk
22. Liên kết bản mật mã và sắp xếp tài khoản WOW
23. Ghép nối Mirror với Desk
24. NFC qua Mirror, USB-C và đọc mã QR
25. Nhà cung cấp công cộng và nút tự vận hành
26. Nhận bitcoin và kiểm tra địa chỉ
27. Gắn nhãn, đóng băng và chọn UTXO
28. Chuẩn bị và kiểm tra khoản thanh toán
29. Ký bằng Original và BIT
30. Hoàn tất, phát giao dịch và xử lý sự cố
31. Có thể quan sát những gì trên Bitcoin?
32. Tách bối cảnh và quản lý tiền thừa
33. Quyền riêng tư trên mạng, Tor và VPN
34. CoinJoin, Payjoin và các giới hạn hiện tại
35. Bài học từ các sự cố thực tế

36. Tạo danh tính và xác minh liên hệ trò chuyện
37. Yêu cầu và thanh toán satoshi qua trò chuyện
38. Chia sẻ bản mật mã một cách có cân nhắc
39. Khôi phục trò chuyện và hiểu siêu dữ liệu
40. Cài đặt hằng ngày và rà soát quyền
41. Thiết kế ví đa chữ ký
42. Tạo lời mời và cung cấp khóa
43. Kiểm tra chính sách bằng Mirror theo thứ tự tùy chọn
44. Điều phối chữ ký và phát giao dịch đa chữ ký
45. Khôi phục và thay đổi ví đa chữ ký
46. Cập nhật phần sụn theo quy trình
47. Mất thiết bị, hỏng hóc và khôi phục khẩn cấp
48. Lừa đảo giả mạo, hỗ trợ và gian lận bằng giọng nói
49. Quyền riêng tư, pháp luật và hồ sơ cá nhân
50. Thừa kế, duy trì khả năng tiếp cận và diễn tập hằng năm
51. Giá, tiết kiệm và phân tích cơ bản
52. Lựa chọn nơi mua bitcoin
53. Tài khoản, lệnh và chi phí khớp lệnh
54. Nến giá, chỉ báo và thiên kiến trong phân tích kỹ thuật
55. Ký quỹ, hợp đồng tương lai và tự động hóa
56. Lightning và các lớp khác
57. Taproot, MuSig2 và tương lai hậu lượng tử
58. Khả năng tương tác và sử dụng độc lập với nhà sản xuất
59. Phòng thực hành kỹ thuật với regtest
60. Dự án cuối khóa và kế hoạch duy trì liên tục
61. Sổ tay học viên
62. Bảng thuật ngữ Bitcoin và tự lưu ký
63. Kiểm tra những gì bạn đã học

M01

Chuẩn bị không gian học

Mục tiêu

Chuẩn bị cho khóa học, phân biệt ba thiết bị và thống nhất những thông tin tuyệt đối không cung cấp cho gia sư.

Tìm hiểu

Bạn sẽ học cách tự quyết định khi nhận, tự lưu ký, chi tiêu và khôi phục bitcoin. Mục tiêu cuối cùng là giải thích được quyết định trước khi phê duyệt. Bạn có thể tự đọc khóa học. Gia sư giọng nói giải thích, đặt câu hỏi và đồng hành mà không cần xem tài sản hay điều khiển thiết bị của bạn.

Cuvex bảo vệ thông tin bí mật và cho phép bạn phê duyệt thao tác trên màn hình thiết bị. Desk quản lý bản mật mã, ví chỉ theo dõi, thanh toán và điều phối trên máy tính. Mirror là cầu nối cục bộ cho các thao tác được hỗ trợ và là công cụ đối chiếu dữ liệu. Mirror không phải thiết bị ký hay ví độc lập. Phiên bản và mẫu thiết bị quyết định quy trình có thể dùng.

Dành một màn hình cho khóa học, màn hình khác cho Desk và để điện thoại cùng Cuvex trong tầm tay. Nếu chỉ có một màn hình, hãy chuyển đổi giữa hai cửa sổ và không chia sẻ màn hình qua cuộc gọi video khi nhập thông tin bí mật. Cuộc gọi có thể kết thúc trước khi xong bài tập. Tạm dừng không phải là thất bại. Chỉ lưu mã bài học, bước đã làm và khó khăn gặp phải.

Cả người hướng dẫn lẫn AI đều không được nhận cụm từ khôi phục, cụm mật khẩu BIP39, mật khẩu, khóa trò chuyện, PIN, tệp riêng tư hoặc mã mua hàng đầy đủ. Họ cũng không cần xpub, descriptor thật hay địa chỉ của bạn. Tuy không cho phép chi tiêu, các dữ liệu này tiết lộ hoạt động. Hãy mô tả thông báo lỗi và dùng dữ liệu giả trong phòng thực hành.

Thực hành

1. Nhận diện máy tính, điện thoại và mẫu Cuvex trước mặt. Ghi các phiên bản vào sổ riêng.
2. Tách môi trường học không có tiền khỏi môi trường lưu ký thật. Không nhập cụm từ khôi phục đang giữ tiền để luyện tập.
3. Mở bài này và tìm nút tạm dừng, phần trợ giúp và bảng thuật ngữ. Nếu ai đó yêu cầu thông tin bí mật, hãy dừng tương tác.

Chứng minh bạn đã hiểu

Giải thích thành phần nào ký, thành phần nào truy vấn mạng và thành phần nào chuyển dữ liệu. Bạn có thể học tiếp khi tự phân biệt được các vai trò.

Câu hỏi thường gặp

Tôi có phải trò chuyện với gia sư mỗi ngày không? Không. Bạn có thể tự học, học lại một buổi hoặc chỉ nhờ giúp ở một quy trình cụ thể. Quyền truy cập khóa học và thời lượng dịch vụ giọng nói là hai quyền riêng.

Điểm tạm dừng

Đã hoàn thành L01, nhận diện các thiết bị và không ghi thông tin bí mật nào vào khóa học.

Gia sư yêu cầu cụm từ khôi phục để kiểm tra bạn đã ghi đúng. Bạn làm gì?

1. Đọc chậm cho gia sư.
2. Từ chối yêu cầu và chỉ kiểm tra cụm từ trong môi trường an toàn của mình.
3. Chỉ gửi vài từ đầu tiên.

> **Xem đáp án: Từ chối yêu cầu và chỉ kiểm tra cụm từ trong môi trường an toàn của mình.**
> Dù chỉ là một phần của thông tin bí mật cũng nằm ngoài phạm vi dịch vụ đào tạo.

M01

Tiền kỹ thuật số và bài toán niềm tin

Mục tiêu

Hiểu vấn đề Bitcoin muốn giải quyết trước khi mở ví.

Tìm hiểu

Số dư ngân hàng là một bút toán do một tổ chức quản lý. Tổ chức này xác thực khách hàng, quyết định xử lý khoản chuyển nào và ghi sổ. Tệp số thông thường rất dễ sao chép: khi gửi ảnh, bạn vẫn có thể giữ một bản. Muốn một đơn vị số hoạt động như tiền, cần ngăn việc chi tiêu nó hai lần.

Bitcoin kết hợp quy tắc xác thực, chữ ký và lịch sử giao dịch được chia sẻ. Thay vì giao toàn bộ sổ cái cho một tổ chức, những người tham gia có thể độc lập kiểm tra giao dịch có tuân thủ quy tắc hay không. Tính khan hiếm phụ thuộc vào việc các quy tắc tiếp tục được xác minh và chấp nhận, không bắt nguồn từ hình ảnh đồng xu hay giá niêm yết trên sàn.

Tự lưu ký thay đổi cách phân bổ trách nhiệm. Bạn giữ quyền chi tiêu mà không phải xin phép bên lưu ký, nhưng cũng có thể mất quyền đó nếu hủy hết sao lưu hoặc ký nhầm khoản thanh toán. Quyền tự quyết vẫn đi kèm nhu cầu bảo mật, phối hợp, kết nối để phát giao dịch và tuân thủ nghĩa vụ hiện hành.

Phân biệt Bitcoin, tên mạng và giao thức, với BTC, đơn vị tiền tệ của nó. Các mạng khác cũng có thể dùng từ blockchain nhưng có đặc tính khác. Một công ty hứa giao thứ được gọi là “bitcoin” không đồng nghĩa với việc bạn nắm một đầu ra Bitcoin bằng khóa của mình.

Thực hành

1. So sánh ba trường hợp: số dư ngân hàng, số dư trên sàn và UTXO do khóa của bạn kiểm soát.
2. Ở mỗi trường hợp, viết ra ai có thể ngăn bạn di chuyển số dư và ai có thể giúp nếu bạn quên cách truy cập.
3. Mô tả điều xảy ra khi sao chép một bức ảnh và khi cố chi tiêu cùng một đầu ra hai lần.

Chứng minh bạn đã hiểu

Dùng lời của bạn giải thích vì sao số dư và khả năng ký là hai khái niệm khác nhau. Không cần học thuộc thuật ngữ.

Câu hỏi thường gặp

Tự lưu ký có làm mọi trung gian biến mất không? Bạn có thể chọn dịch vụ để mua, truy vấn hoặc liên lạc. Điều cần xét là họ còn quyền gì và nhận được dữ liệu nào.

Điểm tạm dừng

Lưu bảng so sánh trách nhiệm nhưng không ghi tên tài khoản thật.

Chỉ riêng chữ ký số không giải quyết được vấn đề tiền tệ nào?

1. Ngăn việc cố chi tiêu cùng một đầu ra hai lần.
2. Chứng minh sự ủy quyền bằng một khóa.
3. Phát hiện nội dung đã ký bị thay đổi.

> **Xem đáp án: Ngăn việc cố chi tiêu cùng một đầu ra hai lần.**
> Chữ ký chứng minh sự cho phép. Quy tắc và đồng thuận xác định thứ tự các khoản chi xung đột.

M01

Lịch sử và giới hạn của Bitcoin

Mục tiêu

Xác định nguồn gốc Bitcoin và phân biệt sự kiện lịch sử với lời quảng bá.

Tìm hiểu

Tài liệu của Satoshi Nakamoto được công bố năm 2008 và mạng bắt đầu hoạt động năm 2009. Tài liệu đề xuất tiền điện tử ngang hàng dựa trên các ý tưởng trước đó về mật mã học, bằng chứng công việc và tiền số. Không cần biết danh tính pháp lý của Satoshi để kiểm tra phần mềm hay giao dịch.

Bitcoin không phát triển nhờ một công ty đơn phương thay quy tắc. Nhà phát triển đề xuất và đánh giá thay đổi, người vận hành chọn phần mềm, thợ đào xây khối, người dùng và dịch vụ quyết định chấp nhận điều gì. Cách phân quyền này có thể gây bất đồng. Phân nhánh không đồng nghĩa với cập nhật ứng dụng.

Nút có thể bác bỏ khối vi phạm quy tắc của nó dù đã tốn nhiều công sức để đào. Đồng thuận không phải bỏ phiếu theo số máy tính. Chạy hàng nghìn bản sao của một nút không tự động tăng quyền quyết định. Tương tự, đa số thợ đào không nhờ đó mà có được khóa riêng của người dùng.

Bitcoin có những giới hạn và đánh đổi có chủ đích về dung lượng khối, chi phí xác minh, thời gian xác nhận biến động và sổ cái công khai. Mặc định không có cơ chế quản trị để đảo ngược thanh toán hay bảo mật toàn diện thông tin. Các lớp và ứng dụng giải quyết nhu cầu cụ thể nhưng mang đến những phụ thuộc mới.

Thực hành

1. Lập dòng thời gian cho tài liệu ban đầu, ngày mạng hoạt động, việc áp dụng SegWit và kích hoạt Taproot. Đối chiếu nguồn trước khi công bố các mốc.
2. Phân loại “công ty đảm bảo giá”, “nút xác minh” và “thợ đào đề xuất khối” vào cam kết thương mại hoặc chức năng kỹ thuật.
3. Nêu một lợi ích và một cái giá của việc không có quản trị viên đảo ngược thanh toán.

Chứng minh bạn đã hiểu

Phân biệt quy tắc đồng thuận, chính sách cục bộ và quyết định của doanh nghiệp. Ứng dụng bạn dùng không phải toàn bộ mạng.

Câu hỏi thường gặp

Phần mềm mới nhất có luôn đổi quy tắc tiền tệ không? Không. Phiên bản mới còn có thể sửa lỗi, tăng hiệu năng hoặc đổi chính sách cục bộ. Hãy đọc ghi chú phát hành và thông tin tương thích.

Điểm tạm dừng

Ghi một đặc tính có thể kiểm chứng và một phát biểu cần thêm bằng chứng.

Một khối chứa khoản chi thiếu ủy quyền hợp lệ. Đa số thợ đào có thể làm nó hợp lệ không?

1. Có, nếu vượt 51%.
2. Chỉ khi sàn giao dịch công bố.
3. Không đối với nút đang áp dụng các quy tắc bác bỏ nó.

> **Xem đáp án: Không đối với nút đang áp dụng các quy tắc bác bỏ nó.**
> Chỉ so sánh công việc tích lũy giữa các lịch sử hợp lệ theo quy tắc của nút.

M01

Satoshi và cách tính chính xác

Mục tiêu

Quy đổi BTC và satoshi, kiểm tra số lượng mà không cần dựa vào tỷ giá.

Tìm hiểu

Một BTC bằng 100.000.000 satoshi. “sat” là đơn vị, không phải một đồng tiền khác. Trên chuỗi cơ sở, giá trị được ghi bằng số satoshi nguyên. 0,001 BTC bằng 100.000 sat, còn 0,00001000 BTC bằng 1.000 sat. Dấu thập phân trên giao diện thay đổi theo ngôn ngữ, đừng ước lượng để thêm số không.

Tỷ giá quy đổi BTC sang một đồng tiền như EUR hoặc USD tại một thời điểm. Nó không làm thay đổi số satoshi bạn kiểm soát. Nếu giữ 100.000 sat, số satoshi vẫn vậy khi giá đổi. Tỷ giá trên Desk có nguồn và ngày, chỉ để tham khảo. Dữ liệu cũ có thể dẫn đến quyết định kinh tế sai dù số dư BTC đúng.

Khi thanh toán, phân biệt số tiền người nhận được, phí mạng và tổng chi. Nếu gửi 50.000 sat và trả phí 600 sat, giá trị ra khỏi ví là 50.600 sat, giả sử không có đầu ra nào khác thuộc bạn. “Gửi tất cả” thường tính số thực nhận thấp hơn số dư khả dụng vì còn phải trả phí.

Ví dụ trong khóa học là bài toán số học, không phải giá thị trường hay mức phí khuyến nghị. Trước khi ký, hãy kiểm tra đơn vị, mạng, người nhận và tổng chi phí trên màn hình tương ứng. Giọng nói có thể đọc “năm mươi nghìn satoshi” đồng thời hiển thị “50.000 sat”, nhưng không được quyết định số tiền từ bản chép lời chưa rõ.

Thực hành

1. Quy đổi 250.000 sat thành 0,0025 BTC. Quy đổi 0,00025000 BTC thành 25.000 sat.
2. Tính khoản gửi 75.000 sat với phí 900 sat: tổng chi 75.900 sat.
3. Trong trình mô phỏng, dùng 120.000 sat, gửi 70.000 và trả phí 1.000. Kiểm tra tiền thừa là 49.000 sat.

Chứng minh bạn đã hiểu

Đọc một số tiền theo BTC và sat, giải thích số nào đã gồm phí. Nếu còn nghi ngờ, tạm dừng thao tác.

Câu hỏi thường gặp

Có cần mua cả một bitcoin không? Không. Bạn có thể mua một phần, tùy mức tối thiểu và chi phí của nhà cung cấp.

Điểm tạm dừng

Chỉ lưu kết quả bài tập.

Bạn có 80.000 sat và muốn gửi tất cả với phí 1.200 sat. Người nhận được bao nhiêu?

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

> **Xem đáp án: 78.800 sat.**
> Trong ví dụ không có đầu ra khác này, người nhận được số dư có thể chi trừ phí.

Xây dựng mô hình mối đe dọa của bạn

Mục tiêu

Chọn biện pháp tương xứng trước nguy cơ mất, trộm, lừa đảo và lộ dữ liệu.

Tìm hiểu

An toàn là giữ khả năng hành động theo ý muốn. Riêng tư là kiểm soát ai biết dữ liệu và các mối quan hệ của bạn. Tính sẵn sàng nghĩa là truy cập được khi cần. Chiếc hộp không ai mở được cũng có thể khóa chính bạn ở ngoài. Bản sao quá tiện lợi có thể lộ quá nhiều thông tin.

Liệt kê tài sản, bên đối địch và tai nạn. Tài sản gồm khóa, bản sao lưu, lịch sử, vị trí bản sao và danh tính liên hệ. Rủi ro gồm phần mềm độc hại, giả mạo, hỏa hoạn, quên, cưỡng ép, hỏng hóc, tử vong và lỗi của chính bạn. Một công cụ không thể giảm mọi rủi ro.

Lập bảng đơn giản về xác suất gần đúng, tác động và biện pháp cụ thể. Mật khẩu dài làm khó việc đoán nhưng không sửa được việc bạn tự phê duyệt kẻ gian làm người nhận. Hai bản sao cùng một túi sẽ cùng mất nếu mất túi. Ví đa chữ ký vẫn có điểm hỏng chung nếu một người kiểm soát hết thiết bị và bản sao.

Khóa học và gia sư cũng thuộc mô hình. Mua hàng, cuộc gọi, thời điểm kết nối và tiến độ có thể tạo siêu dữ liệu. Trang khóa học không nên hỏi địa chỉ hay số dư để cá nhân hóa bài. Desk hoặc Mirror không cần đăng ký thông thường không có nghĩa cửa hàng, nhà cung cấp giọng nói hay dịch vụ truy vấn khác không biết hoạt động của bạn.

Thực hành

1. Ghi ba rủi ro quan trọng nhất mà không nêu giá trị tài sản hay vị trí chính xác.
2. Với từng rủi ro, chọn cách phòng ngừa, phát hiện và khôi phục. Ví dụ với mất thẻ: hai bản sao tách biệt, danh mục kiểm kê và thử khôi phục.
3. Phân biệt người hoặc hệ thống nào có thể thấy việc mua hàng, gọi, truy vấn số dư và giao dịch công khai.

Chứng minh bạn đã hiểu

Giải thích biện pháp tiếp theo xử lý rủi ro nào. Đừng tích lũy độ phức tạp mà bạn không thể duy trì hay giải thích cho người thừa kế.

Câu hỏi thường gặp

Nhiều thiết bị hơn luôn an toàn hơn không? Chỉ khi giảm phụ thuộc chung và bạn có thể thử khôi phục. Thêm thiết bị cũng tăng công bảo trì và nguy cơ nhầm lẫn.

Điểm tạm dừng

Giữ kế hoạch trong hồ sơ riêng. Trong khóa học chỉ ghi “đã rà soát mô hình mối đe dọa”.

Biện pháp nào giúp giảm tốt nhất nguy cơ mất mọi bản sao trong một đám cháy tại chỗ?

1. Đổi màu thẻ.
2. Đặt hai bản sao trong cùng một ngăn kéo.
3. Giữ các bản sao đã kiểm tra ở những nơi có rủi ro độc lập.

> **Xem đáp án: Giữ các bản sao đã kiểm tra ở những nơi có rủi ro độc lập.**
> Bản dự phòng phải chịu được chính sự cố đe dọa bản gốc.

M02

Nút, khai thác và đồng thuận

Mục tiêu

Giải thích xem nút có giá trị gì và khai thác mang lại gì.

Tìm hiểu

Một nút đầy đủ Nhận các khối và các giao dịch, kiểm tra các quy tắc và giữ cho mắt của chuỗi liên lạc. Cô không cần phải tin vào số dư thông báo cho cô một trang. khai thác là quá trình đề xuất các khối thông qua bằng chứng công việc. Đội thợ đào chọn giao dịch hợp pháp và cạnh tranh với việc tìm ra một chiếc khối được chấp nhận.

Bằng chứng công việc khiến việc viết lại lịch sử trở nên tốn kém. Khi có nhiều chuỗi hợp lệ, điều cần so là công việc tích lũy, không đơn thuần đếm khối mà bỏ qua độ khó. Khoảng cách giữa các khối thay đổi. Mười phút là mức trung bình mục tiêu, không phải lịch hẹn cho khoản thanh toán tiếp theo.

Tiền thưởng khai khoáng kết hợp trợ cấp và phí. Tiếp theo là một lịch giảm giá khối; phương pháp phí phụ thuộc vào các giao dịch trong đó. Thêm một khoản chuyển tiền nữa không làm cho chữ ký sai được hợp lệ. Sự an toàn kinh tế và chi phí tấn công không biến một khoản thanh toán không thể thay đổi được.

Một chiếc nút tự vận hành làm giảm nhu cầu cần thiết liên lạc với các nhà cung cấp của người khác và cho phép kiểm tra. Anh vẫn phải bảo vệ hệ điều hành, truy cập và kết nối của họ. Có một nút bật không đồng bộ, hoặc kết nối với một máy chủ khác tham khảo, không tự động cung cấp những lợi thế đó.

Thực hành

1. Hãy xác định những công việc này: kiểm tra chữ ký, chọn giao dịch với khối, bảo vệ hạt giống khôi phục của bạn, và quyết định xem bạn có nhận được tiền thanh toán hay không.
2. Giải thích tại sao thợ đào giữ bitcoin của tôi là một mô tả sai.
3. Trong một mạng lưới phòng thí nghiệm, bạn quan sát chiều cao và đồng bộ; không phải là xuất bản thẻ tín dụng RPC.

Chứng minh bạn đã hiểu

Hãy mô tả sự khác biệt giữa việc kiểm tra và đề xuất. Bạn có thể dùng một phép tương tự, nhưng kết thúc với một chức năng kỹ thuật phù hợp.

Câu hỏi thường gặp

Tôi có cần phải hạ cánh để sử dụng bitcoin không? Không. Bạn cũng không cần phải có một nút tự vận hành mới bắt đầu, mặc dù biết được mức độ tin tưởng của nhà cung cấp của bạn là cần thiết.

Điểm tạm dừng

Ghi lại nhà cung cấp phòng thí nghiệm của hắn, không có URL tư nhân.

Nút đầy đủ được cấu hình đúng mang lại khả năng gì?

1. Kiểm tra quy tắc của chuỗi mà nút chấp nhận.
2. Khôi phục mọi khóa đã mất.
3. Bảo đảm giá tăng.

> **Xem đáp án: Kiểm tra quy tắc của chuỗi mà nút chấp nhận.**
> Xác minh và lưu ký là hai chức năng khác nhau.

M02

UTXO và tiền thừa trong giao dịch

Mục tiêu

Đọc giao dịch như tiêu thụ và tạo ra các đầu ra.

Tìm hiểu

Một chiếc UTXO là một lối thoát khỏi một vụ giao dịch trước mà vẫn chưa tiêu. Một ví Tính toán số dư của bạn bằng cách xác định các số các đầu ra Anh ta có thể kiểm soát. Không có tài khoản chung nào được đặt lại trên một tờ ngân hàng: một đầu ra trước bằng cách nhận dạng giao dịch và vị trí.

Tiêu xài một chiếc UTXO tiêu hết rồi. Nếu bạn phải trả ít hơn giá trị của nó, bạn thường tạo ra một lối thoát cho người nhận và một lối thoát dưới sự kiểm soát của bạn. Với một đầu vào 120.000 sat , người nhận của 70.000 Và phí của 1.000 Sự thay đổi là 49.000 . Tổng của các đầu vào phải bằng các đầu ra cộng với phí.

Một địa chỉ không phải là UTXO. Bạn có thể nhận được nhiều các đầu ra . Cũng không hẳn là một con người. Nhận dạng giao dịch có thể công khai, nhưng kết nối nó với danh tính của bạn hoặc giải thích nó là ai, mỗi đầu ra sẽ thêm vào những thông tin mà chuỗi không tự nó thể hiện.

Cấu trúc này quan trọng với sự riêng tư: kết hợp các đầu vào có thể cho thấy sự kiểm soát thông thường; sự thay đổi có thể liên quan đến việc thanh toán trong tương lai. Sự mâu thuẫn đó không phải là một bằng chứng phổ thông vì có những giao dịch hợp tác. Coin kiểm soát là lựa chọn các đầu ra chi tiêu, biết được hậu quả của việc kết hợp chúng.

Thực hành

1. Vẽ ba đầu vào giả định có giá trị 40.000, 60.000 và 200.000 sat. Chỉ dùng hai đầu vào đầu tiên để trả 70.000 với phí 1.000 sat.
2. Kiểm tra tiền thừa là 29.000 sat và đầu vào thứ ba không được sử dụng.
3. Chỉ cần lặp lại bằng 200.000: sự thay đổi sẽ là 129.000. So sánh chi phí và mối quan hệ, mà không phải kích cỡ giống nhau.

Chứng minh bạn đã hiểu

Xác định mục nhập, người nhận, thay đổi và phí trên biểu đồ khóa học. Nếu anh không thể xác định được lối ra, anh không được ký vào một chiến dịch thực sự.

Câu hỏi thường gặp

Tất cả những gì quay lại ví của tôi là thay đổi? Không. Có thể là chuyển sang một địa chỉ khác. Phân loại đòi hỏi phải biết chính sách và dẫn xuất, chứ không phải đoán xem nó là gì.

Điểm tạm dừng

Hãy để lại những giả thiết; không bao giờ lấy đi di sản của bạn.

Đầu vào 100.000 sat tạo hai đầu ra 30.000 và 69.200. Phí là bao nhiêu?

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

> **Xem đáp án: 800 sat.**
> 100.000 trừ 99.200 bằng 800 sat.

M02

Mempool, xác nhận và tái tổ chức chuỗi

Mục tiêu

Phân biệt một giao dịch sẵn sàng, công bố và xác nhận.

Tìm hiểu

mempool là một tập hợp các giao dịch chưa được xác nhận trong địa phương mà nút giữ theo chính sách của họ. Không có một mempool nào giống nhau trên hành tinh này. Một nhà thám hiểm chỉ ra một khoản tiền trả công có nghĩa là người đó biết anh ta; anh ta không bảo đảm rằng tất cả nút sẽ nhận anh ta hoặc sẽ được xác nhận vào một thời điểm nhất định.

Chuẩn bị PSBT không phát đi gì cả. Ký tạo sự cho phép. Hoàn tất tạo giao dịch có thể phát. Phát là thử truyền giao dịch lên mạng. Xác nhận nghĩa là giao dịch đã nằm trong một khối của chuỗi được nguồn kiểm tra chấp nhận. Xác nhận thứ hai là có thêm một khối tiếp theo, không phải chữ ký thứ hai của người nhận.

Các tổ chức có thể được tổ chức lại để thay đổi một phần chuỗi, và một hoạt động mất số xác nhận hoặc trở lại. Để trả tiền triển lãm nhiều hơn, các bên thường yêu cầu thêm số xác nhận. Không có con số nào có thể loại bỏ bất kỳ rủi ro nào cho tất cả các vấn đề và tình huống.

Nếu Desk cho thấy một trạng thái được lưu, hãy tham khảo ngày tháng. " Xác nhận" theo một hình chụp cũ không nhất thiết phải miêu tả tình trạng hiện tại. Nếu một kiện hàng không xuất hiện, nó bảo tồn danh tính địa phương của bạn và kiểm tra lại các ấn phẩm và lịch sử trước khi bạn sửa chữa lại. Nó có thể tạo ra một khoản thanh toán hợp lệ khác.

Thực hành

1. Hãy sắp xếp những tấm thẻ này: Bản nháp, PSBT, ký tên, giao dịch cuối cùng, phát sóng, bao gồm khối.
2. Mô phỏng sự ngắt kết nối sau khi xuất bản. Hãy quyết định xem có gì để kiểm tra trước khi trả thêm lần nữa.
3. Nó giải thích tại sao một thông điệp trong chat nói rằng "được trả tiền" không thay thế việc kiểm tra mạng lưới.

Chứng minh bạn đã hiểu

Bạn có thể diễn tả tình trạng của một hoạt động và nguồn thông tin đó mà không nhầm lẫn nó với một sự bảo đảm.

Câu hỏi thường gặp

Đóng Desk hủy giao dịch công bố? Không. Những người tham gia nút khác có thể bảo tồn nó. Hủy bỏ một bản nháp địa phương có tầm nhìn khác.

Điểm tạm dừng

Chỉ vào trạng thái mô phỏng, không thêm bộ nhận dạng thực sự vào gia sư.

Máy tính ngắt kết nối ngay sau khi bấm phát. Trước tiên làm gì?

1. Tạo lại khoản thanh toán từ đầu.
2. Xóa ví.
3. Kết nối lại và kiểm tra giao dịch cùng các đầu vào.

> **Xem đáp án: Kết nối lại và kiểm tra giao dịch cùng các đầu vào.**
> Không nhận được phản hồi không chứng minh việc phát đã thất bại.

Phí, kích thước ảo và thay thế giao dịch

Mục tiêu

Ước tính chi phí, giải mã sat nhân vbyte và hiểu RBF và CPFP.

Tìm hiểu

phí mạng là sự khác biệt giữa các đầu vào và các đầu ra. Sự cạnh tranh của họ thường được bày tỏ ở sat/vB : satoshi Vì hệ thống điện tử ảo. Nó không phụ thuộc trực tiếp vào giá trị kinh tế được gửi. Nhiều các đầu vào Họ có thể chi trả một khoản tiền nhỏ, một khoản tiền lớn với một số tiền nhỏ các đầu vào Nó có thể làm việc ít hơn.

Một ví dụ 200 vB a 5 sat/vB ♪ La phí Đúng vậy. 1.000 sat . Trước khi ký, bạn chỉ có thể có một ước tính, vì kích thước cuối cùng có thể phụ thuộc vào chữ ký cấu trúc. Desk cung cấp tốc độ hướng dẫn và giá cả bằng tay; nhãn "tách" không hứa hẹn xác nhận đúng giờ.

RBF là một chính sách thay thế các giao dịch chưa được xác nhận trong một điều kiện nhất định. Cơ chế này cho phép chúng ta đề xuất một khoản chi tiêu tương đối lớn hơn phí; chính sách nút đã tiến hóa và không nên điều trị một dấu hiệu không thay thế để đảm bảo việc chi trả. Một sự thay thế yêu cầu một sự kiểm tra mới và một chữ ký cần thiết.

CPFP là chi tiêu một lối thoát khỏi cuộc phẫu thuật chưa hoàn thành để cho cả cha lẫn con trai có thể trở nên hấp dẫn. Nó đòi hỏi phải kiểm soát một lối thoát có thể sử dụng, thực hiện chính trị và trả tiền cho nó. Đó là khái niệm của bitcoin: bạn không thể giả định một nút CPFP trong phiên bản Cuvex của học sinh.

"Dust" là một kết xuất quá nhỏ dựa trên chính sách áp dụng và chi phí được ước lượng; nó không phải là một ngưỡng phổ thông cho mọi loại văn bản. Nó tránh dạy một con số cố định với tư cách luật đồng thuận. Nếu sự thay đổi không khả thi, hãy kiểm tra lại, các đầu vào hoặc quét và phí hiệu quả.

Thực hành

1. Tính 180 vB a 8 sat/vB : 1.440 sat . Kiểm tra xem nó có vượt quá ngân sách phòng thí nghiệm của anh không.
2. So sánh trường hợp một đầu vào và mười đầu vào. Giải thích vì sao chỉ biết số tiền gửi chưa đủ để ước tính chi phí.
3. Mô phỏng một giao dịch đang chờ và quyết định giữa chờ đợi, RBF hoặc học CPFP, mà không tự động chấp nhận.

Chứng minh bạn đã hiểu

Giải thích phí suất, phí tuyệt đối và chi phí so với số tiền gửi. Từ chối mức phí chưa hiểu rõ.

Câu hỏi thường gặp

RBF có chắc chắn hủy bỏ khoản thanh toán trước không? Không. Các phiên bản cạnh tranh nhau cho đến khi xác nhận và lan truyền đều quan trọng. Không được giao hàng dựa trên lời hứa hủy bỏ.

Điểm tạm dừng

Hãy lưu ý đến quyết định và động cơ của bạn.

250 vB với phí suất 4 sat/vB có phí bao nhiêu?

1. 1.000 sat.
2. 254 sat.
3. 4% số tiền gửi.

> **Xem đáp án: 1.000 sat.**
> Kích thước ảo nhân phí suất bằng phí ước tính.

Mạng, địa chỉ và yêu cầu thanh toán

Mục tiêu

Nhận diện mạng, định dạng địa chỉ và hướng dẫn thanh toán trước khi sao chép hoặc scan.

Tìm hiểu

Mainnet Di chuyển bitcoin Với giá trị kinh tế. Mạng lưới thử nghiệm là để phát triển và học hỏi, nhưng chúng không thể thay đổi lẫn nhau. Regtest là một mạng lưới địa phương được điều khiển bởi người xây dựng phòng thí nghiệm, signet và testnet có những quy tắc và hệ sinh thái riêng của họ. Một chức năng đơn độc xác nhận trong signet không có nghĩa là hồ sơ đa chữ ký của Cuvex thừa nhận mạng lưới đó.

Các địa chỉ mã hóa các điều kiện tiếp tân. Trong mainnet, bạn sẽ tìm thấy định dạng bắt đầu với 1, 3, bc1q, hay bc1p. Tiền tố này giúp nhận ra một gia đình, nhưng nó không chứng minh được người nhận, không đảm bảo sự tương xứng của bên ký và không thay thế sự xác nhận đầy đủ về định dạng.

QR là một thùng chứa hình ảnh. Nó có thể vận chuyển một địa chỉ, một hóa đơn, một tờ descriptor hay một văn bản độc hại. Quét nó không xác thực cho tác giả của bạn. Một liên kết bitcoin: bạn có thể thêm vào nội dung và thông điệp. BIP321 là tham khảo hiện đại để thay thế BIP21; Desk giữ các thuật ngữ và sự tương thích BIP21 trong thực tế. Một sự cải thiện tiêu chuẩn không chỉ mở rộng những gì mà nó hiểu được.

hóa đơn Lightning không phải là địa chỉ của on-chain. Nó có thể bao gồm tiêu hóa và các lĩnh vực khác; bạn không nên dán nó vào chuỗi nếu ứng dụng không cung cấp dòng chảy tương thích. Một chiếc áo len có tên BTC trên một mạng khác cũng không tự động là bitcoin thổ dân.

Thực hành

1. Đánh dấu các mẫu được đánh dấu của khóa học mà không cần dùng địa chỉ có thể sử dụng: địa chỉ, URI bitcoin: intex Lightning và descriptor.
2. Xác định mạng lưới đã được chọn trong phòng thí nghiệm. Trong Cuvex đa chữ ký kiểm tra, độ tương thích của hồ sơ là mainnet/regtest.
3. So sánh toàn bộ văn bản được yêu cầu bởi người nhận thông qua một kênh xác thực trước khi thực hiện thao tác.

Chứng minh bạn đã hiểu

Bạn có thể từ chối một yêu cầu mà bạn không biết và giải thích bạn cần kiểm tra cái gì.

Câu hỏi thường gặp

Tôi có thể gửi BTC cho bất cứ mạng nào cho thấy sàn giao dịch không? Không. Mạng lưới rút lui phải trùng với tiếp tân hoàng gia. Tránh chỉ chọn phí thấp hơn.

Điểm tạm dừng

Chỉ ghi lại kiểu mạng lưới học tập.

Địa chỉ nhận bc1 không tự cho phép rút BTC qua mạng token khác. Còn thiếu gì?

1. Đổi bí danh người nhận.
2. Xác nhận rút trên chuỗi Bitcoin và mọi dữ liệu đều khớp.
3. Nhập hạt giống vào sàn.

> **Xem đáp án: Xác nhận rút trên chuỗi Bitcoin và mọi dữ liệu đều khớp.**
> Tài sản, mạng và phương thức nhận phải tương thích.

M03

Hàm băm, chữ ký và mã hóa

Mục tiêu

Phân biệt chính trực, cho phép và giữ bí mật.

Tìm hiểu

giá trị băm chuyển dữ liệu thành một dấu vân tay cố định. So sánh một dấu vân tay quen thuộc có thể giúp phát hiện những thay đổi, không chỉ liệt kê tập tin hoặc nhận diện người đăng chúng. Nếu bạn tải tập tin và giá trị băm từ cùng một trang bị xâm nhập, kẻ tấn công có thể thay thế cả hai.

khóa riêng cho phép tạo chữ ký; khóa công khai tương ứng để kiểm tra. Chữ ký này liên kết quyền truy cập vào một thông điệp cụ thể dựa trên thuật toán và luật lệ của nó. Không giấu nội dung đã ký. Trong bitcoin, một công ty hợp pháp là một phần của điều kiện để sử dụng một lối thoát.

mã hóa muốn một nội dung chỉ có thể được đọc với khả năng thích hợp. mã hóa có xác thực tăng cường cảm biến. Trong hệ sinh thái Cuvex, có bản mật mã bảo vệ bí mật, các giao dịch được ký kết cho phép chi phí và kênh mật mã vận chuyển thông điệp. Chúng không phải là những vật thể tương tự, dù cho tất cả chúng đều sử dụng mã hóa.

Một mật khẩu người thường có chức năng dẫn xuất trước khi được dùng làm khóa mã hóa. 'AES-256' mô tả thuật toán và kích thước khóa, nhưng nó không biến một mật khẩu có thể dự đoán được thành một lựa chọn mạnh mẽ. Thế hệ, thực hiện, lưu trữ, màn hình hiển thị và phục hồi là một phần của sự an toàn tuyệt đối.

Điều này cũng không hàm ý rằng một chiếc QR là an toàn vì nó có vẻ phức tạp. Chúng ta cần biết những gì trong đó, ai đã tạo ra nó và những gì ứng dụng sẽ làm với nó. Trước khi chấp nhận một hành động, hãy yêu cầu gia sư giải thích mục đích của nó mà không cần hỏi ý kiến riêng.

Thực hành

1. Cộng tác tìm kiếm thay đổi tập tin, "Tiết mã hạt giống khôi phục" và "Khởi động thanh toán" bằng giá trị băm, mã hóa và ký.
2. Nó thay đổi một chữ cái từ một văn bản hư cấu, và nó nhận ra rằng giá trị băm của bạn thay đổi; đừng dùng bí mật để chứng minh điều này.
3. Giải thích tại sao một giao dịch có thể được công khai và ký cùng một lúc.

Chứng minh bạn đã hiểu

Bạn có thể mô tả những gì bảo đảm bạn đang tìm kiếm và cơ chế nào để cung cấp cho nó mà không cần phải được mã hóa để đồng nghĩa với tất cả các an toàn.

Câu hỏi thường gặp

Một chiếc giá trị băm phần sụn chứng nhận không có lỗi? Không. Xác định đượcytes nếu có thể tin cậy. Một cuộc kiểm toán, một công ty sản xuất và một bài kiểm tra vật lý sẽ trả lời cho các câu hỏi khác nhau.

Điểm tạm dừng

Để dành cả ba lá thư trong bài tập đi.

Cơ chế nào che nội dung bí mật?

1. Công bố tên tệp.
2. Ký mà không mã hóa.
3. Mã hóa đúng bằng một khóa được bảo vệ.

> **Xem đáp án: Mã hóa đúng bằng một khóa được bảo vệ.**
> Chữ ký hoặc dấu vân tay không tự bảo đảm bí mật.

Hạt giống, cụm mật khẩu và mật khẩu

Mục tiêu

Tránh sự nhầm lẫn giữa các thẻ thông hành khác nhau của hệ thống.

Tìm hiểu

Cụm từ ghi nhớ BIP39 biểu diễn entropy và tổng kiểm tra bằng từ trong danh sách. Độ dài chuẩn là 12, 15, 18, 21 hoặc 24 từ. Chọn câu dễ nhớ, lời bài hát hay tự chọn từ “ngẫu nhiên” không tương đương tạo an toàn. Tổng kiểm tra phát hiện một số lỗi, không chứng minh ai đã tạo hạt giống hay không ai khác biết nó.

Cụm mật khẩu BIP39 tham gia dẫn xuất hạt giống nhị phân. Cụm khác có thể mở một ví hoàn toàn khác, trông như trống và không nhất thiết báo “sai cụm mật khẩu”. Cụm này không bắt buộc là từ trong danh sách và không phải “từ thứ hai mươi lăm” theo nghĩa đen.

mật khẩu của bản mật mã Cuvex bảo vệ bí mật được lưu trữ. mật khẩu Desk bảo vệ kho hàng địa phương khỏi máy tính. Hệ thống liên lạc PIN cho phép kết nối. khóa Chat đã lấy lại được danh tính thư tín. Không ai trong số họ nên nhầm lẫn với hạt giống khôi phục, và biết một người không có nghĩa là họ có thể xây dựng lại tất cả mọi thứ.

Lưu hạt giống khôi phục và cụm mật khẩu cộng với nhau trong bản mật mã có thể giúp phục hồi, nhưng nó loại bỏ sự tách biệt của bạn trước người có thể giải mã nó. Chia ra làm hai đòi hỏi cho ngươi và những người thừa kế. Quyết định này phải được ghi lại và chứng minh; nó không được đưa ra bởi vì gia sư xem như là một sự lựa chọn cao cấp hơn.

Thực hành

1. Tạo năm thẻ giấy chỉ ghi nhãn, không ghi giá trị bí mật: hạt giống, cụm mật khẩu, mật khẩu Cuvex, mật khẩu Desk và khóa trò chuyện.
2. Viết ra những gì có thể lấy lại được và bạn sẽ mất những gì khi quên nó.
3. Thiết kế thử nghiệm trên ví trống. Nhập các từ và cụm mật khẩu ở nơi riêng tư, chỉ báo kết quả cho gia sư.

Chứng minh bạn đã hiểu

Nó giải thích tại sao khóa học không bao giờ nên yêu cầu mật khẩu để kiểm tra kiến thức của bạn. Xác định bí mật cần thiết cho quá trình phục hồi của anh.

Câu hỏi thường gặp

Có thể đặt lại cụm mật khẩu qua email không? BIP39 không có cơ chế đó. Bên lưu ký có thể có quy trình khôi phục tài khoản nhưng đó là mô hình khác.

Điểm tạm dừng

Đăng ký các giá trị khác nhau.

Bạn đổi một chữ trong cụm mật khẩu BIP39 và thấy số dư bằng không. Giải thích nào đúng?

1. Có thể đây là ví hợp lệ khác được dẫn xuất từ cụm mật khẩu khác.
2. Mạng đã xóa tiền.
3. Desk phải đoán cụm mật khẩu ban đầu.

> **Xem đáp án: Có thể đây là ví hợp lệ khác được dẫn xuất từ cụm mật khẩu khác.**
> Cụm mật khẩu khác có thể sinh một ví khác mà không báo lỗi.

Dẫn xuất khóa, xpub và descriptor

Mục tiêu

Hiểu cách mô tả một chiếc ví mà không đưa ra khả năng chi tiêu.

Tìm hiểu

Một chữ ví cấp bậc bắt nguồn từ chữ các khóa từ gốc. Một con đường cho thấy nhánh nào được dùng. Vào mainnet , BIP84 Thường dùng mét/giây 84 '/ 0 '/ 0 'cho tài khoản đầu tiên. SegWit Xác nhận một mình; BIP48 P2WSH Dùng mét/giây 48 '/ 0 '/ 0 '/ 2 ♪ Trong tài khoản đầu tiên ♪ đa chữ ký . Tờ rơi ghi là dẫn xuất tăng cường. Thay đổi tài khoản, mạng hay kiểu văn lệnh có thể cung cấp địa chỉ khác từ cùng một cụm từ ghi nhớ.

xpub là một khóa công khai mở rộng cho phép con cháu có thể bắt nguồn từ một số khóa công khai. Nó không phải là một chiếc mật khẩu tiêu dùng, nhưng nó có thể cho phép bạn quan sát một gia đình địa chỉ. dấu vân tay khóa chủ là một bộ nhận dạng ngắn có ích để liên kết các bản ghi chép; nó không bảo đảm một người nào đó sẽ được nhận diện hoặc tránh va chạm.

Một descriptor chỉ ra cách xây dựng văn bản và địa chỉ: dạng văn bản, các khóa, nguồn gốc và đạo hàm. Một descriptor chỉ theo dõi với khóa công khai Cho phép quan sát, không ký. Từ " descriptor Không bảo đảm rằng nó chỉ chứa thông tin công cộng: một số định dạng có thể bao gồm khóa riêng . Đừng bao giờ đưa descriptor thật lên lớp.

Để lấy lại một chiếc đa chữ ký, chúng ta thường cần toàn bộ chính sách, chứ không phải chỉ một trong những chữ bên ký. Nó giữ cửa, người tham gia, xpubs, đường dẫn, mạng lưới, kiểu văn bản và dữ liệu khám phá. Tổng kiểm tra descriptor giúp phát hiện lỗi phiên bản; không xác định người tham gia.

Thực hành

1. Đọc một con đường tưởng tượng và giải thích mục đích, tiền xu, tài khoản và chi nhánh. Đừng nhập các khóa thật.
2. Phân loại địa chỉ nhận, xpub người tham gia và descriptor.
3. Hãy chuẩn bị một hồ sơ phục hồi cá nhân với tên trường trống và địa điểm tài liệu riêng biệt.

Chứng minh bạn đã hiểu

Bạn có thể giải thích tại sao một chiếc ví trống rỗng sau khi phục hồi không bị mất gì: bạn phải kiểm tra mạng lưới, cụm mật khẩu, tài khoản, đường dẫn và khám phá.

Câu hỏi thường gặp

xpub có thể được xuất bản mà không có hậu quả gì sao? Tuy nhiên, nó tiết lộ sự riêng tư và có thể tăng thêm những nguy hiểm khác trong các bộ mã hóa.

Điểm tạm dừng

Lưu thẻ không có giá trị nhạy cảm trong khóa học.

Khi chỉ có một hạt giống để khôi phục ví đa chữ ký, có thể thiếu gì?

1. Màu thiết bị.
2. Chính sách và khóa công khai của các bên tham gia khác.
3. Mật khẩu mạng xã hội.

> **Xem đáp án: Chính sách và khóa công khai của các bên tham gia khác.**
> Ngoài việc đủ ngưỡng khóa riêng, việc dựng lại script cần chính sách đầy đủ.

M03

Chọn ví và mô hình lưu ký

Mục tiêu

So sánh các công cụ theo chức năng, lòng tin và sự phục hồi.

Tìm hiểu

Ví là tập hợp công cụ mô tả, quan sát và khi phù hợp, cho phép chi tiêu. Ví nóng giữ khả năng ký trong môi trường có kết nối. Thiết bị ký cách ly nhằm tách bí mật khỏi máy truy vấn mạng. Ví chỉ theo dõi có đủ dữ liệu công khai để quan sát và chuẩn bị, nhưng cần hệ thống khác để ký.

Tại lưu ký, một tài khoản có thể đại diện cho một quyền đối đầu với một công ty. Ở tự lưu ký, bạn duy trì kỹ năng chi tiêu, theo một cách cá nhân hoặc chia sẻ. Sự hồi phục qua email và sức mạnh ngăn chặn việc rút lui thường phản ánh mô hình đầu tiên. Bạn không nên đánh giá cả hai lựa chọn với cùng một cái gọi là trách nhiệm.

So sánh hỗ trợ mạng và văn bản, kiểm tra trên màn hình, sao chép, cập nhật, tương tác, bảo trì, tham khảo các nhà cung cấp lỗi rõ ràng. Một danh sách tiền xu hay một cái kết thể xác là không đủ. Một thiết bị ký cũng không giúp bạn chấp nhận một địa chỉ sai nếu bạn không kiểm tra nó.

Cuvex tách bí mật trong bản mật mã khỏi việc quản lý và truy vấn trong Desk. Mô hình này đòi hỏi giữ bản mật mã và các yếu tố mở khóa. Chống mất thiết bị không đồng nghĩa vẫn khôi phục được nếu mọi bản sao hoặc mật khẩu đều mất. Học trọn quy trình trước khi chuyển tài sản.

Thực hành

1. So sánh Cuvex với ví nóng và sàn giao dịch trong một ma trận: ai ký, ai nhìn vào tư vấn, ai có thể truy cập và điều gì xảy ra khi công ty đóng cửa.
2. Hãy chọn hai tiêu chuẩn mà bạn cần chứng minh bằng chứng chứ không phải bằng quảng cáo.
3. Hãy kiểm tra xem môi trường thực hành không chia sẻ các khóa với khoản tiết kiệm thực tế của anh.

Chứng minh bạn đã hiểu

Anh ta bào chữa cho một vụ án cụ thể mà không tuyên bố một công cụ bất khả xâm phạm nào.

Câu hỏi thường gặp

Một phần cứng ví Ông có giữ mọi giao dịch không? Không. Chủ yếu bảo vệ khả năng ký hiệu và một phần của bản kiểm tra, chuỗi thông tin, tham khảo và đối tác vẫn tiếp tục tạo ra thông tin.

Điểm tạm dừng

Hãy giữ ma trận tiêu chuẩn của bạn mà không cần tên tài khoản.

Ví chỉ theo dõi được cấu hình đúng bằng khóa công khai có thể làm gì?

1. Quan sát và chuẩn bị giao dịch nhưng không tự ký.
2. Thay thế hạt giống đã mất.
3. Bảo đảm ẩn danh.

> **Xem đáp án: Quan sát và chuẩn bị giao dịch nhưng không tự ký.**
> Theo dõi và phê duyệt là hai khả năng tách biệt.

M03

Tạo bản sao lưu có thể khôi phục

Mục tiêu

Thiết kế một bản sao hoàn chỉnh và chứng minh sự phục hồi trước khi phụ thuộc vào bản sao đó.

Tìm hiểu

Một chiếc bản sao lưu hữu ích có thể lấy lại một khả năng, không chỉ là một tập tin. Cho một người duy nhất khẳng định có thể yêu cầu cụm từ ghi nhớ, cụm mật khẩu và dữ liệu dẫn xuất. Với một đa chữ ký, nó đòi hỏi thêm chính trị và số lượng bên ký. Với Desk, có thể cần một bản sao và bản mật khẩu của nó. Đối với chat, lấy lại danh tính không có nghĩa là lấy lại thông điệp lịch sử.

Sự dư thừa có thể che chở bạn khi bị mất mát; sự ly thân che chở bạn khỏi sự ràng buộc. Hai bản sao khác nhau có thể được sao lưu và các nơi có thể giảm thiểu lỗi tương quan. Mỗi bản sao phụ cũng cần phải kiểm soát, kiểm kê và kiểm tra. Tên tập tin và thẻ không được tiết lộ tài sản hoặc dễ dàng định vị tất cả các thành phần.

Một thử nghiệm phải xác nhận một địa chỉ đã được kiểm tra trước và trong môi trường học tập, khả năng ký một thao tác có kiểm soát. Xem hồ sơ mở không chứng minh được nó là đúng ví. Cũng đừng kiểm tra một bản sao bằng cách đưa hạt giống khôi phục vào máy tính nào đó.

Tài liệu phụ thuộc vào những gì nó bao gồm và những gì mà mỗi bản sao không có. Thay đổi mật khẩu hiện tại không tự động thay đổi bản sao cũ. Nếu một mật khẩu trước đó được phát hiện, thì bản sao lưu vẫn bị ảnh hưởng. Xoá tập tin vào kho hiện đại cũng không bảo đảm xóa tất cả các bản sao hay phiên bản của nó.

Thực hành

1. Hoàn tất bảng riêng: đối tượng, nội dung, mật khẩu liên kết, vị trí độc lập, ngày thử nghiệm và có trách nhiệm.
2. Nó phục hồi một bản sao kiến thức trong một môi trường riêng biệt. Kiểm tra mạng lưới, địa chỉ đầu tiên và dẫn xuất.
3. Mô phỏng việc mất máy tính và sau đó mô phỏng thiết bị. Xác định quy trình thay đổi.

Chứng minh bạn đã hiểu

Bạn có thể lấy lại kịch bản thử nghiệm của mình mà không cần trợ giúp và giải thích những thông tin mà bạn vẫn chưa biết cho một kịch bản khác.

Câu hỏi thường gặp

Bản sao toàn cầu của Desk là bản sao của mọi thứ? Anh không nên chấp nhận điều đó. Trong cơ sở kiểm tra, lịch sử và buổi nói chuyện không có trong đó. Chính trị đa chữ ký và khóa riêng Chúng có chức năng khác nhau.

Điểm tạm dừng

Ghi lại ngày tháng và kết quả của thử nghiệm; không bao giờ lưu nội dung của bản sao.

Sau khi đổi mật khẩu Desk, bản sao lưu trước đó thế nào?

1. Tự cập nhật.
2. Tự mất mã hóa.
3. Giữ cách bảo vệ và mật khẩu khi được tạo.

> **Xem đáp án: Giữ cách bảo vệ và mật khẩu khi được tạo.**
> Các bản sao cũ là những đối tượng độc lập.

M04

Làm quen với Original và BIT

Mục tiêu

Chọn đường đi đúng theo thiết bị và phiên bản của nó.

Tìm hiểu

Original sử dụng thẻ NFC để vận chuyển bản mật mã và các thao tác tương thích; Bluetooth góp phần vào việc cập nhật. USB-C của bạn được sử dụng làm thức ăn cho mô hình được ghi nhận. BIT sử dụng USB-C để chia sẻ tập tin và thêm sinh trắc học cho bản mật mã yêu cầu. Đừng di chuyển hướng dẫn NFC hay Bluetooth từ Original đến BIT.

Trong thiết bị này, bạn sẽ tìm thấy chức năng cho mã hóa, giải mã, tạo ví và ký, cộng với điều chỉnh. Original nhập bản sao thẻ; BIT làm việc với các tập tin hỗ trợ USB. Các bảng chữ cái, ngôn ngữ và truy cập có thể thay đổi theo các phiên bản khác. Quyền truy cập mới của mục đích chính trị trên BIT sẽ dẫn đến dòng chảy phù hợp và không thay đổi ai cho phép.

Bài xã luận được duyệt lại Original 1.2.2 Kết thúc rồi. BIT 1.2.3 Kết thúc rồi. Desk Một ly. 9.21 Và Mirror Một ly. 12.12 . Đây là nguồn tham khảo: chữ ký, phân phối và chấp nhận vật lý của mỗi tổ hợp cần được kiểm tra với máy tính. Đừng thay thế phần sụn của bạn bằng một nhị phân mà không có chữ ký trong một gói kỹ thuật.

Trước khi sử dụng một nhóm, hãy kiểm tra nguồn gốc, tiền lệ, ngoại hình và phiên bản. Dấu vết và việc cập nhật cũng có thể giúp chúng ta với những mối đe dọa cụ thể, nhưng chúng không thay thế tất cả các cuộc kiểm tra. Nếu bạn nhìn vào thao tác hoặc phiên bản bất ngờ, bạn dừng việc khởi tạo và tham khảo ý kiến từ một kênh mà bạn đã kiểm tra.

Thực hành

1. Xác định mẫu của anh và ghi lại phiên bản nhìn thấy của anh mà không cần chụp ảnh bí mật.
2. Xác định mã hóa, giải mã, tạo ví, PSBT và điều chỉnh. Đừng xóa hay cập nhật thực đơn.
3. Chọn nhánh Original hoặc BIT trong khóa học. Hãy duy trì sự lựa chọn đó trong lúc luyện tập.

Chứng minh bạn đã hiểu

Giải thích cách thức hoạt động của mô hình của bạn được tiến hành và bạn phải bảo vệ bản thân khỏi những tác phẩm ngoài ý muốn.

Câu hỏi thường gặp

BIT tự động an toàn hơn cho bất cứ ai? Các mô hình đưa ra những quyết định khác nhau về cách vận hành. Câu trả lời phụ thuộc vào mối đe dọa, hồi phục và sử dụng đúng cách.

Điểm tạm dừng

Lưu mẫu và phiên bản trong sổ tay địa phương của bạn; khóa học chỉ cần mô hình được chọn.

Bạn có BIT nhưng hướng dẫn đòi ghi thẻ NFC ngay bằng thiết bị. Bạn làm gì?

1. Kiểm tra hướng dẫn có đúng mẫu không và dùng quy trình USB tương thích.
2. Ép cập nhật phần mềm của Original.
3. Gửi hạt giống sang điện thoại.

> **Xem đáp án: Kiểm tra hướng dẫn có đúng mẫu không và dùng quy trình USB tương thích.**
> Hướng dẫn phải đúng với phương thức truyền thực tế của mẫu thiết bị.

M04

Tạo hạt giống bằng entropy vật lý

Mục tiêu

Hiểu thế hệ và tập lưu mà không chuyển dữ liệu khóa học thành các khóa.

Tìm hiểu

entropy không thể đoán trước được. Một vài con xúc xắc có thể đóng góp entropy nếu chúng thích hợp, thứ tự được thiết lập trước khi khởi động và thuật toán chuyển đổi là đúng. Kết quả từ chối một thủ tục nào đó nên được lặp lại chính xác như bạn nói; thay thế bằng số tối đa hoặc chọn một từ khác để giới thiệu thành kiến.

Quy trình Cuvex đã rà soát dùng một đồng xu và bốn viên xúc xắc. Hàm chuyển đổi lấy giá trị đồng xu × 1.296 rồi cộng số hệ sáu được tạo bằng kết quả từng viên trừ một. Chỉ nhận chỉ số từ 0 đến 2.047. Nếu nằm ngoài từ điển, phải tung lại đồng xu và gieo lại cả bốn viên. Giữ nguyên đồng xu rồi chỉ gieo xúc xắc sẽ gây thiên lệch. Đây là mô tả từ mã nguồn đã rà soát. Màn hình và toàn bộ quy trình phải được xác minh trên từng bản phần sụn phân phối.

Nó không giống với việc chọn từ yêu thích. Đừng biến một cuộc biểu tình công khai thành tài liệu bảo vệ tiền bạc. Bất kỳ hạt giống khôi phục nào có trong vật liệu phân tích đều được biết đến. Từ cuối cùng và kiểm tra của bạn phải được thực hiện bằng thuật toán đầy đủ của thiết bị, chưa hoàn thành cụm từ ghi nhớ bằng tay.

Nó tạo ra một không gian không có máy ảnh, trợ lý giọng nói hoạt động gần đây, thu âm màn hình, hay những người quan sát. gia sư phải dừng lại trong lúc vào và kiểm tra bí mật. Bạn có thể giải thích trước và sau đó đánh giá bằng những câu hỏi về quá trình này, mà không cần nghe kết quả của việc phóng hay từ ngữ.

Sau khi sản xuất ra, bạn phải kiểm tra bản sao lưu, tính toán dựa trên mô hình và thử xem một ví trống có phục hồi không. Một địa chỉ kiểm tra giúp xác nhận chính xác hạt giống khôi phục trên máy tính. Nếu dòng lưu thông chấp nhận các giá trị trái ngược với chỉ thị hoặc có những từ bất ngờ, hãy dừng sử dụng và ghi lại chỉ một phiên bản, màn hình và lỗi.

Thực hành

1. Trong thử nghiệm, anh ta theo bước của thiết bị với vật liệu chưa có tiền. Đặt thứ tự xúc xắc và không thay đổi kết quả.
2. Lặp lại các đầu vào bị từ chối trên màn hình, không sửa đổi để phù hợp với nó.
3. Hãy kiểm tra riêng nội dung, tạo bản sao và xác nhận rằng bạn có thể xây dựng lại cùng một ví kiến thức.

Chứng minh bạn đã hiểu

Giải thích tại sao entropy vật lý, sự cải đạo đúng và bí mật của kết quả là ba điều kiện khác nhau.

Câu hỏi thường gặp

Tôi có thể đếm số của tôi cho AI để kiểm tra thuật toán không? Không phải cho một chiếc hạt giống khôi phục mà anh sẽ dùng. Tham dự làm việc với những ví dụ tổng hợp khác nhau.

Điểm tạm dừng

Nó kết thúc trong trạng thái an toàn của thiết bị; đừng để lại hạt giống khôi phục nhìn thấy trong lúc nghỉ ngơi.

Phần sụn từ chối một kết quả xúc xắc. Cách nào đúng quy trình?

1. Tự chọn một từ.
2. Làm lại theo hướng dẫn thiết bị mà không gây thiên lệch.
3. Giảm số cho đến khi được nhận.

> **Xem đáp án: Làm lại theo hướng dẫn thiết bị mà không gây thiên lệch.**
> Loại một số kết quả là một phần của ánh xạ entropy, không được tự ý thay thế.

M04

Mã hóa và giải mã bí mật bằng Cuvex

Mục tiêu

Tạo ra bản mật mã học tập và kiểm tra sự hồi phục của nó.

Tìm hiểu

Chọn loại nội dung đúng: BIP39, SLIP39, hoặc văn bản khi có trong dòng. Chúng là những dạng khác nhau. mã hóa văn bản SLIP39 không biến Cuvex thành bên ký trong tất cả các mạng mà bạn có thể sử dụng. Lưu trữ bí mật và thực hiện giao thức ký có tầm rộng khác nhau.

Hãy nhập nội dung trực tiếp vào thiết bị khi bạn tìm kiếm nó bên ngoài các thiết bị kết nối. Một phương pháp nhập khẩu từ điện thoại hay PC có thể đã được phát hiện, ngay cả khi sau đó là mã hóa. Màn hình duyệt trước là nơi phát hiện từ, thứ tự, chữ viết hoa và những lĩnh vực khác nhau.

♪ La mật khẩu của bản mật mã Nó phải dài, độc nhất và có thể phục hồi theo kế hoạch của anh. Bàn phím tạo bản in có khả năng cho 40 ký tự và chức năng cần thiết ít nhất 12, chữ hoa và chữ thường ASCII, số và biểu tượng được công nhận. Đừng áp dụng tự động 12 a 1.024 ký tự Desk Bàn phím Cuvex : Desk Nó áp dụng một chính sách khác. Các lĩnh vực phục hồi khác có thể có các giới hạn khác nhau; kiểm tra dòng chảy và phiên bản.

Trong Original, ông viết trên một tấm thiệp đầy đủ và trống rỗng; hãy giữ vị trí cho đến khi có được xác nhận. Trong BIT, lưu trữ các tập tin tạo ra dòng USB, kể cả các thành phần sinh trắc học cần thiết khi nó chạy. Không có danh tiếng hay kết hợp tập tin theo trực giác. Sau đó, ông đọc và giải mã Thử ra trên thiết bị, chưa truyền thông tin bí mật cho gia sư .

Thực hành

1. Chương trình này tạo ra một văn bản có giá trị kỹ thuật, không có giấy chứng nhận và không có giá trị kinh tế.
2. Nhận diện khung và các đối tượng kết quả; ghi riêng biệt bí danh và chức năng của nó.
3. Khởi động lại quá trình giải mã, kiểm tra lại đoạn văn trên màn hình tin tưởng và đóng hình khi bạn hoàn thành.

Chứng minh bạn đã hiểu

Bạn có thể phân biệt nội dung đúng, viết đúng và phục hồi đúng. Tin nhắn "Cấu hình" không chứng minh được cả ba.

Câu hỏi thường gặp

Tên thẻ tín dụng là mật khẩu phải không? Không. Đó là thông tin tổ chức. Đừng bao gồm cả những khoản nợ hoặc mô tả để dễ nhận diện tài sản của bạn.

Điểm tạm dừng

Đừng để lại nội dung giải mã. Chỉ ghi lại thành công hoặc thất bại của bài luận.

Cách nào chứng minh tốt nhất một bản mật mã thử nghiệm có thể khôi phục nội dung?

1. Tên tệp đẹp.
2. Tệp có trong hai thư mục.
3. Đọc và giải mã đúng quy trình, rồi kiểm tra nội dung riêng tư.

> **Xem đáp án: Đọc và giải mã đúng quy trình, rồi kiểm tra nội dung riêng tư.**
> Có bản sao không chứng minh nó dùng được hay khớp dữ liệu cần khôi phục.

M04

Ngưỡng mã hóa và sinh trắc học

Mục tiêu

Tách biệt sự bảo vệ chung của bí mật đa chữ ký từ bitcoin.

Tìm hiểu

Một bản mật mã được bảo vệ bởi nhiều mật khẩu quy định ai có thể thực hiện được giải mã nội dung. Một ví bitcoin đa chữ ký Điều chỉnh điều gì các khóa Họ phải cho phép một chi phí trên mạng. Bạn có thể có một bí mật mã hóa dùng chung để phù hợp với một ví một lần xác nhận, hoặc mỗi bên ký của một đa chữ ký với riêng bản mật mã của nó.

Nếu một vài người mở khóa cùng nhau chỉ một hạt giống khôi phục và hạt giống khôi phục đó là cho phép sử dụng một mình, ngưỡng của chuỗi này vẫn là khóa. Một khi nó được phát hiện, sẽ có người bảo tồn nó. Đừng miêu tả sơ đồ đó như thể hắn bắt cô ta phối hợp với chữ ký cho mỗi lần thanh toán.

sinh trắc học của BIT thêm một điều kiện truy cập vào định dạng mà họ sử dụng. Một ngón tay không phải là một chiếc hạt giống khôi phục hay là một cái thay thế toàn cầu cho chiếc mật khẩu. Hắn lên kế hoạch gây thương tích, thay đổi vân tay, hỏng hóc, có sẵn thiết bị và tài sản thừa kế. Giữ lại và kiểm tra phương pháp hồi phục của bản mật mã trước khi phụ thuộc vào nó.

Xuất khẩu phục hồi có thể tiết lộ bí mật trong máy tính, chính xác để giải quyết tình huống khẩn cấp. Sự tồn tại của chức năng này không biến PC thành một môi trường tương đương với thiết bị. Thực hành thông thường phải giữ sự cô lập; sự phục hồi địa phương được nghiên cứu một cách có ý thức và với kế hoạch di cư sau này nếu đã được tiếp xúc.

Thực hành

1. Vẽ hai chính sách: “hai mật khẩu để mở một hạt giống” và “hai trong ba khóa để chi tiêu”.
2. Trong một cuộc thử nghiệm không tài chính, nó xác định những tập tin nào cần một bản sao sinh trắc học và nơi mà sự hồi phục của nó được kiểm chứng.
3. Giả vờ như một người không còn sẵn sàng. Xác định ngưỡng của giản đồ cho phép bạn tiếp tục.

Chứng minh bạn đã hiểu

Anh có thể giải thích ai có thể biết bí mật này và ai có thể cho phép chi tiêu sau khi giải mã nó.

Câu hỏi thường gặp

Tôi có thể rút lại người tham gia bằng cách thay đổi nhãn hiệu không? Không. Bạn phải phân biệt những thay đổi trong tổ chức với một sự bảo vệ mới cho bí mật và một chính sách chi tiêu mới.

Điểm tạm dừng

Lưu dữ liệu vào không có tên thật hay số liệu sinh trắc học.

Ba người dùng hai mật khẩu mở bản mật mã chứa một hạt giống ví đơn chữ ký. Bitcoin cần mấy khóa để chi?

1. Một nếu chính sách ví quy định như vậy.
2. Hai vì tệp bắt buộc hai mật khẩu.
3. Ba theo số người.

> **Xem đáp án: Một nếu chính sách ví quy định như vậy.**
> Ngưỡng mã hóa không đổi script kiểm soát tiền.

Nhân bản, lưu giữ và kiểm tra các bản sao

Mục tiêu

Xây dựng phần thừa mà không phá hủy bản sao hợp lệ duy nhất.

Tìm hiểu

Cho phép một bản mật mã sao chép dữ liệu được mã hóa; không tạo ra một số dư mới, một hạt giống khôi phục khác hoặc độc lập trước một số mật khẩu. Những bản sao giống hệt nhau giải quyết việc mất đi sự hỗ trợ chứ không phải cam kết của bí mật ban đầu. Đó là lý do tại sao một sự phục hồi và di cư tới các khóa mới phản ứng lại với những tình huống khác nhau.

Trong Original, thẻ bản mật mã và thẻ vận chuyển PSBT. Một hệ thống hỗ trợ thao tác có thể tái sử dụng theo dòng chảy; một thẻ với bản sao lưu của bạn không thể trở thành cái khung đó. Nếu một cuộc giải phẫu từ chối một tấm thiệp chứa một chiếc bản mật mã, đừng cố vượt qua bảo vệ hoặc xóa bỏ nó bằng tay.

Trong BIT, một bản sao phải được bảo tồn và mối quan hệ giữa các tập tin. Một trình quản lý tập tin có thể hiển thị một truyền tải hoàn chỉnh mà không bảo đảm thiết bị đã xác nhận nội dung hoặc hoàn thành thao tác của bạn. Hãy đợi những bang được đề cập và kiểm tra bản sao bằng cách phục hồi.

Hãy giữ một danh sách cá nhân với các bộ nhận dạng bí mật, phiên bản định dạng, ngày tháng và kết quả kiểm tra cuối cùng. Ít nhất là hai bản sao so với những sự kiện mà anh đã xác định. Tránh mang bản sao lưu lên kênh hỗ trợ để chẩn đoán vấn đề; cung cấp cho siêu dữ liệu mã lỗi và X10.

Thực hành

1. Tạo một bản sao của bản mật mã phương pháp của bạn trong một cái khác hỗ trợ thông qua dòng chảy đúng.
2. Tháo bỏ khung gốc và lấy lại đoạn thử ra từ bản sao.
3. Tài liệu cho biết anh sẽ làm gì khi bị mất dữ liệu, bị hư hại, và bị phơi nhiễm mật khẩu. Chúng không giống nhau.

Chứng minh bạn đã hiểu

Bạn có thể nhận ra bản sao mà bạn đã thử và giải thích tại sao bản gốc chưa được viết trên đó.

Câu hỏi thường gặp

Tôi có thể xóa bản gốc sau khi xem tập tin thứ 2 không? Đầu tiên kiểm tra phục hồi và che chắn. Việc loại trừ phải phản ứng với một kế hoạch, không phải số lượng bản sao đơn giản.

Điểm tạm dừng

Lưu các chốt trước khi đóng phiên chạy; đừng để thẻ trộn với chứng cứ thanh toán.

Một người biết mật khẩu và đã lấy bản mật mã. Tạo thêm ba bản sao giải quyết gì?

1. Vô hiệu bản sao của kẻ tấn công.
2. Tăng dự phòng nhưng không thu hồi quyền truy cập đó.
3. Tự đổi hạt giống Bitcoin.

> **Xem đáp án: Tăng dự phòng nhưng không thu hồi quyền truy cập đó.**
> Nhân bản không khắc phục sự lộ lọt đã xảy ra.

M05

Cài đặt và bảo vệ Cuvex Desk

Mục tiêu

Mở một cơ sở xuất xứ xác nhận và bảo vệ kho hàng địa phương.

Tìm hiểu

Chọn gói theo hệ điều hành và kiến trúc: macOS Intel hoặc Apple Silicon, Windows x64 hoặc ARM64, Linux x64 hoặc ARM64 tùy bản được cung cấp. Tệp ZIP mã nguồn, gói Manager và trình cài cho khách là các bản phân phối khác nhau. Khóa học không được hướng học viên tới gói ký riêng.

Kiểm tra nguồn gốc và kiểm tra hệ thống. Một công ty kỹ thuật Windows không tự nó tạo sự tín nhiệm cho nhà xuất bản. Trong Mac, ký hiệu ứng dụng, lưu ý và đánh giá khi mở là những bộ điều khiển khác nhau. Đừng vô hiệu hóa hệ thống bảo vệ chung bằng cách gọi hỗ trợ. Nếu một bản dịch có thông báo bất ngờ, hãy giữ đoạn và sử dụng kênh chính thức.

Desk Tạo ra một nhà kho địa phương mã hóa với mật khẩu . Trong cơ sở đã sửa chữa, bản mật khẩu mới thừa nhận 12 đến 1.024 ký tự; sự trùng hợp các trường được yêu cầu ở nơi có xác nhận. Những giới hạn đó không đủ để đo lường chất lượng. Nó sử dụng một cụm từ độc đáo và tránh dùng lại. sinh trắc học máy tính, khi có thể, là một tiện nghi để truy cập yêu cầu thiết lập của chính nó.

Cấu hình khóa cho hoạt động, và nếu bạn đi, bằng cách chuyển sang nền. Sự trì hoãn sau khi lỗi và sự chọn lọc được nghiên cứu trong sổ tay: Đừng cài đặt một máy xóa tự động trong khi trình diễn. App có thể hoạt động mà không cần tài khoản người dùng thông thường, nhưng dịch vụ tư vấn, chat hoặc tải về có những yêu cầu và thông tin liên lạc cụ thể.

Thực hành

1. Kiểm tra nền tảng, phiên bản nhìn thấy và nguồn của gói mà không đưa ra gia sư người nhận dạng cá nhân.
2. Nó tạo ra một kho lưu trữ học tập và kiểm tra khóa và mở lại. Đưa mật khẩu vào phòng riêng.
3. Lập trình một bản sao mã hóa và giữ mật khẩu theo kế hoạch của anh. Đừng thử khóa lặp lại trong môi trường thực tế.

Chứng minh bạn đã hiểu

Bạn có thể phân biệt mật khẩu địa phương, tài khoản thương mại và giấy ủy nhiệm dịch vụ bạn thêm vào.

Câu hỏi thường gặp

Thay đổi mật khẩu Desk thay đổi thẻ của tôi? Không. Đó là những biện pháp bảo vệ độc lập. Bản sao cổ cũng không tự thay đổi.

Điểm tạm dừng

Khóa Desk và lưu thẻ bài học, không giấy tờ.

Trình cài đặt không đúng kiến trúc máy. Bước đầu tiên là gì?

1. Tắt bảo vệ để ép chạy.
2. Lấy đúng gói chính thức và kiểm tra yêu cầu.
3. Nhập hạt giống vào trang web để tiếp tục.

> **Xem đáp án: Lấy đúng gói chính thức và kiểm tra yêu cầu.**
> Phải giải quyết vấn đề tương thích và nguồn gốc trước khi dùng dữ liệu lưu ký.

Liên kết bản mật mã và sắp xếp tài khoản WOW

Mục tiêu

Hãy nhập mật mã một bản sao và phân biệt nó với tài khoản chỉ theo dõi.

Tìm hiểu

Desk Tổ chức bản mật mã Liên kết bởi NFC , USB hoặc tập tin sao chép phù hợp. Một thiết kế hình ảnh và một biệt danh giúp nhận ra chúng, nhưng chúng không phải là bằng chứng xác định nhân dạng. Bạn có thể tham khảo nguồn và thuộc tính được giải mã bằng app, như định dạng, kích cỡ và tính năng truy cập.

Kính hiển vi quan trọng hoặc tổ chức các đối tượng tương thích, không có nghĩa là giải mã nó trong PC hoặc kiểm tra lại bí mật của nó. WOW Là một ví chỉ theo dõi Nó liên quan đến thông tin công cộng. Một tập hợp các bí mật có thể có các tài khoản hoặc đạo hàm khác nhau: Hiệp hội phải tương ứng với tập hợp ví mà bạn muốn quản lý.

Kích hoạt hoặc nhập vào tài khoản với descriptor hoặc thông tin công cộng xuất khẩu bởi luồng của thiết bị. Kiểm tra mạng lưới, kiểu văn bản, dấu vân tay, đường dẫn và địa chỉ điều khiển. Tên tài khoản là tổ chức; mật mã gốc của một cái tên không nên được coi như một tên mạnh mẽ, vì một cái tên có thể đoán trước được.

Trong cơ sở Desk, tài khoản và chức năng được lưu trữ để xuất bản, nhân bản và xóa sổ tài liệu địa phương. Xóa thẻ giao diện không phá hủy bản sao bên ngoài, cũng không di chuyển quỹ. 'Không có bản sao lưu' có nghĩa là ứng dụng không có bản sao nào được ghi lại theo tiêu chuẩn của nó, không có bản sao lưu tồn tại trên thế giới.

Thực hành

1. Anh ta đánh dấu bản mật mã phương tiện giao thông được chọn và kiểm tra hồ sơ của mình.
2. Nhập khẩu một tài khoản học tập phù hợp với và kiểm tra mạng lưới và địa chỉ kiểm tra mà không hiển thị các khóa đến gia sư.
3. Phân biệt bản ghi bản mật mã, tài khoản WOW và phần thân thể. Xác định thứ gì sẽ biến mất với việc loại bỏ cục bộ.

Chứng minh bạn đã hiểu

Bạn có thể giải thích những dữ liệu nào cần Desk để quan sát và những dữ liệu mà chúng phải được lưu giữ bên ngoài máy tính trong khi sử dụng thông thường.

Câu hỏi thường gặp

Anh có thể đăng nhập một tập tin.bin đảm bảo đó là bản hạt giống khôi phục của tôi không? Không. Anh phải kiểm tra nguồn lực và sự hồi phục của cô ấy. Một phần mở rộng tập tin không được thông báo nội dung.

Điểm tạm dừng

Chỉ bảo tồn trạng thái « Kiểm tra thử ».

Xóa tài khoản WOW cục bộ có chuyển bitcoin của nó không?

1. Không, chỉ xóa dữ liệu cục bộ theo quy trình, không chi các UTXO.
2. Có, chuyển cho nhà sản xuất.
3. Hủy mọi chữ ký người khác đang giữ.

> **Xem đáp án: Không, chỉ xóa dữ liệu cục bộ theo quy trình, không chi các UTXO.**
> Trạng thái cục bộ và trạng thái trên chuỗi khác nhau.

Ghép nối Mirror với Desk

Mục tiêu

Đặt và hoàn thành một liên kết cục bộ được phép mà không nhầm mật mã.

Tìm hiểu

Mirror hỗ trợ thao tác cục bộ với Desk qua quy trình ghép nối, PIN và QR trong ứng dụng. PIN sáu chữ số chỉ thuộc phiên đó, không phải mật khẩu Desk, mật khẩu bản mật mã hay từ khôi phục. Kiểm tra màn hình nào tạo mã và nhập vào đâu. Không dùng mã do người lạ gửi.

Bắt đầu hành động từ bối cảnh Desk: kết nối, đọc QR, vận chuyển PSBT hay phần sụn là những kết quả khác nhau. Cửa sổ báo cáo tìm kiếm, kết nối, phát hiện, PIN, QR và hành động trên thẻ hay tập tin. Một thiết bị sẽ xuất hiện trong cuộc tìm kiếm không chứng minh toàn bộ hoạt động đã kết thúc.

Nó cung cấp những quyền hạn có liên quan theo hệ thống: máy ảnh để đọc và Bluetooth hoặc NFC khi dòng chảy cần thiết. Một chiếc điện thoại mà không có khả năng thể chất cần thiết sẽ không được lắp đặt bởi phần mềm. Trong iOS, có sự khác biệt về thích nghi và xác thực; không nên đưa ra một dự án biên dịch như thể nó đã được phân phối và thử nghiệm trên tất cả iPhone.

Nếu thất bại, xác định được giai đoạn chính xác: không xuất hiện, nhưng không kết nối, PIN từ chối, QR không đọc được, thẻ không đọc được hoặc trả lời không nhận được. Đóng các phiên họp cũ lại, kiểm tra các phiên bản phù hợp và giấy phép, và thử lại theo cách có kiểm soát. Một PIN sai không thể bào chữa cho việc chuyển đổi phần sụn hoặc đưa hạt giống khôi phục vào một nơi khác.

Thực hành

1. Bắt đầu đọc thử từ Desk và kết nối Mirror qua màn hình địa phương.
2. Kiểm tra mục đích trước khi giới thiệu một chiếc QR hay một tấm thẻ hành nghề.
3. Hủy bỏ phiên chạy và xác nhận rằng không áp dụng sau khi đọc văn cảnh trước. Mở lại một phiên mới.

Chứng minh bạn đã hiểu

Bạn có thể mô tả giai đoạn thất bại và các thiết bị liên quan mà không cần giao tiếp mật mã hoạt động hay nội dung nhạy cảm.

Câu hỏi thường gặp

Mirror có cần phải liên lạc với nhau không? Còn tùy vào hoạt động của chúng ta. Đừng xem đó là một dịch vụ lâu dài hoặc giả sử rằng một phiên họp được phép tiếp tục sau khi đóng cửa hoặc chuyển sang nền tảng.

Điểm tạm dừng

Đăng nhập vào phiên chạy liên kết và khoá các ứng dụng mà bạn chưa sử dụng.

Nếu ghép nối thất bại trước khi hiển thị PIN, gia sư nên làm gì?

1. Hỏi hạt giống.
2. Kiểm tra việc tìm thiết bị, quyền, phiên và phiên bản trước khi tiếp tục.
3. Coi kết nối đã hoàn tất.

> **Xem đáp án: Kiểm tra việc tìm thiết bị, quyền, phiên và phiên bản trước khi tiếp tục.**
> Chẩn đoán theo giai đoạn thực tế, không tự khẳng định đã kết nối.

NFC qua Mirror, USB-C và đọc mã QR

Mục tiêu

Sử dụng đúng mục đích và thực hiện đầy đủ kiểm tra cho từng phương thức truyền dữ liệu.

Tìm hiểu

Quy trình NFC trong Cuvex Desktop yêu cầu Cuvex Mirror chạy trên điện thoại thông minh tương thích đã ghép nối với máy tính qua Bluetooth. Cuvex Desktop không hỗ trợ đầu đọc NFC ngoài kết nối qua USB. Loại thẻ, định dạng và dung lượng cũng phải tương thích. Một thẻ nhỏ chứa được bản mật mã có thể không đủ chỗ cho PSBT chứa các giao dịch trước đó. Giới hạn thực tế phụ thuộc vào toàn bộ nội dung, không chỉ số người nhận. Không dùng thẻ sao lưu làm thẻ truyền dữ liệu.

Với Original, Mirror có thể ghi yêu cầu lên thẻ thao tác. Thiết bị xử lý rồi ghi phản hồi để Mirror chuyển về Desk. Xác nhận ghi thành công không có nghĩa Desk đã nhận. Giữ yên thẻ đến khi thiết bị báo kết quả. Nếu hệ thống từ chối để bảo vệ bản mật mã đã nhận diện, hãy tôn trọng việc từ chối đó.

BIT dùng ổ đĩa hoặc thư mục trao đổi qua USB. Ổ đĩa có thể được ngắt kết nối logic rồi xuất hiện lại trong quá trình này. Desk phải chọn đúng thiết bị lưu trữ, xác minh phản hồi và thực hiện bước xác nhận đã nhận. Chép tệp vào một thư mục trùng tên trên máy tính không có nghĩa đã chuyển tệp đến thiết bị.

Máy ảnh có thể không đọc được QR do lấy nét, phản quang, kích thước, chuyển động hoặc mật độ mã. Phóng to mã, điều chỉnh ánh sáng và khoảng cách. Không thay mã định danh dài bằng vài ký tự đầu hay chấp nhận bản chép một phần. Đọc thành công mới là bước đầu để xác minh ý nghĩa dữ liệu.

Thực hành

1. Dùng tài liệu học tập để chỉ ra yêu cầu, phương tiện truyền và phản hồi của Original và BIT trên sơ đồ.
2. Thử hủy đọc mã QR mà không lưu dữ liệu đến muộn. Lặp lại với mục đích khác.
3. Mô phỏng tình huống tệp quá lớn và giải thích vì sao cần đơn giản hóa giao dịch hoặc chọn phương tiện tương thích mà vẫn giữ nguyên các bước xác minh.

Chứng minh bạn đã hiểu

Chỉ rõ thiết bị nào xác nhận giai đoạn nào: đọc, ghi, xác minh, nhận hay gửi xác nhận đã nhận.

Câu hỏi thường gặp

Giá trị băm hoặc thông báo sao chép OK có chứng minh đúng người nhận Bitcoin không? Không. Phải kiểm tra giao dịch và các đầu ra ngay trên thiết bị ký.

Điểm tạm dừng

Tháo và cất các thẻ sao lưu. Đánh dấu rõ phương tiện dùng để truyền.

Original báo đã ghi phản hồi lên thẻ. Còn thiếu bước gì trước khi có thể nói Desk đã nhận?

1. Sơn thẻ màu khác.
2. Tạo một hạt giống mới.
3. Đọc phản hồi và xác minh trong Desk theo quy trình tương ứng.

> **Xem đáp án: Đọc phản hồi và xác minh trong Desk theo quy trình tương ứng.**
> Ghi thành công và nhận thành công là hai sự kiện khác nhau.

Nhà cung cấp công cộng và nút tự vận hành

Mục tiêu

Chọn nguồn truy vấn và hiểu dữ liệu có thể bị lộ cùng các giới hạn của nguồn đó.

Tìm hiểu

Desk có thể truy vấn nhà cung cấp công cộng tương thích hoặc Bitcoin Core do người dùng cấu hình. Nhà cung cấp có thể biết các truy vấn họ nhận, thứ tự và dữ liệu kết nối. Không gửi toàn bộ xpub giúp giảm một dạng lộ thông tin, nhưng các script hoặc giá trị băm của chúng vẫn có thể được liên kết với nhau.

Ngoài REST và nút riêng, Desk 9.21 có lựa chọn rõ ràng dùng Blockstream Electrum qua TLS. TLS bảo vệ kênh trước một số bên quan sát mạng, còn nhà cung cấp vẫn nhận truy vấn. Không có cơ chế âm thầm luân phiên nguồn nào bảo đảm ẩn danh. Hãy hiểu sự đánh đổi quyền riêng tư để lấy tiện lợi khi lựa chọn.

Với Core, cấu hình điểm cuối, xác thực và ví chỉ theo dõi theo hướng dẫn tương ứng. Không công bố cổng RPC hoặc để lộ cổng ra Internet chỉ để ứng dụng “nhìn thấy”. Giới hạn truy cập trong môi trường tin cậy và sử dụng phương thức truyền được bảo vệ thích hợp. Không đọc mật khẩu RPC cho gia sư.

Đồng bộ lần đầu và quét lại có thể tốn thời gian. Tiến độ chỉ phản ánh công việc đang diễn ra, không phải thông báo thành công sớm. Desk tiếp tục xử lý trong nền. Đóng màn hình theo dõi không dừng nút. Khoảng lịch sử tối thiểu trong tài liệu không bảo đảm phát hiện hoạt động trước đó. Nếu ví cũ hơn, hãy kiểm tra ngày nhập và phạm vi quét thực tế.

Việc dò địa chỉ dựa trên lịch sử, không dựa vào số dư dương. Địa chỉ đã chi hết vẫn là địa chỉ từng sử dụng. Với hồ sơ đa chữ ký đã rà soát, mỗi nhánh và người tham gia áp dụng khoảng trống 20 địa chỉ liên tiếp không có lịch sử, với các giới hạn cấp địa chỉ. Không áp một giới hạn chung cho mọi ví.

Thực hành

1. Chọn một nguồn để luyện tập và giải thích nguồn đó có thể thấy thông tin gì.
2. Kiểm tra ngày đồng bộ cuối, mạng và tiến độ. Nếu gặp HTTP 429, hãy chờ theo yêu cầu, không tự ý đổi nhà cung cấp khi chưa cân nhắc.
3. Mô phỏng một ví có số dư bằng không nhưng có lịch sử cũ. Giải thích vì sao “bằng không” khác với “chưa dùng”.

Chứng minh bạn đã hiểu

Xác định xem nguồn có đáp ứng nhu cầu xác minh và riêng tư của bạn không, đồng thời nhận ra trạng thái chưa hoàn tất.

Câu hỏi thường gặp

Tự vận hành nút có giúp tôi ẩn danh không? Không. Nó giảm phụ thuộc vào truy vấn bên ngoài, nhưng vẫn phải xét kết nối, đối tác, việc phát giao dịch và các siêu dữ liệu khác.

Điểm tạm dừng

Chỉ ghi loại nhà cung cấp và việc có cần hoàn tất quét hay không.

Một địa chỉ hiện có số dư bằng không nhưng từng nhận và chi tiền. Khi dò ví nên coi đây là gì?

1. Địa chỉ có lịch sử.
2. Địa chỉ chưa từng dùng.
3. Địa chỉ không hợp lệ.

> **Xem đáp án: Địa chỉ có lịch sử.**
> Lịch sử, không phải số dư hiện tại, quyết định địa chỉ từng được dùng hay chưa.

Nhận bitcoin và kiểm tra địa chỉ

Mục tiêu

Tạo một yêu cầu tiếp tân và kiểm tra trước khi giao nó.

Tìm hiểu

Mở tài khoản WOW và xác nhận mạng lưới và chính trị. Tạo ra hoặc lấy lại yêu cầu tiếp tân. Bạn có thể thêm lý do, quan sát và quan sát quan trọng chờ đợi tổ chức của bạn. Những trường này mô tả thông tin địa phương của bạn; những vấn đề mà bạn mong đợi không ngăn cản ai đó gửi thêm một số lượng nữa.

Hãy kiểm tra địa chỉ bằng cách lưu luồng trên thiết bị và bối cảnh của ví. Nếu cuộc hành trình đó chưa được tính toán kỹ lưỡng trong sự kết hợp của bạn, thì thực hành sẽ được duy trì trong mô phỏng và được quy mô trước khi nhận được vốn quan trọng. So sánh hai màn hình được nuôi dưỡng bởi cùng một nguồn không mang lại sự độc lập mà không có.

Dùng một địa chỉ mới cho một mối quan hệ chia sẻ mới khi dòng chảy cho phép. Trong đa chữ ký, các địa chỉ đã được hiển thị sẽ không được thay đổi hoặc quá hạn bởi vì một người trả tiền có thể sử dụng chúng sau này. Khi đạt đến giới hạn của những địa chỉ mới liên tục mà không có lịch sử nào cả, bạn sẽ lấy lại những yêu cầu trước đây và hiểu được động cơ giới hạn; đừng tua lại mục tiêu.

Sau khi chia sẻ, hãy nhìn vào nguồn gốc của bạn. Một thư điện tử, một lời bào chữa của sàn giao dịch hoặc bắt giữ người trả tiền không chứng minh được thanh lý . Kiểm tra mạng lưới, txid, ra ngoài, và số xác nhận cho thấy nó có liên quan. Đừng mở một nhà thám hiểm công cộng với địa chỉ của bạn để được thoải mái nếu kế hoạch của bạn đòi hỏi bạn phải giữ cho các tư vấn cá nhân.

Thực hành

1. Nó tạo ra một yêu cầu trong phòng thí nghiệm, kiểm tra tài khoản và mạng lưới, và giải thích làm thế nào bạn có thể kiểm tra địa chỉ.
2. Ghi lại một cái nhãn giả và nhận được cùng một yêu cầu sau khi đã đóng cửa sổ.
3. Mô phỏng một khoản tiền cho vấn đề khác nhau, và quyết định làm thế nào để cân bằng nó mà không thay đổi lịch sử.

Chứng minh bạn đã hiểu

Bạn có thể tìm ra địa chỉ, địa chỉ xác nhận, yêu cầu chia sẻ và tiền đã được xác nhận.

Câu hỏi thường gặp

Một địa chỉ cũ không hoạt động khi tạo ra một địa chỉ khác? Thường thì không. Giữ lại khám phá và đăng ký yêu cầu để tránh mất tầm nhìn của người trả chậm.

Điểm tạm dừng

Nó lưu lại tình trạng của yêu cầu phòng thí nghiệm, chứ không phải nó chứa trong gia sư.

Người trả gửi ảnh chụp ghi “đã rút xong”. Bạn kiểm tra gì trước khi nhận là đã thanh toán?

1. Chỉ chất lượng ảnh.
2. Đầu ra tương ứng trên nguồn mạng đáng tin cậy và đủ số xác nhận cần thiết.
3. Mật khẩu của người trả.

> **Xem đáp án: Đầu ra tương ứng trên nguồn mạng đáng tin cậy và đủ số xác nhận cần thiết.**
> Chứng từ thương mại hay ảnh chụp không thay thế xác minh thanh toán.

Gắn nhãn, đóng băng và chọn UTXO

Mục tiêu

Chuẩn bị các đầu vào mà không nhầm lẫn nguồn gốc của nó là ngẫu nhiên.

Tìm hiểu

Các thẻ cho phép chúng ta bảo tồn bối cảnh không có trong chuỗi: nguồn gốc, phần, mục đích và giới hạn sử dụng. Trong Desk, một nhãn UTXO và một ghi chú hướng có thể có chiều dài và chức năng khác nhau. Ghi chú « Khách hàng A » là hữu ích; dùng tài liệu hoặc tên đầy đủ của bạn có thể tạo một bản ghi không cần thiết.

Đóng băng UTXO trong Desk, loại trừ một số lựa chọn địa phương. Nó không ngăn chặn việc chi tiêu của bạn trong bitcoin Bạn không thay đổi văn lệnh và cũng không cản trở một số khác trong các tập lệnh các khóa Dùng nó đi. Nó cũng có thể làm cho tổng dư và số dư có thể khác nhau. Kiểm tra xem đồng xu có bị đông lạnh không, đặt vào bản nháp hoặc thực sự đã bị mòn.

Chọn lọc tự động tối ưu theo thuật toán và ngữ cảnh của nó; nó không nhất thiết phải biết mối quan hệ cá nhân của bạn. Để có tiền thanh toán cụ thể, hãy kiểm tra xem có nên sử dụng một lối thoát từ cùng hoàn cảnh đó thay vì kết hợp tiết kiệm, lương và hoạt động thương mại với nhau không. Sự phân chia hữu ích đòi hỏi sự nhất quán trong tương lai, chứ không chỉ những nhãn đẹp.

Xuất khẩu các thẻ dạng BIP329 sẽ dễ dàng giữ hoặc di chuyển chúng. Định dạng không phải một mình. Desk cung cấp giấy gói mã hóa cho việc xuất khẩu của nó; phân biệt tập tin được bảo vệ với một văn bản phẳng. Trong việc nhập khẩu, hãy kiểm tra khớp với ví và điều trị đông lạnh trước khi ghi đè lên thông tin.

Thực hành

1. Gắn nhãn ba UTXO giả lần lượt là tiết kiệm, hoạt động và quyên góp.
2. Dừng lại và kiểm tra sự khác biệt giữa số dư đã quan sát và khả năng chọn.
3. Nó được xuất bản từ phòng thí nghiệm với mật khẩu, có thể nhập vào một bản sao và kiểm tra kết quả không có dữ liệu cá nhân thực.

Chứng minh bạn đã hiểu

Anh ta bào chữa cho việc chọn các đầu vào với chi phí và triển lãm. Nhận ra rằng đóng băng là một sở thích địa phương.

Câu hỏi thường gặp

Một cái thẻ đi tới người nhận khi trả tiền? Không phải chỉ vì nó là một nhãn hiệu địa phương. Nó có thể được lọc sang bộ xuất khẩu, chia sẻ tập tin, dùng dịch vụ khác hoặc thêm vào một thông điệp.

Điểm tạm dừng

Lưu nhãn luyện tập và trạng thái đóng băng.

Đóng băng một UTXO trong Desk có tác dụng gì?

1. Khóa ở cấp đồng thuận trên mạng.
2. Chuyển nó sang tài khoản đặc biệt.
3. Áp dụng hạn chế cục bộ khi chọn đầu vào theo ứng dụng.

> **Xem đáp án: Áp dụng hạn chế cục bộ khi chọn đầu vào theo ứng dụng.**
> Không tước khả năng chi của các bản sao khóa khác.

Chuẩn bị và kiểm tra khoản thanh toán

Mục tiêu

Tạo một PSBT mà bạn hiểu được và nhận diện mọi chi phí, đầu ra của nó.

Tìm hiểu

Chọn tài khoản, đầu vào có thể chi, người nhận và số tiền. Xác minh nguồn yêu cầu. Sau khi dán hoặc quét, kiểm tra toàn bộ địa chỉ và mạng. Nội dung bộ nhớ tạm và hình ảnh đều có thể bị thay thế. Không chỉ so vài ký tự đầu và cuối khi quy trình cho phép kiểm tra đầy đủ.

Chọn phí suất và kiểm tra phí tuyệt đối, kích thước ước tính, tổng tiền và tiền thừa. Với “Gửi tất cả”, Desk trừ phí từ số tiền khả dụng. Nếu thanh toán từ cuộc trò chuyện và số thực nhận chưa đủ yêu cầu, việc trả một phần phải là quyết định có chủ ý. Yêu cầu ban đầu không bị sửa để che chênh lệch.

Kiểm tra tiền thừa có quá nhỏ hay không có đầu ra tiền thừa. Đầu ra được đánh dấu thuộc về bạn phải được kiểm tra theo chính sách, không dựa vào tên do bên điều phối đặt. Nếu không thể tạo tiền thừa hợp lý, hãy xem lại thao tác quét hết số dư hoặc thêm đầu vào tương thích. Không chấp nhận việc âm thầm biến phần còn lại thành phí quá cao.

PSBT là định dạng chuyển thông tin và chữ ký. Bản thân nó không bảo đảm riêng tư hay xác thực nguồn. Nó có thể chứa giao dịch trước đó, khóa công khai, đường dẫn và siêu dữ liệu. Hồ sơ đa chữ ký trong phần sụn Final đã rà soát dùng PSBT v0/BIP174. “Giao dịch phiên bản 2” không có nghĩa là “PSBT phiên bản 2”.

Thực hành

1. Trong trình mô phỏng, tạo khoản thanh toán có đầu vào 120.000 sat, người nhận 70.000 sat và phí 1.000 sat.
2. Liệt kê mọi đầu ra và giải thích số tiền thừa 49.000 sat. Lặp lại với thao tác quét hết số dư.
3. Hủy bản nháp và giải thích bạn vừa hủy gì ở máy cục bộ. Không dùng trình mô phỏng để ký hay phát bất cứ giao dịch nào.

Chứng minh bạn đã hiểu

Trước khi xuất, giải thích được đầu vào, đầu ra, người nhận, chi phí và sự ủy quyền còn thiếu.

Câu hỏi thường gặp

Tôi có thể gửi toàn bộ số dư hiển thị không? Chỉ khi ứng dụng tính được số tiền thực gửi hợp lệ và đủ trả phí. Số dư có thể bao gồm tiền hiện không khả dụng.

Điểm tạm dừng

Lưu hoặc hủy bản nháp học tập. Không bao giờ lưu PSBT thật vào cổng khóa học.

Màn hình ghi “transaction version 2”. Điều đó có chứng minh tệp là PSBT v2 không?

1. Không, đây là các trường phiên bản khác nhau.
2. Có, luôn như vậy.
3. Điều này chứng minh giao dịch dùng Taproot.

> **Xem đáp án: Không, đây là các trường phiên bản khác nhau.**
> BIP370 phân biệt phiên bản của cấu trúc chứa dữ liệu với phiên bản giao dịch.

Ký bằng Original và BIT

Mục tiêu

Hoàn tất quy trình ký của từng mẫu thiết bị và nhận phản hồi gắn với đúng thao tác.

Tìm hiểu

Original: dùng Cuvex Mirror và thẻ truyền của quy trình tương thích để chuyển PSBT. Đọc yêu cầu trên thiết bị, cung cấp bản mật mã và mở khóa riêng tư. Kiểm tra tất cả đầu ra, số tiền, tiền thừa và phí. Phản hồi được ghi lên thẻ, sau đó phải đọc và xác minh trong Desk. Ghi thẻ thành công không thay thế bước chuyển phản hồi về.

BIT: chọn đúng ổ đĩa và chuyển yêu cầu qua USB-C. Dịch vụ cục bộ của Desk xử lý phần trao đổi theo quy trình trong lúc bạn thao tác trên thiết bị. Cung cấp bản mật mã theo hướng dẫn trên màn hình và kiểm tra trên BIT. “Nhận từ BIT” sẽ nhập phản hồi. Desk xác minh và lưu trước khi xác nhận đã nhận. Nếu mất kết nối, hãy khôi phục đúng thao tác đó, không chọn thao tác khác chỉ vì trông tương tự.

Khi ký đa chữ ký với phần sụn Final, bạn phải xem lại phần tóm tắt, các đầu ra bắt buộc, các cảnh báo liên quan và ba xác nhận cuối của lệnh “Ký PSBT”. Phần kiểm tra mở rộng tùy chọn cho phép xem thêm tham số. Chọn “Không” không loại bỏ các bước kiểm tra bắt buộc. Việc xác minh chính sách độc lập thuộc quy trình khác và kết quả chỉ có giá trị trong phạm vi kiểm tra đó.

Để ký, cần bản mật mã tương thích và có thể xác minh tính xác thực. Một bản sao cũ vẫn có thể khôi phục bí mật nhưng không vì thế mà đủ điều kiện ký. Nếu thiết bị cảnh báo bản sao cũ chưa được xác thực, hãy khôi phục và kiểm tra bí mật, sau đó tạo bản sao mới trước khi ký. Không sửa phần đầu hay bỏ qua việc từ chối.

Hủy nếu địa chỉ không khớp, phí bất thường, thiếu dữ liệu, xuất hiện mạng khác hoặc thiết bị từ chối chính sách. Đừng phê duyệt chỉ vì áp lực phải kết thúc cuộc gọi. AI không nhấn nút, không xác nhận lần cuối và không thể tuyên bố thao tác đã ký khi bạn chưa kiểm tra.

Thực hành

1. Thực hiện quy trình của mẫu thiết bị mình dùng với ví không có tiền hoặc môi trường thực hành đã được nghiệm thu trên thiết bị thật.
2. Mô phỏng việc dừng trước các xác nhận cuối và giải thích vì sao như vậy chưa phải là phê duyệt.
3. Kiểm tra phản hồi quay về, sự tương ứng với bản nháp và, nếu dùng BIT, cả trạng thái nhận lẫn xác nhận đã nhận.

Chứng minh bạn đã hiểu

Thuật lại quy trình mà không tiết lộ thông tin xác thực. Phân biệt phê duyệt trên thiết bị, nhập phản hồi và phát giao dịch.

Câu hỏi thường gặp

Thiết bị ngoại tuyến có biết các đầu vào của tôi vẫn chưa chi tiêu không? Nó không thể tự kiểm tra trạng thái hiện tại của chuỗi. Ứng dụng phải kiểm tra giao dịch cuối cùng với nguồn dữ liệu mạng của mình.

Điểm tạm dừng

Nếu ngắt quá trình ký, hãy hủy hoặc để lại thao tác đang chờ có mã nhận diện theo quy trình và không để lộ thông tin bí mật.

BIT đã ký nhưng Desk chưa xác nhận nhận được. Bạn phải giả định trạng thái nào?

1. Khoản thanh toán chắc chắn đã được phát.
2. Phản hồi đang chờ nhận hoặc xác minh. Hãy khôi phục đúng thao tác đó.
3. Đã mất ví.

> **Xem đáp án: Phản hồi đang chờ nhận hoặc xác minh. Hãy khôi phục đúng thao tác đó.**
> Ký, nhận và phát là các giai đoạn khác nhau.

Hoàn tất, phát giao dịch và xử lý sự cố

Mục tiêu

Đóng chu kỳ thanh toán mà không cần gấp đôi và chẩn đoán lỗi mỗi giai đoạn.

Tìm hiểu

Sau khi xem xét một chữ ký, Desk phải xác nhận rằng nó phù hợp với bản nháp và giữ nguyên ý định. Trong đa chữ ký, bạn có thể thoát khỏi ngưỡng; bạn chỉ có thể xác nhận một chữ ký nhập khẩu cũng không có quyền bỏ qua việc kiểm tra. Hoàn tất việc giao dịch, chuẩn bị phát sóng khi điều kiện đã hoàn tất.

Chỉ xuất bản sau buổi kiểm tra cuối cùng. Một máy chủ trả lời hoặc txid cho thấy kết quả của yêu cầu đó, nhưng việc tiếp cận phải xác nhận và xác nhận. Nếu không có câu trả lời, hãy tham khảo lại trước khi lặp lại. Đừng tạo ra một khoản thanh toán mới để giải quyết vấn đề hình ảnh.

Để trả nợ, hãy kiểm tra hợp pháp, hợp pháp, xung đột và khả năng thực sự RBF. Nếu có sự thay đổi về chính sách hoặc người nhận, đề xuất mới đòi hỏi phải có chữ ký mới. Hủy bỏ địa phương không phá hủy một công ty hoặc giao dịch nào mà đã có người khác, và cũng không hủy bỏ những gì được xác nhận.

Phân tích từng giai đoạn: chuẩn bị, vận chuyển, di chuyển, mở khóa, chỉnh sửa, ký tên, trở lại, kết thúc, hoàn thành, phát sóng và xác nhận. Truy cập hệ thống, phiên bản, mô hình, giai đoạn, thời gian gần và mã lỗi. Các chẩn đoán của app được thiết kế để loại bỏ dữ liệu nhạy cảm, nhưng hãy xem lại trước khi chia sẻ và tránh ghép các bản sao, QR, khóa Chat hoặc giấy thông tin.

Thực hành

1. Sắp xếp các trạng thái thanh toán giả tưởng và xác định nơi anh sẽ tạm dừng an toàn.
2. Giải quyết ba vấn đề: số tiền thiếu, USB không nhận được và xuất bản với kết nối bị gián đoạn.
3. Nó tái thiết một vé sử dụng dữ liệu tổng hợp và kết quả mong đợi có thể kiểm tra được.

Chứng minh bạn đã hiểu

Bạn có thể quyết định xem học sinh, thiết bị, hệ thống điều phối hoặc mạng có bị thiếu hay không, và tránh một khoản thanh toán thứ hai không cần thiết.

Câu hỏi thường gặp

Một sai lầm FIRMWARE_CAPABILITY_REQUIRED có thể giải quyết bằng cách biến phần sụn thành mù quáng? Không. Trong tài liệu của Desk, việc công nhận chiếc buld cuối cùng đòi hỏi phải sửa lại danh mục Desk. Kiểm tra phiên bản và hồ sơ trước khi thay đổi thiết bị.

Điểm tạm dừng

Giữ nguyên trạng thái và hành động tiếp theo. Nếu anh công bố một chiến dịch thực sự ngoài phòng thí nghiệm, thì hãy giữ lại ghi chép của cô ấy trong tài liệu cá nhân của anh.

Thao tác nào tự nó thu hồi được giao dịch đã xác nhận?

1. Xóa bản nháp cục bộ.
2. Đóng Mirror.
3. Không thao tác nào nêu trên.

> **Xem đáp án: Không thao tác nào nêu trên.**
> Xóa cục bộ không viết lại chuỗi hay rút lại ủy quyền đã được truyền đi.

Có thể quan sát những gì trên Bitcoin?

Mục tiêu

Phân biệt dữ liệu công khai, suy luận và dữ liệu bạn bổ sung ngoài chuỗi.

Tìm hiểu

Bitcoin on-chain là công khai. Có thể phân tích script và những địa chỉ có thể biểu diễn, giá trị, quan hệ giữa đầu vào và đầu ra, cùng vị trí trong khối. Tên bạn không nhất thiết xuất hiện, nhưng một giao dịch mua gắn danh tính, hóa đơn công khai hoặc địa chỉ từng chia sẻ có thể liên kết bạn với lịch sử ấy.

Tính giả danh nghĩa là hoạt động bằng định danh tự nó không phải danh tính pháp lý của bạn. Ẩn danh đòi hỏi một tập hợp và những điều kiện khiến người khác không phân biệt được bạn. Chỉ cài ứng dụng không đạt điều đó. Quyền riêng tư tùy ngữ cảnh: cửa hàng biết khoản thanh toán, sàn có thể biết lệnh rút, máy chủ thấy truy vấn và người ở gần có thể thấy thiết bị của bạn.

Phân biệt thực tế với suy luận. “Đầu ra này đã được chi trong giao dịch đó” có thể kiểm tra trên chuỗi. “Tất cả đầu vào này cùng thuộc một người” là quy tắc suy đoán có thể sai. Việc xác định danh tính ngoài chuỗi có thể tăng độ tin cậy của một giả thuyết nhưng không biến mọi cách diễn giải thành chắc chắn.

Dùng lại địa chỉ giúp người khác gộp hoạt động dễ hơn. Gộp UTXO từ các bối cảnh khác nhau có thể nối chúng lại. Lộ xpub cho phép theo dõi rộng hơn việc đưa một địa chỉ. Chia sẻ txid còn có thể làm lộ các đầu ra và quan hệ mà người nhận không cần biết.

Thực hành

1. Trong một giao dịch giả định, đánh dấu dữ liệu nào công khai, nhãn nào do bạn tự đặt.
2. Thêm một hóa đơn có tên và mô tả liên hệ mới xuất hiện.
3. Soạn yêu cầu hỗ trợ đủ để giải quyết lỗi mà không ghi địa chỉ, descriptor hay số dư.

Chứng minh bạn đã hiểu

Nói rõ “điều này quan sát được” hoặc “điều này được suy ra” và giải thích còn thiếu bằng chứng gì.

Câu hỏi thường gặp

Nếu không bao giờ dùng lại địa chỉ thì tôi đã ẩn danh chưa? Chưa. Cách chọn đầu vào, tiền thừa, truy vấn, đối tác và siêu dữ liệu khác vẫn quan trọng.

Điểm tạm dừng

Lưu sơ đồ các bên quan sát, không dùng danh tính hay giao dịch thật.

Dữ liệu nào thường cho phép quan sát cả một nhóm địa chỉ của tài khoản?

1. Màu biểu tượng.
2. xpub của tài khoản và đủ ngữ cảnh dẫn xuất.
3. Nhãn hiệu dây cáp.

> **Xem đáp án: xpub của tài khoản và đủ ngữ cảnh dẫn xuất.**
> Thông tin công khai mở rộng vẫn nhạy cảm về quyền riêng tư dù tự nó không cho phép chi tiêu.

M07

Tách bối cảnh và quản lý tiền thừa

Mục tiêu

Quyết định chi tiêu phù hợp với nguồn gốc của UTXOs.

Tìm hiểu

Sự phân chia ngữ cảnh bắt đầu trước khi có thanh toán. Quyết định một cuộc tiếp tân có thể được xem là tiết kiệm, hoạt động chuyên nghiệp, tiêu dùng hàng ngày hay không, hoặc một mối quan hệ cụ thể. Nó giữ thông tin đó trong những nhãn riêng để sự lựa chọn trong tương lai không bị xóa đi bởi sự thiếu hiểu biết.

Một cái nhãn không phân biệt được các đầu ra. Nếu bạn sử dụng 2 UTXOs hoàn cảnh khác nhau, giao dịch sẽ tạo ra mối quan hệ của họ. Liên kết làm giảm số lượng các đầu vào Trả tiền trong tương lai, nhưng tăng liên kết giữa các các đầu ra Mối liên kết. Làm điều đó với phí thương vong có thể hiệu quả, và cũng có thể trái ngược với mục tiêu riêng tư của bạn.

Thay đổi là một lối thoát mới được điều khiển bởi cùng một chính sách, chứ không phải "tiền tàng hình". Việc sử dụng sau này có thể mở rộng các mối quan hệ trước đó. Đừng đánh dấu một địa chỉ để đổi vì nó có một vấn đề không bình thường; trong một cuộc kiểm tra thực tế, thiết bị này phải xác nhận nó thuộc về ví.

Tránh biến sự riêng tư thành những kiểu mẫu cơ khí về vấn đề nhập khẩu, thời gian hoặc chuyển nhượng liên tục. Những mô hình này cũng có thể nhận ra và tạo ra nhiều phí hơn. Xem thử thông tin mà bạn biết về mỗi phần và thông tin mới nào sẽ được công bố. Không có trình tự xóa lịch sử nào đã được công bố.

Thực hành

1. Tạo ra 5 UTXOs giả mạo của ba bối cảnh và chuẩn bị một khoản thanh toán sử dụng số lượng nhỏ nhất cần thiết.
2. Xác định sự thay đổi và xác định cách đánh dấu.
3. So sánh chi phí và phơi nắng với tất cả các đầu ra bên ngoài để giữ chúng tách biệt.

Chứng minh bạn đã hiểu

Bạn có thể bào chữa cho việc củng cố hoặc từ chối nó với một lý do cụ thể, mà không cần áp dụng một quy tắc tuyệt đối cho mọi trường hợp.

Câu hỏi thường gặp

Chuyển mọi thứ sang một địa chỉ khác của tôi sẽ phá vỡ lịch sử? Không. Việc chuyển tiền sẽ đưa ra thêm một mối quan hệ và có thể thêm vào chi phí mà không giải quyết được mối đe dọa của bạn.

Điểm tạm dừng

Nó giữ lý lẽ của phòng thí nghiệm và chính sách tuyển chọn.

Gộp đầu vào tiền lương và quyên góp trong một giao dịch có thể gây hậu quả gì?

1. Làm lộ mối liên hệ giữa các đầu vào.
2. Xóa nguồn gốc công khai.
3. Biến chúng thành tiền mặt chắc chắn ẩn danh.

> **Xem đáp án: Làm lộ mối liên hệ giữa các đầu vào.**
> Giảm số UTXO có thể làm tăng các liên hệ quan sát được.

Quyền riêng tư trên mạng, Tor và VPN

Mục tiêu

Tách rời quyền riêng tư khỏi mạng lưới.

Tìm hiểu

Một máy chủ tham khảo có thể liên kết các yêu cầu với một kết nối. Nhà cung cấp Internet của bạn có thể quan sát định mệnh hoặc kiểu mẫu giao thông. Một VPN thay thế lòng tin đó cho người điều hành VPN; không loại bỏ thông tin công cộng của bitcoin, cũng không ngăn cản một tài khoản xác định bạn.

Tor định tuyến lưu lượng qua một mạng nhằm giảm một số mối liên hệ giữa nguồn và đích. Nó không biến địa chỉ Bitcoin thành riêng tư và không bảo vệ ứng dụng có lưu lượng không đi qua Tor. Mở Tor Browser không tự cấu hình Desk, Bitcoin Core hay mọi dịch vụ trên máy tính.

Trước khi khẳng định một sự kết nối đã được bảo vệ, chúng ta cần kiểm tra đường dẫn và cấu hình của nó. Không giả định công tắc nào trên căn cứ này. Tor Nhập vào Desk . Việc triển khai với nút hay ủy nhiệm đòi hỏi phải có hướng dẫn kỹ thuật và xác nhận giao thông hoàng gia. Nó không phát minh ra một trường giao diện vì một trường ví khác có nó.

Cũng có rò rỉ DNS, đồng bộ hóa tài khoản, liên lạc và dịch vụ trả giá. Một kế hoạch có thể bảo vệ các tham khảo tiền và tiếp tục tiết lộ các hoạt động khi một nhà thám hiểm công khai mở cửa. Đặt phạm vi của mỗi biện pháp và hành vi khi kết nối bị hỏng; tránh thay đổi thầm lặng đối với một nhà cung cấp ít riêng tư hơn.

Thực hành

1. Vẽ đường dẫn máy tính, nhà cung cấp kết nối, ủy nhiệm nếu nó tồn tại, nút hay dịch vụ, và mạng bitcoin.
2. Hãy chỉ ra ai được tư vấn và ai có thể nhìn thấy danh tính thương mại của bạn.
3. Giả vờ nút không trả lời. Hãy quyết định giữa việc tạm dừng hoặc chuyển nguồn thông tin rõ ràng với kiến thức về triển lãm.

Chứng minh bạn đã hiểu

Anh có thể giải thích mối đe dọa nào làm giảm cấu hình của anh và mối đe dọa vẫn còn tồn tại.

Câu hỏi thường gặp

Tor bảo đảm không ai có thể liên hệ với tôi? Không. Đối lập, nhận dạng thương mại, mẫu hình và lỗi hoạt động có thể tiếp tục xác minh.

Điểm tạm dừng

Ghi lại phạm vi thiết kế, không phải nội bộ hay mật khẩu.

Mở Tor Browser có bắt buộc Desk truy vấn qua Tor không?

1. Có vì cùng máy tính.
2. Có nếu biểu tượng hiển thị.
3. Không. Phải cấu hình và xác minh tuyến kết nối của từng ứng dụng.

> **Xem đáp án: Không. Phải cấu hình và xác minh tuyến kết nối của từng ứng dụng.**
> Bảo vệ của ứng dụng này không tự áp dụng cho ứng dụng khác.

CoinJoin, Payjoin và các giới hạn hiện tại

Mục tiêu

Hiểu được những công cụ hợp tác không có nghĩa là họ ẩn danh hoặc không có sự hòa hợp.

Tìm hiểu

CoinJoin cung cấp tiền cho một số người trong một vụ giao dịch nhằm gây khó khăn cho các cuộc đối thoại về các đầu vào và các đầu ra. Nó không có nghĩa là đưa đồng xu cho một dịch vụ bảo vệ mà hứa sẽ trả lại đồng nào đó. Các thiết kế khác nhau yêu cầu kiểm tra phối hợp, lưu ký, phí, kháng cự những người tham gia gian lận và điều trị sau đó.

Payjoin cho thêm các đầu vào người trả tiền và nhận tiền hợp tác, làm suy yếu một số tài sản chung. Cần có sự hỗ trợ phù hợp ở cả hai đầu và một giao thức cụ thể. Đó là vật liệu hiểu biết kỹ thuật: nguồn tin đã được kiểm tra không được ghi nhận thông qua một dòng Payjoin hoặc CoinJoin tích hợp và hoạt động Cuvex Desk.

Tình trạng cung cấp và bối cảnh pháp lý thay đổi. Tài liệu Wasabi ghi nhận bộ điều phối zkSNACKs đóng ngày 1 tháng 6 năm 2024. Không nên dạy một nút cũ như thể nó bảo đảm dịch vụ hiện nay. Năm 2025, Bộ Tư pháp Hoa Kỳ công bố việc các nhà sáng lập Samourai nhận tội và các bản án sau đó. Không thể từ đó kết luận mọi kỹ thuật riêng tư đều trái luật ở mọi khu vực.

Một công cụ có thể làm giảm sự can thiệp và để lại những thứ khác nguyên vẹn. Nguồn gốc nhận dạng không biến mất khỏi hồ sơ của người khác. Việc lặp lại sau đó, siêu dữ liệu và lỗi của nhóm người tham gia có thể làm giảm sự riêng tư. Ngoài ra, một số dịch vụ có thể áp dụng các chính sách thương mại khác nhau trên các đồng tiền có những câu chuyện nhất định.

Thực hành

1. Nó so sánh giao dịch thông thường, hợp tác với nhau, và dịch vụ nhận được lưu ký, mà không cần thực hiện các hoạt động của hoàng gia.
2. Để có một công cụ cụ cụ thể, hãy tìm kiếm phiên bản, duy trì, tình trạng dịch vụ và tài liệu hiện tại trước khi đề xuất sử dụng.
3. Xác định những rủi ro kỹ thuật, từ lưu ký và luật sư riêng biệt. gia sư không được thiết kế để trốn điều khiển hoặc hứa hẹn "những thông tin không thể theo dõi".

Chứng minh bạn đã hiểu

Bạn có thể giải thích một lợi thế giới hạn và ít nhất là hai rủi ro hoặc đòi hỏi của một kỹ thuật riêng tư.

Câu hỏi thường gặp

Cuvex cần máy trộn để phục vụ cho lưu ký cá nhân? Không. Điều khiển tham khảo, dữ liệu, các khóa và chọn UTXOs đã giải quyết các rủi ro cụ thể, mà không cần hứa hẹn.

Điểm tạm dừng

Ghi lại một công cụ như "tự đào tạo" chứ không phải là "không thể đáp ứng được" mà không có bằng chứng.

Phát biểu nào có cơ sở?

1. CoinJoin bảo đảm ẩn danh vĩnh viễn.
2. Kỹ thuật cộng tác có thể làm một số suy luận khó hơn nhưng có điều kiện và giới hạn.
3. Mọi dịch vụ gọi là mixer đều duy trì tự lưu ký.

> **Xem đáp án: Kỹ thuật cộng tác có thể làm một số suy luận khó hơn nhưng có điều kiện và giới hạn.**
> Đặc tính phụ thuộc giao thức, triển khai, người tham gia và cách dùng sau đó.

Bài học từ các sự cố thực tế

Mục tiêu

Rút ra quyết định có thể kiểm chứng từ sự cố có tài liệu, không công kích đối thủ hay phóng đại khả năng bảo vệ.

Tìm hiểu

Mt. Gox: cáo trạng năm 2023 của Bộ Tư pháp mô tả việc truy cập trái phép máy chủ và khóa, sau đó là tiền khách hàng biến mất. Cáo trạng nêu cáo buộc, không phải phán quyết. Bài học là hỏi ai thực sự kiểm soát khóa và điều gì xảy ra nếu công ty gặp sự cố.

Ledger Connect Kit, tháng 12 năm 2023: Ledger ghi nhận thư viện cho ứng dụng phi tập trung bị phát hành bản độc hại sau khi quyền truy cập của cựu nhân viên bị xâm phạm. Sự cố tác động chuỗi phân phối phần mềm, lừa người dùng DApps trên EVM ký. Nó không chứng minh phần cứng Ledger hay đồng thuận Bitcoin bị phá.

Bybit, tháng 2 năm 2025: FBI quy vụ trộm khoảng 1,5 tỷ đô la tài sản ảo cho Triều Tiên. Sự cố liên quan sàn và tài sản mạng khác, không phải mật mã Bitcoin bị phá. Hãy kiểm tra ý định ký và tránh để nhiều người cùng tin mù quáng vào một màn hình.

Coinbase, tháng 5 năm 2025: công ty thông báo nhân viên hỗ trợ bị mua chuộc đã đánh cắp dữ liệu để tạo điều kiện cho kỹ nghệ xã hội. Công ty cho biết mật khẩu và khóa riêng không bị lộ. Kẻ lừa đảo có thể biết dữ liệu thật.

Bitcoin Core cũng công bố lỗi phần mềm. CVE-2024-35202 mô tả khả năng bị làm ngừng hoạt động từ xa ở phiên bản trước 25.0. Xác minh quy tắc không thay việc bảo trì. Thông báo này không chứng minh mất cắp khóa.

Tháng 1 năm 2026, The Register đưa tin dữ liệu đơn hàng và liên hệ của khách mua Ledger bị lộ qua Global-e, dẫn xác nhận từ cả hai công ty. Theo các tuyên bố đó, khóa khôi phục không bị ảnh hưởng. Việc mua hàng có thể tiết lộ bạn sở hữu thiết bị dù phần cứng chưa bị xâm phạm.

Tháng 4 năm 2026, The Record đưa tin về vụ tấn công Drift và việc nền tảng thông báo tạm dừng nạp, rút. Đây là giao thức tài chính phi tập trung trên Solana, không phải Bitcoin bị phá. Không coi thiệt hại ước tính ban đầu là số cuối hay quy trình thu hồi sau đó là bảo đảm hoàn tiền.

Thực hành

1. Phân loại từng sự cố theo lưu ký, giao diện hoặc phân phối, dữ liệu cá nhân, giao thức mạng khác và tính sẵn sàng.
2. Đề xuất cho mỗi sự cố một biện pháp phòng ngừa và một giới hạn của biện pháp đó.
3. Diễn tập cuộc gọi giả mạo: “Tôi biết bạn đã mua hàng. Hãy chuyển tiền đến địa chỉ an toàn này.” Gác máy và xác minh qua kênh do chính bạn chủ động liên hệ.

Chứng minh bạn đã hiểu

Giải thích vì sao không sự cố nào chứng minh một thương hiệu khác bất khả xâm phạm. Bằng chứng chỉ hỗ trợ kết luận trong phạm vi cụ thể.

Câu hỏi thường gặp

Đây có phải toàn bộ các vụ tấn công mới nhất không? Không. Đây là tuyển chọn đã kiểm tra cho ấn bản ngày 17 tháng 11 năm 2026, không phải danh mục đầy đủ hay theo dõi trực tiếp.

Điểm tạm dừng

Ghi thói quen bạn sẽ thay đổi và cách kiểm tra mình vẫn duy trì.

Người liên hệ biết việc mua hàng của bạn và yêu cầu chuyển đến “ví cứu hộ”. Việc họ biết giao dịch mua chứng minh gì?

1. Có thể đó là dữ liệu bị lộ, không xác thực danh tính hay địa chỉ.
2. Họ chắc chắn là hỗ trợ thật.
3. Bạn phải chia sẻ hạt giống.

> **Xem đáp án: Có thể đó là dữ liệu bị lộ, không xác thực danh tính hay địa chỉ.**
> Dữ liệu thật có thể được dùng để dựng một kịch bản lừa đảo thuyết phục.

Tạo danh tính và xác minh liên hệ trò chuyện

Mục tiêu

Kích hoạt một danh tính chat mà không lộ ra khóa và kiểm tra bên cạnh.

Tìm hiểu

Tại Desk, mạng chat được nối với bản mật mã thông qua một chiếc khóa Chat được sản xuất trên Cuvex. Mặc dù hình ảnh của nó có thể trông giống như xpub, nhưng nó là bí mật và không nên được coi là khóa công khai của một tài khoản WOW. gia sư không bao giờ cần đọc hay xem nó qua QR.

Dòng chảy phân biệt bí danh mới, di chuyển hoặc hồi phục. Trong thực hiện điều chỉnh, bạn sẽ chọn hồ sơ di động iOS hoặc Android tương ứng, bởi vì nhân dạng gốc của lịch sử không thể tương tác bằng trực giác. DEV và sản xuất là những môi trường riêng biệt: thay đổi môi trường không di chuyển các cuộc trò chuyện hoặc biệt danh tự động.

Thêm một bí danh chưa xác minh. Kiểm tra dấu vân tay bằng một kênh riêng biệt và xác thực. Nếu bài App đưa ra những câu hỏi về sự công nhận, nó sử dụng thông tin không được công khai và tránh trả lời cho mật khẩu. Một giọng nói quen thuộc có thể bị bắt chước; trong trường hợp rủi ro, nó kết hợp các phương pháp đã được thỏa thuận trước đó.

Nếu bạn thay đổi danh tính của một người tiếp xúc, tạm dừng và phối hợp cho đến khi bạn giải quyết được. Nó có thể là một sự phục hồi hợp pháp hoặc một sự thay thế ác ý. mã hóa ở cực cực đoan bảo vệ một con kênh dựa trên giao thức và thực hành của nó, nhưng nó không chứng minh được ai đang sử dụng thiết bị bên kia.

Thực hành

1. Trong một môi trường thử nghiệm, nó giải thích dòng chảy của việc tạo ra hoặc phục hồi mà không cần dùng đến khóa Chat.
2. Thêm vào đó một máy thí nghiệm, và nhớ qua kênh khác, kiểm tra dấu vân tay.
3. Mô phỏng việc thay đổi danh tính. Hãy xác định cách bạn xác nhận sự thay đổi trước khi trả tiền.

Chứng minh bạn đã hiểu

Bạn có thể phân biệt bí danh, dấu vân tay công khai, khóa Chat bí mật và sự tin tưởng con người vào một người.

Câu hỏi thường gặp

Một bí danh cổ xưa bảo đảm là cùng một người? Không. Cần kiểm tra sự liên tục và thay đổi của các khóa theo dòng chảy.

Điểm tạm dừng

Chỉ ghi lại bằng chứng xác thực và phương pháp, không cần các khóa hay câu hỏi riêng tư.

Một chuỗi có tên “Khóa trò chuyện” trông như xpub. Desk coi nó là gì?

1. Dữ liệu có thể đăng diễn đàn.
2. Bí mật khôi phục danh tính.
3. Địa chỉ nhận bitcoin.

> **Xem đáp án: Bí mật khôi phục danh tính.**
> Hình thức hiển thị không quyết định tính bí mật hay mục đích của dữ liệu.

Yêu cầu và thanh toán satoshi qua trò chuyện

Mục tiêu

Từ cuộc trò chuyện đến việc thanh toán mà không bị mất kiểm tra hoặc văn cảnh.

Tìm hiểu

Chat cho phép bạn yêu cầu địa chỉ, trả lời với địa chỉ nhận, yêu cầu thanh toán và mở một tài khoản WOW. Giữ ngữ cảnh trên kênh sẽ giảm thiểu lỗi sao chép thông tin giữa các ứng dụng, nhưng không thay đổi mỗi thông điệp thành một mệnh lệnh có hiệu lực.

Trước khi trả lời hoặc trả tiền, hãy kiểm tra lại những liên lạc đã được xác thực, mạng lưới, quan trọng và yêu cầu ban đầu. Đơn chia sẻ chung giữ lại phần chọn của UTXOs và phí. Nếu thông điệp yêu cầu một số lượng và bạn chọn « Gửi tổng số », chữ cái sau phí có thể thấp hơn; nó phải được nhận diện là một phần trả khi thích hợp.

Giấy phép vẫn còn ở mức Cuvex. Chat vận chuyển mục đích và phối hợp; bạn không có quyền ký tự động. Xác nhận thanh toán được gửi cho người tiếp xúc cần nhận thông điệp nhận được rằng có một giao dịch đã được xác nhận. Máy nhận tín hiệu nhận dạng bằng tài khoản hay nguồn tin của mình.

Liên kết ngoài, QR đính kèm và địa chỉ đều chưa đáng tin cho đến khi được xác minh. “Xem trong Mempool” có thể mở dịch vụ bên thứ ba và lộ truy vấn. Nếu chính sách dùng nút riêng, ưu tiên xác minh tương thích trong WOW và cân nhắc mọi lần truy cập dịch vụ công cộng.

Thực hành

1. Nó đại diện cho hai vai trò: người nhận yêu cầu 50.000 sat ; Người trả tiền chuẩn bị chưa xuất bản.
2. Mô phỏng một khoản nợ 48.000 sat sẵn sàng. Giải thích cho việc chấp thuận và thỏa hiệp nào bị mất một phần tiền lương.
3. Nó cố tình thay đổi mạng lưới trong một thông điệp thử nghiệm và dừng dòng chảy.

Chứng minh bạn đã hiểu

Bạn có thể theo dõi mối quan hệ giữa các yêu cầu, địa chỉ, bản nháp và xác nhận, mà không cần thu hẹp lại thành "Chat nói OK".

Câu hỏi thường gặp

Gửi sats từ chat có nghĩa là sử dụng Lightning? Không. Dòng WOW được ghi nhận, chuẩn bị trả phí bitcoin. Từ sats biểu thị một đơn vị, chứ không phải mạng lưới vận chuyển.

Điểm tạm dừng

Hủy bỏ bản nháp phòng thí nghiệm hoặc lục soát nhà nước, không phải in để chứng minh giao diện.

Bạn nhận xác nhận qua trò chuyện. Kiểm tra nào quyết định khoản tiền đã đến?

1. Biểu tượng tin nhắn màu xanh.
2. Đối phương nói “đã xác nhận”.
3. Kiểm tra giao dịch và đầu ra trên mạng bằng nguồn thích hợp.

> **Xem đáp án: Kiểm tra giao dịch và đầu ra trên mạng bằng nguồn thích hợp.**
> Trạng thái tin nhắn không tương đương trạng thái giao dịch.

Chia sẻ bản mật mã một cách có cân nhắc

Mục tiêu

Hiểu rõ việc gửi một bản sao được mật mã cho người khác bao hàm điều gì.

Tìm hiểu

Chia sẻ bản mật mã cho bạn một bản sao của đối tượng mã hóa. Nó không nhất thiết phải gửi bitcoin hoặc tự nhập vào một bên ký mới. Nếu người nhận cũng có đủ phương tiện để mở khóa, họ có thể truy cập nội dung theo kế hoạch. Vì vậy, họ phải quyết định trước bạn sẽ truyền năng lực nào.

mã hóa ở cuối màn hình và mã hóa của tập tin bảo vệ các lớp khác nhau. Một khi tải xong, bộ nhận tín hiệu có thể giữ vật thể bên ngoài phòng chat. Xóa thông điệp của bạn hoặc ghi chép địa phương không bảo đảm rút lại tất cả các bản sao. Một mật khẩu chia sẻ cùng một kênh có thể tập trung các thành phần vào một đường duy nhất.

Trước khi gửi, hãy xác định danh tính, định dạng và mục đích. Nếu app cho phép kết nối một bản mật mã nhận được, nó sẽ tổ chức một bản sao, chứ không phải chứng minh là an toàn giải mã bất kỳ file nào. Đừng dùng những trang bên ngoài để nhập hạt giống khôi phục hay mật khẩu vào một trang bên ngoài.

Sự phục hồi đòi hỏi một sự dàn xếp hoạt động: ai giữ mỗi thành phần, ai có thể mở nó ra, làm thế nào để phát hiện được sự phơi nắng và làm thế nào bạn thay đổi lưu ký nếu mối quan hệ kết thúc. Thông thường trả tiền điện thông thường là một hướng đi bình thường; bạn không cần phải chia sẻ bản mật mã của bạn.

Thực hành

1. Thiết kế một văn bản mã hóa chuyển sang một đối tượng thí nghiệm.
2. Tôi muốn biết cô ta biết gì và người nhận có thể làm gì trước và sau khi cô ta biết mật khẩu.
3. Giả vờ như mối quan hệ kết thúc. Nó giải thích tại sao xóa thông điệp không hủy bản sao hay bản các khóa.

Chứng minh bạn đã hiểu

Bạn có thể phân biệt "chia sẻ dữ liệu", "Tôi chia sẻ một bí mật" và "Tôi đã ký một chi phí".

Câu hỏi thường gặp

Tập tin mã hóa có thể lưu mà không cần kết quả nào sao? Nó có thể tiết lộ siêu dữ liệu, làm cho mật khẩu dễ dàng hơn, và duy trì vô hạn định. Hãy cân nhắc việc chia sẻ tin mừng.

Điểm tạm dừng

Đừng để dưới lưu ký trong khóa học. Chỉ ghi lại kết quả bài tập thôi.

Chia sẻ bản mật mã qua trò chuyện có phải gửi bitcoin không?

1. Không. Bạn truyền một đối tượng có nội dung và phạm vi truy cập riêng.
2. Có nếu tên kết thúc bằng .bin.
3. Nó tự kích hoạt ví đa chữ ký mới.

> **Xem đáp án: Không. Bạn truyền một đối tượng có nội dung và phạm vi truy cập riêng.**
> Truyền bí mật và dịch chuyển UTXO là hai thao tác khác nhau.

M08

Khôi phục trò chuyện và hiểu siêu dữ liệu

Mục tiêu

Kế hoạch thay đổi nhóm và tách biệt danh tính và thông điệp.

Tìm hiểu

Desk cho thấy rằng lịch sử và phiên họp địa phương không phải là một phần của bản sao toàn cầu. khóa Chat cho phép lấy lại danh tính; nó không bảo đảm khôi phục tất cả các cuộc nói chuyện cũ. App bao gồm các trạng thái và hành động cho hoạt động chưa hoàn thành, bảo trì các khóa và phục hồi địa phương khi có vật liệu phù hợp.

Mỗi biệt hiệu nên được dùng trong một thiết bị cùng một lúc, theo sự hướng dẫn của cơ sở đã được chỉnh sửa. Đừng kích hoạt nó cùng lúc trong 2 đội để đồng bộ hóa nếu không được hỗ trợ. Một cuộc chuyển trại phải theo thủ tục và kiểm tra liên lạc.

'Chấp nhận', 'được chấp nhận bởi máy phục vụ',' được chấp nhận' và 'không thể có giải mã' mô tả các giai đoạn khác nhau. Một chuyến hàng chưa được xác nhận không tự động chuyển sang chế độ mù: Trước tiên, bạn cần phải tìm hiểu xem nó có đến hay không. Nếu bạn thiếu một khóa phiên chạy hoặc thay đổi nhân dạng, thì việc giữ lại thông điệp chưa được trình bày không có nghĩa là bạn đã đọc nó.

Nội dung mã hóa không nhất thiết phải che giấu thời gian, kích thước, mối quan hệ giao hàng, bí danh hay dữ liệu kết nối với tất cả các hệ thống liên quan. Điều tương tự cũng xảy ra: mã hóa phương tiện giao thông không biến một cuộc gọi thông thường thành một kênh bí mật. Hãy dùng những thông tin tối thiểu cần thiết để học và giải quyết những vấn đề quan trọng.

Thực hành

1. Mô phỏng mất PC và giải thích những gì có sẵn.
2. Nó phân loại các trạng thái tin nhắn và quyết định khi nào không nên gửi yêu cầu thanh toán.
3. Hãy chuẩn bị một thông báo về sự thay đổi thiết bị mà các đối tác có thể kiểm tra qua kênh riêng.

Chứng minh bạn đã hiểu

Bạn có thể giải thích cuộc đối thoại nào sẽ bị mất và danh tính nào có thể được phục hồi mà không hứa hẹn rằng bản sao lưu không bao gồm.

Câu hỏi thường gặp

Bạn có xóa các tin nhắn ở đầu bên kia không? Anh không cần phải chấp nhận điều đó. Máy nhận tín hiệu có thể lưu lại thông điệp và hồ sơ riêng lẻ.

Điểm tạm dừng

Hắn giữ một kế hoạch di chuyển bằng tên đồng trống, không có khóa Chat.

Theo hướng dẫn đã rà soát, riêng khóa trò chuyện bảo đảm gì?

1. Mọi hội thoại cũ trên mọi máy tính.
2. Khả năng khôi phục danh tính qua quy trình tương thích, không phải mọi tin nhắn cũ.
3. Tự truy cập khóa Bitcoin của người liên hệ.

> **Xem đáp án: Khả năng khôi phục danh tính qua quy trình tương thích, không phải mọi tin nhắn cũ.**
> Khôi phục danh tính và khôi phục kho lịch sử là hai khả năng khác nhau.

Cài đặt hằng ngày và rà soát quyền

Mục tiêu

Kiểm soát các tham số Desk mà không nhầm lẫn với bảo vệ.

Tìm hiểu

Desk cung cấp chủ đề về đêm, ngày hay hệ thống; đồng bộ hóa và thời gian 3 hoặc 5 phút; âm thanh giao dịch; nền của mạng chat; ngôn ngữ và xu tham khảo. Những ưu tiên đó thay đổi cách trình bày hoặc tần số tham khảo. Họ không thay đổi chữ ký của bitcoin, và họ cũng không thêm ẩn danh vào.

Cấu hình bảo mật đã sửa chữa cho phép khoá bởi không hoạt động, khóa khi chuyển sang nền, trì hoãn tối đa sau khi lỗi và xoá tùy chọn. Thời gian được chấp nhận bởi giản đồ không hoạt động là 30 đến 86.400 giây; giao diện có thể cung cấp các lựa chọn được thu hẹp hơn. Nên đọc các giá trị mặc định của phiên bản bạn chạy, chứ không phải là một lớp được khắc.

Liên kết bitcoin: mở một yêu cầu mở khóa, chọn tài khoản và kiểm tra. Hắn không cho phép trả tiền tự động. Trong Linux, hướng dẫn khác nhau về cài đặt tích hợp và App Image để đăng nhập liên kết. Một hóa đơn Lightning yêu cầu một dòng khác nhau; không giải quyết công bố Desk ứng dụng mặc định.

tỷ giá tham khảo, đồ thị giá cả và các liên kết tin tức có thể tham khảo các dịch vụ bên ngoài. Chức năng của họ là thông tin, chứ không phải tín hiệu mua bán. Kiểm tra lại ngày tháng và nguồn tin trước khi sử dụng dữ liệu để dịch các thông tin quan trọng. Một chế độ tối hoặc một cửa sổ nhỏ không nên giấu các nút cuối cùng, địa chỉ hay phí; nếu điều đó xảy ra, bạn dừng lại và báo cáo vấn đề hình học.

Thực hành

1. Điều chỉnh diện mạo và khóa trong kho lưu trữ học tập. Hãy kiểm tra xem anh có thể trở lại đó không.
2. Kiểm tra những tính tự động hoạt động: đồng bộ hóa, âm thanh và kiểm tra phần sụn không giống nhau.
3. Hãy mở một yêu cầu giả định liên kết bitcoin: hủy bỏ trước khi chuẩn bị cho bất kỳ hoạt động thực tế nào.

Chứng minh bạn đã hiểu

Bạn có thể giải thích hiệu quả của mỗi sự điều chỉnh và xác định vị trí của những người tham khảo hoặc hành động nhạy cảm.

Câu hỏi thường gặp

sinh trắc học của PC thay thế cho bản sao lưu của tôi? Không. Nó có thể phụ thuộc vào thiết bị và nhà kho an toàn của hệ thống. Bảo vệ sự phục hồi độc lập.

Điểm tạm dừng

Nó chặn Desk và chỉ ghi lại những ưu tiên của anh.

Chọn đồng bộ ba phút một lần làm thay đổi gì?

1. Tần suất truy vấn dự kiến khi chức năng chạy.
2. Chính sách chữ ký trên chuỗi.
3. Hạt giống của thiết bị.

> **Xem đáp án: Tần suất truy vấn dự kiến khi chức năng chạy.**
> Đây là tùy chọn vận hành, không thay đổi cách lưu ký.

M09

Thiết kế ví đa chữ ký

Mục tiêu

Chọn ngưỡng chống chịu được các tình huống mất hoặc lộ khóa có thể dự kiến.

Tìm hiểu

Trong chính sách M trên N, N là số người có khóa khác nhau và M là số chữ ký cần. Cấu hình 2 trên 3 chịu được việc một khóa không khả dụng, nhưng hai khóa bị lộ có thể phê duyệt khoản chi. Nếu ba hạt giống ở cùng chỗ hoặc cùng bị phơi lộ, tính độc lập giảm.

Hồ sơ đa chữ ký Cuvex đã rà soát dùng P2WSH gốc với sortedmulti và dẫn xuất BIP48. Original hỗ trợ về cấu trúc tối đa sáu khóa chính sách, BIT tối đa mười lăm. Khi cả hai cùng tham gia, phải theo giới hạn của bên có khả năng thấp hơn và dung lượng thật của phương tiện truyền. Giới hạn cấu trúc không bảo đảm chính sách nhiều khóa và đầu vào sẽ vừa.

Ngưỡng ứng dụng hỗ trợ phải phù hợp quan hệ số lượng của chính sách. Cấu hình 1 trên N không đòi hợp tác để chi và phần sụn có cảnh báo riêng về rủi ro này. Tăng ngưỡng còn làm tăng phối hợp, chi phí, dữ liệu khôi phục và nguy cơ tự khóa.

MuSig2 là cơ chế tổng hợp chữ ký Schnorr khác, bản thân là N trên N, không phải ngưỡng tùy ý 3 trên 5. Phần sụn Final đã khảo sát không triển khai ký đầu vào Taproot, MuSig2 hay Miniscript. Hỗ trợ người nhận P2TR không chứng minh có thể ký để chi từ ví Taproot.

Thực hành

1. Hãy thiết kế một chiếc 2 3 với những rủi ro độc lập cho mỗi người tham gia.
2. Mô phỏng mất 1 khóa và 1 thỏa hiệp. Giải thích điều gì có thể và điều gì không thể làm.
3. Hãy kiểm tra các giới hạn theo mô hình trước khi chọn một chính sách lớn hơn.

Chứng minh bạn đã hiểu

Bạn có thể biểu hiện sự khoan dung cho mất mát, ngưỡng tấn công và quan hệ phụ thuộc chung với thiết kế của bạn.

Câu hỏi thường gặp

đa chữ ký đòi hỏi mọi người phải biết hạt giống khôi phục những người còn lại? Không. Mục đích là để duy trì khả năng riêng tư của mỗi người và chia sẻ thông tin công khai cần thiết để xây dựng và khôi phục chính sách.

Điểm tạm dừng

Nó giữ thiết kế với những người tham gia giả tưởng và trách nhiệm của họ.

Trong chính sách 2 trên 3 với khóa độc lập, cần bao nhiêu khóa riêng để phê duyệt khoản chi hợp lệ?

1. Một.
2. Hai.
3. Luôn phải cả ba.

> **Xem đáp án: Hai.**
> Ngưỡng yêu cầu hai khóa và vẫn phải đạt các điều kiện, bước xác minh khác.

Tạo lời mời và cung cấp khóa

Mục tiêu

Xây dựng chính sách với những người tham gia đã được kiểm tra mà không chia sẻ hạt giống khôi phục.

Tìm hiểu

Người sáng tạo chọn tên, mạng lưới, M, N, mối quan hệ, thông tin công cộng và các điều kiện của lời mời. Trong mô hình điều chỉnh, bạn chấp nhận mạng mainnet và regtest cho dòng này, từ 2 đến 15 người tham gia trước khi áp dụng giới hạn thiết bị, và hoạt động tắt từ 1 đến 720 giờ. Đừng sử dụng những giới hạn này như là sự cho phép để vượt qua kiểm tra khả năng.

Mỗi người kiểm tra lời mời, quyết định nhận hoặc từ chối và cung cấp khóa công khai mở rộng của mình cùng dấu vân tay, đường dẫn BIP48 qua quy trình tương thích. Không gửi hạt giống, khóa riêng, địa chỉ rời hay toàn bộ descriptor của ví khác. Khóa sai ngữ cảnh có thể tạo chính sách khác dù trông như xpub hợp lệ.

Người tạo ra sự phối hợp, chứ không thay thế sự xác nhận của mỗi bên ký. Trước khi nhận được quỹ, mọi người phải có khả năng tái xây dựng lại và kiểm tra các thông số tương tự và địa chỉ điều khiển. Tiếp xúc trên mạng không có nghĩa là tự động chấp nhận bất cứ chính sách nào mà ông gửi.

Quá nhiều cho một lời mời là một quy định phối hợp giữa các hợp đồng. Nó không tự thay đổi một văn lệnh đã được tài trợ, nó không xóa chữ ký mà người khác lưu lại, và nó không hoạt động như tin nhắn đồng thuận. Hủy một đề xuất và rút nguồn tài trợ từ một chính sách tồn tại là hành động khác nhau.

Thực hành

1. Trong phòng thí nghiệm regtest, nó tạo ra một bản đề xuất 2 3 với các đối tác thử nghiệm.
2. Nó tượng trưng cho sự chấp nhận, từ chối và đóng góp sai cách. Hãy kiểm tra cái cuối cùng dừng lại.
3. Nó bao gồm những dữ liệu mà mọi người phải lưu lại trước khi tài trợ: mạng lưới, ngưỡng, khóa công khai, nguồn gốc, văn bản và địa chỉ đã được kiểm tra.

Chứng minh bạn đã hiểu

Bạn có thể nhận ra một lời mời không đầy đủ và giải thích sự chấp thuận thiếu sót của bạn mà không cần phải thừa nhận sự tồn tại của lời nói.

Câu hỏi thường gặp

Có phải một ngày trả trước sẽ làm cho người ta không thể chi tiêu sau này? Không phải vì đây là sân chơi. Lệnh cấm bitcoin tạm thời yêu cầu điều kiện văn bản hoặc giao dịch cụ thể và hỗ trợ thực tế.

Điểm tạm dừng

Hãy lưu thẻ căn cước của đề xuất và sự chấp thuận còn chờ đợi.

Để góp phần vào ví đa chữ ký, quy trình trong tài liệu yêu cầu gì?

1. Hạt giống của mọi người tham gia.
2. Một địa chỉ nhận tiền bất kỳ.
3. Khóa công khai mở rộng của bạn, kèm dấu vân tay và nguồn gốc BIP48 tương thích.

> **Xem đáp án: Khóa công khai mở rộng của bạn, kèm dấu vân tay và nguồn gốc BIP48 tương thích.**
> Dữ liệu công khai đúng cho phép lập chính sách mà không lộ khóa riêng.

Kiểm tra chính sách bằng Mirror theo thứ tự tùy chọn

Mục tiêu

So sánh toàn bộ trường và hiểu chính xác kết quả chứng minh điều gì.

Tìm hiểu

Xác minh độc lập hiển thị ngưỡng, mạng, hồ sơ, SIGHASH, ID chính sách, địa chỉ đầu tiên, vị trí người dùng và dữ liệu từng người tham gia. Mục đích là kiểm tra ý định và tính nhất quán. Không được mặc định thiết bị đã đăng ký vĩnh viễn một chính sách. Phạm vi kiểm tra ghi trong tài liệu chỉ là “lần rà soát này”.

Trong Mirror 12.12, bạn có thể đọc QR của Cuvex hoặc Desk trước và chọn bất kỳ dữ liệu nào. Không bắt buộc bắt đầu ở bước 1, quét hết hay giữ đúng thứ tự. Nếu bạn tự đọc văn bản mà bỏ qua quét, Mirror không đánh dấu mục ấy là đã xác minh.

Công cụ so sánh hiển thị trọn văn bản theo đúng ký tự. Khoảng trắng, ngắt dòng, chữ hoa thường và khác biệt Unicode đều được tính. “Khớp” chỉ có nghĩa hai giá trị của cặp đó giống nhau. Nó không xác thực nguồn, không chứng minh hai giá trị thuộc cùng một chính sách và không kích hoạt ví. Việc phê duyệt cuối và phản hồi tương ứng vẫn theo quy trình Cuvex và Desk.

QR hiện tại của Desk chỉ chứa giá trị, không có số thứ tự hay phiên. Mirror không phải lúc nào cũng suy ra được bước. “Chỉ định bước Desk” bổ sung ngữ cảnh thủ công và phải hiển thị rõ đó là thông tin nhập tay. Với N người tham gia có 7 + 4N trường trong sơ đồ đã mô tả: 8+4k là dấu vân tay, 9+4k là đường dẫn, 10+4k là xpub và 11+4k là ID khóa, với k bắt đầu từ 0. Khi N=2, bước 15 là ID của khóa thứ hai và có thể được so sánh trước.

Thực hành

1. Dùng dữ liệu giả để so một ID ghi là bước 15 trước, sau đó so mạng và ngưỡng.
2. Đổi một ký tự. Kiểm tra thông báo “Không khớp”, rồi bắt đầu cặp khác mà không mang kết quả cũ sang.
3. So sánh “2 / 3” và giải thích vì sao riêng văn bản này không phải lúc nào cũng cho biết đó là ngưỡng hay vị trí người dùng.

Chứng minh bạn đã hiểu

Nêu trường đã xác minh, cách xác định ngữ cảnh và phần còn phải phê duyệt. Không biến các kết quả khớp một phần thành phê duyệt toàn bộ.

Câu hỏi thường gặp

Có phải quét hết QR mới được học tiếp không? Không. Bạn tự chọn cách so sánh. Các bước kiểm tra và phê duyệt bắt buộc trên thiết bị ký vẫn có quy trình riêng.

Điểm tạm dừng

Đóng công cụ so sánh. Theo thiết kế đã rà soát, các giá trị phải được xóa khi thoát hoặc chuyển ứng dụng xuống nền.

Mirror so hai mã QR của bước 15 và báo “Khớp”. Điều đó chứng minh gì?

1. Hai giá trị giống hệt theo từng ký tự trong ngữ cảnh đã xác định hoặc được chỉ định.
2. Toàn bộ chính sách đã được phê duyệt.
3. Nguồn của cả hai mã QR đã được xác thực.

> **Xem đáp án: Hai giá trị giống hệt theo từng ký tự trong ngữ cảnh đã xác định hoặc được chỉ định.**
> So sánh không thay thế việc xác thực, kiểm tra tổng thể hoặc phản hồi của phần cứng.

Điều phối chữ ký và phát giao dịch đa chữ ký

Mục tiêu

Mang một đề xuất tới ngưỡng cửa chữ ký mà không hề đánh mất mục đích và kiểm soát.

Tìm hiểu

Một chiến dịch đa chữ ký ghi rõ các đầu vào, người nhận, nhập khẩu, giá cả, thay thế và ghi chú hoạt động. Người sáng tạo có thể yêu cầu chữ ký những người tương thích. Mỗi bên ký tự kiểm tra mạng lưới của mình, chính trị, các đầu vào, tất cả các đầu ra và phí trước khi bạn có thể sử dụng thiết bị này.

Một công ty không tự vận chuyển vốn nếu không có ngưỡng cửa. Khi đạt được nó, người điều phối có thể kết hợp và hoàn thành theo dòng chảy. Báo cáo của những người tham gia hoặc của người điều phối là thông tin phối hợp, không phải thông tin địa phương mà anh đã làm. App phải phân biệt được những chi tiết đó.

Căn cứ cho phép tái tranh cử, tiếp tân, buộc tội, từ chối và chuyển nhượng quyền phối hợp. Một sự dịch chuyển không thay đổi mức các khóa hay ngưỡng của chuỗi. Một câu trả lời được lưu giữ nên tương ứng với đơn xin và hồ sơ hiệu quả được dùng; không chọn một chính sách nào khác vì nó tương tự hoặc vì là chính sách đầu tiên trong danh mục.

Nếu có ai đó thay đổi người nhận hay những điều kiện có liên quan, chúng ta cần xem xét một đề xuất mới và có được các đề xuất chữ ký Phù hợp. Không phải bằng tay một PSBT loại bỏ dữ liệu bảo mật để đưa lên NFC. Các hợp đồng yêu cầu hồ sơ và đánh giá phù hợp, với giới hạn các đầu vào, các đầu ra và kích thước.

Trước khi xuất bản, hãy kiểm tra xem có thỏa thuận nào không và không có phiên bản nào được công bố cả. Tiếp theo là số xác nhận. Từ chối trong bài hát của bạn không tự động hủy bỏ chữ ký mà những người khác đã giữ hoặc ngăn chặn bất kỳ hành động tương thích nào với ngưỡng còn lại.

Thực hành

1. Mô phỏng chính sách 2 trên 3 với ba vai giả định. Một người ký, một người từ chối và người thứ ba yêu cầu làm rõ.
2. Thay đổi hướng trả tiền và giải thích tại sao một lời nói trước đó không được dùng.
3. Mô phỏng một cáo buộc thất bại sau khi giữ chữ ký. Lấy lại công việc cũ, không thanh toán gấp đôi, không thay đổi hồ sơ.

Chứng minh bạn đã hiểu

Bạn có thể chỉ ra ai phối hợp, ai ký, ai hoàn thành và bằng chứng gì tồn tại ở mỗi giai đoạn.

Câu hỏi thường gặp

Hai tin nhắn “OK” có tương đương hai chữ ký không? Không. Ngưỡng được đáp ứng bằng ủy quyền mật mã hợp lệ theo chính sách, không phải bằng tin nhắn.

Điểm tạm dừng

Hồ sơ tiểu bang, chữ ký đóng gói và tiếp theo là không có nội dung cá nhân.

Giao dịch 2 trên 3 có một chữ ký hợp lệ và hai tin nhắn “đồng ý”. Đã đủ ngưỡng chưa?

1. Có vì có ba người tham gia.
2. Chưa, cần thêm một chữ ký mật mã hợp lệ.
3. Có nếu điều phối viên công bố.

> **Xem đáp án: Chưa, cần thêm một chữ ký mật mã hợp lệ.**
> Đồng ý qua hội thoại và chữ ký hợp lệ là bằng chứng khác nhau.

Khôi phục và thay đổi ví đa chữ ký

Mục tiêu

Lấy lại chính sách và lên kế hoạch mất mát hay thay thế những người tham gia.

Tìm hiểu

Sự phục hồi cần hai loại dữ liệu: dữ liệu để tái tạo lại chính sách và khả năng cá nhân để tiêu dùng. Một bản sao chính sách xpubs có thể tiết lộ lịch sử mà không cần thêm hạt giống khôi phục. Một bản sao đã được mật mã thêm sự bảo vệ vào kho lưu trữ, nhưng nó đòi hỏi phải giữ bản mật khẩu của nó. Phần mở rộng.cuvexms không tự nó chứng minh được mã hóa: định dạng và xuất khẩu cần được kiểm tra.

Trong Desk 9.21, phục hồi yêu cầu khóa công khai mở rộng của người tham gia với dấu vân tay và đường dẫn BIP48 xuất khẩu từ thiết bị của họ. Cho phép đọc trên webcam hoặc Mirror từ dòng chảy tương thích. Đừng thay thế sự đóng góp đó bằng một địa chỉ nhận Đừng gửi đi hạt giống khôi phục Để hỗ trợ.

Nếu bạn mất một chiếc khóa trong chiếc 2 3, hai chiếc kia có thể giữ được khả năng chi tiêu. Chính sách cũ vẫn còn hiệu quả, để loại bỏ một người tham gia và thiết lập thêm các khóa, thường có một chính sách mới được thiết lập và chuyển tiền với giấy phép cần thiết. Thay đổi biệt danh hoặc loại bỏ một ví của Desk không thay đổi UTXOs.

Các bản sao phải cho phép xây dựng lại cả hai nhánh và tìm ra lịch sử. Bạn giữ các chỉ số, đơn xin được phát hành và bối cảnh cần thiết để không sử dụng lại địa chỉ hoặc chơi một bản ví trống bởi một bản quét không đầy đủ. Phục hồi và tiếp tục một chiến dịch chưa hoàn thành, nên tôn trọng hồ sơ đã được lưu giữ khi tạo ra nó.

Thực hành

1. Xuất khẩu và khôi phục lại một chính sách phòng thí nghiệm bằng cách sử dụng các hàm số được ghi nhận. Kiểm tra mạng lưới và địa chỉ đã biết.
2. Mô phỏng việc mất một người tham gia và chuẩn bị một kế hoạch quay, mà không cần di chuyển quỹ thực sự.
3. Mô phỏng mất mát dưới ngưỡng cửa. Anh ta nhận ra rằng nó hỗ trợ hoặc AI không thể sản xuất chữ ký.

Chứng minh bạn đã hiểu

Bạn có thể lấy lại sân khấu thử nghiệm và phân biệt thông tin về việc thay đổi kiểm soát tiền xu.

Câu hỏi thường gặp

Gỡ bỏ đa chữ ký trên Desk, tắt ví cho tất cả mọi người? Không. Loại bỏ trạng thái cục bộ theo dòng chảy. Những người và bản sao khác có thể tiếp tục duy trì khả năng chính trị.

Điểm tạm dừng

Bản sao của bản sao thử nghiệm và kế hoạch riêng, chỉ ghi lại kết quả trong khóa học.

Muốn bỏ một người khỏi chính sách đã nhận tiền, chỉ xóa tên trong Desk có đủ không?

1. Có.
2. Có nếu xóa cả trò chuyện.
3. Không, cần lập chính sách mới và chuyển tiền có phê duyệt khi phù hợp.

> **Xem đáp án: Không, cần lập chính sách mới và chuyển tiền có phê duyệt khi phù hợp.**
> Sửa dữ liệu cục bộ không thay script của các UTXO hiện có.

Cập nhật phần sụn theo quy trình

Mục tiêu

Chuẩn bị cập nhật tương thích và kiểm tra kết quả trên thiết bị.

Tìm hiểu

Một bản cập nhật sẽ thay đổi phần mềm sự tin tưởng. Kiểm tra mô hình, kiểm tra phần cứng, phiên bản, nguồn gốc và cơ chế xác thực của nhà sản xuất. Một cú sốc đầy đủ hoặc một cú sốc giá trị băm tương đương với một trang giấy không thay thế việc xác nhận chữ ký và khả thi. Đừng bao giờ thiết lập một ứng dụng phần sụn mà không có chữ ký của kỹ sư như thể nó là một ấn phẩm dành cho khách hàng.

Original cập nhật bởi Bluetooth trong lưu lượng được ghi nhận. BIT Dùng USB-C . Mirror cho phép du lịch chuẩn bị và vận chuyển phù hợp. Không hứa hẹn rằng một tổ hợp cụ thể của PC, điện thoại và thiết bị sẽ hoạt động cho đến khi hoàn thành việc chấp nhận sự kết hợp vật lý. Quá trình cập nhật Original trong Windows đòi hỏi một sự chẩn đoán cụ thể; không giải quyết thành công trong 99%.

Trước khi bắt đầu, hãy kiểm tra bản sao lưu có thể phục hồi, cung cấp thức ăn ổn định và không có các hoạt động khác. Chuẩn bị tập tin chính thức hoặc sao chép trước khi kiểm tra theo bản hợp đồng. Trong khi vận chuyển, sự khác biệt về chuyển giao, xác nhận, cài đặt, cài đặt lại và kiểm tra phiên bản. Cái quầy không phải là bằng chứng cuối cùng.

Sau đó, kiểm tra phiên bản nhìn thấy trên máy tính và ghi ngày tháng và kết quả. Danh mục khớp giữa Desk không có tính toán từ xa bằng phần sụn: firmwaureAttion vẫn còn sai. Chọn một hồ sơ cuối cùng không được ghi rõ màytes thực sự được cài đặt. Nếu sự cập nhật thất bại, nó vẫn còn được ghi lại và duy trì giai đoạn và lỗi mà không ngắt kết nối tại một giai đoạn quan trọng.

Thực hành

1. Kiểm tra một danh sách chuẩn bị mà không cần cập nhật thực tế trong buổi thử nghiệm.
2. Sắp xếp các trạng thái và giải thích tại sao chuyển đổi và "được bảo quản" lại khác nhau.
3. Bản báo cáo thất bại 99% với mô hình, phiên bản, hệ thống, giai đoạn và thông điệp cuối cùng.

Chứng minh bạn đã hiểu

Bạn có thể xác định được những thiết bị phù hợp, phương tiện và tiêu chuẩn thành công cuối cùng.

Câu hỏi thường gặp

Tôi chỉ cần cập nhật để loại bỏ một sai lầm Desk? Đầu tiên xác định nguồn gốc. Một sự mâu thuẫn trong danh mục có thể cần phải sửa đổi Desk ♪ Và giữ lấy ♪ phần sụn Tôi vô dụng.

Điểm tạm dừng

Một bản cập nhật thực sự chỉ tạm dừng trong một trạng thái chắc chắn của thủ tục, chứ không phải là để kết thúc cuộc gọi.

Bản thân danh mục rõ ràng của Desk xác minh được gì?

1. Các tham chiếu tương thích được hỗ trợ, không đo từ xa phần sụn đã cài.
2. Chứng thực vật lý mọi thiết bị kết nối.
3. Không có lỗ hổng.

> **Xem đáp án: Các tham chiếu tương thích được hỗ trợ, không đo từ xa phần sụn đã cài.**
> Tương thích, chữ ký, đo lường và nghiệm thu trên thiết bị là bằng chứng khác nhau.

Mất thiết bị, hỏng hóc và khôi phục khẩn cấp

Mục tiêu

Chọn sự phục hồi tỉ lệ thuận với sự cố và bảo tồn những bằng chứng hữu ích.

Tìm hiểu

Sau một sự cố, trước hết hãy phân loại những gì đã bị mất hoặc phơi bày: máy tính, thiết bị, thẻ, tập tin, mật khẩu, hạt giống khôi phục, cụm mật khẩu hay chính trị. "Tôi không thể vào" không nhất thiết có nghĩa là "tôi đã bị đánh cắp". Nếu có nghi ngờ đính hôn, đừng tiếp tục đưa những bí mật vào đội nghi ngờ.

Mất thiết bị có thể được giải quyết bằng sự hỗ trợ và khả năng phục hồi tương thích. Mất máy tính có thể cần thiết để phục hồi lại nhà kho của Desk và tái xây dựng lại quan sát. Mất tất cả phương tiện mở khóa hoặc tất cả các khóa cần thiết dưới ngưỡng có thể không có giải pháp kỹ thuật. Không có AI nào có thể đảm bảo giải cứu các khóa không tồn tại.

Desk bao gồm việc phục hồi địa phương cho các định dạng và xuất khẩu tài liệu phục hồi tương ứng. giải mã trên PC có thể tiết lộ bí mật này cho hệ điều hành hay phần mềm độc hại. Đó là một quyết định phi thường: sử dụng một môi trường được chuẩn bị, vật liệu phù hợp và kế hoạch chuyển sang các khóa mới nếu bí mật đó có thể bị xâm nhập. Đừng miêu tả nó như một cuộc phẫu thuật tương đương với sự cô lập thông thường của Cuvex.

Nếu một hạt giống khôi phục rò rỉ, thay đổi mật khẩu Desk sẽ không hủy hạt giống khôi phục. Anh phải đánh giá việc chuyển một chiếc ví mới và bảo vệ nó từ một đội đáng tin cậy. Bạn không nên đăng chi tiết về sự kiện có thể giúp đỡ hoặc trả các dịch vụ hứa sẽ phục hồi lại để đổi lấy một hạt giống khôi phục khác hoặc một sự ứng nghiệm gian lận.

Thực hành

1. Nó giải quyết bốn tấm thẻ giả: PC, thẻ bị mất, thẻ bị vỡ với bản sao hợp lệ, mật khẩu bị lãng quên và hạt giống khôi phục được phơi bày.
2. Đối với mỗi vật liệu, nó nhận diện những vật liệu cần thiết, rủi ro về hành động và sự phục hồi.
3. Hãy tập luyện thủ tục chỉ với dữ liệu học tập; đừng tải về gia sư tập tin khẩn cấp thực tế.

Chứng minh bạn đã hiểu

Bạn có thể chọn giữa phục hồi, cấu hình lại quan sát, di chuyển quyền kiểm soát hoặc leo lên một chuyên gia mà không cần phải nói đến những giải pháp không tưởng.

Câu hỏi thường gặp

Thay đổi mật khẩu lần nữa tất cả những bí mật mà mọi người đã từng thấy? Không. Một bản sao rõ ràng hoặc một bản hạt giống khôi phục được biết đến vẫn còn được biết đến.

Điểm tạm dừng

Hãy giữ kín sự việc theo thứ tự và hành động an toàn tiếp theo; dừng nói lại nếu bạn định làm việc với những bí mật.

Hạt giống đã bị công bố, nhưng bạn đổi mật khẩu máy tính. Khả năng chi của kẻ tấn công đã bị thu hồi chưa?

1. Rồi.
2. Chưa, hạt giống vẫn kiểm soát các khóa cũ và cần biện pháp ứng phó lưu ký.
3. Rồi nếu đổi cả hình nền trò chuyện.

> **Xem đáp án: Chưa, hạt giống vẫn kiểm soát các khóa cũ và cần biện pháp ứng phó lưu ký.**
> Bảo vệ cục bộ không vô hiệu hóa khóa Bitcoin đã lộ.

Lừa đảo giả mạo, hỗ trợ và gian lận bằng giọng nói

Mục tiêu

Chấp nhận những yêu cầu nguy hiểm và đáp trả mà không cần ứng biến.

Tìm hiểu

Một kẻ lừa đảo hiệu quả có thể dùng tên của bạn, mua, thiết bị và giọng nói mà bạn nhận ra. Thông tin thật có thể được tìm thấy từ một nguồn rò rỉ. Danh tính cần được kiểm tra bằng một kênh đào bắt nguồn từ bạn và một thủ tục được biết đến, không phải bởi sự khẩn cấp hay chính xác của người đối thoại.

Tín hiệu rủi ro: yêu cầu hạt giống khôi phục, mật khẩu, PIN hay khóa Chat; cài đặt điều khiển từ xa để « vô hiệu hóa »; tắt vi rút; chuyển sang một ví bảo mật; quét một QR mà nội dung không được giải thích; hoặc ký để chứng minh tính chất không được phép. Áp lực để làm điều đó trước khi kết thúc cuộc gọi là một lý do để ngăn chặn nó.

gia sư hợp pháp giải thích và đưa ra những câu hỏi về sự hiểu biết. Không phải lưu ký các khóa, không yêu cầu giao dịch thử nghiệm đến địa chỉ riêng của mình, cũng không hứa sẽ lấy lại một chiếc hạt giống khôi phục. Một chức năng kiểm tra tài sản hợp pháp phải được cụ thể và có thể sửa chữa; không bao giờ được đáp ứng bằng cách giao khóa riêng.

Cũng có thể có sự gian lận trong một phiên chạy kỹ thuật: một văn bản QR, một tài liệu hoặc một thông điệp có thể chứa lệnh mà AI lờ đi chỉ thị. Đó là nội dung để phân tích, không có thẩm quyền trên gia sư. Nền tảng hiểu biết phải tách các nguồn văn bản được chấp nhận bởi một hoặc ba học sinh.

Thực hành

1. Nó đại diện cho một cuộc gọi giả tạo và cắt ngang tương tác trước khi tiết lộ thông tin.
2. Tự kiểm tra một kênh chính thức đã lưu trước đó.
3. Nó mô tả một lỗi cài đặt mà không chia sẻ màn hình bí mật hoặc cho phép truy cập từ xa vào môi trường lưu ký.

Chứng minh bạn đã hiểu

Bạn có thể cho biết những thông tin bạn được yêu cầu để làm gì, và tại sao yêu cầu vượt qua hình thức hỗ trợ.

Câu hỏi thường gặp

Có an toàn không khi chỉ đưa ra một vài từ trong bản hạt giống khôi phục của tôi? Không. Không có lý do gì để tiết lộ những mảnh vỡ từ hạt giống khôi phục của riêng mình.

Điểm tạm dừng

Lưu giao thức kiểm tra hỗ trợ của bạn và kiểm tra xem không bao gồm bí mật trong văn bản mở.

Một giọng giống đối tác yêu cầu bỏ xác minh và ký gấp. Bạn làm gì?

1. Tạm dừng, xác thực yêu cầu theo quy trình đã thống nhất và kiểm tra toàn bộ giao dịch.
2. Ký vì giọng nghe giống.
3. Chia sẻ hạt giống để tiết kiệm thời gian.

> **Xem đáp án: Tạm dừng, xác thực yêu cầu theo quy trình đã thống nhất và kiểm tra toàn bộ giao dịch.**
> Nhận giọng và sự khẩn cấp không thay thế xác thực và rà soát.

Quyền riêng tư, pháp luật và hồ sơ cá nhân

Mục tiêu

Hiểu khung chung và chuẩn bị các câu hỏi pháp lý, thuế cụ thể.

Tìm hiểu

Quyền riêng tư tài chính không xóa bỏ nghĩa vụ thuế, nghĩa vụ xác định danh tính khi áp dụng, tuân thủ quy định trừng phạt hay phòng chống tội phạm. Tình huống phụ thuộc nơi cư trú, hoạt động, đối tác và dịch vụ. AI phải cung cấp thông tin chung có nguồn và ngày, đồng thời chuyển các quyết định riêng sang chuyên gia đủ năng lực.

Tại EU, MiCA điều chỉnh một số tài sản và dịch vụ mã hóa. Việc áp dụng chung bắt đầu ngày 30 tháng 12 năm 2024. Thời kỳ chuyển tiếp tối đa nêu trong quy định kéo dài đến ngày 1 tháng 7 năm 2026, tùy quyết định của mỗi quốc gia. Kiểm tra tình trạng cấp phép và phạm vi trên sổ đăng ký chính thức hiện hành. Thông tin cũ về việc từng đăng ký là chưa đủ. Giấy phép không bảo đảm giá, khả năng thanh toán hay bồi hoàn toàn bộ.

Quy định 2023/1113 đặt ra yêu cầu về thông tin đi kèm giao dịch chuyển khi có nhà cung cấp thuộc đối tượng có nghĩa vụ. Với giao dịch trên 1.000 euro liên quan địa chỉ tự lưu ký, quy định nêu các biện pháp đánh giá quyền sở hữu hoặc kiểm soát. Ngưỡng đó không tạo miễn trừ chung về xác định danh tính cho số tiền thấp hơn. Giao dịch trực tiếp giữa cá nhân không có nhà cung cấp tham gia được loại khỏi phạm vi quy định này, nhưng các nghĩa vụ khác vẫn tồn tại.

Lưu đủ tài liệu về mua, bán, phí và nguồn gốc theo trường hợp của bạn, đồng thời ngăn việc truy cập không cần thiết. Không cần công bố toàn bộ lịch sử để lập hồ sơ riêng. Khóa học không hướng dẫn chia nhỏ giao dịch để tránh kiểm soát, khai sai thông tin hay che giấu thu nhập.

Nếu có ghi âm hoặc chép lời giọng nói và theo dõi tiến độ gắn được với một cá nhân, dịch vụ phải xác định mục đích, cơ sở pháp lý, việc lưu giữ, quyền truy cập, các bên xử lý và những quyền áp dụng. Cấu hình quyền riêng tư của dịch vụ thương mại phải được xác minh trước khi bán, không tùy cơ quyết định trong cuộc gọi.

Thực hành

1. Soạn tình huống giả định cho cố vấn, ghi nơi cư trú, hoạt động và giao dịch, không ghi khóa.

2. Kiểm tra nơi có thể xác minh giấy phép nhà cung cấp và ngày của thông tin.
3. Thiết kế sổ theo dõi biến động riêng tư cùng chính sách tối thiểu về dữ liệu học viên.

Chứng minh bạn đã hiểu

Phân biệt quy định pháp luật, chính sách sàn giao dịch và khả năng kỹ thuật của Bitcoin.

Câu hỏi thường gặp

Mọi hình thức tự lưu ký đều bị cấm tại EU phải không? Không thể rút ra kết luận đó từ các quy định vừa nêu. Tránh tiêu đề tuyệt đối và kiểm tra đúng điều khoản, phạm vi áp dụng.

Điểm tạm dừng

Lưu câu hỏi còn lại cho cố vấn, không nhập hồ sơ cá nhân vào gia sư.

Ngưỡng 1.000 euro nêu cho một số biện pháp xác minh quyền kiểm soát địa chỉ có xóa mọi nghĩa vụ dưới ngưỡng không?

1. Có.
2. Chỉ khi bạn chia nhỏ giao dịch.
3. Không. Đây không phải miễn trừ chung về xác định danh tính hay các nghĩa vụ khác.

> **Xem đáp án: Không. Đây không phải miễn trừ chung về xác định danh tính hay các nghĩa vụ khác.**
> Phải diễn giải quy định theo biện pháp cụ thể và phạm vi áp dụng. Không biến một ngưỡng thành miễn trừ phổ quát.

Thừa kế, duy trì khả năng tiếp cận và diễn tập hằng năm

Mục tiêu

Tạo ra một kế hoạch cho phép những người có thẩm quyền hành động mà không cần phải vạch trần trước.

Tìm hiểu

Di sản phối hợp pháp luật, vị trí của vật liệu và kỹ thuật. Một người có quyền thừa kế và không biết xây dựng lại ví; người khác có thể có khóa và không có quyền sử dụng nó. Kế hoạch phải giải quyết cả hai chiều với những lời khuyên thích hợp.

Nó tách ra những hướng dẫn công khai về truy cập bí mật. Bản kê khai này mô tả cái gì tồn tại, cái gì được liên lạc và những gì kiểm tra, mà không đưa tất cả các khóa và mật khẩu vào một tài liệu có thể truy cập rộng rãi. Tránh in hạt giống khôi phục trong di chúc hoặc hồ sơ mà có thể lưu giữ ngoài tầm kiểm soát của anh.

Trong đa chữ ký nhà thiết kế người bảo tồn chính sách và sao chép, ngưỡng nào sẵn có sau khi mất, và điều gì sẽ xảy ra nếu một người khóa chết. Một bên lưu ký lưu trữ đủ các thành phần có thể trở thành điểm duy nhất của lạm dụng. Sự phân bố quá phức tạp có thể làm cho tài sản của chúng ta trở nên không thể phục hồi.

Bao gồm việc phục hồi mật khẩu của bản mật mã Và cụm mật khẩu Nếu nó tồn tại, dữ liệu dẫn xuất Khả năng tương thích của thiết bị và phương pháp nếu nhà sản xuất ngừng hoạt động. Đừng cho rằng một tập tin sở hữu hoặc một dấu vân tay sinh trắc học có thể được sử dụng mà không cần chuẩn bị trước. Sự tương tác phải được thực hiện bằng dữ liệu thử nghiệm và định dạng được ghi lại.

Kiểm tra những thay đổi trong gia đình, địa chỉ nhà, chính trị, phần mềm, hay những người tham gia, và thực hiện một cuộc diễn tập trên báo. Tập thể dục phải chứng tỏ rằng một người đáng tin cậy hiểu rõ các lời chỉ dẫn mà không cho biết tài sản của mình hoặc làm giàu một cách không cần thiết.

Thực hành

1. Hoàn thành một mẫu riêng với trách nhiệm, thành phần, quyền truy cập và thay thế.
2. Nó đưa cho người khác chỉ dẫn từ phòng thí nghiệm mà không giải thích bằng miệng và quan sát nơi nó bị khóa.

3. Sửa chữa mơ hồ và ghi lại ngày sửa chữa. Khóa học không tự động tạo ra những sự nhắc nhở.

Chứng minh bạn đã hiểu

Bạn có thể giải thích điều gì sẽ xảy ra nếu bạn không có mặt và thông tin nào bạn cần mỗi vai trò ở mỗi giai đoạn.

Câu hỏi thường gặp

2 3 thay thế cho kế hoạch thừa kế? Không. Đó là một công cụ kỹ thuật. Những người kế tự vẫn cần đến bối cảnh, vật chất, sự phối hợp và hợp pháp.

Điểm tạm dừng

Lưu kế hoạch ra khỏi khóa học và chỉ đánh dấu "đồng hồ kiểm tra".

Tiêu chí nào hữu ích để đánh giá kế hoạch thừa kế?

1. Người được phép có thể diễn tập theo tài liệu mà không phải ứng biến hay nhận bí mật trước thời điểm cần thiết.
2. Kế hoạch thật nhiều trang.
3. Chỉ dựa vào việc nhớ một mật khẩu.

> **Xem đáp án: Người được phép có thể diễn tập theo tài liệu mà không phải ứng biến hay nhận bí mật trước thời điểm cần thiết.**
> Phải kiểm tra thực tế khả năng khôi phục và kiểm soát truy cập.

Giá, tiết kiệm và phân tích cơ bản

Mục tiêu

Phân tích các đối số đầu tư mà không nhầm chúng với các tính năng kỹ thuật có thể kiểm chứng.

Tìm hiểu

Giá cả là kết quả của việc trao đổi tại các thị trường cụ thể, và nó có thể khác nhau giữa các nền tảng. thanh khoản, tỷ giá tham khảo, độ sâu, thời gian của các nhà cung cấp ngân hàng và cầu ảnh hưởng đến kết quả mà bạn có thể thực hiện. Một chiếc tỷ giá tham khảo trên màn hình không phải là một đề nghị bảo đảm cho âm lượng của anh.

Phân tích căn bản về những yếu tố như nhận nuôi, yêu cầu, cạnh tranh, an ninh kinh tế, quy định và đề nghị. Một lịch trình phát thanh được biết đến không chỉ quyết định giá cả trong tương lai. Những đánh giá về lợi nhuận hoặc "sự đánh giá nội tâm" tùy thuộc vào những giả định; không có một con số khách quan nào mà AI có thể đưa ra để chứng minh sự chắc chắn của toàn cầu.

Một chiến lược mua sắm định kỳ sẽ phân phát thời gian vào cửa, nhưng không bảo đảm có lợi hay tránh mất mát lâu dài. Tiền tiết kiệm dài hạn cũng cần thanh khoản cho nghĩa vụ, sự khoan dung và kế hoạch lưu ký. Khóa học không chỉ định tỷ lệ tài sản của bạn, hay đưa ra quyết định cho bạn.

Tách ra ba câu hỏi: Có hiểu được tài sản không? Tôi có thể bảo vệ nó và lấy lại nó không? Tôi có thể chấp nhận rủi ro kinh tế của anh không? Giới hạn các khóa không tự động đáp ứng đến mức độ 3. Việc đào tạo không biến một hình chiếu giá cả hay đồ thị lịch sử thành một sự giới thiệu cá nhân.

Thực hành

1. Ông viết một luận văn giả tạo, những giả định và hành động có thể vô hiệu hóa nó.
2. Mô phỏng sự suy giảm của 50% và nhu cầu của thanh khoản cùng lúc, mà không giới thiệu tài sản hoàng gia của bạn.
3. Xác định được dữ liệu của đối số là có thể kiểm chứng và những gì là mong đợi.

Chứng minh bạn đã hiểu

Bạn có thể thảo luận về đầu tư mà không hứa hẹn thu nhập hay nhầm lẫn sự tin tưởng với bằng chứng.

Câu hỏi thường gặp

Sự khan hiếm có đảm bảo giá cả tăng lên không? Không. Nhu cầu và các điều kiện khác vẫn còn rất quan trọng đối với giá thị trường.

Điểm tạm dừng

Nó lưu giữ những giả định của phòng thí nghiệm, chứ không phải chỉ thị mua sắm tự động.

Mua định kỳ bảo đảm gì?

1. Có lãi dài hạn.
2. Không bảo đảm lợi suất, chỉ phân bổ thời điểm mua theo quy tắc đã chọn.
3. Bảo vệ khỏi mất khóa.

> **Xem đáp án: Không bảo đảm lợi suất, chỉ phân bổ thời điểm mua theo quy tắc đã chọn.**
> Phân bổ điểm mua không loại rủi ro kinh tế hay vận hành.

Lựa chọn nơi mua bitcoin

Mục tiêu

Đánh giá một nhà cung cấp cho phép, chi phí, rút lui, riêng tư và mạo hiểm lưu ký.

Tìm hiểu

So sánh các nhà cung cấp thông qua các tiêu chuẩn xác nhận: thực thể pháp lý và thẩm quyền, các dịch vụ có thẩm quyền, mạng lưới rút lui, phí, các trường hợp khác nhau về giá cả, giới hạn, hỗ trợ, xác thực và điều trị dữ liệu. Tên thương mại hoặc tài trợ không cho phép dịch vụ đặc biệt.

Toàn bộ chi phí có thể bao gồm tiền gửi, chuyển hóa, chênh lệch giá, phí, giảm chi phí ngân hàng. Một cuộc đàm phán không có phí có thể có một sự phân biệt lớn hơn. Hãy kiểm tra số lượng liên lạc và đồng xu tham khảo. Ngân sách phải bao gồm cả việc loại trừ tự lưu ký khi đó là mục tiêu của bạn.

Trong khi anh giữ một khoản nợ, anh phụ thuộc vào nhà cung cấp. Một cuộc thử nghiệm dự trữ không phải chỉ cho thấy những gì bị động, tài sản tài chính hoặc sự giải phóng trong tương lai. Kiểm tra và rút lui một chút trước khi phụ thuộc vào một dòng chảy mới.

Chứng minh thư thương mại có thể liên kết danh tính của anh với việc rút lui. Việc bảo vệ thông tin đó sau này không có nghĩa là xóa đi những gì nhà cung cấp biết. Đừng làm sai số liệu hoặc sử dụng khóa học để trốn tránh trách nhiệm. Việc mua một mã huấn luyện cũng tạo ra một bản ghi thương mại riêng biệt với ví của anh.

Thực hành

1. Điền vào một ma trận giả với hai nhà cung cấp: chi phí tổng thể, mạng lưới, thu hồi tối thiểu, cho phép và thông tin yêu cầu.
2. Tính toán hệ số cho thao tác học tập với mọi cáo buộc đã ghi rõ.
3. Thiết kế một cuộc kiểm tra địa chỉ đã kiểm tra trước, chưa chạy nó từ phần mềm nhỏ này.

Chứng minh bạn đã hiểu

Anh có thể bào chữa cho một lựa chọn cho vụ án của anh và nhận ra thông tin đã hết hạn hoặc chưa được kiểm tra.

Câu hỏi thường gặp

Khóa học đề nghị sàn giao dịch là khóa học tốt nhất cho tất cả chúng ta? Không. Giấy phép, phí tổn, các quốc gia được chăm sóc và điều kiện đã thay đổi. Sự so sánh này đòi hỏi ngày tháng và trường hợp.

Điểm tạm dừng

Giữ ma trận không giấy tờ, không giấy chứng minh.

So sánh gì hữu ích hơn chỉ nhìn phí giao dịch?

1. Tổng chi phí đến khi nhận BTC trên đúng mạng và địa chỉ mong muốn.
2. Số người theo dõi nhà cung cấp.
3. Màu ứng dụng.

> **Xem đáp án: Tổng chi phí đến khi nhận BTC trên đúng mạng và địa chỉ mong muốn.**
> Giá cuối có thể gồm khoản nằm ngoài phí quảng cáo.

M11

Tài khoản, lệnh và chi phí khớp lệnh

Mục tiêu

Hiểu những mệnh lệnh cơ bản và bảo vệ tài khoản mà không chuyển đổi khóa học thành một giai đoạn cuối của trading.

Tìm hiểu

Lệnh thị trường ưu tiên thi hành, có nguy cơ trượt giá. Một lệnh giới hạn đặt giá mua bán tối đa hoặc tối thiểu, nhưng có thể không thực hiện hoặc thực hiện một phần. Một lệnh dừng hoạt động một hành động khác theo quy tắc của nhà cung cấp; không bảo đảm một cái giá cuối cùng.

sổ lệnh cho thấy các đề nghị sẵn sàng, chứ không phải cam kết rằng tất cả các tập sẽ tồn tại. Một cú ngã hay một cú ngã thanh khoản Kết quả có thể khác với kết quả cuối cùng. tỷ giá tham khảo . Lệnh top-market và hạn chế có các rủi ro khác nhau: chạy với giá thấp hơn trước khi có thể không thực hiện.

Bảo vệ truy cập với mật khẩu Độc nhất, có khả năng xác thực lừa đảo giả mạo Khi nào có thể, kiểm tra và kiểm tra chính xác. Kiểm tra lại yếu tố thứ hai một cách độc lập Một khóa API để tự động hóa có thể có quyền hạn nguy hiểm hơn là cần đọc dữ liệu; không được đưa nó vào gia sư hay phần nhỏ.

Trước khi nghỉ hưu, hãy kiểm tra tài sản và mạng bitcoin, địa chỉ của ví và số lượng liên kết. Một nền tảng có thể sử dụng cùng một biểu tượng cho các sản phẩm khác nhau. Khi kết thúc, hãy giữ lại tài liệu mua sắm, thực hiện, phí và rút lui theo cách của bạn; đừng nhầm lẫn việc rút lui của bạn với một chiếc ví mới.

Thực hành

1. Mô phỏng sổ lệnh với 1 đơn vị ở giá 100 và 1 đơn vị ở giá 102. Giải thích vì sao mua hai đơn vị bằng lệnh thị trường không bảo đảm giá trung bình 100.
2. Nó thiết kế một trật tự giới hạn và mô tả cảnh không hoàn chỉnh.
3. Cho phép API giả mạo và rút lui nếu cần thiết.

Chứng minh bạn đã hiểu

Anh có thể mô tả ưu tiên, giá cả và rủi ro không được thực hiện cho mỗi thứ tự.

Câu hỏi thường gặp

Chính xác thì một người quá cố luôn hạn chế mất mát? Không. Gaps, thanh khoản, trượt giá và luật lệ của nhà cung cấp có thể ngăn chặn điều đó.

Điểm tạm dừng

Nó lưu lại kết quả của bài tập không có lệnh thực sự, không có các khóa API.

Lệnh giới hạn mua ở giá 100 vẫn có rủi ro gì?

1. Không khớp hoặc chỉ khớp một phần.
2. Buộc phải khớp ở mọi giá.
3. Tự tạo bản sao lưu.

> **Xem đáp án: Không khớp hoặc chỉ khớp một phần.**
> Đổi lại việc kiểm soát giá là khả năng không khớp lệnh.

Nến giá, chỉ báo và thiên kiến trong phân tích kỹ thuật

Mục tiêu

Đọc đồ thị như dữ liệu lịch sử và đánh giá chiến lược mà không nhầm lẫn các mẫu hình.

Tìm hiểu

nến giá tóm tắt mở rộng tối đa và kết thúc một giai đoạn. Âm lượng phụ thuộc vào nguồn. Thay đổi nền tảng, tiền tệ, thời gian biểu có thể thay đổi những gì bạn nhìn thấy. nến giá không cho thấy mọi thứ tự thời gian di chuyển trong khoảng thời gian đó.

Một chiếc điện thoại di động làm dịu giá cả quá khứ. Một chỉ số thời gian chuyển đổi dữ liệu được quan sát dưới một công thức. Không ai biết trước tương lai. Hai tín hiệu xuất phát từ cùng một chuỗi có thể cung cấp thông tin tương quan, dù màu sắc và tên của chúng khác nhau.

Để đánh giá một quy tắc xác định đầu vào, đầu ra, không xác định, chi phí, kích thước và dữ liệu trước khi xem xét kết quả. Tránh chỉ chọn những ví dụ người thắng cuộc, điều chỉnh tham số cho đến khi phù hợp hoặc sử dụng dữ liệu tương lai trong quyết định quá khứ. Phân loại dữ liệu đào tạo và xác nhận thời gian.

Một phản hồi phải xem chênh lệch giá, phí, trượt giá, có sẵn dữ liệu và thực hiện. Sự tính toán kỹ lưỡng, tỷ lệ đúng, mất mát tối đa và phân phối mất mát phản hồi với những câu hỏi khác nhau. Một hệ thống với nhiều sự chính xác có thể mất tiền nếu thất bại lớn. Không có dấu hiệu mua bán nào là chắc chắn cả.

Thực hành

1. Hãy đọc nến giá tin tức và giải thích những thông tin tạm thời không có trong đó.
2. Viết một quy tắc trước khi đánh giá 10 kết quả tổng hợp, với chi phí và tiêu chuẩn.
3. So sánh 9 lợi nhuận 1 với việc mất đi 15. Kết quả thô là -6 mặc dù 90% của độ chính xác.

Chứng minh bạn đã hiểu

Bạn có thể chỉ trích một kết quả hấp dẫn bởi chọn lọc, chi phí hoặc rủi ro mà không cần thực hiện các thao tác.

Câu hỏi thường gặp

Liên kết nhiều chỉ số có đảm bảo tín hiệu tốt hơn không? Không. Nó có thể tăng sự ngẫu nhiên và phức tạp mà không cần cung cấp thông tin độc lập.

Điểm tạm dừng

Giữ nguyên quy định và kết quả phòng thí nghiệm, không phải lệnh thị trường.

Chín giao dịch mỗi giao dịch lãi 1, một giao dịch lỗ 15. Kết quả trước chi phí là gì?

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

> **Xem đáp án: -6.**
> Lãi chín đơn vị trừ lỗ mười lăm thành lỗ sáu.

Ký quỹ, hợp đồng tương lai và tự động hóa

Mục tiêu

Nhận diện phơi nắng, thanh lý và lỗi tự động trước khi xem xét các sản phẩm phức tạp.

Tìm hiểu

đòn bẩy đang tiếp xúc với vốn đóng góp. Trong một ví dụ đơn giản, 100 dư cho một cuộc triển lãm 1.000 có nghĩa là một chuyển động bất lợi của 5 phần trăm cơ sở vật chất tương đương với 50 trước khi chi phí: một nửa số lề ban đầu. Quy tắc bảo trì thực sự, thanh lý, và phí có thể làm cho kết quả tồi tệ hơn và kích hoạt sớm hơn dự kiến.

Tương lai và vĩnh cửu có thể kết hợp với thanh lý vì khác biệt, tỷ lệ tài trợ và giá cả tham khảo khác nhau trong lần trao đổi trước. Chúng không tương đương với việc loại trừ bitcoin thổ dân sang Cuvex. Bảo vệ một chiếc hạt giống khôi phục không bảo vệ vị trí đối diện với thanh lý hoặc bị lỗi.

Một robot tự động đặt ra luật lệ, kể cả lỗi lầm của nó. Nó cần giới hạn vị trí, giấy phép tối thiểu, quyền hạn của mệnh lệnh, sự hòa giải, kiểm soát mất mát, sự gián đoạn khẩn cấp và giám sát. Yêu cầu tăng gấp đôi sau khi dùng thuốc nhuộm có thể tăng gấp đôi khả năng tiếp xúc nếu bạn không biết kết quả trước đó.

AI có thể giải thích khái niệm và phát hiện những sai sót trong một vụ án tưởng tượng. Bạn không nên nhận các khóa API, kích hoạt Trading hoặc hứa hẹn một chiến lược sinh lợi. Với mục tiêu chính của khóa học này, hiểu được những rủi ro này giúp chúng ta quyết định không sử dụng những sản phẩm mà mình không hiểu.

Thực hành

1. Giải quyết các ví dụ về phơi nắng và lề mà không giả định mức độ thanh lý Hãy là chính xác 10 %.
2. Mô phỏng API thực hiện lệnh, nhưng không có câu trả lời. Điều này giải thích tại sao trước khi nói lại, bạn cần phải hòa giải.
3. Hãy thiết kế một nút dừng để ngăn chặn lệnh mới và kiểm tra các lệnh đã mở, chưa kết nối đến người chơi.

Chứng minh bạn đã hiểu

Bạn có thể mô tả một rủi ro mà có thể tồn tại trong siêu nhỏ, một rủi ro khác sống sót qua con robot, và một trong số đó sống sót sau khi sử dụng tự lưu ký quỹ từ bên ngoài.

Câu hỏi thường gặp

Tự động hóa để loại bỏ cảm xúc và vì thế đảm bảo kết quả? Không. Sự can thiệp hấp tấp có thể giảm bớt và tăng thêm lỗi thiết kế hoặc thực hiện.

Điểm tạm dừng

Đánh dấu cách mở rộng này như là không dùng các sản phẩm phức tạp.

Giá trị vị thế 1.000, ký quỹ 100. Lỗ 5% trên vị thế tương đương bao nhiêu trước chi phí?

1. Lỗ 5.
2. Lỗ 50, bằng 50% tiền ký quỹ.
3. Không lỗ nếu dùng bot.

> **Xem đáp án: Lỗ 50, bằng 50% tiền ký quỹ.**
> Đòn bẩy và chi phí làm kết quả trên ký quỹ khác biến động của tài sản.

Lightning và các lớp khác

Mục tiêu

Hiểu chi phí qua kênh đào và nhận ra những chức năng mà dòng Cuvex không cung cấp.

Tìm hiểu

Lightning dùng kênh và cơ chế cập nhật để thanh toán mà không ghi từng lần trao đổi lên chuỗi cơ sở. Mở, đóng kênh và một số trường hợp khôi phục có thể cần giao dịch on-chain. Tính sẵn sàng, thanh khoản vào ra và giám sát tùy thiết kế ví và dịch vụ.

Hóa đơn có thể ghi số tiền, mô tả và hạn thanh toán. Có thể dùng satoshi hoặc millisatoshi tùy ngữ cảnh, nhưng millisatoshi không có nghĩa chuỗi cơ sở có đầu ra nhỏ hơn một satoshi. Việc trả hóa đơn cần tương thích và tuyến khả dụng. Mã QR không bảo đảm mọi ứng dụng đều trả được.

Dịch vụ lưu ký và không lưu ký có mô hình rất khác nhau. Tốc độ thường nhanh không chứng minh không có rủi ro. Lightning không hoàn toàn ẩn danh vì vẫn có bên quan sát, tuyến, đối tác và siêu dữ liệu.

Trò chuyện Cuvex có thể điều phối yêu cầu tính bằng sat thanh toán trên chuỗi qua tài khoản WOW. Ấn bản này không khẳng định Desk có nút Lightning, quản lý kênh hay ký hóa đơn Lightning. Nếu có nhiều phương thức, kiểm tra phương thức bạn hiểu và phương thức ứng dụng sẽ thực sự dùng.

Thực hành

1. Nó mô tả một địa chỉ On-chain, một địa chỉ URI bitcoin: và một đường biên tập Lightning.
2. So sánh với việc trả tiền cho chuỗi và mỗi kênh để xác nhận, thanh khoản, lưu ký và phục hồi.
3. Điều này giải thích tại sao một người dùng hết hạn nên kiểm tra lại với người nhận và không hiểu lại như một địa chỉ.

Chứng minh bạn đã hiểu

Bạn có thể từ chối một phương pháp không phù hợp mà không lộ ra các khóa Hay cho rằng mình đã sai lầm. Cuvex .

Câu hỏi thường gặp

Tất cả các khoản thanh toán trong sats là Lightning? Không. satoshi biểu hiện giá trị; phương thức phụ thuộc vào giao thức đã được sử dụng.

Điểm tạm dừng

Giữ lại các phương thức tập thể dục, không có hóa đơn thực sự.

Thông tin nào đủ để biết yêu cầu được thanh toán qua Lightning?

1. Có từ sats.
2. Đến qua trò chuyện.
3. Định dạng và phương thức tương thích, không chỉ đơn vị hay kênh nhận tin.

> **Xem đáp án: Định dạng và phương thức tương thích, không chỉ đơn vị hay kênh nhận tin.**
> Đơn vị tính và mạng thanh toán là hai khía cạnh khác nhau.

Taproot, MuSig2 và tương lai hậu lượng tử

Mục tiêu

Phân biệt tiêu chuẩn, đề xuất và khả năng thực hiện.

Tìm hiểu

Taproot cho phép các điều kiện sử dụng đường khóa và văn bản. chữ ký Schnorr và sự bổ sung có thể cải thiện một số cấu trúc nhất định, nhưng kết quả của sự riêng tư phụ thuộc vào cách mà nó được kết cấu và khí đốt. Một địa chỉ là bc1p không cho thấy rằng không có người tham gia hoặc cho biết tất cả các điều kiện ẩn giấu của nó.

MuSig2 cho phép một tập bên ký thêm các khóa và tạo ra một chữ ký Schnorr tương tác với nhau. Tiêu chuẩn căn cứ là N. Một ngưỡng tự do M của N yêu cầu thêm một công trình hoặc giao thức khác. Việc quản lý ký kết và phiên điều trị là phê bình và không thực hiện bằng cách trao đổi tin nhắn một cách bình thường.

PSBT v2 tổ chức lại thông tin so với v0. Tệp chứa giao dịch phiên bản 2 không tự động được nâng cấp. Phần sụn Final trong ấn bản này vẫn dùng PSBT v0, P2WSH/sortedmulti và SIGHASH_ALL cho hồ sơ đa chữ ký. Khả năng tương lai cần đặc tả giao tiếp và xác minh riêng.

NIST xuất bản 2024 tiêu chuẩn thời gian đầu tiên. Nó không tự thay đổi chữ ký của bitcoin. Sử dụng một thuật toán theo chu kỳ để xác thực phần sụn sẽ bảo vệ lớp đó; nó sẽ không tự động chuyển đổi ECDSA hay Schnorr của UTXO thành chữ ký nhân. Cũng không có ngày tấn công tương lai mà gia sư hứa chắc chắn.

Thực hành

1. Nó xác nhận năm lời tuyên bố như tiêu chuẩn, thực hiện xác thực, đề xuất hay quảng cáo.
2. Giải thích tại sao "Nhấp nhận người nhận Taproot" không chứng minh "tin tưởng vào mục Taproot".
3. Vẽ các lớp riêng biệt: ký phần sụn, mã hóa bí mật, chat và ký ký kết sử dụng bitcoin.

Chứng minh bạn đã hiểu

Bạn có thể yêu cầu bằng chứng cụ thể của một lớp và tránh di chuyển sự bảo đảm giữa các giao thức.

Câu hỏi thường gặp

Tôi có nên chuyển tiền của mình cho một tiêu đề về tính toán lượng tử không? Một quyết định thực sự đòi hỏi bằng chứng kỹ thuật hiện tại, có thể kiểm tra, đánh giá rủi ro và một kế hoạch di cư an toàn; khóa học không chỉ ra lệnh cho các phong trào hàng đầu.

Điểm tạm dừng

Ghi lại những câu hỏi kỹ thuật mà không tạo ra một kế hoạch tiêu dùng tự động.

Nếu chữ ký hậu lượng tử được triển khai và xác minh trong bộ nạp khởi động, nó có đổi điều kiện ký của UTXO hiện có không?

1. Không, chúng thuộc các lớp khác nhau.
2. Có, chuyển toàn mạng sang thuật toán khác.
3. Không cần sao lưu nữa.

> **Xem đáp án: Không, chúng thuộc các lớp khác nhau.**
> Xác thực bản cập nhật không viết lại điều kiện chi tiêu Bitcoin.

Khả năng tương tác và sử dụng độc lập với nhà sản xuất

Mục tiêu

Lập kế hoạch liên tục nếu bạn thay đổi phần mềm, thiết bị hoặc nhà cung cấp.

Tìm hiểu

Khả năng tương tác không được chứng minh bằng danh sách các chữ số. Bạn phải bảo tồn mạng lưới, văn bản, dẫn xuất, các khóa, chính trị, định dạng giao dịch và ngữ nghĩa chữ ký. Hai ứng dụng có thể hiểu BIP174, nhưng vẫn không thừa nhận cùng một lĩnh vực, kích cỡ hoặc kiểu nhập.

Để thoát khỏi sự lệ thuộc của giao diện, chị lưu trữ thông tin phục hồi được ghi lại và tập với ví bài học. Một cụm từ ghi nhớ tiêu chuẩn có thể cho phép đạo hàm các khóa, nhưng lấy lại một đa chữ ký yêu cầu chính sách của nó. Thẻ BIP329 thêm vào bối cảnh riêng tư; lịch sử chat có một phạm vi khác.

Đừng biến một bài kiểm tra khả năng tương thích thành một bản hạt giống khôi phục thật sự. Đầu tiên kiểm tra xuất khẩu descriptor và phục hồi chỉ theo dõi. Nếu một tình huống khẩn cấp đòi hỏi phải xây dựng lại các khóa, bạn sẽ sử dụng một môi trường được thiết kế để làm điều đó và sau đó xem xét việc di cư. ví không tương thích với số 0 không chứng minh rằng quỹ đã bị mất.

Hãy lưu một bản kiểm tra tài liệu, phiên bản khóa học và các công cụ cần thiết. Chữ ký ứng dụng, chứng nhận hết hạn và thay đổi hệ thống có thể gây ảnh hưởng đến việc cài đặt. Một mã nguồn mở có thể không đảm bảo rằng bất cứ ai cũng có thể biên dịch nó nhiều năm sau đó mà không cần phải bảo vệ sự phụ thuộc và hiểu biết.

Thực hành

1. Hãy thiết kế một cuộc kiểm tra kết xuất với một tài khoản rỗng: mạng lưới, chính trị và chỉ huy trong hai tài khoản.
2. Nó cho biết những bộ phận nào là tiêu chuẩn và những bộ phận cần thiết để chuyển đổi hoặc tài liệu về định dạng Cuvex.
3. Xác định kết quả nào có thể cho thấy sự tương xứng và phần cứng đang theo dõi hay ký tên thật.

Chứng minh bạn đã hiểu

Bạn có thể mô tả một tuyến đường phục hồi mà không phụ thuộc vào việc một công ty tiếp tục cung cấp cùng một dịch vụ.

Câu hỏi thường gặp

Mã nguồn mở có nghĩa là nhà sản xuất không còn quan trọng nữa? Không. Cung cấp, bảo dưỡng, các thành phần vật lý và kinh nghiệm hoạt động vẫn còn quan trọng. Nó cho phép kiểm tra và duy trì tiềm năng, chứ không phải tự động bảo đảm.

Điểm tạm dừng

Nó lưu lại kết quả thí nghiệm với các phiên bản và giới hạn được quan sát.

Bằng chứng nào mạnh hơn về khả năng tương tác?

1. Cả hai ứng dụng đều ghi “Bitcoin”.
2. Dựng lại và kiểm tra cùng chính sách và địa chỉ trong phòng thực hành với phiên bản đã xác định.
3. Biểu tượng giống nhau.

> **Xem đáp án: Dựng lại và kiểm tra cùng chính sách và địa chỉ trong phòng thực hành với phiên bản đã xác định.**
> Bài thử phải giữ các điều kiện liên quan và cho kết quả kiểm chứng được.

Phòng thực hành kỹ thuật với regtest

Mục tiêu

Hiểu môi trường thực hành có thể tái lập và phân biệt kiểm thử trên dữ liệu giả với sử dụng thiết bị thật.

Tìm hiểu

Regtest cho phép tạo chuỗi cục bộ có kiểm soát để sinh khối và thử giao dịch không có giá trị kinh tế. Phải dùng thư mục và thông tin xác thực riêng, không nhập dữ liệu thật. Kết quả tự nó không chứng minh khả năng tương thích USB, NFC, Bluetooth hay máy ảnh của thiết bị vật lý.

Phòng thực hành đầy đủ ghi phiên bản, cấu hình mạng, chính sách, đầu vào thử, PSBT, chữ ký, giao dịch cuối và kết quả chấp nhận. Có thể kiểm tra tổng giá trị có khớp không, chữ ký bị sửa có bị từ chối không và khoản thanh toán hợp lệ có vào khối cục bộ không. Phải thử cả tình huống thất bại, không chỉ luồng thành công.

Tài liệu xác minh Desk 9.21 báo cáo các thử nghiệm với Bitcoin Core 31 regtest và các bài kiểm tra tự động cho bộ máy xử lý cùng UI mô phỏng. Ấn bản này dùng tài liệu đó làm bằng chứng chứ không tuyên bố đã thực hiện lại các thử nghiệm hay vận hành thiết bị. Kiểm tra một gói phần mềm cũng không chứng minh đã cài trên mọi hệ thống.

Trước buổi học kỹ thuật, kỹ sư cần cung cấp phòng thực hành đã thiết lập và quy trình tương thích với phiên bản của học viên. Không mở RPC ra Internet cho gia sư điều khiển. AI có thể hướng dẫn đọc kết quả giả lập nhưng không được có thông tin xác thực hoặc quyền quản trị.

Thực hành

1. Trong môi trường đã chuẩn bị, quan sát một giao dịch hợp lệ và một giao dịch có chữ ký bị sửa. Ghi lại kết quả chấp nhận hoặc từ chối.
2. Kiểm tra một tình huống tiền thừa sai và một tình huống không đúng mạng.
3. Phân biệt trong báo cáo “kiểm thử bộ máy xử lý”, “giao diện mô phỏng” và “phần cứng vật lý”.

Chứng minh bạn đã hiểu

Mô tả chính xác phần đã thử và phần còn thiếu. Không trình bày mô phỏng như chứng nhận.

Câu hỏi thường gặp

Nếu regtest chạy được, tôi có thể bán khóa học với tuyên bố đã xác minh cho mọi thiết bị chưa? Chưa. Vẫn cần thử quy trình trên thiết bị thật, cài đặt, khả năng tiếp cận, khôi phục và dịch vụ thương mại.

Điểm tạm dừng

Dừng và lưu môi trường theo hướng dẫn, chỉ giữ dữ liệu giả.

Kiểm thử bộ máy với regtest có chứng minh một điện thoại cụ thể đọc được NFC thật không?

1. Có, vì cả hai đều dùng Bitcoin.
2. Có nếu PSBT nhỏ.
3. Không, cần thử riêng trên thiết bị thật.

> **Xem đáp án: Không, cần thử riêng trên thiết bị thật.**
> Các môi trường xác minh có phạm vi khác nhau.

Dự án cuối khóa và kế hoạch duy trì liên tục

Mục tiêu

Chứng minh sự tự chủ từ chuẩn bị cho đến phục hồi và riêng tư.

Tìm hiểu

Kết quả của khóa học không phải là ghi nhớ một trình đơn: đó là khả năng giải thích mục đích, xác minh kết quả và ngăn chặn một hoạt động mà bạn không hiểu. Đánh giá kết hợp các khái niệm, thực hành và một vụ án độc lập. Nó không bao giờ phụ thuộc vào việc tiết lộ hạt giống khôi phục tài sản cá nhân cho người đánh giá.

Trường hợp A: Hãy thiết lập một môi trường học tập, xác định các mô hình và phiên bản, bảo vệ Desk, kết nối với bản mật mã, và tái tạo lại một tài khoản chỉ theo dõi. Giải thích xem bản sao lưu cần thiết gì và dữ liệu gì mà nhà cung cấp của bạn có thể quan sát.

Trường hợp B: thiết kế một khoản thanh toán với UTXOs tư liệu từ các ngữ cảnh khác nhau, biện minh cho sự lựa chọn, kiểm tra người nhận, thay đổi và phí, và ghi lại chi nhánh ký hiệu tương ứng với thiết bị của bạn. Giải quyết một cuộc đình công và một vụ xuất bản khác mà không cần thanh toán gấp đôi. Nếu không có phần cứng vật lý được chấp nhận, phần này được ghi là mô phỏng và vẫn còn chờ đợi.

Trường hợp C: Ông thiết kế một chiếc 2 3, đại diện cho giấy mời và kiểm tra, so sánh với Mirror một lĩnh vực tự do được chọn và giải thích phạm vi OK. Lấy lại chính sách học tập, giả vờ mất một người tham gia và chuẩn bị cho sự liên tục và di sản.

Việc vượt qua đề xuất đòi hỏi ít nhất 80% kiến thức và tất cả các kiểm tra chính xác: không tiết lộ bí mật, kiểm tra mạng lưới và các đầu ra, không nhầm lẫn giai đoạn và phục hồi. Một lỗi nghiêm trọng đòi hỏi phải xem xét lại và thực hành mới; không thể bù đắp bằng những câu hỏi thị trường. Một giấy chứng nhận thương mại, nếu được phát hành, phải xác định những gì đã được đánh giá, và liệu có sự quan sát vật lý hay chỉ là mô phỏng.

Thực hành

1. Hoàn thành 3 vụ với dữ liệu tổng hợp và lời giải thích riêng.
2. Giải quyết bản đánh giá cuối cùng của khớp nối và kiểm tra từng câu trả lời sai.
3. Chỉ gửi một tờ kết quả mà không có bí mật, với bằng chứng rõ ràng và chưa được giải quyết.

Chứng minh bạn đã hiểu

Bạn có thể tự mình dừng lại khi một chiến dịch thiếu bằng chứng và bạn biết cần phải làm gì để tiếp tục.

Câu hỏi thường gặp

Kết thúc trang web có nghĩa là chúng ta sẵn sàng để bảo vệ bất kỳ quan trọng nào? Không. Khả năng đó phải được thử nghiệm và rủi ro sẽ được cân nhắc tùy theo hoàn cảnh của bạn. Đọc sách và thử nghiệm không đảm bảo kết quả trong tương lai.

Điểm tạm dừng

Hãy giữ kế hoạch kiểm tra và thực tập của anh. Bạn có thể quay lại chương cần thiết mà không cần lặp lại toàn bộ khóa học.

Yêu cầu quan trọng nào để hoàn thành đào tạo thực hành?

1. Đã mở tất cả các trang.
2. Chứng minh khả năng khôi phục và rà soát giao dịch trong phạm vi được ghi nhận mà không lộ bí mật.
3. Dự đoán giá tháng sau.

> **Xem đáp án: Chứng minh khả năng khôi phục và rà soát giao dịch trong phạm vi được ghi nhận mà không lộ bí mật.**
> Kết quả học tập thể hiện qua khả năng và giới hạn đã kiểm chứng, không phải lượt xem hay dự đoán.

Sổ tay học viên

Sổ tay vận hành Cuvex

Sổ tay đi cùng các bài học. Mỗi quy trình mô tả luồng trong mã nguồn đã rà soát, các bước kiểm tra và điểm dừng. Đây là ấn bản đề xuất cho giai đoạn thí điểm, không xác nhận nhóm biên soạn đã tự thử trên Original, BIT, điện thoại hay từng nền tảng máy tính. Trước khi dạy với tiền thật, nhóm phải hoàn tất ma trận nghiệm thu và sửa các nhãn hoặc màn hình không khớp.

Phiên bản tham chiếu: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 và Mirror 1.0.0-beta.12.12. Chọn hồ sơ trong Desk chỉ thể hiện tương thích công bố, không đo phần sụn từ xa. Ảnh màn hình Mirror trong sổ tay được chụp từ trình giả lập Android của gói 12.12. Ảnh sản phẩm là tư liệu doanh nghiệp, không chứng minh phiên bản hiển thị trên thiết bị hiện tại.

P01 | Kiểm tra nguồn gốc và phiên bản | Cuvex | L16,L21 | C01,C02

Chuẩn bị chứng từ mua và kênh chính thức có thể xác minh độc lập. Chưa nhập bất kỳ bí mật nào.

1. Kiểm tra bao bì và niêm phong. Nếu có dấu hiệu can thiệp, dừng khởi tạo và giữ bằng chứng không nhạy cảm.
2. Dùng quy trình kiểm tra tính nguyên vẹn và niêm phong trong ứng dụng tương thích với lô hàng. Chỉ nhập mã ở đó, không đưa cho gia sư.
3. Xác định Original hay BIT và bản sửa đổi hiện có. Kiểm tra phiên bản hiển thị trên thiết bị và các ứng dụng.
4. Đối chiếu ma trận do nhóm công bố. Danh mục hay giá trị băm không thay thế xác thực phần sụn hoặc nghiệm thu thiết bị thật.

Kết quả: đã xác định mẫu, phiên bản và kiểm tra nguồn gốc mà không lộ bí mật. Nếu mã không hợp lệ hoặc giao diện khác, không ép dùng theo hướng dẫn cũ.

Dừng trước khi nạp dữ liệu lưu ký. Khả năng truy xuất nguồn gốc thương mại không tự bảo đảm không có can thiệp tinh vi.

P02 | Cập nhật Original qua Bluetooth | Original | L46 | C01,C02,C03

Chuẩn bị bản sao có thể khôi phục, nguồn điện ổn định, gói chính thức tương thích và quy trình đã nghiệm thu cho hệ thống của bạn. Khóa học chưa xác nhận toàn bộ quy trình thực tế trên mọi nền tảng.

1. Trong mục thiết bị hoặc phần sụn của ứng dụng, chọn Original và bản tải chính thức hoặc tệp cục bộ xác thực tương ứng.
2. Đưa thiết bị vào chế độ cập nhật theo menu rồi kết nối theo quy trình ứng dụng. Để thiết bị gần và tránh phiên kết nối cạnh tranh.
3. Nhập mã hiển thị trên Original vào ô chỉ định. Không nhầm mã này với mật khẩu bản mật mã.
4. Theo dõi truyền, xác minh, cài đặt và khởi động lại. Tỷ lệ phần trăm không chứng minh đã cài xong.
5. Kiểm tra phiên bản cuối trên Original và ghi vào ứng dụng nếu có trường tương ứng.

Kết quả: xác minh phiên bản trên màn hình sau khởi động lại và xác nhận quy trình hoàn tất. Nếu lỗi trước PIN, trong khi truyền gói hoặc ở cuối, hãy ghi giai đoạn và mã. Đừng ngắt kết nối hay tùy tiện đổi phần mềm để “vượt 99%”.

P03 | Cập nhật BIT qua USB | BIT | L46 | C01,C02,C03

Xác định phương tiện lưu trữ thực của BIT, nguồn điện và gói chính thức tương thích. Giữ bản sao trước khi đổi phần mềm.

1. Chọn BIT trong quy trình cập nhật phần sụn tương thích của Desk hoặc Mirror.
2. Kết nối bằng cáp và bộ chuyển đổi truyền dữ liệu phù hợp. Cho phép truy cập ổ đĩa hoặc thư mục khi ứng dụng yêu cầu.
3. Chọn phần sụn xác thực đúng mẫu, rồi kiểm tra phiên bản và dữ liệu tương thích trước khi gửi.
4. Chờ các giai đoạn truyền và xác minh của thiết bị. Ổ đĩa có thể biến mất hoặc được gắn lại theo giao thức.
5. Sau khi khởi động lại, kiểm tra phiên bản trên BIT và kết quả cuối trong ứng dụng.

Kết quả: đã xác minh cài đặt trên chính thiết bị. Nếu ổ không xuất hiện, kiểm tra chế độ thiết bị, cáp dữ liệu, quyền, trạng thái gắn ổ và phiên khác đang hoạt động. Không tạo thư mục trùng tên trên máy tính để thay thế. Khôi phục sau cập nhật lỗi cần quy trình chính thức của phần cứng này.

P04 | Tạo ví bằng đồng xu và xúc xắc | Cuvex | L17 | C01

Chuẩn bị nơi riêng tư, xúc xắc phù hợp và đồng xu, không có máy ảnh hay micrô gia sư đang bật. Dùng ví thực hành.

1. Mở chức năng tạo ví và quy trình entropy của phần sụn. Ấn định thứ tự bốn viên xúc xắc trước khi gieo.
2. Nhập kết quả đồng xu và từng viên theo màn hình, không thay kết quả theo ý thích.
3. Mã nguồn đã rà soát tính chỉ số = giá trị đồng xu × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Chỉ nhận chỉ số từ 0 đến 2.047.
4. Nếu bị từ chối, tung lại đồng xu và gieo lại tất cả xúc xắc. Thông báo giữ các từ trước đó và yêu cầu làm lại cả bộ.
5. Hoàn tất thuật toán của thiết bị, kể cả xác minh cuối. Bảo vệ cụm từ ghi nhớ và kiểm tra khôi phục ở nơi riêng tư.

Kết quả: ví được tạo qua toàn bộ quy trình, không phải từ tự chọn. Nếu màn hình khác mã nguồn, hãy dừng. Không dùng ví dụ công khai về kết quả xúc xắc, hạt giống hay khóa làm dữ liệu riêng.

P05 | Mã hóa bí mật | Cuvex | L18,L19 | C01

Chuẩn bị: chọn mẫu, định dạng nội dung và cách bảo vệ. Việc nhập trên máy tính hay điện thoại làm lộ nội dung ở nguồn dù đích đến được mã hóa.

1. Chọn mã hóa và loại BIP39, SLIP39, Monero hoặc văn bản tương thích. Không dùng lẫn từ điển. Bàn phím văn bản thuần đã rà soát nhận tối đa 500 ký tự. Lưu được định dạng khác không có nghĩa ký được trên mạng tương ứng.
2. Nhập trực tiếp trên thiết bị để giữ cách ly, rồi kiểm tra thứ tự, ký tự và các trường phụ trên chính màn hình đó.
3. Chọn bảo vệ cá nhân hoặc chia sẻ theo quy trình, và sinh trắc học trên BIT nếu phù hợp. Phân biệt ngưỡng này với ngưỡng chi Bitcoin.
4. Nhập và xác nhận mật khẩu ở nơi riêng tư theo bộ kiểm tra của phần sụn. Không tự động áp dụng quy tắc của Desk.
5. Với Original, ghi vào thẻ trống tương thích. Với BIT, giữ các đối tượng xuất qua quy trình USB. Chờ xác nhận.
6. Thực hiện thử khôi phục để kiểm tra nội dung, rồi đóng phần hiển thị bí mật khi xong.

Kết quả: bản mật mã đã thử khôi phục. Nếu đọc hoặc ghi lỗi, bảo vệ bản gốc và làm theo chỉ dẫn thử lại. Không xóa phần đầu hay ép ghi đè.

P06 | Giải mã trên thiết bị | Cuvex | L18 | C01,C02

Chuẩn bị nơi riêng tư và đủ yếu tố mở khóa. Tắt micrô và chức năng ghi màn hình ở gần bí mật.

1. Mở chức năng giải mã trên đúng mẫu. Cung cấp bản mật mã qua NFC với Original hoặc theo quy trình USB của BIT.
2. Kiểm tra bí danh và thông tin định danh đối tượng trước khi nhập thông tin xác thực.
3. Cung cấp các mật khẩu cần thiết và yếu tố sinh trắc học khi định dạng yêu cầu. Không liên tục thử sau lỗi vì có kiểm soát truy cập và khóa.
4. Chỉ kiểm tra nội dung trên màn hình quy định. Mã QR chứa bí mật nhạy cảm như chính văn bản đó.
5. Đóng hoặc kết thúc theo thiết bị, rồi giữ phương tiện và thông tin xác thực riêng theo kế hoạch.

Kết quả: khôi phục nội dung riêng tư và kết thúc phiên. Nếu không nhận dạng định dạng, xác thực lỗi hoặc nội dung bất ngờ, đừng “sửa” bằng ứng dụng lạ. Báo phiên bản, định dạng và lỗi cho hỗ trợ, không gửi bí mật.

P07 | Chuẩn bị khôi phục bản mật mã bảo vệ bằng sinh trắc học | BIT | L19,L47 | C01,C02

Chuẩn bị: bản mật mã học tập và tài liệu về định dạng của bạn. Đừng định nghĩa việc lấy lại bản sao của nó.

1. Trong hồ sơ của Desk, nó xác định mục sinh trắc học và mục xuất khẩu nào có sẵn.
2. Nó lưu lại những tập tin mà dòng chảy liên kết và bản sao độc lập, với bộ nhận diện bí mật.
3. Thử mở khóa thông thường BIT Và ghi lại những gì mật khẩu Điều kiện và điều kiện cần thiết.
4. Nó nghiên cứu về phương pháp phục hồi độc đáo của địa phương và các định dạng của nó. Hãy kiểm tra xem vật liệu cần thiết có tồn tại trước khi cần thiết.
5. Trình bày với dữ liệu không có quỹ ... tình huống thiết bị bị bị hỏng hoặc vân tay không sẵn sàng.

Kết quả: Một kế hoạch đã được thử nghiệm, với giới hạn của nó, cho định dạng cụ thể. Người ta không cho rằng bất cứ sinh trắc học nào cũng có thể bị loại trừ hoặc một dấu vân tay thay thế cho bản sao. Nếu bạn lấy lại được một bí mật trong một chiếc PC, bạn sẽ đánh giá cuộc triển lãm và nhu cầu di cư sau đó.

P08 | Tạo và kiểm tra bản sao của bản mật mã | Cuvex và Desk | L20 | C01,C02

Chuẩn bị: Một bản sao gốc được xác định và một số phận phù hợp mà không cần dữ liệu để bảo tồn.

1. Đối với Original, nó sử dụng bản sao của thiết bị hoặc chức năng tương thích Desk, và nó có nguồn gốc và đích theo thứ tự đã định.
2. Giữ thẻ ổn định và tôn trọng sự từ chối của máy trợ giúp đã chứa bản mật mã.
3. Đối với BIT hay tập tin, xuất ra tập hợp các thành phần của dòng chảy và giữ lại tên hoặc mối quan hệ cần thiết.
4. Bản gốc được riêng biệt và có khả năng đọc và hồi phục từ bản mới.
5. Nó lưu lại ngày tháng, định dạng và kết quả; nó lưu trữ các bản sao với các rủi ro vật lý độc lập.

Kết quả: Một bản sao thứ hai đã được thử nghiệm. Nó không có nghĩa là một ví khác biệt, sự bãi bỏ mật khẩu và cũng không bảo vệ trước một chiếc hạt giống khôi phục đã bị rò rỉ. Nếu số phận thất bại, hãy giữ nguyên bản gốc mà không cố gắng sửa đổi nó để phù hợp với cả hai.

P09 | Tạo kho Desk, mở khóa và đổi mật khẩu | Desk | L21,L40 | C02

Chuẩn bị: Cài đặt kiểm tra, kiến trúc thích hợp và kế hoạch bản sao lưu từ nhà kho.

1. Tạo ra kho lưu trữ có mật khẩu riêng từ 12 đến 1.024 ký tự và xác nhận khớp.
2. Khóa cửa lại và mở lại để kiểm tra xem anh có thể tiếp cận được không. mật khẩu chỉ được giới thiệu vào Desk.
3. Trong Bảo mật và Truy cập và khóa, kiểm tra cài đặt khi không hoạt động và khi chuyển xuống nền. Không bật xóa tùy chọn khi trình diễn.
4. Để thay đổi mật khẩu, bạn cung cấp một sản phẩm hiện tại và xác nhận dòng chảy mới.
5. Nếu anh dùng sinh trắc học của PC Anh nên thiết lập lại theo chỉ dẫn. Tạo bản sao hiện có và bảo tồn mối quan hệ với các bản sao trước.

Kết quả: Đã kiểm tra. Bản sao trước đó lưu giữ bản mật khẩu và mã hóa gốc. sinh trắc học của PC Và sinh trắc học của BIT Chúng là những cơ chế khác nhau. Nếu truy cập không thành công, hãy dừng lại và kiểm tra lại mà không yêu cầu gia sư giữ thẻ tín dụng.

P10 | Liên kết và kiểm tra bản mật mã trong Desk | Desk | L22 | C02

Chuẩn bị bản mật mã thử có nguồn gốc rõ ràng và phương tiện truyền khả dụng.

1. Mở mục bản mật mã hoặc thẻ rồi chọn liên kết bằng NFC, USB hoặc bản sao tương thích.
2. Chọn thiết kế và nguồn. Với NFC, dùng Cuvex Mirror đã ghép nối với máy tính qua Bluetooth. Cách khác là dùng ổ đĩa Cuvex BIT kết nối qua USB-C. Cuvex Desktop không hỗ trợ đầu đọc NFC ngoài kết nối qua USB.
3. Kiểm tra bí danh, nguồn gốc, kích thước, định dạng và các điều kiện đã diễn giải trên thẻ thông tin. Đây là siêu dữ liệu, không phải nội dung đã giải mã.
4. Kiểm tra có tài khoản đã giữ nào đang chờ liên kết không và chỉ liên kết tài khoản đã xác minh.
5. Nếu mức dự phòng chưa đủ, xuất bản sao rồi thử khôi phục riêng.

Kết quả: đối tượng được quản lý cục bộ. “Đã liên kết” không chứng minh tính xác thực của hạt giống hay số dư. Với đối tượng không nhận dạng, kiểm tra định dạng và phiên bản, không đổi đuôi hoặc xóa dữ liệu để buộc ứng dụng chấp nhận.

P11 | Kích hoạt tài khoản WOW chỉ theo dõi | Desk và Cuvex | L13,L22 | C01,C02

Chuẩn bị: Thông tin công khai bị thu hút từ dòng điện của thiết bị và điều khiển riêng từ nguồn của nó.

1. Mở WOW hoặc thêm tài khoản từ bản mật mã.
2. Nhập vào descriptor hay tài liệu công cộng được hỗ trợ bởi tập tin, webcam hay Mirror theo chức năng.
3. Kiểm tra mạng lưới, văn bản, nguồn gốc, vân tay, đường dẫn và tổng kiểm tra khi phù hợp. Đừng nhập hạt giống khôi phục hay xprv.
4. Hãy ghi tên vào tài khoản và chọn một nguồn tham khảo với sự đồng ý.
5. Hãy kiểm tra một địa chỉ kiểm soát và phạm vi khám phá trước khi giải mã nó.

Kết quả: ví chỉ theo dõi đã được liên kết. Nếu thấy số không, hãy kiểm tra mạng, cụm mật khẩu ban đầu, dẫn xuất, tài khoản, nhà cung cấp và quá trình quét, đừng kết luận tiền đã biến mất. Giao diện chung có thể hỗ trợ mạng mà hồ sơ đa chữ ký không hỗ trợ. Phải xét đúng ngữ cảnh.

P12 | Cấu hình nút và đồng bộ | Desk | L25,L33 | C02

Chuẩn bị: xác định nhu cầu riêng tư. Nếu dùng Core, cần truy cập được nút đã bảo vệ và đồng bộ.

1. Trong mục Bảo mật, Quyền riêng tư và nút, chọn tài khoản WOW và kiểm tra nhà cung cấp.
2. Chủ động chọn nhà cung cấp công cộng tương thích hoặc Core. Với Core, chỉ nhập điểm cuối, ví và thông tin xác thực trong ứng dụng.
3. Cho phép truy vấn sau khi hiểu mỗi dịch vụ sẽ nhận gì. TLS không che truy vấn khỏi nhà cung cấp.
4. Đồng bộ rồi kiểm tra ngày, đỉnh chuỗi, tiến độ và trạng thái hoàn tất. Khi quét lại, so thời gian lịch sử được bao phủ và việc quét có còn tiếp tục không.
5. Gặp 429 thì chờ theo yêu cầu. Khi lỗi, không mặc định nút khác đã được kích hoạt vì cấu hình không âm thầm chuyển nút.

Kết quả: đã biết nguồn và trạng thái. Không mở RPC ra Internet, chia sẻ mật khẩu hay chỉ dò địa chỉ có số dư. Lịch sử trống có thể là kết quả chưa đầy đủ.

P13 | Tạo và tìm lại yêu cầu nhận tiền | Desk và Cuvex | L26 | C01,C02

Chuẩn bị: Tài khoản, mạng lưới và chính sách đã được kiểm tra.

1. Bạn nhận được và tạo ra hoặc nhận được yêu cầu thích hợp.
2. Thêm người quan sát, động lực và quan tâm chỉ khi nào bạn cần đến siêu dữ liệu địa phương.
3. Kiểm tra địa chỉ của thiết bị tương thích trước khi tính tiền. Nếu không được chấp nhận về thể chất, hãy ngừng thực hành trong Trình Mô Phỏng.
4. Chỉ chia sẻ những thông tin cần thiết qua kênh nhận tín hiệu.
5. Kiểm tra nhập cảnh, nhập khẩu và mua sắm số xác nhận tại nguồn cung cấp thông tin của anh.

Kết quả: Tôi không chỉ có những yêu cầu được công bố. Trong đa chữ ký địa chỉ được hiển thị để trả nợ muộn và không được cài đặt lại. Nếu giới hạn của địa chỉ mới chưa có lịch sử mới được thực hiện, nó sẽ lấy lại những yêu cầu trước đó; không cần phải đăng ký bằng tay.

P14 | Gắn nhãn, đóng băng và BIP329 | Desk | L27 | C02,B13

Chuẩn bị: Tài khoản phòng thí nghiệm UTXOs và mật khẩu cho việc xuất khẩu được bảo vệ.

1. Đánh dấu một mục nhập với hoàn cảnh của bạn mà không cần dữ liệu cá nhân.
2. Đóng băng nó hoặc là vô hiệu hóa nó một cách vô thức và kiểm tra lượng dư có thể sử dụng. Giới hạn là ở địa phương.
3. Nó mở rộng các thẻ qua hàm bảo vệ. Phân loại BIP329 theo định dạng mã hóa của tập tin.
4. Nó có trong một bản sao tương thích; kiểm tra khớp của các tham chiếu, nhãn và đông lạnh.
5. Nó giữ một chiếc siêu dữ liệu bản sao lưu, cùng với chiếc mật khẩu, theo kế hoạch của anh.

Kết quả: Hoàn cảnh được bảo tồn và chọn lọc được hiểu rõ. Nhập khẩu không nên được dùng để tự động kích hoạt đồng tiền đông lạnh mà không cần điều chỉnh. Đừng gửi tập tin thẻ cho gia sư: nó có thể tiết lộ phần bổ sung và mối quan hệ, mặc dù nó không bao gồm các khóa chi tiêu.

P15 | Chuẩn bị thanh toán và gửi toàn bộ số dư | Desk | L28 | C02

Chuẩn bị: Yêu cầu được kiểm tra và có đủ các đầu vào tiêu dùng.

1. Mở từ WOW, UTXOs hay chat và xác nhận tài khoản và mạng lưới.
2. Chọn các đầu vào , người nhận Và quan trọng hơn, và kiểm tra lại các bối cảnh liên quan.
3. Chọn giá và kiểm tra phí, thay đổi và cảnh báo. Nếu có, hãy kiểm tra các phương án thay thế mà không cần nhận phí ẩn.
4. Để hoàn thành việc kiểm tra kết quả sau phí. Trên mạng, họ xác nhận rõ ràng một phần tiền lương nếu không thanh toán hóa đơn.
5. Chuẩn bị bản nháp và kiểm tra tất cả các dữ liệu trước khi xuất khẩu.

Kết quả: Mục đích dễ hiểu và PSBT của chiến dịch đó. Một mẫu đơn tổng quát có thể chấp nhận nhiều hơn các đầu vào hay người nhận so với phần cứng áp dụng giới hạn hiệu quả của bên ký và vận chuyển. Nếu bạn thay đổi các đầu ra hay điều kiện, một cuộc kiểm tra mới sẽ bắt đầu.

P16 | Ký và chuyển trả PSBT bằng Original | Original và Mirror | L29 | C01,C02,C03

Chuẩn bị bản nháp đúng, thẻ truyền tương thích, bản mật mã tương thích đã xác thực và phương tiện mở khóa riêng tư. Bản cũ chưa xác thực có thể phải được khôi phục, kiểm tra và tạo lại trước khi ký. Không sửa phần đầu để vượt kiểm tra.

1. Xuất yêu cầu bằng quy trình NFC tương thích từ Desk/Mirror.
2. Chuyển yêu cầu đến Original, cung cấp bản mật mã khi được nhắc và mở khóa mà không đọc thông tin xác thực.
3. Kiểm tra mạng, tóm tắt, toàn bộ đầu ra, phí, tiền thừa và các cảnh báo bắt buộc.
4. Với đa chữ ký Final, chọn có xem tham số mở rộng hay không. Chỉ thực hiện ba xác nhận cuối nếu mọi mục đều khớp.
5. Chờ ghi phản hồi lên thẻ và đọc lại từ thẻ.
6. Đọc phản hồi bằng Cuvex Mirror và xác minh trong thao tác tương ứng của Desk.

Kết quả: đã nhận chữ ký gắn với bản nháp, chưa phải phát giao dịch. Nếu ghi lỗi, giữ trạng thái và làm theo quy trình thử lại. Không dùng thẻ sao lưu làm phương tiện thanh toán có thể hy sinh.

P17 | Ký, nhận và xác nhận đã nhận với BIT | BIT và Desk | L29 | C01,C02

Chuẩn bị bản nháp đúng, bản mật mã tương thích đã xác thực và chọn ổ đĩa BIT thật. Nếu bản cũ bị từ chối ký, thực hiện khôi phục và làm mới theo hướng dẫn, không ép định dạng.

1. Chuyển yêu cầu qua USB-C bằng dịch vụ Desk rồi làm theo màn hình thiết bị để cung cấp bản mật mã.
2. Mở khóa ở nơi riêng tư và kiểm tra tóm tắt, toàn bộ đầu ra, phí cùng cảnh báo.
3. Với đa chữ ký Final, có thể xem chi tiết mở rộng. Phải thực hiện các xác nhận cuối bắt buộc để phê duyệt.
4. Trong Desk dùng “Nhận từ BIT” để nhập và xác minh phản hồi của đúng tác vụ.
5. Kiểm tra việc lưu và xác nhận đã nhận. Nếu xác nhận lỗi sau khi đã nhận, thử lại đúng thao tác đó, không chọn một thao tác mới theo mẫu.

Kết quả: chữ ký được xác minh và trạng thái trao đổi nhất quán. Nếu ngắt trước khi nhận hoặc sau khi lưu, giữ hồ sơ yêu cầu. Không chuyển sang phần sụn khác trong danh mục chỉ để khớp phản hồi đang chờ.

P18 | Hoàn tất, phát và theo dõi giao dịch | Desk | L30,L44 | C02

Chuẩn bị: chữ ký kiểm tra và ngưỡng đủ khi phù hợp.

1. Kiểm tra lại lần nữa, các đầu vào, các đầu ra, phí và mạng lưới.
2. Nó kết thúc bằng hành động tương ứng và chứng minh rằng không thiếu chữ ký hay điều kiện.
3. Nó cho phép phát sóng và duy trì kết quả địa phương. Nếu bạn mất phản ứng mạng, hãy tham khảo lại trước khi lặp lại.
4. Tiếp theo là mempool và số xác nhận trong nhà cung cấp đã chọn với ngày tháng đồng bộ.
5. Nếu có ai hỏi RBF Kiểm tra lại chiến dịch mới và lấy cho tôi cái đó. chữ ký Cần thiết. Đừng giả vờ như là có một hàm CPFP tích hợp.

Kết quả: Đã kiểm tra nguồn. Hủy một bản nháp không hủy bỏ chữ ký đã xuất khẩu và không ghi lại các khoản thanh toán được xác nhận. Một tin nhắn từ phòng chat hay một cuộc bắt giữ không thay thế được việc theo dõi.

P19 | Tự chọn so sánh hai mã QR của chính sách | Mirror | L43 | C03,C02

Chuẩn bị: hiển thị trường trên Desk và Cuvex. Khi thực hành chỉ dùng mẫu giả trong khóa học.

1. Mở “So sánh chính sách” và đọc bên nào trước cũng được.
2. Chọn dữ liệu cần kiểm tra. Có thể bắt đầu ở bước 15 và bỏ qua những mục đã rà soát bằng tay.
3. Đọc mục tương ứng bên kia và rà soát cả hai văn bản đầy đủ. Nếu bước không rõ, dùng “Chỉ định bước Desk” và hiểu đây là ngữ cảnh do người dùng nhập.
4. Chỉ diễn giải “Khớp” hoặc “Không khớp” cho đúng cặp ký tự này. Khoảng trắng, chữ hoa thường và mã hóa đều có ý nghĩa.
5. Bắt đầu cặp khác theo thứ tự tùy chọn. Thoát hoặc chuyển xuống nền để kết thúc theo hành vi xóa dữ liệu đã rà soát.

Kết quả: chỉ xác nhận phép so cục bộ tại thời điểm đó, không xác thực nguồn, phiên, phê duyệt chung hay kích hoạt. Làm rõ khác biệt từ hai nguồn, không chuẩn hóa văn bản để ép kết quả OK.

P20 | Kích hoạt, khôi phục và chuyển trò chuyện | Desk và Cuvex | L36,L39 | C02

Chuẩn bị: Môi trường DEV hoặc sản xuất, một bí danh khóa Chat trong thiết bị, không bao giờ trong khóa học.

1. Mở hoặc lấy lại lời thoại từ bối cảnh của bản mật mã.
2. Chọn bí danh mới hoặc di chuyển và hồ sơ di động phù hợp với hồ sơ của app.
3. Nhập hoặc đọc khóa Chat riêng biệt trong dòng chảy cá nhân. Đừng dùng hạt giống khôi phục, PIN, và khóa WOW.
4. Hãy kiểm tra hoạt động với dịch vụ; nếu bạn đang chờ đợi, bạn có sử dụng hành động hoàn thành hay kiểm tra, mà không cho đúng cách.
5. Kiểm tra liên lạc sau khi di chuyển và tránh sử dụng cùng một biệt hiệu trong nhiều nhóm.

Kết quả: Danh tính được kích hoạt hoặc phục hồi trong môi trường thích hợp. Lịch sử và phiên họp trước đó không tự động phục hồi với khóa Chat hay với bản sao toàn cầu Desk. Giữ các giới hạn của tài liệu sẵn có.

P21 | Xác minh danh tính liên hệ | Desk | L36,L48 | C02

Chuẩn bị: Đã thỏa thuận với người đó.

1. Thêm bí danh vào và tham khảo danh tính công khai của anh ta thông qua app.
2. So sánh dấu vân tay trên kênh xác thực, không chỉ trong cuộc trò chuyện vừa được tạo ra.
3. Nếu bạn sử dụng sự công nhận, hãy tránh thông tin công cộng hoặc những bí mật được sử dụng lại ở các dịch vụ khác.
4. Chỉ xác nhận sau khi giải quyết các mối bất hòa. Thay đổi danh tính, thanh toán và phối hợp cho đến khi kiểm tra.
5. Tài liệu này cung cấp phương pháp kiểm tra mà không lưu lại những phản ứng nhạy cảm trong khóa học.

Kết quả: Sự tin tưởng ngữ cảnh vào liên lạc, không phải đảm bảo tất cả yêu cầu của bạn trong tương lai. Giọng nói có thể bị bắt chước và một nhóm hợp pháp đã bị tổn thương. Mỗi chiến dịch đều có một sự kiểm tra.

P22 | Xin địa chỉ, yêu cầu thanh toán và trả tiền qua trò chuyện | Desk và Cuvex | L37 | C02,C01

Chuẩn bị: Liên lạc và tính WOW tương thích.

1. Hãy chọn xin địa chỉ, trả lời theo địa chỉ hoặc yêu cầu trả tiền tùy ý.
2. Kiểm tra các yêu cầu ban đầu, mạng lưới, quan trọng và ghi chú trước khi gửi.
3. Để trả nợ, hãy mở tài khoản sẵn sàng, chọn UTXOs và kiểm tra giá trị của nó.
4. Cô ta được cấp cho Cuvex thông qua thủ tục mô hình. Chat không tự động ký.
5. Hãy tiếp tục xuất bản và xác nhận nguồn tin của bạn; bạn có thể trả phần nào với yêu cầu ban đầu.

Kết quả: Hệ thống điều khiển duy trì bản kiểm tra lưu ký. Trạng thái giao dịch và thông điệp không giống nhau. Một liên kết đến duyệt web có thể gửi thông tin tới một người thứ ba: kiểm tra xem người đó có dùng nó trước khi mở hay không.

P23 | Chia sẻ và liên kết bản mật mã đã nhận | Desk | L38 | C02

Chuẩn bị: Cần phải chia sẻ, liên lạc và định nghĩa phương tiện tiếp cận mà bạn sẽ nhận được.

1. Hãy chọn chia sẻ bản mật mã từ hành động chat và kiểm tra đối tượng.
2. Đừng đăng ký mật khẩu, hạt giống khôi phục hay khóa Chat để bình luận.
3. Người nhận xác nhận nguồn và liên kết vật thể phù hợp với nhau qua hành động tiếp nhận.
4. Hãy xem bạn có được khả năng nào ngay bây giờ và bạn sẽ nhận được gì nếu bạn có đủ giấy phép để mở khóa.
5. Nó giữ một kế hoạch bãi bỏ thực tế: xóa thông điệp không rút lại bản sao bên ngoài hay các khóa được biết đến.

Kết quả: Chuyển sang mục tiêu mã hóa. Nó không phải là một khoản thanh toán, cũng không phải là chỉ đưa khóa vào một đa chữ ký. Nếu phụ tá yêu cầu đến một trang không rõ cho giải mã, thì dừng dòng chảy lại.

P24 | Sao lưu toàn bộ và khôi phục Desk | Desk | L15,L21 | C02

Chuẩn bị kho dữ liệu luyện tập và nơi lưu bản sao mà bạn kiểm soát.

1. Mở chức năng sao lưu kho, đặt mật khẩu theo chỉ dẫn và ghi rõ mật khẩu ứng với bản sao cụ thể này.
2. Lưu bản sao ngoài thiết bị duy nhất đang dùng và kiểm tra nguồn gốc, tính toàn vẹn theo quy trình.

3. Khôi phục trong môi trường thử riêng, kiểm tra tài khoản, cấu hình và dữ liệu thuộc phạm vi.
4. Rà soát mục loại trừ. Không mặc định có dữ liệu trò chuyện, phiên và lịch sử. Chính sách đa chữ ký và khóa riêng không thay được nhau.
5. Sao lưu lại sau thay đổi quan trọng và giữ hướng dẫn khôi phục.

Kết quả: đã biết phạm vi và mật khẩu bản sao. Bản cũ vẫn dùng mật khẩu cũ. Khi đổi thông tin truy cập hoặc có lộ lọt, cũng phải đánh giá các bản sao đó, không chỉ sửa kho hiện tại.

P25 | Tạo và chấp nhận ví đa chữ ký | Desk và Cuvex | L41,L42 | C01,C02

Chuẩn bị người tham gia độc lập, liên hệ đã xác minh, mạng và giới hạn thực tế đã thống nhất.

1. Người tạo chọn tên, M/N, mạng, người tham gia và thời hạn hiệu lực vận hành.
2. Cung cấp đúng khóa công khai mở rộng cùng dấu vân tay và đường dẫn BIP48 qua quy trình tương thích.
3. Mỗi bên rà soát, chấp nhận hoặc từ chối và cung cấp dữ liệu công khai của mình. Không bao giờ chia sẻ hạt giống.
4. Lập chính sách đầy đủ và chuẩn bị xác minh trên từng thiết bị.
5. Giữ các bản sao chính sách trước khi nạp tiền. Kiểm tra địa chỉ đối chiếu và khả năng khôi phục.

Kết quả: đề xuất đầy đủ, kiểm chứng được. Nhận lời mời không thay việc kiểm tra trên thiết bị. Nếu dùng Original, áp dụng tối đa sáu khóa và giới hạn dung lượng NFC. BIT không tăng khả năng của các bên còn lại.

P26 | Xác minh chính sách và nhận xác nhận | Desk và Cuvex | L43 | C01,C02,C03

Chuẩn bị: mọi người có cùng chính sách đầy đủ, đúng hồ sơ phần sụn và không có thao tác cạnh tranh trên thiết bị.

1. Bắt đầu xác minh chính sách trong ngữ cảnh tương thích. Với Original phải chọn rõ hồ sơ đã cài. BIT thương lượng khả năng theo đặc tả giao tiếp.
2. Chuyển yêu cầu qua NFC/Mirror hoặc USB-C tùy mẫu thiết bị.
3. Rà soát các trường chính sách trên thiết bị. Có thể dùng Mirror để so những cặp đã chọn theo thứ tự tùy ý.
4. Hoàn tất xác nhận trên thiết bị rồi chuyển phản hồi về bằng phương thức tương ứng.
5. Trong Desk, xác minh phản hồi gắn với yêu cầu. Dấu OK trên công cụ so sánh không thay bước này.

Kết quả: việc rà soát gắn với yêu cầu và chỉ có giá trị cho lần này. Danh mục không chứng thực phần sụn từ xa và thiết bị không được coi là kho lưu chính sách lâu dài. Khi thấy FIRMWARE_CAPABILITY_REQUIRED, trước tiên kiểm tra phiên bản Desk và cặp mẫu/bản dựng.

P27 | Yêu cầu, nhận chữ ký và chuyển giao điều phối | Desk và Cuvex | L44 | C01,C02

Chuẩn bị: Xác nhận chính sách, chiến dịch được xác nhận và người nhận đã thỏa thuận.

1. Chuẩn bị các đầu vào, các đầu ra, phí và yêu cầu chữ ký người tham gia tương thích.
2. Mỗi người tham gia sẽ kiểm tra và ký vào nhóm của họ để xem họ có thể di chuyển được gì.
3. Nhận, ký và lưu mỗi chữ ký, giải quyết các cáo buộc chưa được công bố mà không thay đổi hồ sơ lưu trữ.
4. Nếu có thể xâm nhập vào hệ thống, bộ nhận tín hiệu sẽ chấp nhận dòng chảy và kiểm tra trạng thái. Nó không thay đổi vì lý do đó M/N hay tài sản của các khóa.
5. Khi đến ngưỡng cửa, hãy kiểm tra và kết thúc trước khi xuất bản. Tiếp tục giao dịch trên mạng.

Kết quả: Hợp tác với những bằng chứng khác nhau. Báo cáo tiến triển của điều phối viên không phải là kiểm tra địa phương của anh. Hủy bỏ hoặc từ chối trong một hợp đồng, không nhất thiết phải phá hủy chữ ký đã được bảo quản bởi người thứ ba.

P28 | Xuất, khôi phục và xóa ví đa chữ ký cục bộ | Desk | L45 | C02

Chuẩn bị: Chính sách được biết đến và sao chép với mật khẩu độc nhất.

1. Nó được lưu giữ bởi Desk. Dòng chảy hiện tại sử dụng một thùng chứa CVXMSBK1 xác thực để xuất khẩu.
2. Giữ bản sao và mật khẩu với nguy cơ độc lập. Đừng dùng mã hóa trong tập tin lịch sử.
3. Để phục hồi nó, mật khẩu và khóa công khai số người tham gia có nguồn gốc chính xác trên webcam hoặc Mirror nếu bạn đến.
4. Kiểm tra chính sách, mạng lưới, địa chỉ và khám phá trước khi phẫu thuật.
5. Để loại bỏ nội bộ, hãy kiểm tra và xác nhận và lưu lại nếu bạn muốn phục hồi. Phục hồi sau đó là giải thích.

Kết quả: Chính sách có thể phục hồi hoặc loại bỏ địa phương có ý thức. Gỡ bỏ không phải là di chuyển tiền, không xóa các khóa của bên ký khác, cũng không hủy bỏ chính các hoạt động mà người khác đang thực hiện.

P29 | Khôi phục ngoại lệ trên máy tính | Desk | L47 | C02

Chuẩn bị: Vật liệu được chấp nhận, môi trường sạch sẽ và bản sao lưu. Thao tác này có thể tiết lộ một bí mật cho PC; nó sử dụng dữ liệu học tập trong khóa học.

1. Bắt đầu phục hồi địa phương từ ngữ ngữ chuẩn và đọc những hạn chế của định dạng và thông báo.
2. Hãy chấp nhận rủi ro một cách ý thức và ngắt kết nối mạng lưới theo yêu cầu của dòng; cửa sổ kiểm tra trạng thái trước khi cho phép tiếp tục.
3. Chỉ cần đưa giấy tờ cần thiết vào cửa sổ tư nhân. Chúng không được quyết định, chúng dán vào lớp học, và chia sẻ với hỗ trợ.
4. Nó kích hoạt chỉ trong một không gian không có máy ảnh hay người tham dự lắng nghe; nó tôn trọng thời gian biểu và đóng cửa.
5. Cuối cùng, kiểm tra xem có thể có những sự phơi nhiễm nào tồn tại và lên kế hoạch di cư tới các khóa mới nếu nó tiến hành.

Kết quả: Sự hồi phục phi thường, không đảm bảo xóa sổ pháp y hay tương đương với phần cứng cách ly. Nếu không xác thực, định dạng hay vật liệu truy cập, đừng thử công cụ Internet với bản sao thật của bạn.

P30 | Rà soát tùy chọn, sinh trắc học và khóa | Desk | L40 | C02

Chuẩn bị: mật khẩu Biết và biết bản sao lưu Hãy thử trước khi thay đổi an ninh.

1. Truy cập và chặn mật khẩu, sinh trắc học sẵn sàng, không hoạt động và khóa khi chuyển sang chế độ thứ hai.
2. Ông hiểu sự chậm trễ sau khi lỗi được thiết lập và mức độ tối đa trước khi thay đổi.
3. Hãy giữ bộ xoá đã tắt cho đến khi bạn hiểu được điều kiện, ngưỡng và sự phục hồi. Đừng thử sản xuất.
4. Thiết lập ngôn ngữ điều chỉnh, sắc thái, tiền tệ, đồng bộ 3 Không 5 phút và âm thanh.
5. Nếu bạn đăng nhập liên kết bitcoin: hãy kiểm tra xem việc mở một đơn có thể mở khóa, chọn lọc và sửa chữa; không tự nó trả tiền.

Kết quả: Hiểu rồi. sinh trắc học của hệ điều hành phụ thuộc vào nhóm và không thay thế mật khẩu hay bản sao lưu. Thiết lập thị giác không thay đổi chính sách bitcoin.

P31 | Xóa bản ghi và hiểu đúng phạm vi tác động | Desk | L22,L45 | C02

Chuẩn bị: Xác định xem bạn sẽ loại bỏ bản mật mã địa phương, tài khoản WOW, chat hay đa chữ ký và bản sao nào bạn lưu.

1. Đọc đối tượng đã chọn và thông báo. Xác nhận bí danh chính xác hay tình trạng rõ ràng khi hợp đồng được yêu cầu.
2. Xuất khẩu và kiểm tra lại xem có cần lấy lại trạng thái đó không.
3. Chỉ gỡ bỏ đối tượng đã định và kiểm tra các mối quan hệ giữ lại hoặc rút lưu lượng.
4. Kiểm tra xem còn ai hoạt động hay người ngoài không. Đừng cho rằng các tin nhắn, chữ ký hay hồ sơ của các nhóm khác bị mất.
5. Nó cung cấp thông tin về sự thay đổi trong danh sách cá nhân của bạn mà không có dữ liệu nhạy cảm trong khóa học.

Kết quả: Trạng thái địa phương được quản lý có ý thức. Không có hành động nào trong số này tự thay đổi bản thân các tập lệnh UTXOs được tài trợ, phá hủy một tập hạt giống khôi phục mà người thứ ba biết hoặc đảo ngược các giao dịch được xác nhận.

P32 | Chẩn đoán mà không lộ bí mật | Desk và Mirror | L23,L30,L48 | C02,C03

Chuẩn bị: ghi thời gian gần đúng, hệ thống, kiến trúc, phiên bản và giai đoạn. Không lặp lại thao tác nhạy cảm khi chưa rõ trạng thái.

1. Xác định lỗi ở bước tìm, ghép nối, đọc, ghi, xác minh, ký, chuyển trả, mạng hay hiển thị.
2. Chép mã và nội dung lỗi, không kèm QR hay dữ liệu riêng. Dùng công cụ chẩn đoán ứng dụng khi thích hợp.
3. Rà tệp trước khi chia sẻ. Không đính kèm bản sao kho, bản mật mã, hạt giống, khóa trò chuyện, descriptor hay thông tin xác thực RPC.
4. Với sự cố giao diện, dùng cảnh giả và ghi kích thước cửa sổ, độ thu phóng cùng các nút điều khiển bị ẩn.
5. Gửi kết quả mong đợi và các bước tái hiện qua kênh chính thức. Khóa học không tự gửi tin nhắn tới hỗ trợ.

Kết quả: báo cáo đủ để điều tra với dữ liệu tối thiểu. Nếu chưa có bằng chứng cho một giai đoạn, ghi “đang chờ”, không ghi “đã hoàn tất”. Hỗ trợ giọng nói không cần truy cập từ xa thiết bị lưu ký.

Bảng thuật ngữ Bitcoin và tự lưu ký

Bitcoin

Mạng và tập hợp quy tắc để chuyển giá trị và kiểm chứng lịch sử mà không cần một quản trị viên duy nhất cho sổ cái.

BTC

Đơn vị tiền tệ của Bitcoin. Một BTC bằng một trăm triệu satoshi.

Satoshi

Đơn vị trên chuỗi cơ sở, bằng một phần một trăm triệu BTC.

Blockchain

Lịch sử các khối được liên kết và xác minh theo quy tắc. Riêng thuật ngữ này không mô tả hết đặc tính của một mạng.

Khối

Tập dữ liệu gồm các giao dịch và phần tiêu đề có thể xác minh.

Nút đầy đủ

Phần mềm kiểm tra việc tuân thủ quy tắc của các khối và giao dịch mà nó chấp nhận.

Khai thác

Xây dựng khối bằng bằng chứng công việc theo quy tắc của mạng.

Bằng chứng công việc

Cơ chế yêu cầu thực hiện công việc tính toán có thể kiểm tra để đề xuất một khối.

Đồng thuận

Sự tương thích giữa những người tham gia về các quy tắc và lịch sử hợp lệ mà họ chấp nhận.

Chính sách mempool

Quy tắc cục bộ về tiếp nhận và chuyển tiếp giao dịch, không nhất thiết trùng với quy tắc đồng thuận.

Mempool

Tập hợp giao dịch chưa xác nhận được một nút lưu cục bộ.

Xác nhận

Việc giao dịch được đưa vào một khối của chuỗi được chấp nhận và độ sâu sau đó của khối ấy.

Tái tổ chức chuỗi

Thay đổi một đoạn của chuỗi được chấp nhận, có thể làm thay đổi các xác nhận.

UTXO

Đầu ra giao dịch chưa chi tiêu. Có thể chi tiêu khi đáp ứng điều kiện của nó.

Đầu vào

Tham chiếu đến đầu ra trước đó và dữ liệu cần để cho phép chi tiêu đầu ra ấy.

Đầu ra

Giá trị và điều kiện chi tiêu do một giao dịch tạo ra.

Tiền thừa

Đầu ra đưa một phần giá trị đầu vào về quyền kiểm soát của người chi sau khi thanh toán và trừ phí.

Phí giao dịch

Chênh lệch giữa tổng giá trị đầu vào và đầu ra của giao dịch.

vbyte

Đơn vị kích thước ảo dùng để biểu thị chi phí tương đối của một giao dịch.

sat trên mỗi vbyte

Phí suất tính bằng satoshi trên mỗi đơn vị kích thước ảo.

Đầu ra nhỏ (dust)

Đầu ra có giá trị nhỏ xét theo chính sách và chi phí chi tiêu. Ngưỡng phụ thuộc bối cảnh và script.

RBF

Thay thế giao dịch chưa xác nhận theo chính sách tương thích. Không phải cơ chế hủy được bảo đảm.

CPFP

Dùng giao dịch con để tăng động lực đưa cả nó lẫn giao dịch cha vào khối.

Giá trị băm (hash)

Dấu vân tay dữ liệu giúp kiểm tra tính toàn vẹn. Nó không mã hóa dữ liệu hoặc tự xác định tác giả.

Khóa riêng

Khả năng mật mã dùng để tạo ủy quyền theo cơ chế tương ứng.

Khóa công khai

Dữ liệu cho phép kiểm tra chữ ký và tạo một số điều kiện nhất định mà không làm lộ khóa riêng.

Chữ ký số

Bằng chứng mật mã về sự cho phép đối với thông điệp cụ thể. Chữ ký không che nội dung thông điệp.

Mã hóa

Bảo vệ tính bí mật bằng một khóa và một thuật toán.

Mã hóa có xác thực

Mã hóa kèm khả năng phát hiện sửa đổi theo thiết kế.

AES GCM

Họ cơ chế mã hóa có xác thực dùng trong các định dạng của hệ sinh thái. Đặc tính phụ thuộc vào cách triển khai và quản lý khóa.

Cụm từ ghi nhớ

Cách biểu diễn bằng từ ngữ dữ liệu tạo sinh và kiểm tra theo một định dạng cụ thể.

Hạt giống

Dữ liệu để dẫn xuất các khóa. Trong cách nói thông thường, từ này cũng có thể chỉ cụm từ ghi nhớ, nên cần làm rõ ngữ cảnh.

Entropy

Mức độ không thể dự đoán của dữ liệu tạo sinh. Chọn những từ dễ nhớ không tạo ra entropy.

Tổng kiểm tra (checksum)

Giá trị dùng để phát hiện một số lỗi, không xác thực tác giả.

BIP39

Đặc tả cụm từ ghi nhớ và cách dẫn xuất hạt giống với cụm mật khẩu tùy chọn.

Cụm mật khẩu BIP39

Đầu vào bổ sung cho quá trình dẫn xuất. Một cụm khác có thể sinh ra ví hợp lệ khác, không có tiền.

BIP32

Đặc tả dẫn xuất khóa theo cấu trúc phân cấp.

Đường dẫn dẫn xuất

Chuỗi các nhánh dùng để tạo khóa từ một gốc.

Dẫn xuất tăng cường

Bước dẫn xuất thường được ghi bằng dấu nháy hoặc chữ h, với đặc tính khác dẫn xuất công khai thông thường.

xpub

Khóa công khai mở rộng có ngữ cảnh dẫn xuất. Đây là dữ liệu nhạy cảm về quyền riêng tư.

xprv

Khóa riêng mở rộng. Không được chia sẻ hoặc nhập vào khóa học.

Dấu vân tay khóa chủ

Mã định danh ngắn của một gốc, hữu ích để liên kết nhưng chưa đủ chứng minh danh tính.

Descriptor

Biểu thức tạo script từ khóa và thông tin dẫn xuất. Có thể chỉ chứa dữ liệu công khai hoặc có cả dữ liệu riêng.

Ví chỉ theo dõi

Ví quan sát không đủ khả năng ký riêng để tự ký giao dịch.

WOW

Tên gọi các tài khoản theo dõi và quản lý ví trong hệ sinh thái Cuvex.

Ví nóng

Công cụ có khả năng ký trong môi trường đang kết nối.

Tự lưu ký

Mô hình trong đó người dùng giữ khả năng kỹ thuật để tự chi tiêu hoặc phối hợp chi tiêu theo chính sách của mình.

Bên lưu ký

Tổ chức kiểm soát quyền chi tiêu thay khách hàng và áp dụng các điều kiện truy cập của mình.

Bản mật mã Cuvex

Đối tượng đã mã hóa để bảo vệ bí mật, tự thân không phải giao dịch hay số dư.

Mật khẩu Desk

Mật khẩu bảo vệ kho dữ liệu cục bộ. Nó khác với hạt giống và mật khẩu mở bản mật mã.

Khóa trò chuyện

Bí mật để khôi phục danh tính trò chuyện. Hình thức có thể trông như dữ liệu công khai dù thực ra phải bảo mật.

PIN ghép nối

Mã tạm thời của phiên kết nối, không phải mật khẩu lưu ký tài sản.

Cách ly vật lý (air gap)

Tách biệt các môi trường khi vận hành. Dữ liệu chuyển giữa các môi trường vẫn phải được xác minh.

NFC

Công nghệ truyền thông tầm gần sử dụng với thẻ và thiết bị đọc tương thích.

USB Mass Storage

Giao diện trao đổi tệp của mẫu BIT, đòi hỏi giao thức, bước xác minh và xác nhận đã nhận riêng.

PSBT

Định dạng chứa thông tin và chữ ký để phối hợp tạo lập và phê duyệt giao dịch.

PSBT v0

Phiên bản định dạng do BIP174 quy định, được dùng trong hồ sơ đa chữ ký Final đã rà soát.

PSBT v2

Phiên bản do BIP370 quy định. Giao dịch có phiên bản 2 không đồng nghĩa PSBT dùng định dạng này.

SIGHASH ALL

Chế độ cam kết của chữ ký trong hồ sơ đã rà soát. Phải kiểm tra phạm vi dữ liệu được cam kết khi xác minh giao dịch.

P2WPKH

Loại điều kiện SegWit dùng một khóa, thường đi với tài khoản BIP84.

P2WSH

Điều kiện SegWit cam kết với một script, được dùng trong quy trình đa chữ ký Final đã rà soát.

P2TR

Loại đầu ra Taproot. Hỗ trợ thanh toán tới đầu ra này không đồng nghĩa hỗ trợ ký để chi tiêu từ nó.

sortedmulti

Cấu trúc đa chữ ký sắp xếp khóa theo thứ tự xác định để tạo script.

Ngưỡng M trên N

Số M ủy quyền cần từ N người tham gia theo chính sách cụ thể.

MuSig2

Giao thức tổng hợp chữ ký Schnorr có cơ chế cơ sở là N trên N, khác với một ngưỡng tùy ý.

Taproot

Tập hợp cơ chế chi tiêu và cam kết của Bitcoin với đường dùng khóa và đường dùng script.

Miniscript

Ngôn ngữ mô tả và phân tích một số chính sách script. Hồ sơ Final đã rà soát không triển khai ngôn ngữ này.

Regtest

Mạng thực hành cục bộ do người thiết lập môi trường kiểm soát, không có giá trị kinh tế.

Signet

Mạng thử nghiệm có đặc tính riêng, không thể mặc định dùng thay regtest.

Mainnet

Mạng Bitcoin phục vụ hoạt động kinh tế thực.

Giới hạn khoảng trống địa chỉ (gap limit)

Tiêu chí phát hiện địa chỉ dựa trên số địa chỉ liên tiếp chưa có lịch sử. Phạm vi áp dụng phụ thuộc ví.

Kiểm soát đầu vào (coin control)

Chủ động chọn các UTXO dùng để chi tiêu.

Gộp đầu ra

Kết hợp các đầu ra để giảm phân mảnh, có tác động đến chi phí và quyền riêng tư.

Tính giả danh

Dùng mã định danh không trực tiếp là tên pháp lý, không tự động bảo đảm ẩn danh.

Tính ẩn danh

Khả năng không bị phân biệt bởi những người quan sát xác định trong một bối cảnh. Nhãn của ứng dụng không bảo đảm đặc tính này.

Siêu dữ liệu

Thông tin về liên lạc hoặc hoạt động như thời gian, kích thước và mối liên hệ, khác với nội dung.

CoinJoin

Cách xây dựng giao dịch cộng tác làm một số suy luận khó hơn, không bảo đảm ẩn danh vĩnh viễn.

Payjoin

Thanh toán cộng tác với đầu vào của cả người trả lẫn người nhận theo giao thức tương thích.

Tor

Mạng và các công cụ bảo vệ kết nối. Cần cấu hình và xác minh việc sử dụng cho từng ứng dụng.

VPN

Kênh chuyển một phần sự tin cậy trong kết nối sang đơn vị vận hành, không che giấu dữ liệu trên chuỗi.

Lightning

Hệ thống thanh toán qua kênh, có yêu cầu và rủi ro khác giao dịch trên chuỗi.

Hóa đơn thanh toán (invoice)

Yêu cầu thanh toán có cấu trúc. Cần xác định định dạng và phương thức thanh toán.

RPC

Giao diện gọi một dịch vụ như Bitcoin Core. Phải xác thực và bảo vệ giao diện này.

TLS

Cơ chế bảo vệ truyền tải trước một số mối đe dọa. Máy chủ nhận vẫn thấy yêu cầu.

SRTP

Cơ chế bảo vệ âm thanh trên một số chặng VoIP. Nó không tự động bảo đảm bí mật trước nhà vận hành.

Tính lũy đẳng

Đặc tính ngăn tạo hiệu lực trùng lặp khi gửi lại cùng một yêu cầu đã được định danh.

Webhook

Sự kiện được gửi giữa các máy chủ. Cần kiểm tra tính xác thực và khả năng gửi trùng.

RAG

Truy xuất các đoạn tri thức để làm căn cứ cho câu trả lời theo đúng ngữ cảnh và phiên bản.

Diễn giải lại (teach back)

Kiểm tra mức độ hiểu bằng cách yêu cầu học viên trình bày lại bằng lời của mình.

Lừa đảo giả mạo (phishing)

Mạo danh và dựng bối cảnh thuyết phục để chiếm quyền truy cập hoặc dụ nạn nhân thực hiện một hành động.

Kỹ nghệ xã hội

Thao túng quyết định của con người, có thể bằng thông tin thật và cảm giác khẩn cấp.

Công chứng ứng dụng của Apple

Biện pháp kiểm soát phân phối của Apple, khác với kiểm toán sản phẩm hoặc thử nghiệm trực tiếp mọi quy trình.

Chứng thực trạng thái

Bằng chứng trạng thái theo cơ chế cụ thể. Danh mục tương thích của Desk không phải phép đo từ xa.

MiCA

Khung pháp lý châu Âu áp dụng cho một số tài sản và dịch vụ mã hóa, không bảo đảm lợi nhuận hay bồi hoàn toàn bộ.

Travel Rule

Nghĩa vụ cung cấp thông tin đối với giao dịch chuyển thuộc phạm vi điều chỉnh, không được miễn chỉ vì tự lưu ký.

Điểm tiếp tục học (checkpoint)

Điểm lưu vị trí học để tiếp tục, chỉ giữ dữ liệu tối thiểu, không chứa thông tin ví.

Kiểm tra những gì bạn đã học

Thực hành mà không dùng tiền thật. Bài đánh giá mở cho mọi người và không yêu cầu tài khoản.

Khi dùng Cuvex theo quy trình thông thường, ai phê duyệt khoản chi?

1. Thiết bị sau khi người dùng kiểm tra
2. Gia sư giọng nói
3. Máy chủ khóa học

> **Xem đáp án: Thiết bị sau khi người dùng kiểm tra**
> Quy trình phê duyệt vẫn diễn ra trên Cuvex.

0,001 BTC bằng bao nhiêu satoshi?

1. 1.000
2. 100.000
3. 1.000.000

> **Xem đáp án: 100.000**
> Một BTC bằng 100.000.000 sat.

Đầu vào là 120.000 sat, đầu ra là 119.000 sat. Phí là bao nhiêu?

1. 1.000 sat
2. 119.000 sat
3. 1 sat/vB mà không cần thêm dữ liệu

> **Xem đáp án: 1.000 sat**
> Hiệu giữa tổng giá trị đầu vào và đầu ra là phí tuyệt đối.

Một giao dịch đã ký nhưng chưa phát đi ở trạng thái nào?

1. Đã xác nhận
2. Không thể đảo ngược vì đã ký
3. Đã được cho phép nhưng chưa chắc đã được phát

> **Xem đáp án: Đã được cho phép nhưng chưa chắc đã được phát**
> Ký và phát giao dịch là hai giai đoạn khác nhau.

200 vB với phí suất 6 sat/vB tương đương bao nhiêu?

1. 206 sat
2. 1.200 sat
3. 6% số tiền gửi

> **Xem đáp án: 1.200 sat**
> Lấy kích thước ảo nhân với phí suất.

Trước khi rút tiền khỏi sàn, bạn cần kiểm tra gì?

1. Chỉ cần xem phí thấp nhất
2. Tài sản, mạng, địa chỉ và số tiền thực nhận phải phù hợp
3. Hạt giống khôi phục của đối tác

> **Xem đáp án: Tài sản, mạng, địa chỉ và số tiền thực nhận phải phù hợp**
> Không phải mạng nào có ký hiệu BTC cũng là mạng Bitcoin on-chain.

Chỉ riêng chữ ký số làm được gì?

1. Ẩn toàn bộ thông điệp
2. Xác nhận việc cho phép đối với thông điệp có thể xác minh theo cơ chế chữ ký
3. Xóa dữ liệu đã công bố

> **Xem đáp án: Xác nhận việc cho phép đối với thông điệp có thể xác minh theo cơ chế chữ ký**
> Giữ bí mật nội dung cần một cơ chế khác.

Thay đổi cụm mật khẩu BIP39 có thể dẫn đến điều gì?

1. Tạo một ví hợp lệ khác trông như không có tiền
2. Luôn có thể đặt lại qua email
3. Thay đổi lịch sử thanh toán công khai trước đây

> **Xem đáp án: Tạo một ví hợp lệ khác trông như không có tiền**
> Cụm mật khẩu tham gia vào quá trình dẫn xuất.

Nên đối xử với xpub của một tài khoản như thế nào?

1. Dữ liệu hoàn toàn vô hại
2. Giống hệt hạt giống riêng
3. Thông tin nhạy cảm về quyền riêng tư

> **Xem đáp án: Thông tin nhạy cảm về quyền riêng tư**
> Nó có thể mở rộng phạm vi theo dõi hoạt động.

Tại sao một hạt giống duy nhất có thể không đủ trong ví đa chữ ký?

1. Thiếu chính sách ví và các ủy quyền cần để đạt ngưỡng
2. Bitcoin không cho phép khôi phục bất cứ thứ gì
3. Cần biết màu gốc của ứng dụng

> **Xem đáp án: Thiếu chính sách ví và các ủy quyền cần để đạt ngưỡng**
> Lưu chính sách và giữ khả năng ký riêng là hai yêu cầu khác nhau.

Nếu kết quả gieo xúc xắc bị từ chối trong thuật toán Final đã được rà soát, bạn phải làm gì?

1. Chỉ tung lại đồng xu đến khi chấp nhận
2. Tung lại đồng xu và gieo lại cả bốn viên xúc xắc
3. Chọn một từ quen thuộc

> **Xem đáp án: Tung lại đồng xu và gieo lại cả bốn viên xúc xắc**
> Chỉ làm lại một phần có thể gây thiên lệch trong phép ánh xạ.

Việc cần hai mật khẩu để mở hạt giống của ví đơn chữ ký có nghĩa gì?

1. Trên chuỗi bắt buộc dùng hai khóa
2. Đó là ví đa chữ ký Taproot
3. Ngưỡng truy cập bí mật tách biệt với ngưỡng chi tiêu Bitcoin

> **Xem đáp án: Ngưỡng truy cập bí mật tách biệt với ngưỡng chi tiêu Bitcoin**
> Mã hóa không thay đổi script chi tiêu.

Khi đánh giá bản sao lưu toàn bộ của Desk, cần biết điều gì?

1. Bản sao luôn bao gồm toàn bộ cuộc trò chuyện
2. Có giới hạn phạm vi và mục loại trừ, không thể mặc định rằng có lịch sử trò chuyện
3. Bản sao này cập nhật mọi bản sao cũ

> **Xem đáp án: Có giới hạn phạm vi và mục loại trừ, không thể mặc định rằng có lịch sử trò chuyện**
> Khôi phục danh tính và khôi phục tin nhắn là hai việc khác nhau.

Một nút tự vận hành được cấu hình đúng có tác dụng gì?

1. Loại bỏ mọi rò rỉ
2. Giảm phụ thuộc vào truy vấn bên thứ ba và cho phép tự xác minh
3. Khôi phục khóa bị mất

> **Xem đáp án: Giảm phụ thuộc vào truy vấn bên thứ ba và cho phép tự xác minh**
> Nút không đảm bảo ẩn danh hay khôi phục bí mật.

Đóng băng một UTXO trong Desk có nghĩa là gì?

1. Một hạn chế cục bộ do ứng dụng áp dụng
2. Thay đổi điều kiện đồng thuận
3. Vô hiệu hóa các bản sao hạt giống khác

> **Xem đáp án: Một hạn chế cục bộ do ứng dụng áp dụng**
> Đây không phải lệnh cấm chi tiêu trên toàn mạng.

Mất kết nối ngay lúc phát giao dịch, nên làm gì?

1. Thanh toán lại ngay
2. Xóa ví
3. Trước tiên kiểm tra giao dịch đã được phát chưa

> **Xem đáp án: Trước tiên kiểm tra giao dịch đã được phát chưa**
> Hết thời gian chờ không chứng minh thao tác không có hiệu lực.

Dùng lại địa chỉ hoặc gộp UTXO từ nhiều bối cảnh có thể dẫn đến điều gì?

1. Giúp người quan sát dễ nhận ra liên hệ
2. Xóa lịch sử
3. Bảo đảm ẩn danh

> **Xem đáp án: Giúp người quan sát dễ nhận ra liên hệ**
> Quyền riêng tư phụ thuộc vào bối cảnh và cách sử dụng sau đó.

Mở Tor Browser có tự cấu hình Desk không?

1. Có
2. Không
3. Chỉ khi dùng giao diện tối

> **Xem đáp án: Không**
> Phải kiểm tra tuyến kết nối của từng ứng dụng.

Khóa trò chuyện có hình thức giống xpub là gì?

1. Thông tin có thể công bố
2. Địa chỉ nhận tiền
3. Thông tin xác thực danh tính cần giữ bí mật

> **Xem đáp án: Thông tin xác thực danh tính cần giữ bí mật**
> Mục đích sử dụng quyết định mức độ nhạy cảm.

Một tin nhắn ghi “đã thanh toán” có ý nghĩa gì?

1. Thay thế các xác nhận
2. Vẫn phải kiểm chứng khoản thanh toán độc lập trên mạng
3. Thay đổi mạng của yêu cầu

> **Xem đáp án: Vẫn phải kiểm chứng khoản thanh toán độc lập trên mạng**
> Trạng thái tin nhắn không phải trạng thái thanh toán.

Hồ sơ đa chữ ký của bản Final đã rà soát sử dụng gì?

1. MuSig2 và PSBT v2
2. P2WSH, sortedmulti, BIP48 và PSBT v0
3. Bất kỳ script Bitcoin nào

> **Xem đáp án: P2WSH, sortedmulti, BIP48 và PSBT v0**
> Mong muốn hoặc tên thương mại không mở rộng phạm vi hỗ trợ thực tế.

Trong Mirror 12.12, bạn có thể bắt đầu đối chiếu ở đâu?

1. Chỉ ở mục 1
2. Bất kỳ mục nào bạn chọn, kể cả mục 15
3. Chỉ ở mục cuối sau khi xong tất cả

> **Xem đáp án: Bất kỳ mục nào bạn chọn, kể cả mục 15**
> Mỗi cặp có thể được đối chiếu tự do và độc lập.

Thông báo “Khớp” trong Mirror chứng minh điều gì?

1. Toàn bộ quy trình đã được duyệt
2. Nguồn gốc xác thực của cả hai mã QR
3. Hai mục đang so sánh giống hệt nhau

> **Xem đáp án: Hai mục đang so sánh giống hệt nhau**
> Những phần kiểm tra còn lại và bước phản hồi vẫn chưa hoàn tất.

Nếu hạt giống đã lộ, việc đổi mật khẩu Desk sẽ thế nào?

1. Tước quyền của kẻ tấn công
2. Không vô hiệu hóa các khóa dẫn xuất từ hạt giống đó
3. Xóa mọi bản sao

> **Xem đáp án: Không vô hiệu hóa các khóa dẫn xuất từ hạt giống đó**
> Cần đánh giá cách chuyển quyền kiểm soát an toàn.

Khi kết thúc huấn luyện thực hành, cần nêu những gì?

1. Phần nào đã đọc, đã mô phỏng, đã thử trên thiết bị thật và còn thiếu gì
2. Chỉ nêu số giờ đã bán
3. Cam kết việc lưu ký không thể bị xâm phạm

> **Xem đáp án: Phần nào đã đọc, đã mô phỏng, đã thử trên thiết bị thật và còn thiếu gì**
> Mỗi loại bằng chứng có phạm vi riêng.