CUVEX

CUVEX ACADEMY · 0.1

배우고 이해하고 직접 관리하세요.

비트코인과 자기 수탁을 차근차근 배워 보세요. 강의, 설명서, 용어집, 실습은 회원 가입 없이 무료로 이용할 수 있습니다. 원하는 곳에서 시작하세요.

무료 · 가입 불필요

모든 섹션

1. 학습 환경 준비하기
2. 디지털 화폐와 신뢰의 문제
3. 비트코인의 역사와 한계
4. 사토시 단위로 정확히 계산하기
5. 나의 위협 모델
6. 노드와 채굴, 합의
7. UTXO와 거래의 거스름돈
8. 멤풀, 확인, 체인 재구성
9. 수수료, 가상 크기와 거래 대체
10. 네트워크, 주소와 인보이스
11. 해시, 서명, 암호화
12. 시드, 패스프레이즈, 비밀번호
13. 키 파생, xpub와 디스크립터
14. 지갑과 수탁 방식 선택하기
15. 복구할 수 있는 백업
16. Original과 BIT 알아보기
17. 물리적 엔트로피로 시드 생성하기
18. Cuvex로 비밀 정보 암호화 및 복호화하기
19. 암호화 임계치와 생체 인증
20. 사본 복제, 보관 및 검증
21. Cuvex Desk 설치 및 보호
22. 암호문 연결과 WOW 정리
23. Mirror와 Desk 연결하기
24. Mirror를 통한 NFC, USB-C 및 QR 읽기
25. 공개 제공자와 자체 노드
26. 비트코인 받기와 주소 확인
27. UTXO 라벨 지정, 동결 및 선택
28. 결제 준비 및 검토
29. Original과 BIT로 서명하기
30. 최종화, 전파 및 장애 해결
31. 비트코인에서 관찰할 수 있는 정보
32. 용도 분리와 거스름돈 관리
33. 네트워크 프라이버시, Tor와 VPN
34. CoinJoin, Payjoin과 현재의 한계
35. 실제 사고에서 얻는 교훈

36. 채팅 신원 생성과 연락처 확인
37. 채팅에서 사토시 요청 및 결제
38. 암호문을 이해하고 공유하기
39. 채팅 복구와 메타데이터
40. 일상 설정과 권한 점검
41. 멀티시그 지갑 설계하기
42. 초대 생성 및 키 제공
43. Mirror로 원하는 순서로 정책 대조하기
44. 멀티시그 서명 조율과 발행
45. 멀티시그 복구와 변경
46. 절차에 따른 펌웨어 업데이트
47. 분실, 고장 및 긴급 복구
48. 피싱, 지원 사칭 및 음성 사기
49. 프라이버시, 법규와 개인 기록
50. 상속, 연속성 및 연례 훈련
51. 가격, 저축과 기본적 분석
52. 비트코인 구매처 선택
53. 계정, 주문 및 체결 비용
54. 캔들, 지표와 기술적 분석의 편향
55. 증거금, 선물과 자동화
56. Lightning과 기타 계층
57. Taproot, MuSig2와 양자 내성의 전망
58. 상호 운용성과 제조사 의존에서 벗어나기
59. regtest 기술 실습
60. 최종 과제와 연속성 계획
61. 수강생 설명서
62. 비트코인과 자기 수탁 용어집
63. 배운 내용 확인하기

M01

학습 환경 준비하기

학습 목표

강좌를 준비하고 세 장비의 역할을 구별하며 튜터에게 절대 알려 주지 않을 정보를 정합니다.

이해하기

비트코인을 받고 보관하고 쓰고 복구하는 법을 스스로 판단할 수 있도록 배웁니다. 최종 목표는 승인하기 전에 결정의 이유를 설명하는 것입니다. 혼자서도 읽을 수 있습니다. 음성 튜터는 설명과 질문으로 학습을 도우며 자산을 보거나 기기를 조작할 필요가 없습니다.

Cuvex는 비밀 정보를 보호하고 자체 화면에서 작업을 승인하는 기기입니다. Desk는 컴퓨터에서 암호문, 관찰 전용 지갑, 결제와 협업을 관리합니다. Mirror는 지원되는 작업을 로컬에서 중계하고 데이터를 대조합니다. 직접 서명하거나 독립된 지갑으로 작동하지 않습니다. 사용할 경로는 모델과 버전에 따라 달라집니다.

강좌와 Desk에 화면을 하나씩 배정하고 휴대전화와 Cuvex를 곁에 둡니다. 화면이 하나라면 전환해서 쓰되 비밀을 입력할 때는 영상 통화로 공유하지 마세요. 실습 도중 통화를 끝내도 됩니다. 잠시 멈추는 것은 실패가 아닙니다. 강의 번호와 진행 단계, 어려웠던 점만 저장하세요.

사람 강사나 AI에게 시드, BIP39 패스프레이즈, 비밀번호, 채팅 키, PIN, 비공개 파일, 구매 코드 전체를 알려 주지 마세요. 실제 xpub, 디스크립터, 주소도 필요 없습니다. 이를 사용해 지출할 수 없어도 활동은 노출됩니다. 오류 메시지를 설명하고 실습용 가상 데이터를 사용하세요.

실습

1. 컴퓨터와 휴대전화, Cuvex 기종을 실물로 확인하고 버전을 개인 노트에 적으세요.
2. 자금이 없는 학습 환경과 실제 보관 환경을 분리하세요. 실습을 위해 실제 시드를 가져오지 마세요.
3. 이 강의에서 일시 정지, 도움말, 용어집을 찾으세요. 누군가 비밀을 요구하면 대화를 중단하세요.

이해 확인

누가 서명하고 네트워크를 조회하며 데이터를 전달하는지 설명하세요. 도움 없이 역할을 구별할 수 있으면 다음으로 넘어갑니다.

자주 묻는 질문

매일 튜터와 대화해야 하나요? 아니요. 혼자 공부하거나 수업을 반복하고 특정 절차에서만 도움을 받을 수 있습니다. 강좌 이용 권한과 음성 서비스 잔여 시간은 별개입니다.

잠시 멈추기

L01 완료. 장비를 확인했고 강좌에 비밀 정보는 기록하지 않았습니다.

튜터가 시드 문구를 제대로 적었는지 확인하겠다며 알려 달라고 합니다. 어떻게 할까요?

1. 천천히 읽어 준다.
2. 요청을 거절하고 안전한 개인 환경에서만 확인한다.
3. 앞부분 몇 단어만 보낸다.

> **정답 보기: 요청을 거절하고 안전한 개인 환경에서만 확인한다.**
> 비밀 정보는 일부라도 학습 서비스에 제공하지 않습니다.

M01

디지털 화폐와 신뢰의 문제

학습 목표

지갑을 열기 전에 비트코인이 해결하려는 문제를 이해합니다.

이해하기

은행 잔액은 금융기관이 관리하는 기록입니다. 은행이 고객을 인증하고 처리할 이체를 결정하며 장부를 유지합니다. 일반 디지털 파일은 쉽게 복제됩니다. 사진을 보내도 사본이 남습니다. 디지털 단위가 돈으로 쓰이려면 이중 지불을 방지해야 합니다.

비트코인은 검증 규칙과 서명, 공유 거래 내역을 결합합니다. 단일 기관에 장부 전체를 맡기지 않고 독립된 참여자가 거래의 규칙 준수 여부를 확인할 수 있습니다. 희소성은 그 규칙이 계속 검증되고 받아들여질 때 유지됩니다. 코인 이미지나 거래소 시세에서 생기는 것이 아닙니다.

자기 수탁은 책임을 바꿉니다. 수탁자의 허가 없이 쓸 수 있지만 백업을 모두 파기하거나 잘못된 결제에 서명하면 자산을 잃을 수 있습니다. 자유롭게 운용해도 보안, 협업, 전파에 필요한 연결, 적용되는 의무의 준수는 필요합니다.

네트워크와 프로토콜인 Bitcoin과 화폐 단위인 BTC를 구별하세요. 블록체인이라는 이름을 쓰는 다른 네트워크의 성질은 다를 수 있습니다. 기업이 '비트코인'이라고 부르는 지급 약속과 자신의 키로 비트코인 출력을 통제하는 것도 다릅니다.

실습

1. 은행 잔액, 거래소 잔액, 내 키로 관리하는 UTXO를 비교하세요.
2. 각각 누가 자금 이동을 막을 수 있는지, 접근 방법을 잊으면 누가 도울 수 있는지 적으세요.
3. 사진을 복제할 때와 같은 출력을 두 번 쓰려 할 때 어떤 일이 생기는지 설명하세요.

이해 확인

잔액과 서명 권한이 어떻게 다른지 자신의 말로 설명하세요. 전문 용어를 외울 필요는 없습니다.

자주 묻는 질문

자기 수탁을 하면 모든 중개자가 사라지나요? 구매, 조회, 연락에 쓸 서비스를 선택할 수 있습니다. 중요한 것은 각 서비스의 권한과 받는 데이터입니다.

잠시 멈추기

실제 계좌 이름을 제외하고 책임을 비교한 내용을 보관하세요.

전자 서명만으로 해결할 수 없는 화폐상의 문제는 무엇인가요?

1. 같은 출력을 두 번 쓰려는 시도를 막는다.
2. 키로 승인했음을 증명한다.
3. 서명한 메시지가 바뀌었음을 감지한다.

> **정답 보기: 같은 출력을 두 번 쓰려는 시도를 막는다.**
> 서명은 승인을 나타내며 양립할 수 없는 지출의 순서는 규칙과 합의로 결정됩니다.

M01

비트코인의 역사와 한계

학습 목표

비트코인의 기원을 살펴보고 역사적 사실과 홍보 문구를 구별합니다.

이해하기

사토시 나카모토의 논문은 2008년에 발표됐고 네트워크는 2009년에 시작됐습니다. 암호학, 작업 증명, 디지털 화폐의 선행 연구를 활용한 개인 간 전자 현금 제안입니다. 소프트웨어나 거래를 검증하는 데 사토시의 실제 신원은 필요하지 않습니다.

한 기업이 일방적으로 규칙을 바꾸며 발전시킨 것이 아닙니다. 개발자는 변경을 제안·검토하고 운영자는 소프트웨어를 선택하며 채굴자는 블록을 만들고 사용자와 서비스는 무엇을 수용할지 결정합니다. 이 과정에서 이견이 생길 수 있습니다. 포크와 앱 업데이트는 다른 개념입니다.

작업량이 아무리 많아도 노드는 자체 규칙을 위반한 블록을 거부할 수 있습니다. 합의는 컴퓨터 대수로 정하는 단순 투표가 아닙니다. 노드를 수천 개 복제해도 자동으로 결정권이 늘지 않고 채굴자 과반도 사용자의 개인 키를 얻지는 못합니다.

블록 용량, 검증 비용, 가변적인 확인 시간, 공개 기록에는 의도적인 한계와 절충이 있습니다. 관리자가 결제를 취소해 주거나 기본적으로 완전한 기밀성을 제공하지 않습니다. 각 계층과 앱은 특정 용도를 해결하는 대신 새로운 의존성을 만듭니다.

실습

1. 최초 논문, 네트워크 시작, SegWit 채택, Taproot 활성화를 연표에 놓으세요. 공개하기 전에 출처로 날짜를 확인하세요.
2. ‘기업이 가격을 보장한다’, ‘노드가 검증한다’, ‘채굴자가 블록을 제안한다’를 상업적 약속과 기술적 역할로 분류하세요.
3. 결제를 취소하는 관리자가 없을 때의 이점과 대가를 하나씩 설명하세요.

이해 확인

합의 규칙, 로컬 정책, 기업의 결정을 구별하세요. 사용하는 앱은 네트워크의 일부입니다.

자주 묻는 질문

최신 소프트웨어는 항상 통화 규칙을 바꾸나요? 아니요. 오류 수정, 성능 개선, 로컬 정책 변경도 있습니다. 릴리스 노트와 호환성을 확인하세요.

잠시 멈추기

검증할 수 있는 성질 하나와 추가 증거가 필요한 주장 하나를 적으세요.

유효한 승인 없이 지출하는 블록을 채굴자 다수가 유효하게 만들 수 있나요?

1. 네, 51%를 넘으면 가능합니다.
2. 거래소가 발표할 때만 가능합니다.
3. 이를 거부하는 규칙을 적용하는 노드에는 유효하지 않습니다.

> **정답 보기: 이를 거부하는 규칙을 적용하는 노드에는 유효하지 않습니다.**
> 누적 작업량은 해당 노드의 규칙에 따라 유효한 이력끼리 비교합니다.

M01

사토시 단위로 정확히 계산하기

학습 목표

BTC와 사토시를 환산하고 시세에 의존하지 않고 수량을 확인합니다.

이해하기

1 BTC는 100,000,000사토시입니다. sat는 별도의 화폐가 아닌 단위입니다. 기본 체인은 금액을 사토시 정수로 기록합니다. 0.001 BTC는 100,000 sat, 0.00001000 BTC는 1,000 sat입니다. 언어에 따라 소수점 표기가 다르니 눈대중으로 0을 더하지 마세요.

환율은 그 시점의 BTC를 EUR나 USD 등으로 환산합니다. 내가 관리하는 사토시 수는 바뀌지 않습니다. 100,000 sat는 가격이 바뀌어도 그대로입니다. Desk 시세는 출처와 날짜가 있는 참고값이며 BTC 잔액이 맞더라도 오래된 시세는 잘못된 경제적 판단을 부를 수 있습니다.

결제할 때 수취액, 네트워크 수수료, 총지출을 구별하세요. 50,000 sat를 보내고 수수료가 600 sat라면 다른 자기 소유 출력이 없을 때 지갑 지출은 50,600 sat입니다. '전액 보내기'는 보통 수수료를 제외하므로 수취액이 가용 잔액보다 적습니다.

예시는 계산 연습으로, 시세나 권장 수수료가 아닙니다. 서명 전 해당 화면에서 단위, 네트워크, 수취인, 총비용을 확인하세요. 음성으로 '오만 사토시'라고 하며 '50,000 sat'로 표시할 수 있지만 불확실한 음성 인식 결과로 금액을 결정해서는 안 됩니다.

실습

1. 250,000 sat를 BTC로 환산하면 0.0025 BTC입니다. 0.00025000 BTC는 25,000 sat입니다.
2. 75,000 sat를 수수료 900 sat로 보내면 총지출은 75,900 sat입니다.
3. 시뮬레이터에서 120,000 sat 중 70,000 sat를 수수료 1,000 sat로 보내고 거스름돈이 49,000 sat인지 확인하세요.

이해 확인

금액을 BTC와 sat로 읽고 어떤 금액에 수수료가 포함되는지 설명하세요. 의심스러우면 작업을 일시 정지합니다.

자주 묻는 질문

비트코인을 한 개씩 사야 하나요? 아니요. 제공자의 최소 금액과 비용 조건에 따라 일부만 살 수 있습니다.

잠시 멈추기

연습 결과만 보관하세요.

80,000 sat 전액을 수수료 1,200 sat로 보내면 수취인은 얼마를 받나요?

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

> **정답 보기: 78,800 sat.**
> 다른 출력이 없는 이 예에서 수취액은 쓸 수 있는 잔액에서 수수료를 뺀 값입니다.

M01

나의 위협 모델

학습 목표

분실, 도난, 사기, 데이터 노출에 비례하는 대책을 선택합니다.

이해하기

보안은 내 의도대로 행동할 능력을 지키는 것이고, 개인정보 보호는 누가 내 데이터와 관계를 아는지 통제하는 것이며, 가용성은 필요할 때 접근할 수 있는 것입니다. 아무도 못 여는 금고는 나도 못 열 수 있고 지나치게 편리한 사본은 정보를 과도하게 노출할 수 있습니다.

자산, 공격자, 사고를 정의하세요. 자산에는 키, 백업, 이력, 사본 위치, 연락처의 신원이 포함됩니다. 악성코드, 피싱, 화재, 망각, 강요, 고장, 사망, 자신의 실수는 같은 도구 하나로 해결되지 않습니다.

대략적인 가능성, 영향, 구체적 대책을 표로 정리하세요. 긴 비밀번호는 추측을 어렵게 해도 직접 승인한 사기 수취인을 바로잡지 못합니다. 한 가방에 둔 사본 두 개는 가방을 잃으면 소용없고, 한 사람이 멀티시그 기기와 백업을 전부 통제하면 공통 장애점이 남습니다.

강좌와 튜터도 모델에 포함하세요. 구매, 통화, 접속 시간, 진도는 메타데이터가 될 수 있습니다. 수업을 개인화하려고 사이트가 주소나 잔액을 요구해서는 안 됩니다. Desk나 Mirror에 일반 가입이 필요 없어도 스토어, 음성 제공자, 조회를 받는 제삼자는 활동을 알 수 있습니다.

실습

1. 자산 규모와 정확한 위치를 빼고 주요 위험 세 가지를 적으세요.
2. 위험마다 예방·탐지·복구 대책을 정하세요. 카드 분실의 경우 사본 두 개 분산 보관, 재고 점검, 복구 연습이 예입니다.
3. 구매, 통화, 잔액 조회, 공개 거래를 어떤 사람이나 시스템이 볼 수 있는지 구분하세요.

이해 확인

다음 대책이 어떤 위험을 해결하는지 설명하세요. 유지하거나 상속인에게 설명하기 어려울 만큼 복잡하게 만들지 마세요.

자주 묻는 질문

기기가 많을수록 안전한가요? 공통 의존성을 줄이고 복구를 시험할 수 있을 때만 그렇습니다. 기기가 늘면 유지보수와 혼동 가능성도 늘어납니다.

잠시 멈추기

계획은 개인 문서에 보관하고 강좌에는 '위협 모델 검토 완료'만 기록하세요.

한 곳의 화재로 모든 사본을 잃을 위험을 가장 잘 줄이는 방법은 무엇인가요?

1. 카드 색을 바꾼다.
2. 사본 두 개를 같은 서랍에 둔다.
3. 검증한 사본을 각기 독립적인 위험에 노출되는 장소에 보관한다.

> **정답 보기: 검증한 사본을 각기 독립적인 위험에 노출되는 장소에 보관한다.**
> 이중화는 원본을 위협하는 바로 그 사고를 견딜 수 있어야 합니다.

M02

노드와 채굴, 합의

학습 목표

노드가 무엇을 검증하고 채굴이 어떤 역할을 하는지 설명합니다.

이해하기

풀 노드는 블록과 거래를 받아 규칙을 검증하고 체인의 상태를 유지합니다. 웹사이트가 알려 주는 잔액을 신뢰할 필요가 없습니다. 채굴은 작업 증명으로 블록을 제안하는 과정입니다. 채굴자는 유효한 거래를 골라 허용되는 블록을 찾기 위해 경쟁합니다.

작업 증명은 이력을 다시 쓰는 비용을 높입니다. 유효한 후보 체인은 난이도를 무시한 블록 개수가 아니라 누적 작업량으로 비교합니다. 블록 간격은 변동합니다. 10분은 목표 평균이며 다음 결제가 처리될 예정 시각이 아닙니다.

채굴 보상은 블록 높이에 따른 일정으로 줄어드는 보조금과 포함된 거래의 수수료를 합한 것입니다. 높은 수수료도 잘못된 서명을 유효하게 만들지 못합니다. 경제적 보안과 공격 비용이 최근 결제의 불가역성을 수학적으로 보장하지는 않습니다.

자체 노드는 제삼자에게 보낼 조회를 줄이고 직접 검증할 수 있게 합니다. 운영체제, 접근권, 연결은 여전히 보호해야 합니다. 동기화하지 않았거나 앱이 다른 서버를 조회한다면 노드를 켜기만 해서는 이점을 얻을 수 없습니다.

실습

1. 서명 검증, 블록에 넣을 거래 선정, 시드 보관, 결제 수락 판단의 담당자를 구분하세요.
2. ‘채굴자가 내 비트코인을 보관한다’는 설명이 왜 틀리는지 말하세요.
3. 실습 네트워크에서 높이와 동기화 상태를 확인하세요. RPC 인증 정보를 공개하지 마세요.

이해 확인

검증과 제안을 구별해 설명하세요. 비유를 쓰더라도 마지막에는 기술적 역할을 정확히 말하세요.

자주 묻는 질문

비트코인을 쓰려면 채굴해야 하나요? 아니요. 시작할 때 자체 노드도 필수는 아니지만 제공자를 얼마나 신뢰하는지는 알아야 합니다.

잠시 멈추기

실습 제공자의 유형만 기록하고 비공개 URL은 적지 마세요.

올바르게 구성한 풀 노드가 사용자에게 제공하는 것은 무엇인가요?

1. 수용하는 체인의 규칙을 검증한다.
2. 분실한 키를 모두 복구한다.
3. 가격 상승을 보장한다.

> **정답 보기: 수용하는 체인의 규칙을 검증한다.**
> 검증과 수탁은 다른 기능입니다.

UTXO와 거래의 거스름돈

학습 목표

거래를 출력을 소비하고 새 출력을 만드는 과정으로 읽습니다.

이해하기

UTXO는 이전 거래에서 아직 지출되지 않은 출력입니다. 지갑은 자신이 통제할 수 있는 출력을 찾아 잔액을 계산합니다. 은행처럼 공통 계좌에서 차감하지 않고 입력에서 거래 ID와 위치로 이전 출력을 참조합니다.

UTXO를 쓰면 전체가 소모됩니다. 일부만 지불할 때는 보통 수취인 출력과 자신이 통제하는 거스름돈 출력을 만듭니다. 입력 120,000 sat, 수취액 70,000, 수수료 1,000이면 거스름돈은 49,000입니다. 입력 합계는 출력 합계와 수수료의 합과 같습니다.

주소와 UTXO는 다르며 한 주소가 여러 출력을 받을 수 있습니다. 주소가 반드시 한 사람인 것도 아닙니다. 거래 ID가 공개되어도 이를 신원이나 각 출력의 소유자와 연결하면 체인에 없던 정보가 더해집니다.

여러 입력을 합치면 공동 소유를 추정할 수 있고 거스름돈은 이후 결제를 연결할 수 있습니다. 협업 거래도 있으므로 이 추정이 항상 증거가 되지는 않습니다. 코인 컨트롤은 조합의 영향을 이해하고 사용할 출력을 고르는 것입니다.

실습

1. 40,000, 60,000, 200,000 sat의 가상 입력을 그리고 처음 두 개만으로 70,000을 수수료 1,000에 지불하세요.
2. 거스름돈은 29,000 sat이고 세 번째 입력은 사용하지 않았는지 확인하세요.
3. 200,000만 쓰면 거스름돈은 129,000입니다. 거래 크기가 같다고 가정하지 말고 비용과 연결 가능성을 비교하세요.

이해 확인

그림에서 입력, 수취인, 거스름돈, 수수료를 찾으세요. 식별할 수 없는 출력이 있는 실제 거래에는 서명하지 마세요.

자주 묻는 질문

내 지갑으로 들어오는 것은 모두 거스름돈인가요? 다른 내 주소로 보낸 송금일 수도 있습니다. 금액으로 추측하지 말고 정책과 파생 정보를 확인하세요.

잠시 멈추기

가상 도식만 보관하고 실제 자산의 화면 캡처는 남기지 마세요.

100,000 sat 입력에서 30,000과 69,200의 출력이 생겼습니다. 수수료는 얼마인가요?

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

> **정답 보기: 800 sat.**
> 100,000에서 99,200을 빼면 800 sat입니다.

M02

멤풀, 확인, 체인 재구성

학습 목표

거래가 준비된 상태, 전파된 상태, 확인된 상태를 구별합니다.

이해하기

멤풀은 노드가 자체 정책에 따라 보관하는 미확인 거래 집합입니다. 전 세계에 동일한 멤풀은 없습니다. 탐색기에 결제가 보인다는 것은 그 서비스가 안다는 뜻이며, 모든 노드의 수용이나 일정 시간 내 확인을 보장하지 않습니다.

PSBT 준비는 아무것도 전파하지 않습니다. 서명은 권한을 부여하고 최종화는 전파 가능한 거래를 조립하며 발행은 전송을 시도합니다. 확인은 검증 출처가 인정한 체인의 블록에 들어갔다는 뜻입니다. 두 번째 확인은 블록 하나가 더 쌓였다는 뜻으로 수취인의 추가 서명이 아닙니다.

체인 재구성으로 일부 블록이 바뀌면 확인 수가 줄거나 거래가 대기 상태로 돌아갈 수 있습니다. 위험 노출이 큰 결제에서는 보통 더 많은 확인을 요구합니다. 모든 금액과 상황의 위험을 없애는 확인 수는 없습니다.

Desk가 저장된 상태를 보여 주면 동기화 시각을 확인하세요. 오래된 '확인됨'은 현재 상태와 다를 수 있습니다. 송금이 안 보이면 로컬 ID를 보관하고 전파 여부와 이력을 확인한 뒤 다시 준비하세요. 서두르면 유효한 결제가 또 생길 수 있습니다.

실습

1. 초안, PSBT, 서명, 최종 거래, 전파, 블록 포함 카드를 순서대로 놓으세요.
2. 발행 직후 연결 중단을 가정하고 재결제 전에 무엇을 확인할지 정하세요.
3. 채팅의 '결제 완료'가 네트워크 검증을 대신하지 못하는 이유를 상점에 설명하세요.

이해 확인

거래 상태, 정보의 출처와 시각을 보장과 혼동하지 않고 말해 보세요.

자주 묻는 질문

Desk를 닫으면 전파된 거래가 취소되나요? 아니요. 다른 노드와 참여자가 보관할 수 있습니다. 로컬 초안 취소와는 범위가 다릅니다.

잠시 멈추기

모의 거래 상태만 기록하고 실제 ID는 튜터에게 주지 마세요.

발행 버튼을 누르자마자 컴퓨터 연결이 끊겼습니다. 먼저 무엇을 할까요?

1. 같은 결제를 처음부터 다시 준비한다.
2. 지갑을 삭제한다.
3. 다시 연결한 뒤 거래와 입력을 확인한다.

> **정답 보기: 다시 연결한 뒤 거래와 입력을 확인한다.**
> 응답이 없었다고 전파가 실패한 것은 아닙니다.

M02

수수료, 가상 크기와 거래 대체

학습 목표

비용을 추산하고 가상 바이트당 sat와 RBF, CPFP를 이해합니다.

이해하기

네트워크 수수료는 입력과 출력의 차이입니다. 보통 가상 바이트당 사토시(sat/vB)로 경쟁력을 나타냅니다. 송금액에 직접 비례하지 않습니다. 소액도 입력이 많으면 비쌀 수 있고 큰 금액도 입력이 적으면 크기가 작을 수 있습니다.

200 vB에 5 sat/vB라면 수수료는 1,000 sat입니다. 최종 크기는 서명과 구조에 따라 달라져 서명 전에는 추정치만 압니다. Desk는 예상 속도와 수동 수수료율을 제공합니다. '빠름'이 특정 시각의 확인을 약속하지 않습니다.

RBF는 조건에 따라 미확인 거래를 대체하는 정책입니다. 더 높은 수수료의 상충 지출을 제안할 수 있습니다. 노드 정책은 변해 왔으므로 대체 불가 신호를 입금 보장으로 삼지 마세요. 대체 시 새로 검토하고 필요한 서명을 받아야 합니다.

CPFP는 대기 중인 거래의 출력을 지출해 부모·자식 거래를 함께 포함할 유인을 높이는 방식입니다. 쓸 수 있는 출력의 통제권, 정책 준수, 수수료가 필요합니다. 비트코인 개념이며 사용 중인 Cuvex에 CPFP 버튼이 있다고 전제하지 않습니다.

'더스트'는 적용 정책과 예상 지출 비용에 비해 너무 작은 출력입니다. 모든 스크립트에 공통인 기준이 아니므로 고정값을 합의 규칙처럼 가르치지 마세요. 거스름돈을 만들기 어렵다면 금액과 입력, 전액 송금, 실질 수수료를 다시 보세요.

실습

1. 180 vB × 8 sat/vB = 1,440 sat입니다. 실습 예산을 넘는지 확인하세요.
2. 입력 한 개와 열 개를 비교하고 송금액만으로 비용을 추산할 수 없는 이유를 설명하세요.
3. 미확인 거래를 모의로 만들고 자동 호환을 전제하지 않은 채 대기, RBF, CPFP 검토 중 선택하세요.

이해 확인

수수료율, 절대 수수료, 송금액 대비 비용을 설명하고 이해할 수 없는 수수료는 거부하세요.

자주 묻는 질문

RBF가 원래 결제를 확실히 취소하나요? 아니요. 확인까지 두 버전이 경쟁하며 전파 상태도 영향을 줍니다. 취소 약속만 믿고 물건을 넘기지 마세요.

잠시 멈추기

실습에서 선택한 방법과 이유를 보관하세요.

250 vB에 4 sat/vB를 적용한 수수료는 얼마인가요?

1. 1,000 sat.
2. 254 sat.
3. 송금액의 4%.

> **정답 보기: 1,000 sat.**
> 가상 크기와 수수료율을 곱하면 예상 수수료입니다.

M02

네트워크, 주소와 인보이스

학습 목표

복사하거나 스캔하기 전에 네트워크, 주소 형식, 결제 요청을 식별합니다.

이해하기

mainnet에서는 경제적 가치가 있는 비트코인이 이동합니다. 개발과 학습을 위한 시험망들은 서로 호환되지 않습니다. regtest는 실습 운영자가 통제하는 로컬 망이고 signet과 testnet은 각각의 규칙과 생태계가 있습니다. signet에서 단일 서명이 가능해도 Cuvex 멀티시그가 이 망을 지원한다는 뜻은 아닙니다.

주소는 수신 조건을 인코딩합니다. mainnet에는 1, 3, bc1q, bc1p로 시작하는 형식이 있습니다. 접두부는 유형을 파악하는 데 도움을 주지만 수취인 확인, 서명기 호환성 보장, 전체 형식 검증을 대신하지 않습니다.

QR은 주소, 청구서, 디스크립터, 악성 텍스트까지 담을 수 있는 시각적 매체입니다. 스캔해도 작성자가 인증되지는 않습니다. bitcoin: 링크는 금액과 메시지를 추가할 수 있습니다. BIP321이 BIP21을 대체하지만 검토한 Desk 구현은 BIP21 용어와 호환성을 유지합니다. 표준이 바뀌어도 앱이 이해하는 범위가 저절로 넓어지지는 않습니다.

Lightning 인보이스는 온체인 주소와 다르며 만료 시각 등의 필드가 있을 수 있습니다. 앱에서 지원하지 않는다면 온체인 송금에 붙여 넣지 마세요. 다른 망에서 BTC라 부르는 토큰도 비트코인 그 자체라고 볼 수 없습니다.

실습

1. 실제 지출 가능한 주소 없이 강좌의 예시를 주소, bitcoin: URI, Lightning 인보이스, 디스크립터로 분류하세요.
2. 실습에서 선택한 망을 확인하세요. 검토된 Cuvex 멀티시그 프로필이 지원하는 망은 mainnet/regtest입니다.
3. 실제 거래 전 인증된 채널로 수취인이 요청한 텍스트 전체를 대조하세요.

이해 확인

망이나 방식이 불분명한 요청은 거절하고 확인할 사항을 설명하세요.

자주 묻는 질문

거래소에 나오는 아무 망으로 BTC를 보낼 수 있나요? 아니요. 출금망이 실제 수신망과 일치해야 합니다. 수수료가 낮다는 이유만으로 고르지 마세요.

잠시 멈추기

학습용 네트워크의 유형만 기록하세요.

수신 주소가 bc1이라는 사실만으로 다른 토큰 망에서 BTC를 출금할 수는 없습니다. 무엇이 필요한가요?

1. 수취인 별명을 바꾼다.
2. 출금이 비트코인 온체인을 사용하며 모든 정보가 일치하는지 확인한다.
3. 거래소에 시드를 입력한다.

> **정답 보기: 출금이 비트코인 온체인을 사용하며 모든 정보가 일치하는지 확인한다.**
> 자산, 망, 수신 방식이 호환되어야 합니다.

M03

해시, 서명, 암호화

학습 목표

무결성, 승인, 기밀성을 구별합니다.

이해하기

해시 함수는 데이터를 고정 길이 지문으로 바꿉니다. 알려진 지문과 대조하면 변경을 찾을 수 있지만 파일을 암호화하거나 게시자를 식별하지는 않습니다. 침해된 같은 페이지에서 파일과 해시를 받으면 공격자가 둘 다 바꿨을 수 있습니다.

개인 키로 서명을 만들고 대응하는 공개 키로 검증합니다. 서명은 알고리즘과 규칙에 따라 승인을 특정 메시지에 연결합니다. 서명한 내용은 숨겨지지 않습니다. 비트코인에서 유효한 서명은 출력을 쓰기 위한 조건 중 하나입니다.

암호화는 적절한 권한이 있어야 내용을 읽도록 보호합니다. 인증 암호는 변조도 검출합니다. Cuvex 생태계에는 비밀을 보호하는 암호문, 지출을 승인하는 서명된 거래, 메시지를 운반하는 암호화 채널이 있습니다. 모두 암호 기술을 쓰지만 서로 다른 객체입니다.

사람이 정한 비밀번호는 보통 키 파생 함수를 거쳐 암호 키로 쓰입니다. ‘AES-256’은 알고리즘과 키 길이를 나타내며 예측 가능한 비밀번호를 강하게 만들지는 않습니다. 생성, 구현, 저장, 화면 확인, 복구가 전체 보안에 관여합니다.

복잡해 보인다고 QR이 안전한 것은 아닙니다. 무엇을 담고 누가 만들었으며 앱이 무엇을 할지 확인하세요. 승인하기 전 비공개 값을 요구하지 않는 방식으로 튜터에게 목적을 설명해 달라고 하세요.

실습

1. ‘파일 변경 탐지’, ‘시드 숨기기’, ‘결제 승인’을 해시, 암호화, 서명에 연결하세요.
2. 가상 문장의 한 글자를 바꿔 해시 변화를 보세요. 시연에 비밀을 쓰지 마세요.
3. 거래가 공개되면서 동시에 서명될 수 있는 이유를 설명하세요.

이해 확인

안전한 것을 전부 ‘암호화’로 부르지 말고 필요한 보장과 이를 제공하는 메커니즘을 설명하세요.

자주 묻는 질문

펌웨어 해시가 무결점임을 인증하나요? 아니요. 기준값을 신뢰할 수 있으면 바이트를 식별합니다. 감사, 제조사 서명, 실물 시험은 다른 질문에 답합니다.

잠시 멈추기

연습의 세 가지 대응 관계를 보관하세요.

비밀의 내용을 숨기는 방법은 무엇인가요?

1. 파일 이름을 공개한다.
2. 암호화하지 않고 서명한다.
3. 보호된 키로 올바르게 암호화한다.

> **정답 보기: 보호된 키로 올바르게 암호화한다.**
> 서명이나 지문만으로 기밀성을 얻을 수는 없습니다.

M03

시드, 패스프레이즈, 비밀번호

학습 목표

시스템에서 쓰는 각 인증 정보를 혼동하지 않도록 구별합니다.

이해하기

BIP39 니모닉은 엔트로피와 체크섬을 사전의 단어로 나타냅니다. 표준 길이는 12, 15, 18, 21, 24단어입니다. 기억에 남는 문구나 노랫말, 사람이 임의로 고른 단어로 안전한 생성을 재현할 수 없습니다. 체크섬은 일부 오류를 검출할 뿐 작성자나 타인이 시드를 모른다는 사실을 증명하지 않습니다.

BIP39 패스프레이즈는 바이너리 시드 파생에 쓰입니다. 다른 값을 쓰면 전혀 다른 지갑이 열려 비어 보일 수 있습니다. '패스프레이즈가 틀렸다'는 메시지가 반드시 뜨지는 않습니다. 사전 단어일 필요도 없고 실제 25번째 단어도 아닙니다.

Cuvex 암호문 비밀번호는 저장된 비밀을, Desk 비밀번호는 컴퓨터의 로컬 저장소를 보호합니다. 연결 PIN은 통신 세션을 승인하고 채팅 키는 메시징 신원을 복구합니다. 어느 것도 시드와 같지 않으며 하나를 안다고 나머지를 모두 재구성할 수 있는 것은 아닙니다.

시드와 패스프레이즈를 같은 암호문에 두면 복구가 쉬워지지만 복호화할 수 있는 사람에게는 둘의 분리 보호가 사라집니다. 분리하면 자신과 상속인의 부담이 커집니다. 튜터가 '고급'이라고 해서 선택하지 말고 결정을 기록하고 시험하세요.

실습

1. 비밀값 없이 종이 카드 다섯 장에 시드, 패스프레이즈, Cuvex 비밀번호, Desk 비밀번호, 채팅 키를 적으세요.
2. 각각 무엇을 복구하며 잊으면 무엇을 잃는지 적으세요.
3. 빈 지갑에서 시험을 설계하세요. 단어와 패스프레이즈는 비공개로 입력하고 튜터에게 결과만 알리세요.

이해 확인

학습 '검증'을 위해 강좌가 비밀번호를 요구하면 안 되는 이유를 설명하고 자신의 복구 절차에 필요한 비밀을 식별하세요.

자주 묻는 질문

이메일로 패스프레이즈를 재설정할 수 있나요? BIP39에는 그런 기능이 없습니다. 수탁업체 계정 복구는 다른 모델입니다.

잠시 멈추기

값을 적지 말고 '인증 정보 구별 완료'라고 기록하세요.

BIP39 패스프레이즈 한 글자를 바꿨더니 잔액이 0입니다. 올바른 해석은 무엇인가요?

1. 다른 패스프레이즈에서 파생된 별개의 유효한 지갑일 수 있다.
2. 네트워크가 자금을 삭제했다.
3. Desk가 원래 패스프레이즈를 추측해야 한다.

> **정답 보기: 다른 패스프레이즈에서 파생된 별개의 유효한 지갑일 수 있다.**
> 다른 패스프레이즈는 오류 표시 없이 다른 지갑을 생성할 수 있습니다.

M03

키 파생, xpub와 디스크립터

학습 목표

지출 권한을 넘기지 않고 지갑 구성을 기술하는 방법을 이해합니다.

이해하기

계층형 지갑은 하나의 루트에서 많은 키를 파생하며 경로가 사용할 분기를 나타냅니다. mainnet에서는 BIP84의 첫 단일 서명 SegWit 계정에 보통 m/84'/0'/0', BIP48 P2WSH의 첫 멀티시그 계정에 m/48'/0'/0'/2'를 사용합니다. 작은따옴표는 강화 파생을 나타냅니다. 동일한 니모닉도 계정, 망, 스크립트 유형에 따라 다른 주소가 나올 수 있습니다.

xpub는 특정 하위 공개 키를 파생할 수 있는 확장 공개 키입니다. 지출 비밀번호는 아니지만 주소군을 관찰할 수 있습니다. 마스터 지문은 기록을 연계하는 짧은 식별자로 그 자체가 신원을 보장하거나 충돌을 방지하지는 않습니다.

디스크립터는 스크립트 유형, 키, 기원, 파생을 지정해 스크립트와 주소를 구성하는 방법을 나타냅니다. 공개 키만 있는 관찰 전용 디스크립터로 관찰은 가능하지만 서명은 못 합니다. 디스크립터 중에는 개인 키를 담을 수 있는 형식도 있습니다. 실제 것을 강좌에 올리지 마세요.

멀티시그 복구에는 보통 한 서명자의 단어뿐 아니라 전체 정책이 필요합니다. 임계치, 참여자, xpub, 경로, 망, 스크립트 유형, 탐색 정보를 보관하세요. 디스크립터 체크섬은 전사 오류를 찾는 데 도움이 되지만 참여자를 인증하지 않습니다.

실습

1. 가상 경로를 읽고 목적, 화폐, 계정, 분기를 설명하세요. 실제 키는 입력하지 마세요.
2. 입금 주소, 참여자 xpub, 전체 디스크립터를 구별하세요.
3. 필드 이름만 있는 개인 복구 양식을 준비하고 문서 보관 장소를 분리하세요.

이해 확인

복원 후 빈 지갑이 곧 손실 증거가 아닌 이유를 설명하세요. 망, 패스프레이즈, 스크립트, 계정, 경로, 탐색을 확인해야 합니다.

자주 묻는 질문

xpub를 아무 영향 없이 공개할 수 있나요? 일반적으로 단독 지출 능력은 없지만 프라이버시가 노출되고 특정 암호학적 조합에서 다른 위험도 늘 수 있습니다.

잠시 멈추기

강좌에는 민감한 값을 뺀 양식을 보관하세요.

시드 하나만으로 멀티시그를 복구할 때 무엇이 부족할 수 있나요?

1. 기기의 색상.
2. 정책과 다른 참여자들의 공개 키.
3. SNS 비밀번호.

> **정답 보기: 정책과 다른 참여자들의 공개 키.**
> 스크립트 재구성에는 임계치만큼의 개인 키에 더해 완전한 정책이 필요합니다.

M03

지갑과 수탁 방식 선택하기

학습 목표

기능, 신뢰 전제, 복구 방법을 기준으로 도구를 비교합니다.

이해하기

지갑은 구성을 기술하고 관찰하며 필요에 따라 지출을 승인하는 도구 모음입니다. 핫 월렛은 연결된 환경에 서명 능력을 둡니다. 격리한 서명기는 비밀을 망 조회 기기와 분리합니다. 관찰 전용 지갑은 관찰과 준비에 필요한 공개 정보를 가지며 서명에는 다른 시스템이 필요합니다.

제삼자 수탁의 계정은 기업에 대한 청구권을 나타낼 수 있습니다. 자기 수탁에서는 본인이 단독 또는 공동으로 지출할 기술적 능력을 갖습니다. 이메일 계정 복구나 사업자의 출금 차단 권한은 보통 제삼자 수탁의 특징입니다. 두 방식을 같은 책임 전제로 평가하지 마세요.

지원 망과 스크립트, 화면 검증, 백업, 업데이트, 상호 운용성, 유지보수, 제공자 조회, 오류 설명을 비교하세요. 지원 화폐 목록이나 외관만으로는 부족합니다. 서명기를 사용해도 주소를 검토하지 않으면 잘못된 수취처를 승인할 수 있습니다.

Cuvex는 암호문으로 비밀을 보호하고 Desk에서 정리·조회하는 일을 분리합니다. 암호문과 잠금 해제 수단을 모두 보관해야 합니다. 기기 분실에 대비했어도 모든 사본이나 비밀번호마저 잃으면 복구된다는 뜻은 아닙니다. 자산을 옮기기 전에 전 과정을 배우세요.

실습

1. Cuvex, 핫 월렛, 거래소를 표로 비교하세요. 누가 서명·조회 관찰·접근 복구를 하는지, 회사 폐업 시 어떻게 되는지 적으세요.
2. 광고가 아니라 증거로 검증할 기준 두 가지를 고르세요.
3. 실습 환경이 실제 저축과 키를 공유하지 않는지 확인하세요.

이해 확인

도구가 무적이라고 하지 않고 구체적인 사례에 맞는 선택의 근거를 설명하세요.

자주 묻는 질문

하드웨어 지갑이 모든 거래를 비공개로 만드나요? 아니요. 주로 서명 능력과 검토 일부를 보호합니다. 체인, 조회, 상대방에서는 계속 정보가 생깁니다.

잠시 멈추기

계정 이름 없이 기준표를 보관하세요.

공개 키로 올바르게 설정한 관찰 전용 지갑은 무엇을 할 수 있나요?

1. 거래를 관찰하고 준비하지만 스스로 서명하지는 못한다.
2. 잃어버린 시드를 바꾼다.
3. 익명성을 보장한다.

> **정답 보기: 거래를 관찰하고 준비하지만 스스로 서명하지는 못한다.**
> 관찰 능력과 승인 능력은 분리할 수 있습니다.

M03

복구할 수 있는 백업

학습 목표

완전한 백업을 설계하고 의존하기 전에 실제 복구를 검증합니다.

이해하기

유용한 백업은 단순한 파일이 아니라 작업 능력을 복구합니다. 단일 서명에는 니모닉, 패스프레이즈, 파생 정보가 필요할 수 있고 멀티시그에는 정책과 충분한 서명자도 필요합니다. Desk는 암호화 사본과 비밀번호가 필요할 수 있습니다. 채팅 신원 복구와 과거 메시지 복구는 다릅니다.

이중화는 우발적 손실에 대비하고 분리는 동시 침해를 막습니다. 다른 매체와 장소에 사본 두 개를 두면 연관된 장애를 줄일 수 있습니다. 사본마다 접근 통제, 목록화, 검토가 필요합니다. 파일명과 라벨로 자산을 노출하거나 모든 구성 요소의 위치를 쉽게 찾게 하지 마세요.

시험에서는 미리 검증한 주소를 대조하고 학습 환경에서 통제된 거래에 서명할 수 있는지 확인합니다. 파일이 열려도 올바른 지갑 것인지는 알 수 없습니다. 사본을 확인하려고 아무 컴퓨터에나 실제 시드를 입력하지 마세요.

각 사본이 포함하고 제외하는 내용을 기록하세요. 현재 비밀번호를 바꿔도 옛 사본은 자동으로 바뀌지 않습니다. 옛 비밀번호가 노출되었다면 해당 사본은 계속 위험합니다. 현대 저장장치에서 파일을 지워도 모든 사본과 버전이 삭제됐다고 보장할 수 없습니다.

실습

1. 객체, 내용, 해당 비밀번호, 독립 보관 위치, 시험일, 담당자를 개인 표에 기록하세요.
2. 분리한 환경에 실습 사본을 복원하고 망, 첫 주소, 파생을 검증하세요.
3. 먼저 컴퓨터 분실, 다음으로 기기 분실을 가정하고 달라지는 절차를 찾으세요.

이해 확인

임기응변식 도움 없이 실습 환경을 복구하고 다른 경우에 어떤 정보가 부족할지 설명하세요.

자주 묻는 질문

Desk 전체 백업에 모든 것이 있나요? 그렇게 가정할 수 없습니다. 검토한 버전에는 채팅 이력과 세션이 포함되지 않습니다. 멀티시그 정책과 개인 키도 역할이 다릅니다.

잠시 멈추기

시험 날짜와 결과만 기록하고 사본 내용은 기록하지 마세요.

Desk 비밀번호를 변경하면 예전 사본은 어떻게 되나요?

1. 자동으로 갱신된다.
2. 자동으로 암호화가 풀린다.
3. 생성할 때의 보호 방식과 비밀번호가 유지된다.

> **정답 보기: 생성할 때의 보호 방식과 비밀번호가 유지된다.**
> 이전 사본은 독립된 객체입니다.

M04

Original과 BIT 알아보기

학습 목표

기기와 버전에 맞는 절차를 선택합니다.

이해하기

Original은 NFC 카드로 암호문과 호환 작업을 전달하고 업데이트에는 Bluetooth를 사용합니다. 문서화된 모델의 USB-C는 전원용입니다. BIT는 USB-C로 파일을 교환하며 필요한 암호문에 생체 인증을 추가합니다. Original의 NFC나 Bluetooth 절차를 BIT에 적용하지 마세요.

기기에는 설정 외에 암호화, 복호화, 지갑 생성, 서명 기능이 있습니다. Original은 카드 복제를 지원하고 BIT는 USB 매체의 파일을 다룹니다. 표시 문구, 언어, 진입점은 버전에 따라 다릅니다. BIT의 새 '정책 검증'은 호환 절차로 연결될 뿐 승인 주체를 바꾸지 않습니다.

교재가 검토한 기준은 Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21, Mirror beta.12.12입니다. 자료에 따른 기준이며 각 조합의 서명, 배포, 실물 인수 검증은 담당팀과 확인해야 합니다. 엔지니어링 패키지의 서명 없는 바이너리로 펌웨어를 교체하지 마세요.

사용 전 출처, 봉인, 외관, 버전을 확인하세요. 유통 이력과 업데이트 서명은 특정 위협에 도움이 되지만 모든 검증을 대신하지 않습니다. 조작 흔적이나 예상 밖의 버전이 있으면 초기화를 멈추고 직접 확인한 지원 채널에 문의하세요.

실습

1. 비밀을 촬영하지 않고 모델과 표시 버전을 기록하세요.
2. 암호화, 복호화, 지갑 생성, PSBT, 설정을 찾으세요. 메뉴 탐색을 위해 삭제나 업데이트를 시작하지 마세요.
3. 강좌에서 Original 또는 BIT 절차를 고르고 실습 중 같은 선택을 유지하세요.

이해 확인

자신의 모델로 작업이 어떻게 들어가고 돌아오는지, 어떤 매체를 덮어쓰기에서 지켜야 하는지 설명하세요.

자주 묻는 질문

누구에게나 BIT가 자동으로 더 안전한가요? 모델은 운영상 선택이 다릅니다. 위협, 복구, 올바른 사용에 따라 답이 달라집니다.

잠시 멈추기

모델과 버전은 개인 노트에 보관하세요. 강좌에는 선택한 모델만 필요합니다.

BIT를 쓰는데 안내서가 기기 자체에서 NFC 카드에 쓰라고 합니다. 어떻게 하나요?

1. 안내서 대상 모델을 확인하고 호환되는 USB 절차를 쓴다.
2. Original 업데이트를 강제한다.
3. 시드를 휴대전화로 보낸다.

> **정답 보기: 안내서 대상 모델을 확인하고 호환되는 USB 절차를 쓴다.**
> 절차는 해당 모델이 실제 사용하는 전송 수단과 일치해야 합니다.

M04

물리적 엔트로피로 시드 생성하기

학습 목표

생성 원리를 배우고 강좌 데이터를 자신의 실제 키로 사용하지 않으면서 절차를 연습합니다.

이해하기

엔트로피는 예측 불가능성입니다. 적절한 주사위를 쓰고 던지기 전에 순서를 정하고 변환 알고리즘이 정확하면 엔트로피를 얻을 수 있습니다. 거부된 결과는 지시대로 다시 던지세요. 최댓값으로 바꾸거나 다른 단어를 고르면 편향이 생깁니다.

검토한 Cuvex 절차는 동전 하나와 주사위 네 개를 씁니다. 동전 값×1,296에 각 주사위 눈에서 1을 뺀 값을 각 자릿수로 하는 6진수를 더합니다. 허용 인덱스는 0~2,047입니다. 결과가 사전 범위 밖이면 동전과 주사위 네 개를 모두 다시 던지세요. 동전 결과를 유지하고 주사위만 던지면 편향됩니다. 검토한 소스의 설명이며 배포 펌웨어마다 화면과 전체 절차를 확인해야 합니다.

좋아하는 단어를 고르는 것과는 다릅니다. 공개 시연 자료로 실제 자금을 보관하지 마세요. 교재에 나오는 시드는 모두 알려진 것으로 간주합니다. 마지막 단어와 검사는 기기의 전체 알고리즘으로 생성해야 하며 니모닉을 손으로 완성하지 마세요.

카메라, 주변의 활성 음성 비서, 화면 녹화, 지켜보는 사람이 없는 곳을 마련하세요. 비밀 입력·검토 중에는 튜터를 멈춥니다. 튜터는 사전에 설명하고 이후 절차를 질문하되 던진 결과나 단어를 듣지 않습니다.

생성 후 백업을 확인하고 모델에 맞게 암호화한 뒤 빈 지갑 복구를 시험하세요. 확인용 주소로 시드를 컴퓨터에 노출하지 않고 일관성을 확인할 수 있습니다. 지침과 모순되는 값을 받거나 예상치 못한 단어를 보이면 사용을 멈추고 버전, 화면, 오류만 기록하세요.

실습

1. 자금 없는 자료로 기기 절차를 따르며 주사위 순서를 정하고 결과를 바꾸지 마세요.
2. 거부되면 화면 지시대로 다시 하고 허용되도록 값을 고치지 마세요.
3. 비공개로 내용을 검토해 사본을 만들고 같은 실습 지갑을 재구성할 수 있는지 확인하세요.

이해 확인

물리적 엔트로피, 정확한 변환, 결과 비밀 유지가 세 가지 별도 요건인 이유를 설명하세요.

자주 묻는 질문

알고리즘을 확인하려고 AI에 던진 결과를 알려 줘도 되나요? 사용할 시드라면 안 됩니다. 지원은 별도의 합성 예시로 합니다.

잠시 멈추기

기기를 안전한 상태로 마치고 쉬는 동안 시드를 화면에 남겨 두지 마세요.

펌웨어가 주사위 입력을 거부했습니다. 절차에 맞는 조치는 무엇인가요?

1. 수동으로 단어를 고른다.
2. 값에 편향을 주지 않고 기기 지시에 따라 다시 한다.
3. 허용될 때까지 수를 줄인다.

> **정답 보기: 값에 편향을 주지 않고 기기 지시에 따라 다시 한다.**
> 거부는 엔트로피 변환의 일부이며 임의 값으로 대체하면 안 됩니다.

M04

Cuvex로 비밀 정보 암호화 및 복호화하기

학습 목표

실습용 암호문을 만들고 복구를 검증합니다.

이해하기

사용하는 절차가 지원하는 BIP39, SLIP39, Monero, 텍스트 중 올바른 유형을 고르세요. 각각 다른 형식입니다. SLIP39 텍스트를 암호화한다고 Cuvex가 그 텍스트를 쓰는 모든 망에서 서명할 수 있는 것은 아닙니다. 비밀 저장과 서명 프로토콜 실행은 범위가 다릅니다.

연결 기기 밖에 비밀을 두려면 본체에 직접 입력하세요. 휴대전화나 PC에서 가져오면 나중에 암호화해도 원본 환경에서 이미 노출됐을 수 있습니다. 사전 검토 화면에서 단어, 순서, 대소문자, 잘못 입력한 필드를 찾아내세요.

암호문 비밀번호는 길고 고유하며 자신의 계획에 따라 복구할 수 있어야 합니다. 검토한 생성 키보드는 최대 40자이고 검증기는 12자 이상, ASCII 대문자·소문자, 숫자, 인식되는 기호를 요구합니다. Desk의 12~1,024자 정책을 Cuvex 키보드에 그대로 적용하지 마세요. 다른 복구 필드는 제한이 다를 수 있으므로 절차와 버전을 확인하세요.

Original에서는 적합한 빈 카드에 쓰고 확인될 때까지 움직이지 마세요. BIT에서는 해당하는 생체 인증 구성 요소를 포함해 USB 절차가 만든 파일을 보관합니다. 추측으로 이름을 바꾸거나 합치지 마세요. 그 뒤 기기에서 시험 삼아 읽고 복호화하되 비밀은 튜터에게 알리지 마세요.

실습

1. 인증 정보나 금전적 가치가 없는 연습용 텍스트를 암호화하세요.
2. 매체와 결과 객체를 식별하고 별명과 역할을 비공개로 적으세요.
3. 복호화를 다시 시작하고 신뢰 화면에서 텍스트를 확인한 뒤 표시를 닫으세요.

이해 확인

올바른 내용, 성공적인 기록, 성공적인 복구를 구분하세요. ‘파일 복사됨’은 세 가지 전체를 입증하지 않습니다.

자주 묻는 질문

카드 별명이 비밀번호인가요? 아니요. 정리용 정보입니다. 자산을 쉽게 식별할 수 있는 잔액이나 설명을 넣지 마세요.

잠시 멈추기

복호화 내용을 화면에 남기지 말고 실습 성공·실패만 기록하세요.

실습용 암호문에서 내용을 복구할 수 있음을 가장 잘 입증하는 방법은?

1. 예쁜 이름을 붙인다.
2. 파일이 두 폴더에 존재한다.
3. 올바른 경로로 읽고 복호화해 비공개로 내용을 확인한다.

> **정답 보기: 올바른 경로로 읽고 복호화해 비공개로 내용을 확인한다.**
> 사본이 존재한다고 유용성이나 원본과의 일치가 입증되지는 않습니다.

M04

암호화 임계치와 생체 인증

학습 목표

비밀을 공동 보호하는 방식과 비트코인 멀티시그를 구분합니다.

이해하기

여러 비밀번호로 보호된 암호문은 누가 내용을 복호화할 수 있는지 정합니다. 비트코인 멀티시그는 망에서 지출을 승인하는 데 어떤 키가 필요한지 정합니다. 단일 서명 지갑의 비밀을 공동으로 암호화하거나 멀티시그의 각 서명자가 개별 암호문을 가질 수 있습니다.

여러 사람이 함께 시드 하나를 열더라도 그 시드만으로 지출할 수 있으면 체인 임계치는 키 하나입니다. 공개된 뒤 누군가 사본을 남길 수 있습니다. 매 결제마다 여러 서명이 필요한 방식이라고 설명하지 마세요.

BIT 생체 인증은 해당 형식에서 접근 조건을 추가합니다. 손가락은 시드도 모든 비밀번호의 대체물도 아닙니다. 부상, 지문 변화, 고장, 기기 가용성, 상속을 고려하고 그 암호문의 문서화된 복구 경로를 보관·검증한 뒤 의존하세요.

긴급 복구용 내보내기는 컴퓨터에 비밀을 드러낼 수 있습니다. 그런 기능이 있다고 PC가 본체와 동등한 환경이 되는 것은 아닙니다. 일상 운용은 격리를 유지하고 로컬 복구는 영향을 이해한 뒤 노출 시 이전 계획과 함께 검토하세요.

실습

1. ‘시드를 열기 위한 비밀번호 두 개’와 ‘지출에 키 세 개 중 두 개’라는 두 정책을 그리세요.
2. 자금 없는 시험에서 생체 인증 사본에 필요한 파일과 복구 확인 위치를 찾으세요.
3. 한 사람이 부재한 상황을 가정하고 자신의 방식이 임계치를 충족해 계속할 수 있는지 판단하세요.

이해 확인

누가 비밀을 알 수 있고 복호화 후 누가 지출을 승인할 수 있는지 설명하세요.

자주 묻는 질문

라벨을 바꾸면 참여자를 제외할 수 있나요? 아니요. 정리 변경, 비밀 보호 변경, 지출 정책 변경을 구별해야 합니다.

잠시 멈추기

실명이나 생체 정보 없이 도식을 보관하세요.

세 사람이 비밀번호 두 개로 단일 서명 시드 하나를 담은 암호문을 엽니다. 비트코인 지출에는 키 몇 개가 필요한가요?

1. 지갑 정책이 단일 서명이면 하나.
2. 파일에 비밀번호 두 개가 필요했으니 둘.
3. 사람이 셋이니 셋.

> **정답 보기: 지갑 정책이 단일 서명이면 하나.**
> 암호화 임계치는 코인을 통제하는 스크립트를 바꾸지 않습니다.

M04

사본 복제, 보관 및 검증

학습 목표

유효한 유일한 사본을 손상하지 않고 중복 사본을 마련합니다.

이해하기

암호문 복제는 암호화된 데이터를 복사합니다. 새 잔액이나 시드를 만들거나 노출된 비밀번호로부터 독립시키지 않습니다. 동일 사본은 매체 분실에 대비하지만 원래 비밀의 침해는 해결하지 못합니다. 복구와 새 키로의 이전은 다른 상황에 대응합니다.

Original에서는 암호문 카드와 PSBT 전송 카드를 구별하세요. 작업용 매체는 절차에 따라 재사용할 수 있지만 백업 카드를 전용하지 마세요. 암호문이 든 카드가 거부되면 보호를 우회하거나 헤더를 직접 지우지 마세요.

BIT 사본은 필요한 파일 전체와 파일 간 관계를 유지해야 합니다. 파일 관리자에 전송 완료가 표시돼도 기기가 내용을 검증하거나 처리를 끝냈다는 보장은 없습니다. 안내된 상태를 기다리고 통제된 복구로 사본을 검증하세요.

눈에 띄지 않는 식별자, 형식 버전, 마지막 시험 날짜와 결과를 개인 목록에 보관하세요. 정한 사고에 대비해 최소 두 사본을 분리합니다. 진단을 위해 지원 채널에 백업을 올리지 말고 민감한 정보를 뺀 메타데이터와 오류 코드만 제공하세요.

실습

1. 올바른 경로로 실습 암호문을 다른 매체에 복사하세요.
2. 원본 매체를 분리하고 사본에서 시험 텍스트를 복구하세요.
3. 분실, 파일 손상, 비밀번호 노출에 대한 대응을 각각 기록하세요. 같은 절차가 아닙니다.

이해 확인

시험한 사본을 식별하고 원본이 덮어써지지 않은 이유를 설명하세요.

자주 묻는 질문

두 번째 파일이 보이면 원본을 지워도 되나요? 먼저 복구와 범위를 검증하세요. 단순한 사본 수가 아니라 계획에 따라 삭제해야 합니다.

잠시 멈추기

세션 종료 전 매체를 보관하고 결제 실습 카드와 섞이지 않게 하세요.

비밀번호를 아는 사람이 암호문 사본을 얻었습니다. 사본 세 개를 더 만들면 무엇이 해결되나요?

1. 공격자의 사본이 취소된다.
2. 중복성은 늘지만 이미 얻은 접근권은 취소되지 않는다.
3. 비트코인 시드가 자동 변경된다.

> **정답 보기: 중복성은 늘지만 이미 얻은 접근권은 취소되지 않는다.**
> 복제는 이미 발생한 침해를 해소하지 않습니다.

M05

Cuvex Desk 설치 및 보호

학습 목표

출처를 확인한 설치본을 실행하고 로컬 저장소를 보호합니다.

이해하기

배포된 것 중 운영체제와 아키텍처에 맞는 패키지를 고르세요. macOS는 Intel 또는 Apple Silicon, Windows와 Linux는 각각 x64 또는 ARM64입니다. 소스 ZIP, Manager용 패키지, 고객용 설치 파일은 다릅니다. 비공개 서명용 패키지로 수강생을 안내하지 않습니다.

출처와 운영체제의 검사를 확인하세요. Windows 개발용 서명만으로 게시자에 대한 공적 신뢰가 성립하지 않습니다. Mac의 앱 서명, 공증, 실행 시 평가는 별도 검사입니다. 지원팀을 사칭한 전화에 따라 전반적인 보호를 끄지 마세요. 예상 밖의 경고가 나오면 문구를 기록하고 공식 채널을 쓰세요.

Desk는 비밀번호로 암호화한 로컬 저장소를 만듭니다. 검토한 버전의 새 비밀번호는 12~1,024자이며 확인란이 있으면 값이 일치해야 합니다. 길이만으로 강도를 보장하지 않습니다. 고유한 문구를 쓰고 재사용하지 마세요. 컴퓨터 생체 인증은 지원되는 경우 별도 설정하는 접근 편의 기능입니다.

비활동 시 잠금과 필요한 경우 백그라운드 전환 시 잠금을 설정하세요. 실패 후 지연과 선택적 삭제는 설명서에서 다룹니다. 시연 중 자동 삭제를 켜지 마세요. 일반 계정 없이 작동할 수 있지만 조회, 채팅, 다운로드는 각각의 요건과 통신이 있습니다.

실습

1. 튜터에게 비공개 식별자를 주지 않고 플랫폼, 표시 버전, 패키지 출처를 검증하세요.
2. 실습 저장소를 만들고 잠금·다시 열기를 확인하세요. 비밀번호는 비공개로 입력하세요.
3. 암호화 사본을 계획하고 비밀번호를 계획에 따라 보관하세요. 운영 환경에서 반복 잠금 시험을 하지 마세요.

이해 확인

로컬 비밀번호, 상업용 계정, 추가 서비스의 인증 정보를 구별하세요.

자주 묻는 질문

Desk 비밀번호를 바꾸면 카드 비밀번호도 바뀌나요? 아니요. 독립된 보호이며 옛 사본도 저절로 바뀌지 않습니다.

잠시 멈추기

Desk를 잠그고 인증 정보 없이 강의 ID만 보관하세요.

설치 프로그램이 아키텍처에 맞지 않습니다. 첫 조치는 무엇인가요?

1. 보호 기능을 끄고 강제로 실행한다.
2. 알맞은 공식 패키지를 구해 요구 사항을 확인한다.
3. 계속하려고 웹사이트에 시드를 입력한다.

> **정답 보기: 알맞은 공식 패키지를 구해 요구 사항을 확인한다.**
> 수탁 자료를 쓰기 전에 호환성과 출처를 확인합니다.

M05

암호문 연결과 WOW 정리

학습 목표

암호화된 사본을 연결하고 이를 관찰 전용 계정과 구별합니다.

이해하기

Desk는 NFC, USB, 호환 백업 파일로 연결한 암호문을 정리합니다. 시각 디자인과 별명은 구별에 도움을 주지만 암호학적 신원 증거는 아닙니다. 세부 화면에서 출처, 형식, 크기, 접근 조건 등 앱이 해석한 속성을 볼 수 있습니다.

연결은 호환 객체를 가져오거나 정리하는 작업이며 PC에서 복호화하거나 비밀을 확인하는 과정이 아닙니다.
WOW는 호환되는 공개 정보로 연결한 관찰 전용 지갑입니다. 같은 비밀 집합에도 서로 다른 계정이나 파생이 있을 수 있으므로 관리하려는 지갑과 일치시켜야 합니다.

기기 절차에서 내보낸 디스크립터 또는 공개 정보로 계정을 활성화하거나 가져오세요. 망, 스크립트 유형, 지문, 경로, 확인 주소를 검토합니다. 이름은 정리용입니다. 이름에서 얻은 ID는 예측 가능한 이름을 추측할 수 있으므로 강한 익명화가 아닙니다.

검토한 Desk는 연결 대기 계정을 보관하며 사본 내보내기, 복제, 로컬 기록 삭제를 제공합니다. 화면에서 카드를 삭제해도 외부 사본이 없어지거나 자금이 이동하지 않습니다. ‘백업 없음’은 앱의 기준으로 백업을 확인하지 못했다는 뜻이며 어디에도 사본이 없다는 뜻은 아닙니다.

실습

1. 선택한 전송 수단으로 실습 암호문을 연결하고 세부 화면을 검토하세요.
2. 호환 실습 계정을 가져오고 튜터에게 키를 보이지 않은 채 망과 확인 주소를 점검하세요.
3. 암호문 기록, WOW 계정, 물리 매체를 구별하고 로컬 삭제로 무엇이 없어지는지 확인하세요.

이해 확인

Desk의 관찰에 필요한 데이터와 일반 사용 중 PC 밖에 둬야 할 데이터를 설명하세요.

자주 묻는 질문

.bin 파일을 연결하면 내 시드임을 보장하나요? 아니요. 출처와 복구를 확인해야 합니다. 확장자는 내용을 인증하지 않습니다.

잠시 멈추기

‘연습 연결 검증 완료’ 상태만 보관하세요.

WOW 계정을 로컬에서 삭제하면 비트코인이 이동하나요?

1. 아니요. 절차에 따라 로컬 정보만 지우고 UTXO를 쓰지 않는다.
2. 네. 제조사로 보낸다.
3. 다른 사람이 보관하는 모든 서명도 취소된다.

> **정답 보기: 아니요. 절차에 따라 로컬 정보만 지우고 UTXO를 쓰지 않는다.**
> 로컬 상태와 체인 상태는 다릅니다.

M05

Mirror와 Desk 연결하기

학습 목표

코드를 혼동하지 않고 승인된 로컬 연결을 설정하고 종료합니다.

이해하기

Mirror는 앱이 표시하는 연결, PIN, QR 절차로 Desk와 로컬 작업을 수행합니다. 6자리 PIN은 해당 세션용이며 Desk나 암호문 비밀번호, 복구 단어가 아닙니다. 어느 화면에서 생성해 어디에 입력하는지 확인하고 모르는 사람이 보낸 코드는 쓰지 마세요.

Desk의 올바른 화면에서 시작하세요. 연결, QR 읽기, PSBT 전달, 펌웨어 작업은 목적이 다릅니다. 창은 검색, 연결, 발견, PIN, QR, 카드·파일 작업을 안내합니다. 검색에 기기가 보였다고 전체 작업이 끝난 것은 아닙니다.

운영체제와 용도에 맞게 광학 읽기에는 카메라, 필요한 경우 Bluetooth나 NFC 권한을 허용하세요. 물리 기능이 없는 전화에 소프트웨어를 설치해도 생기지 않습니다. iOS는 어댑터와 검증에 차이가 있으며 빌드 가능한 프로젝트가 모든 iPhone에 배포·검증된 것은 아닙니다.

실패하면 미발견, 연결 실패, PIN 거부, QR 판독 실패, 카드 읽기 실패, 응답 미수신 중 정확한 단계를 찾으세요. 예전 세션을 닫고 버전 호환성과 권한을 확인한 뒤 통제된 방식으로 재시도합니다. PIN 오류 때문에 펌웨어를 바꾸거나 다른 곳에 시드를 입력하지 마세요.

실습

1. Desk에서 시험 읽기를 시작하고 로컬 화면을 통해 Mirror를 연결하세요.
2. 연습 QR이나 카드를 제시하기 전에 목적을 확인하세요.
3. 세션을 취소하고 이전 맥락의 뒤늦은 읽기가 적용되지 않는지 확인한 뒤 새 세션을 여세요.

이해 확인

활성 코드나 민감한 내용을 공개하지 않고 실패 단계와 관련 기기를 설명하세요.

자주 묻는 질문

Mirror를 항상 연결해야 하나요? 작업에 따라 다릅니다. 상시 서비스처럼 취급하거나 종료·백그라운드 전환 후에도 세션 승인이 유지된다고 가정하지 마세요.

잠시 멈추기

연결 세션을 닫고 쓰지 않는 앱을 잠그세요.

PIN이 뜨기 전에 연결이 실패하면 튜터는 어떻게 하나요?

1. 시드를 요구한다.
2. 기기 검색, 권한, 세션, 버전을 확인한 다음 진행한다.
3. 연결됐다고 처리한다.

> **정답 보기: 기기 검색, 권한, 세션, 버전을 확인한 다음 진행한다.**
> 확인한 단계에 맞춰 진단하며 연결에 성공했다고 지어내지 않습니다.

M05

Mirror를 통한 NFC, USB-C 및 QR 읽기

학습 목표

각 전송 방식의 용도를 지키고 필요한 검사를 수행합니다.

이해하기

Cuvex Desktop의 NFC 작업에는 호환 스마트폰의 Cuvex Mirror를 Bluetooth로 컴퓨터에 연결해야 합니다. Cuvex Desktop은 외장 USB NFC 리더기를 지원하지 않습니다. 카드의 종류, 형식, 용량도 호환되어야 합니다. 작은 카드에 암호문이 들어가더라도 이전 거래를 포함한 PSBT는 안 들어갈 수 있습니다. 실제 한도는 수취인 수뿐 아니라 전체 내용에 따라 달라집니다. 백업 카드를 전송 카드로 전용하지 마세요.

Original에서는 Mirror가 작업 카드에 요청을 쓰면 기기가 이를 처리해 응답을 기록하고, Mirror가 그 응답을 Desk로 반환합니다. 쓰기 확인은 Desk가 받았다는 뜻이 아닙니다. 기기에 결과가 표시될 때까지 카드를 움직이지 마세요. 인식된 암호문을 보호하기 위해 작업이 거부되면 그 결정을 따르세요.

BIT는 USB 교환용 볼륨 또는 폴더를 사용합니다. 처리 중 볼륨이 마운트 해제됐다가 다시 나타날 수 있습니다. Desk에서 올바른 매체를 선택하고 응답을 검증해 정해진 수신 확인을 보내야 합니다. PC의 같은 이름 폴더에 파일을 복사해도 기기에 전달된 것은 아닙니다.

QR이 읽히지 않으면 초점, 반사, 크기, 흔들림, 정보 밀도를 살펴보세요. 표시를 확대하고 조명과 거리를 조절하세요. 긴 식별자를 앞 글자만으로 대체하거나 일부만 옮겨 적은 값을 받아들이지 마세요. 스캔 성공은 내용의 의미를 검증하는 첫 단계입니다.

실습

1. 교육 자료의 그림에서 Original과 BIT 각각의 요청, 매체, 응답을 식별하세요.
2. QR 읽기를 취소해 뒤늦게 들어온 값이 저장되지 않는지 시험하세요. 다른 용도로도 반복하세요.
3. 너무 큰 파일을 가정하고 검증을 빼지 않으면서 거래를 단순화하거나 호환 매체를 골라야 하는 이유를 설명하세요.

이해 확인

읽기, 쓰기, 검증, 수신, 수신 확인 중 어느 단계를 어떤 기기가 확인했는지 설명하세요.

자주 묻는 질문

해시나 복사 성공 표시 ‘OK’가 비트코인 수취처가 올바르다는 증거인가요? 아니요. 서명기에서 거래와 출력을 검토해야 합니다.

잠시 멈추기

백업 카드를 꺼내 보관하고 전송용 매체를 구별해 두세요.

Original이 카드에 응답을 썼다고 표시합니다. Desk가 받았다고 하려면 무엇이 더 필요한가요?

1. 카드 색을 바꾼다.
2. 새 시드를 만든다.
3. 정해진 절차로 응답을 읽고 Desk에서 검증한다.

> **정답 보기: 정해진 절차로 응답을 읽고 Desk에서 검증한다.**
> 쓰기 성공과 수신 성공은 서로 다른 사건입니다.

M05

공개 제공자와 자체 노드

학습 목표

조회 출처를 선택하고 정보 노출 가능성과 한계를 이해합니다.

이해하기

Desk는 호환되는 공개 제공자나 사용자가 설정한 Bitcoin Core를 조회할 수 있습니다. 제공자는 요청과 그 순서, 연결 정보를 알 수 있습니다. xpub 전체를 보내지 않으면 특정 노출은 줄지만 스크립트나 해시도 서로 연계될 수 있습니다.

Desk 9.21은 REST나 자체 노드 외에 TLS를 통한 Blockstream Electrum을 명시적으로 선택할 수 있습니다. TLS는 일부 망 관찰자로부터 채널을 보호하지만 제공자는 조회 내용을 받습니다. 보이지 않는 순환으로 익명성이 보장되지는 않습니다. 편의와 맞바꾸는 프라이버시를 이해하고 선택하세요.

Core에서는 해당 안내서에 따라 엔드포인트, 인증, 관찰 전용 지갑을 설정합니다. 앱이 '보게' 하려고 RPC 포트를 인터넷에 공개하지 마세요. 신뢰 환경으로 접근을 한정하고 적절히 보호된 전송 경로를 사용하세요. RPC 비밀번호를 튜터에게 읽어 주지 마세요.

초기 동기화와 재검색에는 시간이 걸릴 수 있습니다. 진행률은 작업 상태로, 완료를 미리 보장하지 않습니다. Desk는 백그라운드로 작업하므로 화면을 닫아도 노드는 멈추지 않습니다. 문서의 최소 이력 기간이 더 오래된 활동의 발견을 보장하지 않습니다. 오래된 지갑은 가져온 날짜와 실제 검색 범위를 확인하세요.

탐색은 양의 잔액이 아니라 이력에 근거합니다. 잔액을 다 쓴 주소도 사용된 주소입니다. 검토한 멀티시그는 분기별·참여자별로 이력 없는 연속 20개 주소의 갭을 적용하고 발급 한도도 둡니다. 모든 지갑에 하나의 한도를 일반화하지 마세요.

실습

1. 학습용 출처를 정하고 어떤 정보를 볼 수 있는지 설명하세요.
2. 마지막 동기화 시각, 망, 진척을 확인하세요. HTTP 429면 기다리고 의도 없이 제공자를 바꾸지 마세요.
3. 잔액 0이지만 오래된 이력이 있는 지갑을 모의로 만들고 '0'과 '미사용'의 차이를 확인하세요.

이해 확인

선택한 출처가 검증·프라이버시 요구를 충족하는지 결정하고 미완료 상태를 알아보세요.

자주 묻는 질문

자체 노드면 익명인가요? 아니요. 조회 의존성은 줄지만 연결, 상대, 전파, 기타 메타데이터를 고려해야 합니다.

잠시 멈추기

제공자 유형과 검색 완료 필요 여부만 기록하세요.

받은 자금을 모두 써서 잔액이 0인 주소를 지갑 탐색 시 어떻게 취급하나요?

1. 이력이 있는 주소.
2. 한 번도 쓰지 않은 주소.
3. 유효하지 않은 주소.

> **정답 보기: 이력이 있는 주소.**
> 사용 여부는 현재 잔액이 아니라 이력으로 판단합니다.

비트코인 받기와 주소 확인

학습 목표

입금 요청을 만들고 전달하기 전에 검증합니다.

이해하기

올바른 WOW 계정을 열어 망과 정책을 확인하고 입금 요청을 생성하거나 다시 불러오세요. 정리를 위해 목적, 관찰자, 예상 금액을 추가할 수 있습니다. 이는 로컬 정보이며 예상액을 적어도 다른 금액을 보내는 것을 막지 않습니다.

기기에서 지원하는 경로와 지갑 맥락을 통해 주소를 확인하세요. 해당 조합의 실물 검증이 안 됐다면 실습은 시뮬레이션에 그치고 큰 자금을 받기 전에 담당자에게 확인합니다. 한 출처의 두 화면을 비교해도 독립 검증이 되지 않습니다.

가능하면 새로운 수금 관계에 새 주소를 쓰세요. 검토한 멀티시그에서는 지급인이 나중에 쓸 수 있어 이미 표시된 주소를 재할당하거나 만료시키지 않습니다. 이력 없는 새 주소의 연속 발급 한도에 이르면 적절한 이전 요청을 다시 불러오고 한도의 이유를 이해하세요. 인덱스를 되감지 마세요.

공유 후 자신이 사용하는 검증 출처에서 입금을 확인하세요. 이메일, 거래소 증빙, 지급인 화면은 정산 완료를 입증하지 않습니다. 위험에 맞춰 망, txid, 출력, 금액, 확인 수를 점검하세요. 조회를 비공개로 유지해야 한다면 편의상 공개 탐색기에 주소를 입력하지 마세요.

실습

1. 실습 입금 요청을 만들고 계정과 망을 확인한 뒤 주소를 어떻게 검증할지 설명하세요.
2. 가상 라벨을 기록하고 화면을 닫은 뒤 같은 요청을 다시 불러오세요.
3. 다른 금액의 입금을 가정해 이력을 바꾸지 않고 어떻게 대조할지 정하세요.

이해 확인

주소 생성, 주소 검증, 요청 공유, 입금 확인을 구별하세요.

자주 묻는 질문

새 주소를 만들면 기존 주소가 작동하지 않나요? 보통은 계속 작동합니다. 탐색 정보와 요청 기록을 유지하면 늦은 입금도 확인할 수 있습니다.

잠시 멈추기

실습 요청의 상태만 보관하고 튜터에게 내용은 남기지 마세요.

지급인이 ‘출금 완료’ 화면을 보냈습니다. 수금 인정 전에 무엇을 확인하나요?

1. 화면 화질만.
2. 신뢰할 수 있는 네트워크 출처에서 해당 출력과 필요한 확인 수.
3. 지급인의 비밀번호.

> **정답 보기: 신뢰할 수 있는 네트워크 출처에서 해당 출력과 필요한 확인 수.**
> 업체 증빙이나 화면 캡처가 결제 검증을 대신하지 못합니다.

M06

UTXO 라벨 지정, 동결 및 선택

학습 목표

서로 다른 출처의 자금을 실수로 섞지 않도록 입력을 준비합니다.

이해하기

라벨에는 체인에 없는 출처, 상대, 목적, 사용 제한을 기록할 수 있습니다. Desk의 UTXO 라벨과 주소 메모는 길이와 기능이 다를 수 있습니다. '고객 A'로 충분할 때 신분증이나 실명을 기록하면 불필요하게 민감한 기록이 됩니다.

Desk에서 UTXO를 동결하면 일부 로컬 선택에서 제외됩니다. 비트코인 지출이 차단되거나 스크립트가 바뀌지 않으며 키를 가진 다른 앱은 쓸 수 있습니다. 총잔액과 가용 잔액이 달라질 수도 있습니다. 동결, 초안 예약, 실제 지출 여부를 구분하세요.

자동 선택은 알고리즘과 상황에 따라 최적화하며 사용자의 사적 관계까지 알지는 못합니다. 결제할 때 저축·급여·사업 자금을 합치기보다 같은 맥락의 출력을 고를지 검토하세요. 분리를 유지하려면 라벨뿐 아니라 이후에도 일관되게 사용해야 합니다.

BIP329 라벨 내보내기는 보관과 이전에 유용합니다. 형식 자체에는 암호화가 없습니다. Desk의 암호화된 내보내기와 호환 평문 파일을 구별하세요. 가져올 때는 덮어쓰기 전에 지갑 일치 여부와 동결 정보 처리 방식을 확인하세요.

실습

1. 가상 UTXO 세 개에 저축, 사업, 기부 라벨을 붙이세요.
2. 하나를 동결하고 관찰 잔액과 선택 가능한 잔액의 차이를 확인하세요.
3. 실습 라벨을 비밀번호로 내보내 사본에 가져오고 실제 비공개 데이터 없이 결과를 검토하세요.

이해 확인

비용과 노출 측면에서 입력 선택을 설명하고 동결이 로컬 설정임을 이해하세요.

자주 묻는 질문

결제하면 라벨이 수취인에게 전달되나요? 로컬 라벨이라는 이유만으로는 아닙니다. 내보내기, 파일 공유, 다른 서비스, 메시지에 추가하는 과정에서 노출될 수 있습니다.

잠시 멈추기

실습 라벨과 동결 상태를 보관하세요.

Desk에서 UTXO를 동결하면 어떻게 되나요?

1. 네트워크 합의로 지출이 금지된다.
2. 특별 계정으로 이전된다.
3. 앱의 입력 선택에 로컬 제한이 적용된다.

> **정답 보기: 앱의 입력 선택에 로컬 제한이 적용된다.**
> 다른 키 사본의 지출 능력이 취소되지는 않습니다.

M06

결제 준비 및 검토

학습 목표

내용을 이해할 수 있는 PSBT를 구성하고 모든 비용과 출력을 확인합니다.

이해하기

계정, 지출 가능한 입력, 수취인, 금액을 고르고 요청 출처를 검증하세요. 붙여 넣거나 스캔할 때 주소 전체와 망을 확인합니다. 클립보드와 이미지는 바뀔 수 있으므로 전체 확인이 가능하면 앞뒤 몇 글자에만 의존하지 마세요.

수수료율을 고르고 절대 수수료, 예상 크기, 총액, 거스름돈을 확인하세요. '전액 보내기'에서는 Desk가 가용액에서 수수료를 뺍니다. 채팅 요청에서 순액이 요청액에 못 미치면 일부 결제임을 알고 실행해야 합니다. 차이를 숨기려고 원래 요청이 변경되지는 않습니다.

거스름돈이 작거나 거스름돈 출력이 없는지도 보세요. 본인 소유 표시를 조율자의 명칭이 아닌 정책으로 확인합니다. 거스름돈 생성이 어려우면 전액 송금을 재검토하거나 호환 입력을 추가하세요. 조용히 과도한 수수료로 바뀌는 것을 받아들이지 마세요.

PSBT는 정보와 서명을 전달하는 형식으로 프라이버시나 출처의 진위를 자동 보장하지 않습니다. 이전 거래, 공개키, 경로, 메타데이터를 포함할 수 있습니다. 검토한 Final 펌웨어의 멀티시그는 PSBT v0/BIP174를 사용합니다. '거래 버전 2'는 'PSBT 버전 2'가 아닙니다.

실습

1. 시뮬레이터에서 입력 120,000 sat, 수취인 70,000 sat, 수수료 1,000 sat의 결제를 구성하세요.
2. 모든 출력을 열거하고 거스름돈 49,000 sat를 설명하세요. 전액 송금으로도 반복하세요.
3. 초안을 취소하고 로컬에서 취소한 대상을 설명하세요. 시뮬레이터로 서명하거나 발행하지 마세요.

이해 확인

내보내기 전 무엇이 들어오고 나가며 누가 받고 얼마가 들고 어떤 승인이 남는지 설명하세요.

자주 묻는 질문

표시 잔액을 전부 보낼 수 있나요? 앱이 수수료를 충당할 수 있는 실행 가능한 순액을 계산할 때만 가능합니다. 잔액에 쓸 수 없는 코인이 포함될 수 있습니다.

잠시 멈추기

연습 초안을 저장하거나 취소하세요. 실제 PSBT는 강좌 포털에 남기지 마세요.

화면에 ‘transaction version 2’라고 표시됩니다. 파일이 PSBT v2라는 증거인가요?

1. 아니요. 서로 다른 버전 필드입니다.
2. 네, 항상 그렇습니다.
3. Taproot 사용을 증명합니다.

> **정답 보기: 아니요. 서로 다른 버전 필드입니다.**
> BIP370은 컨테이너 버전과 거래 버전을 구분합니다.

M06

Original과 BIT로 서명하기

학습 목표

모델별 서명 절차를 마치고 정확한 거래에 연결된 응답을 받습니다.

이해하기

Original에서는 Cuvex Mirror와 지원되는 전송 카드를 사용해 PSBT를 전달합니다. 기기에서 요청을 읽고 암호문을 제시한 뒤 비공개로 잠금을 해제하세요. 모든 출력, 금액, 거스름돈, 수수료를 확인하세요. 응답이 카드에 기록되면 Desk에서 다시 읽고 검증합니다. 카드에 기록되었다고 이 반환 과정을 생략할 수 없습니다.

BIT에서는 올바른 볼륨을 선택하고 USB-C로 요청을 전달합니다. 사용자가 기기를 조작하는 동안 Desk 로컬 서비스가 교환 절차를 처리합니다. 화면에 따라 암호문을 제시하고 BIT에서 확인하세요. ‘BIT에서 받기’로 응답을 가져오면 Desk가 검증·저장한 뒤 수신을 확인합니다. 연결이 끊기면 비슷해 보이는 다른 작업이 아니라 같은 작업을 복구하세요.

Final 펌웨어의 멀티시그 서명에서는 요약과 필수 출력, 해당 경고를 검토하고 ‘PSBT 서명’의 마지막 세 차례 확인을 거칩니다. 선택적 상세 검토에서 추가 항목을 살펴볼 수 있으며 ‘아니요’를 선택해도 필수 검토는 사라지지 않습니다. 독립적인 정책 검증은 별도 경로이며 해당 검토의 범위만 가집니다.

서명하려면 진위를 검증할 수 있는 호환 암호문이 필요합니다. 예전 사본에서 비밀을 복구할 수 있어도 그대로 서명할 수 있다는 뜻은 아닙니다. 기기가 진위 미검증 구형 사본이라고 경고하면 비밀을 복구·확인하고 새 사본을 만든 뒤 서명하세요. 헤더를 변경하거나 거부를 우회하지 마세요.

주소 불일치, 예상 밖의 수수료, 데이터 누락, 다른 네트워크 표시, 기기의 정책 거부가 있으면 취소하세요. 통화를 끝내야 한다는 압박으로 승인하지 마세요. AI는 버튼을 누르거나 최종 확인을 수행하지 않으며 사용자가 확인하지 않은 것을 서명 완료라고 하지 않습니다.

실습

1. 자금 없는 지갑 또는 실물 검증을 마친 실습 환경에서 자신의 모델에 맞는 경로를 따르세요.
2. 최종 확인 직전에 멈추는 연습을 하고 그것이 승인이 아닌 이유를 설명하세요.
3. 응답 반환과 초안의 연관성을 확인하고 BIT에서는 수신 및 수신 확인 상태도 점검하세요.

이해 확인

인증 정보를 밝히지 않고 경로를 설명하며 기기 승인, 응답 가져오기, 거래 발행을 구별하세요.

자주 묻는 질문

오프라인 기기가 입력이 여전히 미사용인지 아나요? 혼자서는 현재 체인 상태를 확인할 수 없습니다. 앱이 네트워크 출처를 통해 최종 거래를 검증해야 합니다.

잠시 멈추기

서명을 중단하면 비밀이 보이지 않도록 하고 절차에 따라 취소하거나 식별할 수 있는 보류 작업으로 남겨 두세요.

BIT가 서명했지만 Desk의 수신 확인이 없습니다. 어떤 상태로 봐야 하나요?

1. 결제가 확실히 발행되었다.
2. 응답 수신 또는 검증 대기 상태다. 같은 작업을 복구한다.
3. 지갑을 잃었다.

> **정답 보기: 응답 수신 또는 검증 대기 상태다. 같은 작업을 복구한다.**
> 서명, 수신, 전파는 별개 단계입니다.

M06

최종화, 전파 및 장애 해결

학습 목표

결제를 중복하지 않고 마무리하며 단계별로 오류를 진단합니다.

이해하기

서명을 가져온 뒤 Desk는 초안과 일치하고 의도가 유지되는지 확인해야 합니다. 멀티시그는 아직 임계치에 못 미칠 수 있고 단일 서명도 가져오기만으로 검토를 생략하지 않습니다. 조건이 갖춰지면 최종화해 전파할 거래를 만듭니다.

최종 검토 후에만 발행하세요. 서버 응답이나 txid는 해당 요청의 결과를 나타내지만 추적을 통해 수용과 체인 상태를 확인해야 합니다. 앱이 응답을 받지 못했다면 반복하기 전에 조회하세요. 표시 문제를 해결하려고 새 결제를 만들지 마세요.

대기 중이면 수수료율, 유효성, 충돌, 실제 RBF 가능 여부를 확인하세요. 정책이나 수취처가 바뀐 새 제안에는 적절한 새 서명이 필요합니다. 로컬 취소는 다른 사람이 가진 서명이나 거래를 없애거나 확인된 거래를 되돌리지 않습니다.

준비, 전송, 잠금 해제, 검토, 서명, 응답 반환, 검증, 최종화, 전파, 확인 단계로 나눠 진단하세요. 시스템, 버전, 모델, 단계, 대략의 시각, 오류 코드를 기록합니다. 진단 정보는 민감한 데이터를 빼도록 설계됐지만 공유 전 직접 검토하고 사본, QR, 채팅 키, 인증 정보를 첨부하지 마세요.

실습

1. 가상 결제의 상태를 순서대로 놓고 안전하게 멈출 지점을 찾으세요.
2. 잔액 부족, USB 응답 미수신, 발행 중 연결 중단 세 사례를 해결하세요.
3. 합성 데이터와 검증 가능한 기대 결과로 문의 티켓을 작성하세요.

이해 확인

수강생, 기기, 조율자, 망 중 누구의 조치가 필요한지 판단해 불필요한 두 번째 결제를 피하세요.

자주 묻는 질문

FIRMWARE_CAPABILITY_REQUIRED면 무작정 펌웨어를 바꾸면 되나요? 아니요. 문서화된 Desk 사례에서는 Final 빌드를 인식하도록 Desk 목록을 수정해야 했습니다. 기기를 바꾸기 전에 버전과 프로필을 확인하세요.

잠시 멈추기

상태와 다음 조치를 보관하세요. 실습 밖에서 실제 거래를 발행했다면 개인 문서에 기록하세요.

이미 확인된 거래를 단독으로 취소할 수 있는 조치는 무엇인가요?

1. 로컬 초안을 삭제한다.
2. Mirror를 닫는다.
3. 두 조치 모두 아니다.

> **정답 보기: 두 조치 모두 아니다.**
> 로컬 삭제는 체인을 다시 쓰거나 이미 유통된 승인을 회수하지 않습니다.

M07

비트코인에서 관찰할 수 있는 정보

학습 목표

공개 데이터, 추론, 체인 밖에서 자신이 추가하는 정보를 구별합니다.

이해하기

비트코인 온체인은 공개적이어서 스크립트, 표시 가능한 주소, 금액, 입출력 관계, 블록 내 위치를 분석할 수 있습니다. 이름이 직접 나오지 않아도 신원이 확인된 구매, 공개 청구서, 공유한 주소가 본인과 이력을 연결할 수 있습니다.

가명성은 그 자체가 실명이 아닌 식별자로 활동하는 것입니다. 익명성에는 구별할 수 없는 집합과 조건이 필요하며 앱을 설치한다고 얻어지지 않습니다. 상점은 결제를, 거래소는 출금을, 서버는 조회를 알고 누군가는 기기를 볼 수 있습니다. 프라이버시는 맥락에 따라 다릅니다.

사실과 추론을 구별하세요. '이 출력이 그 거래에서 쓰였다'는 체인에서 검증할 수 있습니다. '이 입력들은 모두 한 사람 소유다'는 틀릴 수 있는 경험칙입니다. 체인 밖에서 신원을 확인하면 가설의 신뢰도는 높아지지만 모든 해석이 확실해지지는 않습니다.

주소를 재사용하면 활동을 모아 보기 쉽고 다른 맥락의 UTXO 결합은 관계를 드러낼 수 있습니다. xpub 공개는 주소 하나보다 넓은 관찰을 허용합니다. txid를 공유하면 상대에게 필요 없던 다른 출력과 관계도 보일 수 있습니다.

실습

1. 가상 거래에서 공개 데이터와 자신의 라벨을 구별해 표시하세요.
2. 이름이 적힌 청구서를 더하고 새로 드러나는 관계를 설명하세요.
3. 주소, 디스크립터, 잔액 없이 오류 해결을 위한 지원 요청을 작성하세요.

이해 확인

'관찰된다'와 '추론된다'를 구분하고 어떤 증거가 부족한지 설명하세요.

자주 묻는 질문

주소를 재사용하지 않으면 익명인가요? 아니요. 입력 선택, 거스름돈, 조회, 상대, 기타 메타데이터도 중요합니다.

잠시 멈추기

실제 신원이나 거래 없이 관찰자 관계도를 보관하세요.

한 계정의 주소 묶음을 관찰하는 데 보통 필요한 정보는?

1. 아이콘 색.
2. xpub와 충분한 파생 정보.
3. 케이블 상표.

> **정답 보기: xpub와 충분한 파생 정보.**
> 확장 공개 정보만으로는 지출을 승인하지 못해도 프라이버시에는 민감합니다.

M07

용도 분리와 거스름돈 관리

학습 목표

UTXO 출처에 맞는 지출 결정을 내립니다.

이해하기

맥락 분리는 결제 전부터 시작합니다. 입금이 저축, 업무, 생활비, 특정 관계 중 어디에 해당하는지 정하고 개인 라벨에 보관해 이후 모르고 섞지 않게 하세요.

라벨은 출력을 암호학적으로 분리하지 않습니다. 다른 맥락의 UTXO 둘을 같이 쓰면 거래가 관계를 공개합니다. 통합은 미래 결제의 입력 수를 줄이는 대신 합친 출력 사이의 연결을 강화합니다. 수수료가 낮을 때 통합하면 효율적이면서도 프라이버시 목적에는 어긋날 수 있습니다.

거스름돈은 같은 정책으로 통제하는 새 출력이며 '보이지 않는 돈'이 아닙니다. 나중에 사용하면 이전 관계가 확장될 수 있습니다. 금액이 특이하다고 거스름돈으로 표시하지 말고 실제 검토 시 기기가 지갑 소속을 검증해야 합니다.

프라이버시를 금액, 시간, 반복 송금의 기계적 패턴으로 만들지 마세요. 패턴 자체가 식별될 수 있고 수수료도 늘어납니다. 각 당사자가 아는 정보와 제안 거래가 새로 공개할 정보를 평가하세요. 어떤 절차도 이미 공개된 이력을 지우지 못합니다.

실습

1. 세 맥락의 가상 UTXO 다섯 개를 만들고 필요한 최소한의 맥락만 사용해 결제를 준비하세요.
2. 발생하는 거스름돈을 찾아 어떤 라벨을 붙일지 정하세요.
3. 모든 출력을 합치는 경우와 분리 보관하는 경우의 비용과 노출을 비교하세요.

이해 확인

모든 경우에 절대 규칙을 적용하지 말고 구체적인 이유로 통합을 정당화하거나 거절하세요.

자주 묻는 질문

다른 내 주소로 전부 보내면 이력이 끊기나요? 아니요. 관계 하나를 더 공개하며 위협을 해결하지 않고 비용만 늘릴 수 있습니다.

잠시 멈추기

실습의 판단 근거와 선택한 입력 정책을 보관하세요.

급여와 기부금을 한 거래로 통합하면 어떤 결과가 생길 수 있나요?

1. 입력 사이의 관계가 보인다.
2. 공개된 출처가 사라진다.
3. 익명 현금으로 확실히 전환된다.

> **정답 보기: 입력 사이의 관계가 보인다.**
> UTXO를 줄이면 관찰 가능한 연결이 늘 수 있습니다.

M07

네트워크 프라이버시, Tor와 VPN

학습 목표

연결 프라이버시와 체인 프라이버시를 구별합니다.

이해하기

조회 서버는 요청을 연결과 연계할 수 있습니다. 인터넷 제공자는 전송 방식에 따라 목적지나 패턴을 볼 수 있습니다. VPN은 연결 신뢰 일부를 VPN 운영자에게 옮길 뿐 비트코인 공개 정보를 없애거나 신원 확인 계정이 사용자를 알아보는 것을 막지 못합니다.

Tor는 망을 통해 트래픽을 우회시켜 출발지와 목적지 사이의 일부 연계를 줄입니다. 비트코인 주소가 비공개가 되거나 Tor를 거치지 않는 앱이 보호되지는 않습니다. Tor Browser를 열어도 Desk, Bitcoin Core, 컴퓨터의 모든 서비스가 자동 설정되지는 않습니다.

보호되는 연결이라고 말하기 전에 경로와 설정을 검증하세요. 검토한 버전에서 Desk에 Tor 전환 기능이 있다고 전제하지 않습니다. 노드나 프록시 배포에는 기술 안내와 실제 트래픽 검증이 필요합니다. 다른 지갑에 있다고 존재하지 않는 화면 필드를 가정하지 마세요.

DNS, 계정 동기화, 탐색기 링크, 시세 서비스에서도 정보가 샐 수 있습니다. 잔액 조회를 보호해도 공개 탐색기를 열면 활동이 드러날 수 있습니다. 각 대책의 범위와 연결 실패 시 동작을 정하고 프라이버시가 낮은 제공자로 몰래 전환하지 마세요.

실습

1. 컴퓨터, 인터넷 제공자, 있다면 프록시, 노드 또는 서비스, 비트코인 망까지의 경로를 그리세요.
2. 누가 조회를 받고 누가 거래 고객으로서의 신원을 보는지 표시하세요.
3. 비공개 노드가 응답하지 않는 상황에서 노출을 이해하고 일시 정지 또는 명시적 출처 변경을 선택하세요.

이해 확인

자신의 설정으로 줄어드는 위협과 남는 위협을 설명하세요.

자주 묻는 질문

Tor가 아무도 결제를 나와 연결하지 못하게 보장하나요? 아니요. 상대, 상업적 신원 확인, 패턴, 운영 실수가 연결 고리가 될 수 있습니다.

잠시 멈추기

설계 범위만 기록하고 비공개 엔드포인트나 비밀번호는 기록하지 마세요.

Tor Browser를 열면 Desk 조회도 반드시 Tor를 거치나요?

1. 같은 컴퓨터라서 그렇다.
2. 아이콘이 보이면 그렇다.
3. 아니다. 앱마다 경로를 설정하고 검증해야 한다.

> **정답 보기: 아니다. 앱마다 경로를 설정하고 검증해야 한다.**
> 한 앱의 보호가 다른 앱으로 자동 승계되지는 않습니다.

CoinJoin, Payjoin과 현재의 한계

학습 목표

협업 거래 도구를 이해하고 실제로 제공되지 않는 익명성이나 호환성을 전제하지 않습니다.

이해하기

CoinJoin은 여러 사람의 기여를 한 거래에 모아 입출력에 관한 일부 추론을 어렵게 합니다. 다른 코인을 돌려주겠다는 수탁 서비스에 코인을 맡기는 것과 다릅니다. 설계별로 조율, 수탁, 수수료, 악성 참여자에 대한 내성, 이후 처리를 검토해야 합니다.

Payjoin은 지급인과 수취인의 입력을 협업 결제에 포함해 공통 소유를 추정하는 일부 경험칙을 약화합니다. 양쪽의 호환 지원과 특정 프로토콜이 필요합니다. 기술 이해를 위한 내용이며 검토 자료에서는 Cuvex Desk에 통합되어 작동하는 Payjoin이나 CoinJoin 절차가 입증되지 않았습니다.

제공 여부와 법적 상황은 달라집니다. Wasabi 문서에 따르면 zkSNACKs 코디네이터는 2024년 6월 1일 종료됐습니다. 예전 버튼이 현재 서비스를 보장하는 것처럼 가르치지 마세요. 미국 법무부는 2025년 Samourai 창립자들의 유죄 인정과 이후 선고를 발표했습니다. 이 사건으로 모든 관할에서 모든 프라이버시 기술이 불법이라고 단정할 수 없습니다.

한 추론을 줄여도 다른 추론은 남습니다. 식별된 출처가 상대 기록에서 사라지지 않습니다. 이후 재결합, 메타데이터, 참여자 집합의 실패가 프라이버시를 약화할 수 있습니다. 특정 이력의 코인에 다른 영업 정책을 적용하는 서비스도 있습니다.

실습

1. 실제 거래를 하지 않고 일반 거래, 협업 거래, 자금을 수탁하는 서비스를 비교하세요.
2. 도구 사용을 제안하기 전에 버전, 유지관리자, 서비스 상태, 최신 문서를 확인하세요.
3. 기술·수탁·법률 위험을 각각 식별하세요. 튜터는 통제 회피를 설계하거나 ‘추적 불가능한 자금’을 약속해서는 안 됩니다.

이해 확인

프라이버시 기법의 제한적 이점 하나와 위험 또는 요건을 적어도 두 개 설명하세요.

자주 묻는 질문

Cuvex로 비공개 수탁을 하려면 믹서가 필요한가요? 아니요. 조회, 데이터, 키, UTXO 선택을 관리해도 구체적 위험에 대응할 수 있으며 완전한 은폐를 약속하지 않습니다.

잠시 멈추기

근거 없이 ‘호환’이라고 하지 말고 ‘학습함’으로 기록하세요.

근거가 있는 설명은 무엇인가요?

1. CoinJoin은 영구적 익명성을 보장한다.
2. 협업 기법은 일정 요건과 한계 아래 일부 추론을 어렵게 할 수 있다.
3. 믹서라는 모든 서비스가 자기 수탁을 유지한다.

> **정답 보기: 협업 기법은 일정 요건과 한계 아래 일부 추론을 어렵게 할 수 있다.**
> 특성은 프로토콜, 구현, 참여자, 이후 사용에 따라 달라집니다.

M07

실제 사고에서 얻는 교훈

학습 목표

문서화된 사고를 검증 가능한 결정에 반영합니다. 경쟁사를 공격하거나 보호 효과를 과장하지 않습니다.

이해하기

Mt. Gox에 대한 미국 법무부의 2023년 기소장은 서버와 키에 대한 무단 접근 및 이후 고객 자금 소실을 기술했습니다. 기소장은 혐의에 대한 주장이지 판결이 아닙니다. 수탁의 교훈은 실제 키 통제자가 누구이고 회사가 기능하지 못하면 어떻게 되는지 묻는 것입니다.

2023년 12월 Ledger Connect Kit 사고에서 Ledger는 전 직원의 접근 권한 침해 후 분산형 앱용 라이브러리의 악성 버전이 배포됐다고 기록했습니다. 소프트웨어 공급망이 영향을 받았고 EVM DApps 이용자가 속아 서명했습니다. Ledger 하드웨어나 비트코인 합의가 깨졌다는 증거는 아닙니다.

2025년 2월 Bybit 사건에서 FBI는 약 15억 달러 규모의 가상자산 절도를 북한의 소행으로 지목했습니다. 거래소와 다른 네트워크 자산에 관한 사고이며 비트코인 암호가 깨진 사례가 아닙니다. 서명 의도를 검토하고 여러 사람이 같은 화면을 맹신하지 않는 것이 교훈입니다.

2025년 5월 Coinbase는 사회공학 사기를 돕도록 매수된 지원 담당자에 의한 데이터 절도를 발표했습니다. 비밀번호와 개인 키는 노출되지 않았다고 밝혔습니다. 상대가 실제 정보를 알고 있어도 사기범일 수 있다는 점이 교훈입니다.

Bitcoin Core도 소프트웨어 결함을 공개합니다. CVE-2024-35202 공지는 25.0 이전 버전의 원격 종료 가능성을 설명했습니다. 규칙을 검증해도 소프트웨어 유지보수는 필요합니다. 이 공지로 키 도난을 추론할 수 없습니다.

2026년 1월 The Register는 Global-e를 통해 Ledger 구매자의 주문·연락처 정보가 노출됐으며 양사가 이를 확인했다고 보도했습니다. 해당 설명에서 복구 키는 영향을 받지 않았습니다. 하드웨어가 침해되지 않아도 구매 기록으로 기기 보유가 드러날 수 있습니다.

2026년 4월 The Record는 Drift 공격과 플랫폼이 발표한 입출금 중단을 보도했습니다. Solana상의 탈중앙화 금융 프로토콜에 관한 사례이며 비트코인이 깨진 것이 아닙니다. 초기 추정 손실이나 이후 복구 과정을 확정 금액이나 환불 보장으로 제시하면 안 됩니다.

실습

1. 각 사고를 수탁, 인터페이스 또는 배포, 개인정보, 다른 망의 프로토콜, 가용성으로 분류하세요.
2. 각각 예방책 하나와 그 한계 하나를 제시하세요.
3. ‘당신의 구매를 안다. 이 안전한 주소로 옮겨라’라는 사기 전화를 연습하세요. 끊고 직접 시작한 채널로 확인하세요.

이해 확인

어떤 사고도 다른 브랜드가 무적임을 입증하지 않는 이유를 설명하세요. 증거가 뒷받침하는 범위는 구체적입니다.

자주 묻는 질문

이것이 최신 해킹의 전부인가요? 아니요. 2026년 11월 17일 판을 위해 확인한 사례 선정이며 전체 목록이나 실시간 모니터링이 아닙니다.

잠시 멈추기

바꿀 습관과 이를 지키는지 확인할 방법을 적으세요.

구매 내역을 아는 사람이 '구제용 지갑'으로 송금하라고 합니다. 구매를 안다는 사실은 무엇을 증명하나요?

1. 유출 정보일 수 있으며 신원이나 주소를 인증하지 못한다.
2. 반드시 정식 지원팀이다.
3. 시드를 공유해야 한다.

> **정답 보기: 유출 정보일 수 있으며 신원이나 주소를 인증하지 못한다.**
> 실제 정보도 그럴듯한 사기를 꾸미는 데 쓰일 수 있습니다.

M08

채팅 신원 생성과 연락처 확인

학습 목표

키를 노출하지 않고 채팅 신원을 활성화한 후 상대를 확인합니다.

이해하기

Desk는 Cuvex에서 생성한 채팅 키로 채팅을 암호문에 연결합니다. xpub처럼 보여도 비밀이며 WOW 계정의 공개 키처럼 취급하면 안 됩니다. 튜터가 이를 읽거나 QR로 볼 필요는 없습니다.

새 별명 생성과 기존 별명 이전·복구는 다른 절차입니다. 검토한 구현에서는 해당 iOS 또는 Android 프로필을 선택합니다. 과거 방식으로 파생한 신원을 임의로 서로 바꿔 쓸 수 없기 때문입니다. DEV와 운영 환경은 분리되며 전환해도 대화나 별명이 자동 이전되지 않습니다.

별명을 추가해도 신원이 확인되지는 않습니다. 독립적으로 인증된 채널에서 지문을 대조하세요. 본인 확인 질문이 있으면 비공개 정보를 쓰되 비밀번호가 드러나는 답은 피하세요. 익숙한 목소리도 모방할 수 있으므로 위험 상황에서는 미리 합의한 수단을 조합하세요.

연락처 신원이 바뀌면 원인을 확인할 때까지 결제와 조율을 멈추세요. 정상 복구일 수도 악의적 교체일 수도 있습니다. 종단 간 암호화는 프로토콜과 구현에 따라 채널을 보호하지만 반대편 기기를 누가 사용하는지는 증명하지 않습니다.

실습

1. 시험 환경에서 채팅 키를 제공하지 않고 생성 또는 복구 절차를 설명하세요.
2. 실습 연락처를 추가하고 다른 채널로 지문 검증 방법을 합의하세요.
3. 신원 변경을 모의로 재현하고 결제 전 어떻게 확인할지 정하세요.

이해 확인

별명, 공개 지문, 비밀 채팅 키, 사람에 대한 신뢰를 구별하세요.

자주 묻는 질문

오래된 별명이면 같은 사람임을 보장하나요? 아니요. 연속성과 키 변경을 절차대로 검증해야 합니다.

잠시 멈추기

키나 비공개 질문 없이 ‘실습 연락처 확인 완료’와 방법만 기록하세요.

xpub처럼 생긴 문자열을 채팅 키라고 합니다. Desk에서는 어떻게 취급하나요?

1. 게시판에 공개해도 되는 정보.
2. 신원을 복구하는 비밀.
3. 비트코인 입금 주소.

> **정답 보기: 신원을 복구하는 비밀.**
> 겉보기 형식이 정보의 기밀성이나 용도를 결정하지 않습니다.

M08

채팅에서 사토시 요청 및 결제

학습 목표

요청 맥락과 검토 절차를 유지하며 대화에서 결제로 넘어갑니다.

이해하기

채팅에서 주소를 요청하고 입금 주소로 답하고 결제를 요청하며 WOW 계정에서 결제 준비를 열 수 있습니다. 맥락을 같은 채널에 유지하면 앱 간 복사 오류는 줄지만 모든 메시지가 인증된 지출 명령이 되지는 않습니다.

응답하거나 지급하기 전 검증된 연락처, 망, 금액, 원래 요청을 확인하세요. 공통 양식은 UTXO 선택과 수수료를 유지합니다. '전액 보내기'를 선택하면 수수료 차감 후 금액이 요청액보다 적을 수 있으므로 해당할 때 부분 결제로 명시하세요.

승인은 Cuvex에서 이루어집니다. 채팅은 의도와 조율 정보를 전달하지만 자동 서명 권한은 없습니다. 상대에게 결제 알림을 보낼 때 메시지 수신과 확인된 거래가 실제 존재함을 구별해야 합니다. 수취인은 자신의 계정이나 출처로 검증합니다.

외부 링크, 첨부 QR, 주소는 검증 전까지 신뢰하지 않습니다. 'Mempool에서 보기'는 제삼자 서비스를 열어 조회를 드러낼 수 있습니다. 자체 노드를 쓰는 정책이라면 WOW의 호환 검증을 우선하고 공개 서비스로의 이동을 검토하세요.

실습

1. 수취인이 50,000 sat를 요청하고 지급인이 발행 없이 준비하는 두 역할을 연기하세요.
2. 순가용 잔액 48,000 sat를 가정하고 일부 결제에 필요한 동의와 대조를 설명하세요.
3. 시험 메시지의 망을 의도적으로 바꾸고 절차를 중단하세요.

이해 확인

'채팅에 OK가 떴다'로 끝내지 말고 요청, 주소, 초안, 서명, 확인의 관계를 추적하세요.

자주 묻는 질문

채팅에서 sat를 보내면 Lightning인가요? 아니요. 문서화된 WOW는 비트코인 온체인 결제를 준비합니다. sat는 단위이며 전송망이 아닙니다.

잠시 멈추기

실습 초안을 취소하거나 상태를 기록하세요. 화면을 시연하려고 발행하지 마세요.

채팅에서 확인 메시지를 받았습니다. 수금을 판단하는 결정적 검사는?

1. 메시지 아이콘이 녹색이다.
2. 상대가 '확인됨'이라고 말한다.
3. 적절한 출처에서 네트워크 거래와 출력을 검증한다.

> **정답 보기: 적절한 출처에서 네트워크 거래와 출력을 검증한다.**
> 메시지 상태와 거래 상태는 다릅니다.

M08

암호문을 이해하고 공유하기

학습 목표

암호화한 사본을 타인에게 전달하는 의미를 이해합니다.

이해하기

암호문 공유는 암호화 객체의 사본 전달입니다. 반드시 비트코인을 보내거나 새 서명자를 자동 추가하는 것이 아닙니다. 수취인이 충분한 해제 수단까지 얻으면 방식에 따라 내용에 접근할 수 있으므로 어떤 능력을 이전하는지 미리 정하세요.

채팅 종단 간 암호화와 파일 암호화는 다른 계층을 보호합니다. 다운로드한 상대는 채팅 밖에 사본을 보관할 수 있습니다. 자신의 메시지나 로컬 기록을 삭제해도 모든 사본을 거둘 수는 없습니다. 같은 채널로 비밀번호까지 주면 구성 요소가 한 경로에 모입니다.

전송 전 신원, 형식, 목적을 검증하세요. 받은 암호문 연결 기능은 사본을 정리할 뿐 아무 파일이나 안전하게 복호화할 수 있다는 증거가 아닙니다. 외부 페이지에 시드나 비밀번호를 입력하도록 요구하는 첨부물은 사용하지 마세요.

복구에는 각 구성 요소 보관자와 열 수 있는 사람, 노출 탐지 방법, 관계 종료 시 수탁 변경 방법에 대한 합의가 필요합니다. 일반 결제에는 보통 검증된 주소면 충분하며 자신의 암호문을 공유할 필요가 없습니다.

실습

1. 암호화한 교육용 텍스트를 실습 연락처에 전달하는 절차를 설계하세요.
2. 비밀번호를 알기 전과 후 수취인이 무엇을 알고 무엇을 할 수 있는지 열거하세요.
3. 관계 종료를 가정하고 메시지 삭제로 사본이나 키가 취소되지 않는 이유를 설명하세요.

이해 확인

‘데이터를 공유했다’, ‘비밀 접근권을 공유했다’, ‘지출에 서명했다’를 구별하세요.

자주 묻는 질문

암호화 파일은 아무 영향 없이 유통할 수 있나요? 메타데이터를 드러내고 비밀번호 시도를 쉽게 하며 무기한 보관될 수 있습니다. 공유할 필요성을 평가하세요.

잠시 멈추기

수탁 첨부물을 강좌에 남기지 말고 연습의 결론만 기록하세요.

채팅으로 암호문을 공유하면 비트코인을 보낸 것인가요?

1. 아니다. 내용과 접근 범위가 다른 객체를 전송한 것이다.
2. .bin으로 끝나면 그렇다.
3. 새 멀티시그가 자동 활성화된다.

> **정답 보기: 아니다. 내용과 접근 범위가 다른 객체를 전송한 것이다.**
> 비밀 전송과 UTXO 이동은 다른 작업입니다.

M08

채팅 복구와 메타데이터

학습 목표

기기 변경을 계획하고 신원 복구와 메시지 복구를 구분합니다.

이해하기

Desk는 이력과 세션을 로컬 암호화하고 전체 백업에는 포함하지 않는다고 안내합니다. 채팅 키는 신원을 복구하지만 과거 대화 전체는 보장하지 않습니다. 앱은 활성화 대기, 키 유지관리, 호환 자료가 있을 때 로컬 복구 상태와 작업을 제공합니다.

검토한 안내서에 따르면 별명 하나는 한 번에 기기 하나에서만 사용합니다. 지원되지 않는다면 '동기화 시험'을 위해 두 기기에 동시에 활성화하지 마세요. 이전 절차를 따르고 연락처와 연속성을 확인하세요.

'대기', '서버 수락', '수신', '복호화 실패'는 다른 단계입니다. 확인 안 된 전송은 무작정 재전송하지 말고 먼저 도착 여부를 확인하세요. 세션 키 누락이나 신원 변경 시 대기 메시지를 보관해도 읽었다는 뜻은 아닙니다.

내용을 암호화해도 시각, 크기, 전달 관계, 별명, 연결 정보가 모든 관련 시스템에서 숨겨지는 것은 아닙니다. 음성도 비슷합니다. 전송 암호화만으로 일반 통화가 비밀 전달에 적합해지지는 않습니다. 학습과 문제 해결에 필요한 최소 정보만 사용하세요.

실습

1. PC 분실을 가정하고 각 자료로 무엇을 복구하는지 설명하세요.
2. 메시지 상태를 분류하고 결제 요청을 다시 보내지 말아야 할 때를 판단하세요.
3. 연락처가 독립 채널로 확인할 수 있는 기기 변경 안내를 준비하세요.

이해 확인

백업 범위를 넘는 복구를 약속하지 않고 어떤 대화가 사라지고 어떤 신원을 복원할 수 있는지 설명하세요.

자주 묻는 질문

로컬 채팅을 지우면 반대편 메시지도 삭제되나요? 그렇게 가정하지 마세요. 수취인은 메시지와 파일을 독립적으로 보관할 수 있습니다.

잠시 멈추기

필드 이름만 둔 이전 계획을 보관하고 채팅 키는 넣지 마세요.

검토된 안내서에서 채팅 키 자체가 보장하는 것은?

1. 모든 PC에서 과거 대화 전체 복구.
2. 호환 절차로 신원을 복구할 능력이며 모든 과거 메시지 복구는 아님.
3. 연락처의 비트코인 키에 자동 접근.

> **정답 보기: 호환 절차로 신원을 복구할 능력이며 모든 과거 메시지 복구는 아님.**
> 신원 복구와 과거 기록 보관은 별개의 능력입니다.

M08

일상 설정과 권한 점검

학습 목표

편의성과 보호 효과를 혼동하지 않고 Desk 설정을 관리합니다.

이해하기

Desk에는 야간·주간·시스템 테마, 자동 동기화와 3분 또는 5분 간격, 거래 소리, 채팅 배경, 언어, 기준 통화가 있습니다. 표시나 조회 빈도를 바꾸며 비트코인 서명을 변경하거나 익명성을 더하지는 않습니다.

검토한 보안 설정은 비활동 잠금, 백그라운드 전환 잠금, 실패 후 최대 지연, 선택적 삭제를 제공합니다. 비활동 설정 스키마는 30~86,400초를 허용하지만 화면 선택지는 좁을 수 있습니다. 기본값은 녹화 수업으로 가정하지 말고 실행 중인 버전에서 보세요.

bitcoin: 링크는 잠금 해제, 계정 선택, 검토를 위한 요청을 열며 자동 결제를 승인하지 않습니다. Linux에서 링크 등록은 통합 설치와 AppImage가 다릅니다. Lightning 인보이스에는 별도의 호환 절차가 필요하며 Desk를 기본 앱으로 정한다고 해결되지 않습니다.

시세, 가격 차트, 정보 링크는 외부 서비스를 조회할 수 있습니다. 정보 제공용이며 매수 신호가 아닙니다. 환산 전 날짜와 출처를 확인하세요. 다크 모드 또는 작은 창에서 최종 버튼, 주소, 수수료가 가려지면 멈추고 레이아웃 문제를 보고하세요.

실습

1. 실습 저장소의 외관과 잠금을 조정한 뒤 다시 들어갈 수 있는지 확인하세요.
2. 켜는 자동 기능을 확인하세요. 동기화, 소리, 펌웨어 확인은 서로 다릅니다.
3. 가상 bitcoin: 링크 요청을 열고 실제 거래를 준비하기 전에 취소하세요.

이해 확인

각 설정의 효과를 설명하고 조회나 민감한 작업이 수반되는 항목을 찾으세요.

자주 묻는 질문

PC 생체 인증이 복구 사본을 대체하나요? 아니요. 기기와 운영체제 보안 저장소에 의존할 수 있습니다. 독립 복구 수단을 유지하세요.

잠시 멈추기

Desk를 잠그고 변경한 설정만 기록하세요.

3분마다 동기화하도록 선택하면 무엇이 바뀌나요?

1. 기능이 실행될 때 예정된 조회 빈도.
2. 체인의 서명 정책.
3. 기기의 시드.

> **정답 보기: 기능이 실행될 때 예정된 조회 빈도.**
> 운영 설정이며 수탁 방식이 달라지지는 않습니다.

M09

멀티시그 지갑 설계하기

학습 목표

예상 가능한 분실과 침해를 견디는 서명 임계치를 선택합니다.

이해하기

N명 중 M명 정책에서 N은 서로 다른 키를 가진 참여자 수, M은 필요한 서명 수입니다. 3명 중 2명은 한 키를 쓸 수 없어도 되지만 두 키가 침해되면 지출을 승인할 수 있습니다. 세 시드를 같은 곳에 두거나 같은 노출에서 생성하면 독립성이 줄어듭니다.

검토된 Cuvex 멀티시그는 네이티브 P2WSH, sortedmulti, BIP48 파생을 씁니다. 구조상 정책 키 한도는 Original이 6개, BIT가 15개입니다. 함께 사용하면 더 제한적인 참여자와 실제 전송 용량을 따라야 합니다. 구조상 최대치 이내여도 키와 입력이 많은 정책이 들어간다는 보장은 없습니다.

앱은 정책 관계에 맞는 임계치를 지원하지만 N명 중 1명이면 지출에 협력이 필요하지 않습니다. 펌웨어는 이 위험을 따로 경고합니다. 숫자를 키우면 조율, 비용, 복구 자료, 잠길 가능성도 늘어납니다.

MuSig2는 별도의 Schnorr 서명 집계 방식으로 기본은 N명 중 N명이며 임의의 5명 중 3명이 아닙니다. 검토한 Final 펌웨어에는 Taproot 입력 서명, MuSig2, Miniscript가 구현되지 않았습니다. P2TR를 수취처로 허용해도 Taproot 지갑의 지출을 서명할 수 있다는 증거는 아닙니다.

실습

1. 참여자별 위험이 독립적인 가상 3명 중 2명 구성을 설계하세요.
2. 키 하나 분실과 키 하나 침해를 각각 가정하고 가능한 일과 불가능한 일을 설명하세요.
3. 더 큰 정책을 선택하기 전 모델별 한도를 확인하세요.

이해 확인

설계의 손실 내성, 공격 임계치, 공통 의존성을 설명하세요.

자주 묻는 질문

멀티시그는 서로의 시드를 알아야 하나요? 아니요. 각자 비밀 권한을 유지하고 정책 구성·복구에 필요한 공개 정보만 공유하는 것이 목적입니다.

잠시 멈추기

가상 참여자와 책임을 포함해 설계를 보관하세요.

독립된 키를 쓰는 3명 중 2명 정책에서 유효한 지출을 승인하려면 개인 키가 몇 개 필요한가요?

1. 하나.
2. 둘.
3. 항상 셋 전부.

> **정답 보기: 둘.**
> 임계치는 둘이며 다른 조건과 검증도 충족해야 합니다.

M09

초대 생성 및 키 제공

학습 목표

시드를 공유하지 않고 확인된 참여자와 정책을 구성합니다.

이해하기

생성자는 이름, 망, M, N, 연락처, 자신의 공개 정보, 초대 운영 조건을 정합니다. 검토된 스키마는 mainnet과 regtest를 지원하고 기기 한도 적용 전 참여자는 2~15명, 운영 만료 시간은 1~720시간입니다. 범위 안이어도 용량 확인을 건너뛰지 마세요.

각 참여자는 초대를 검토해 수락 또는 거절하고 호환 절차로 자신의 확장 공개 키, 지문, BIP48 경로를 제공합니다. 시드, 개인 키, 개별 주소, 다른 지갑의 전체 디스크립터를 주지 않습니다. 유효한 xpub처럼 보여도 잘못된 맥락의 키는 다른 정책을 만들 수 있습니다.

생성자는 조율하며 각 서명자의 검증을 대신하지 않습니다. 입금 전 모두 같은 매개변수와 확인 주소를 재구성하고 검증할 수 있어야 합니다. 채팅에서 연락처를 수락해도 그 사람이 보내는 모든 정책을 자동 승인하지 않습니다.

초대 만료는 앱의 조율 규칙입니다. 자금이 있는 스크립트를 바꾸거나 다른 사람이 보관한 서명을 지우지 않고 합의 타임록도 아닙니다. 제안 취소와 기존 정책에서 자금을 인출하는 일은 다릅니다.

실습

1. 준비한 regtest 실습망에서 연습 연락처로 3명 중 2명 제안을 만드세요.
2. 수락, 거절, 틀린 망에서의 자료 제공을 재현하고 마지막 경우 절차가 멈추는지 확인하세요.
3. 자금을 넣기 전 모두 보관할 망, 임계치, 공개 키, 기원, 스크립트, 검증 주소를 열거하세요.

이해 확인

불완전한 초대를 알아보고 채팅이 있다는 이유로 추정하지 말고 부족한 승인을 설명하세요.

자주 묻는 질문

초대 만료일 뒤에는 지출이 불가능한가요? 초대 필드만으로는 아닙니다. 비트코인 시간 제한에는 특정 스크립트나 거래 조건과 실제 지원이 필요합니다.

잠시 멈추기

실습 제안 ID와 남은 승인을 보관하세요.

멀티시그에 자신의 몫을 제공할 때 문서화된 절차가 요구하는 것은?

1. 모든 참여자의 시드.
2. 아무 입금 주소.
3. 호환 지문과 BIP48 기원 정보가 붙은 자신의 확장 공개 키.

> **정답 보기: 호환 지문과 BIP48 기원 정보가 붙은 자신의 확장 공개 키.**
> 올바른 공개 정보로 개인 키를 드러내지 않고 정책을 구성할 수 있습니다.

M09

Mirror로 원하는 순서로 정책 대조하기

학습 목표

각 필드 전체를 대조하고 결과가 무엇을 입증하는지 정확히 이해합니다.

이해하기

독립 검증은 임계치, 망, 프로필, SIGHASH, 정책 ID, 첫 주소, 사용자 위치, 참여자별 데이터를 표시합니다. 의도와 일관성을 확인하는 절차입니다. 기기가 정책을 영구 등록했다고 전제하지 않으며 문서화된 범위는 '이번 검토'에 한정됩니다.

Mirror 12.12에서는 Cuvex 또는 Desk 어느 쪽 QR부터 읽어도 되고 원하는 항목을 선택할 수 있습니다. 단계 1에서 시작하거나 모두 스캔하거나 순서를 지킬 필요는 없습니다. 수동으로 검토한 항목의 스캔을 생략해도 Mirror 검증 완료로 표시되지는 않습니다.

비교기는 전체 원문을 표시하며 공백, 줄바꿈, 대소문자, Unicode 차이도 구별합니다. '일치'는 해당 쌍의 값이 같다는 뜻으로 출처 인증, 같은 정책이라는 증명, 지갑 활성화를 의미하지 않습니다. 최종 승인과 연결된 응답은 Cuvex와 Desk 경로를 따릅니다.

현재 Desk QR에는 값만 있고 순번이나 세션이 없어 Mirror가 단계를 항상 추론할 수 없습니다. 'Desk 단계 지정'은 수동 맥락을 추가하며 그렇게 표시해야 합니다. N명이면 7 + 4N개 필드이고 k를 0부터 세어 8+4k는 지문, 9+4k는 경로, 10+4k는 xpub, 11+4k는 키 ID입니다. N=2일 때 단계 15는 두 번째 키 ID로 먼저 비교할 수 있습니다.

실습

1. 합성 데이터로 단계 15라 표시한 ID부터 비교하고 이어 망과 임계치를 비교하세요.
2. 한 글자를 바꿔 '불일치'를 확인한 뒤 결과를 이어받지 않고 다른 쌍을 시작하세요.
3. '2 / 3'을 비교하고 텍스트만으로 임계치인지 사용자 위치인지 항상 구분할 수 없는 이유를 설명하세요.

이해 확인

검증한 필드, 부여한 맥락, 남은 승인을 설명하세요. 일부 일치를 전체 승인으로 간주하지 마세요.

자주 묻는 질문

학습을 계속하려면 모든 QR을 스캔해야 하나요? 아니요. 비교는 자유롭습니다. 서명자의 필수 검토와 승인은 자체 절차를 따릅니다.

잠시 멈추기

비교기를 닫으세요. 검토한 설계에서는 종료 또는 백그라운드 전환 시 값이 삭제되어야 합니다.

Mirror가 단계 15의 QR 두 개를 비교해 '일치'를 표시했습니다. 무엇을 입증하나요?

1. 식별하거나 지정한 맥락에서 해당 쌍의 값이 글자 그대로 같다.
2. 정책 전체 승인.
3. 두 QR 출처가 진짜임.

> **정답 보기: 식별하거나 지정한 맥락에서 해당 쌍의 값이 글자 그대로 같다.**
> 대조는 인증, 전체 검토, 하드웨어 응답을 대신하지 않습니다.

M09

멀티시그 서명 조율과 발행

학습 목표

의도와 통제권을 유지하면서 제안에 임계치만큼의 서명을 모읍니다.

이해하기

멀티시그 거래에는 입력, 수취인, 금액, 수수료율, 대체 조건, 운영 메모를 지정합니다. 생성자는 호환되는 참여자에게 서명을 요청할 수 있습니다. 각 서명자는 기기에서 승인하기 전 망, 정책, 입력, 모든 출력과 수수료를 독립적으로 검토합니다.

임계치가 부족하면 부분 서명만으로 자금이 움직이지 않습니다. 임계치에 도달하면 조율자가 절차에 따라 결합하고 최종화할 수 있습니다. 다른 참여자나 조율자의 보고는 조율 정보이며 내가 수행한 로컬 검증은 아닙니다. 앱은 출처를 구별해야 합니다.

검토한 버전은 재시도, 서명 수신, 수신 확인, 거절, 조율 인계를 제공합니다. 인계해도 체인의 키나 임계치는 바뀌지 않습니다. 저장된 응답은 실제 사용한 요청과 프로필에 연결해야 합니다. 비슷하거나 목록의 첫 항목이라는 이유로 다른 정책을 고르지 마세요.

수취인이나 중요한 조건이 바뀌면 새 제안을 검토하고 해당 서명을 다시 받아야 합니다. NFC 용량에 맞추려고 보안 정보를 제거해 PSBT를 직접 '고치지' 마세요. 펌웨어는 호환 프로필과 검증을 요구하며 입력 수, 출력 수, 크기에 한도가 있습니다.

발행 전에 합의한 거래인지, 이미 전파된 버전은 없는지 확인하고 이후 선택한 출처로 확인 수를 추적하세요. 자신의 앱에서 거절해도 타인이 보관한 서명이 자동 취소되거나 나머지 임계치로 가능한 모든 작업을 막지는 않습니다.

실습

1. 가상 세 역할로 3명 중 2명을 연습하세요. 한 명은 서명하고 한 명은 거절하며 한 명은 설명을 요구합니다.
2. 시험 결제 주소를 바꾸고 이전 구두 승인을 재사용할 수 없는 이유를 설명하세요.
3. 서명 저장 후 확인 응답 실패를 가정하고 중복 결제나 프로필 변경 없이 같은 작업을 복구하세요.

이해 확인

조율, 서명, 최종화 담당자와 단계별 증거를 지목하세요.

자주 묻는 질문

채팅의 OK 두 개가 서명 두 개와 같나요? 아니요. 정책상 유효한 암호학적 승인이 임계치를 충족하며 메시지는 아닙니다.

잠시 멈추기

비공개 내용 없이 상태, 대기 서명, 다음 담당자를 기록하세요.

3명 중 2명 거래에 유효한 서명 하나와 '동의' 메시지 두 개가 있습니다. 임계치에 도달했나요?

1. 참여자가 셋이므로 그렇다.
2. 아니다. 유효한 암호학적 서명 하나가 더 필요하다.
3. 조율자가 발표하면 그렇다.

> **정답 보기: 아니다. 유효한 암호학적 서명 하나가 더 필요하다.**
> 대화상의 동의와 유효한 서명은 다른 증거입니다.

M09

멀티시그 복구와 변경

학습 목표

정책을 복구하고 참여자 상실이나 교체에 대비합니다.

이해하기

복구에는 정책 재구성 데이터와 지출에 충분한 개인 키 사용 능력이 필요합니다. xpub가 든 정책 사본은 시드가 없어도 이력을 드러낼 수 있습니다. 암호화 사본은 파일을 보호하지만 비밀번호를 보관해야 합니다. .cuvexms 확장자만으로 암호화를 증명하지 않으므로 실제 형식과 내보내기 방법을 확인하세요.

Desk 9.21 복구는 참여자 기기에서 내보낸 확장 공개 키와 지문, BIP48 경로를 요구합니다. 호환 경로에서 웹캠이나 Mirror로 읽을 수 있습니다. 이를 입금 주소로 대체하거나 지원팀에 시드를 보내지 마세요.

3명 중 2명 정책에서 키 하나를 잃어도 나머지 두 개로 지출할 수 있습니다. 이전 정책은 그대로이며 참여자를 실질적으로 제외하고 키를 변경하려면 보통 새 정책을 만들고 필요한 승인으로 자금을 이동합니다. Desk의 별명 변경이나 지갑 삭제는 기존 UTXO를 바꾸지 않습니다.

백업으로 양쪽 분기를 재구성하고 이력을 탐색할 수 있어야 합니다. 인덱스, 발급한 요청, 필요한 맥락을 보관해 주소 재사용과 불완전한 검색에 따른 빈 지갑 오인을 피하세요. 보류 작업 복원·재개에는 생성 시 저장한 프로필을 따라야 합니다.

실습

1. 문서화된 기능으로 실습 정책을 내보내고 복원하며 망과 알려진 주소를 확인하세요.
2. 참여자 한 명 상실을 가정하고 실제 자금 이동 없이 교체 계획을 준비하세요.
3. 손실로 임계치 미만이 된 상황을 가정하고 지원팀이나 AI가 부족한 서명을 만들어 낼 수 없음을 이해하세요.

이해 확인

시험 상황을 복구하고 정보 복원과 코인 통제권 변경을 구별하세요.

자주 묻는 질문

Desk에서 멀티시그를 삭제하면 모두의 지갑이 비활성화되나요? 아니요. 절차에 따라 로컬 상태만 삭제합니다. 다른 사람이나 사본은 정책에 부합하는 능력을 유지할 수 있습니다.

잠시 멈추기

시험한 사본과 개인 계획을 보관하고 강좌에는 결과만 기록하세요.

이미 자금이 들어 있는 정책에서 한 사람을 제외할 때 Desk에서 이름만 지우면 되나요?

1. 예.
2. 채팅도 지우면 된다.
3. 아니다. 필요한 경우 새 정책과 승인된 자금 이동을 계획해야 한다.

> **정답 보기: 아니다. 필요한 경우 새 정책과 승인된 자금 이동을 계획해야 한다.**
> 로컬 기록을 수정해도 기존 UTXO의 스크립트는 바뀌지 않습니다.

M10

절차에 따른 펌웨어 업데이트

학습 목표

호환되는 업데이트를 준비하고 기기에서 결과를 확인합니다.

이해하기

업데이트는 신뢰해 사용하는 소프트웨어의 변경입니다. 모델, 하드웨어 리비전, 버전, 출처, 제조사의 인증 방식을 확인하세요. 다운로드 완료나 페이지의 해시 일치는 서명·호환성 검증을 대신하지 않습니다. 기술자용 미서명 펌웨어를 고객용 릴리스처럼 설치하지 마세요.

문서 절차에서 Original은 Bluetooth, BIT는 USB-C로 업데이트합니다. Mirror는 호환되는 준비·전송 경로를 제공합니다. PC, 전화, 기기의 특정 조합은 실물 인수 시험 전까지 작동을 약속하지 않습니다. Windows의 과거 Original 업데이트 문제는 개별 진단이 필요하며 99%에서 성공으로 처리해도 해결되지 않습니다.

시작 전 복구 가능한 백업, 안정된 전원, 다른 작업이 없는지 확인하고 앱에 맞는 공식 파일이나 사전 검증된 사본을 준비하세요. 전송, 검증, 설치, 재시작, 버전 확인을 구분하세요. 진행 막대는 최종 증거가 아닙니다.

완료 후 기기에 표시된 버전을 확인하고 날짜와 결과를 기록하세요. Desk 호환성 목록은 펌웨어를 원격 측정하지 않으며 firmwareAttestation은 false입니다. Final 프로필 선택이 실제 설치 바이트를 증명하지 않습니다. 실패하면 중요한 단계에서 무작정 연결을 끊지 말고 단계와 오류를 기록해 문서화된 복구 절차를 따르세요.

실습

1. 실습 중 실제 업데이트를 시작하지 말고 준비 목록을 검토하세요.
2. 상태를 순서대로 놓고 ‘전송됨’과 ‘설치됨’의 차이를 설명하세요.
3. 99%에서의 가상 실패에 관해 모델, 버전, 시스템, 단계, 마지막 메시지를 포함한 보고서를 쓰세요.

이해 확인

맞는 파일, 전송 수단, 최종 성공 기준을 식별하세요.

자주 묻는 질문

Desk 오류를 없애기 위해 업데이트해야 하나요? 먼저 원인을 확인하세요. 목록 비호환은 검증된 펌웨어를 유지하고 Desk를 수정해야 할 수 있습니다.

잠시 멈추기

실제 업데이트는 절차에서 명시적으로 안전한 단계에서만 멈추세요. 통화 종료만으로 중단하지 마세요.

Desk의 명시적 목록만으로 확인하는 것은 무엇인가요?

1. 지원 호환성 기준이며 설치된 펌웨어를 원격 측정하지는 않는다.
2. 연결된 모든 기기의 실물 증명.
3. 취약점이 없음.

> **정답 보기: 지원 호환성 기준이며 설치된 펌웨어를 원격 측정하지는 않는다.**
> 호환성, 서명, 측정, 실물 인수 검사는 서로 다른 증거입니다.

M10

분실, 고장 및 긴급 복구

학습 목표

사고에 맞는 복구 방법을 고르고 유용한 증거를 보존합니다.

이해하기

사고 시 컴퓨터, 기기, 카드, 파일, 비밀번호, 시드, 패스프레이즈, 정책 중 무엇을 잃었거나 노출했는지 먼저 분류하세요. '들어갈 수 없다'가 반드시 '도난당했다'는 뜻은 아닙니다. 침해가 의심되는 기기에 계속 비밀을 입력하지 마세요.

기기 분실은 호환 복구 매체와 인증 정보로 해결할 수 있습니다. 컴퓨터 분실은 Desk 저장소 복원과 관찰 환경 재구성이 필요할 수 있습니다. 모든 해제 수단을 잃거나 이용 가능한 키가 임계치 아래로 떨어지면 기술적 해법이 없을 수 있습니다. 존재하지 않는 키를 되찾아 준다고 보장할 수 있는 AI는 없습니다.

Desk에는 지원 형식의 로컬 복구와 해당 복구 자료 내보내기가 있습니다. PC에서 복호화하면 운영체제나 악성코드에 비밀이 노출될 수 있습니다. 예외적 결정으로서 준비한 환경, 호환 자료, 침해 가능성이 있을 때 새 키로 이전할 계획을 마련하세요. 보통의 Cuvex 격리 작업과 동등한 것으로 설명하지 마세요.

시드가 유출되면 Desk 비밀번호를 바꿔도 시드는 취소되지 않습니다. 신뢰할 수 있는 기기에서 새 지갑을 보호하고 승인된 이전을 검토하세요. 공격자에게 도움이 되는 사고 세부 사항을 공개하거나 다른 시드나 사기성 선금을 요구하며 복구를 약속하는 서비스에 돈을 내지 마세요.

실습

1. PC 분실, 유효 사본이 있는 카드 파손, 비밀번호 분실, 시드 노출이라는 가상 사례 넷에 대응하세요.
2. 각 사례에 필요한 자료, 행동 위험, 복구 기준을 식별하세요.
3. 학습 데이터만 사용해 절차를 연습하세요. 실제 긴급 복구 파일을 튜터에게 올리지 마세요.

이해 확인

불가능한 해결을 약속하지 않고 복원, 관찰 환경 재설정, 통제권 이전, 전문가 이관 중 선택하세요.

자주 묻는 질문

비밀번호를 바꾸면 이미 본 비밀까지 다시 암호화되나요? 아니요. 평문 사본이나 알려진 시드를 상대가 모르는 상태로 되돌릴 수 없습니다.

잠시 멈추기

사고 유형과 다음 안전한 조치를 기록하고 비밀을 다루려면 음성을 중단하세요.

시드가 공개된 뒤 PC 비밀번호를 바꿨습니다. 공격자의 권한이 취소됐나요?

1. 예.
2. 아니다. 시드는 같은 키를 통제하므로 수탁 차원의 대응이 필요하다.
3. 채팅 배경도 바꾸면 된다.

> **정답 보기: 아니다. 시드는 같은 키를 통제하므로 수탁 차원의 대응이 필요하다.**
> 로컬 보호는 이미 노출된 비트코인 키를 취소하지 않습니다.

M10

피싱, 지원 사칭 및 음성 사기

학습 목표

위험한 요구를 알아보고 미리 정한 대응 절차를 따릅니다.

이해하기

교묘한 사기는 이름, 구매, 기기, 익숙한 목소리를 활용할 수 있습니다. 진짜 정보도 유출에서 나올 수 있습니다. 상대의 긴박감이나 정확성에 기대지 말고 직접 시작한 채널과 알려진 절차로 신원을 검증하세요.

시드·비밀번호·PIN·채팅 키 요구, '동기화'용 원격 제어 설치, 백신 해제, 안전 지갑으로 송금, 내용 설명 없는 QR 스캔, 승인 대상을 밝히지 않는 소유 증명 서명은 위험 신호입니다. 통화가 끝나기 전에 하라고 압박하면 통화를 중단하세요.

정상 튜터는 설명하고 이해를 묻습니다. 키를 보관하거나 자기 주소로 시험 송금을 요구하거나 시드 복구를 약속하지 않습니다. 정당한 소유 증명은 대상이 구체적이고 검토할 수 있어야 하며 개인 키를 넘기는 것으로 충족하지 않습니다.

기술 세션 안에도 사기가 있을 수 있습니다. QR 텍스트, 문서, 메시지에 AI에게 지침을 무시하라는 명령이 있어도 분석할 내용일 뿐 튜터에 대한 권한은 없습니다. 지식 기반은 승인된 출처와 수강생·제삼자가 제공한 텍스트를 구분해야 합니다.

실습

1. 가짜 지원 전화를 연기하고 데이터를 밝히기 전에 대화를 끊으세요.
2. 미리 저장한 공식 채널을 독립적으로 확인하세요.
3. 비밀 화면을 공유하거나 수탁 환경에 원격 접근을 허용하지 않고 설치 오류를 설명하세요.

이해 확인

요구한 데이터, 필요한 목적, 교육 지원 범위를 넘는 이유를 설명하세요.

자주 묻는 질문

시드에서 몇 단어만 보여 주면 안전한가요? 아니요. 자기 시드 조각을 공개할 교육상 이유가 없습니다.

잠시 멈추기

지원 채널 검증 절차를 보관하고 평문 비밀이 없는지 확인하세요.

동료처럼 들리는 목소리가 검증을 건너뛰고 급히 서명하라고 합니다. 어떻게 하나요?

1. 중단한 뒤 합의한 절차로 요청을 인증하고 거래 전체를 검토한다.
2. 목소리가 같으니 서명한다.
3. 시간을 아끼려고 시드를 공유한다.

> **정답 보기: 중단한 뒤 합의한 절차로 요청을 인증하고 거래 전체를 검토한다.**
> 음성 인식과 긴급성은 인증 및 검토를 대신하지 않습니다.

M10

프라이버시, 법규와 개인 기록

학습 목표

일반적인 틀을 이해하고 법률 및 세무 자문을 위한 구체적인 질문을 준비합니다.

이해하기

금융 프라이버시는 세금, 해당하는 신원 확인, 제재, 범죄 예방 의무를 없애지 않습니다. 거주지, 활동, 상대, 서비스에 따라 다릅니다. AI는 출처와 날짜가 있는 일반 정보를 제공하고 개별 판단은 적격 전문가에게 연결해야 합니다.

EU에서 MiCA는 특정 암호자산과 서비스를 규제합니다. 일반 적용은 2024년 12월 30일 시작됐고 규정상 최대 전환 기간은 회원국 결정에 따라 2026년 7월 1일까지였습니다. 옛 등록 언급에 기대지 말고 최신 공식 등록부에서 인가와 범위를 확인하세요. 인가는 가격, 지급 능력, 전액 보상을 보장하지 않습니다.

규정 2023/1113은 의무 적용 제공자가 관여한 이전에 수반되는 정보를 정합니다. 자기 수탁 주소 관련 1,000유로 초과 이전에는 소유 또는 통제를 평가하는 조치가 있습니다. 그 이하에 일반적인 신원 확인 면제가 생기지는 않습니다. 제공자 없는 개인 간 이전은 해당 규정의 적용 범위에서 제외되지만 다른 의무는 남습니다.

상황에 맞게 구매, 판매, 수수료, 출처 기록을 충분히 보관하고 불필요한 접근으로부터 보호하세요. 개인 기록을 유지하려고 이력 전체를 공개할 필요는 없습니다. 통제 회피를 위한 분할, 허위 정보, 소득 은닉도 가르치지 않습니다.

음성 녹음·전사와 식별 가능한 진도가 있다면 서비스는 목적, 법적 근거, 보관, 접근, 처리 위탁자, 적용 권리를 정해야 합니다. 상용 개인정보 설정은 판매 전에 검증하고 통화 도중 즉흥적으로 정하지 않습니다.

실습

1. 전문가에게 제시할 가상 사례를 키 없이 거주지, 활동, 거래를 명시해 작성하세요.
2. 제공자 인가 확인처와 정보 날짜를 알아보세요.
3. 자금 이동의 개인 기록과 최소 수강생 데이터 정책을 설계하세요.

이해 확인

법규, 거래소 정책, 비트코인의 기술적 능력을 구별하세요.

자주 묻는 질문

EU에서 모든 자기 수탁이 금지되나요? 인용 규정에서 그런 결론은 나오지 않습니다. 단정적인 제목을 피하고 해당 조항과 범위를 확인하세요.

잠시 멈추기

튜터에 개인 문서를 입력하지 말고 전문가에게 물을 사항을 보관하세요.

특정 주소 통제 확인 조치의 기준인 1,000유로보다 낮으면 모든 의무가 사라지나요?

1. 예.
2. 거래를 나누면 그렇다.
3. 아니다. 신원 확인이나 다른 의무의 일반적 면제가 아니다.

> **정답 보기: 아니다. 신원 확인이나 다른 의무의 일반적 면제가 아니다.**
> 임계치를 보편적 면제로 간주하지 말고 조치와 적용 범위에 따라 규정을 해석해야 합니다.

M10

상속, 연속성 및 연례 훈련

학습 목표

미리 모든 것을 노출하지 않으면서 권한 있는 사람이 필요할 때 행동할 계획을 세웁니다.

이해하기

상속에는 법적 정당성, 자료의 위치, 기술적 능력이 필요합니다. 상속권이 있어도 지갑을 재구성하지 못하거나 키가 있어도 사용할 권한이 없을 수 있습니다. 적절한 자문을 받아 두 측면 모두 계획에 반영하세요.

공개 가능한 지침과 비밀 접근을 분리하세요. 목록에는 무엇이 있고 누구에게 연락하며 무엇을 확인할지 적되 모든 키와 비밀번호를 널리 읽을 수 있는 한 문서에 두지 마세요. 통제 밖으로 유통될 유언장이나 서류에 시드를 공개하지 마세요.

멀티시그에서는 누가 정책과 사본을 보관할지, 분실 후 어떤 임계치가 가능한지, 핵심 인물 사망 시 어떻게 할지 정하세요. 한 수탁자가 충분한 요소를 가지면 단일 남용 지점이 되고 지나치게 복잡한 분산은 자산 복구를 불가능하게 합니다.

암호문 비밀번호와 있는 경우 패스프레이즈 복구, 파생 정보, 기기 호환성, 제조사 운영 종료 시 절차를 포함하세요. 독자 형식 파일이나 생체 지문을 준비 없이 쓸 수 있다고 가정하지 마세요. 문서화된 형식과 시험 데이터로 상호 운용성을 연습하세요.

가족, 거주지, 정책, 소프트웨어, 참여자가 바뀌면 검토하고 정기적으로 모의 훈련하세요. 믿을 만한 사람이 자산을 노출하거나 필요 없이 돈을 옮기지 않고 지침을 이해하는지 확인해야 합니다.

실습

1. 담당자, 구성 요소, 승인된 접근, 대체자를 개인 양식에 작성하세요.
2. 구두 설명 없이 다른 사람에게 실습 지침을 주고 어디서 막히는지 보세요.
3. 모호한 부분을 고치고 검토 날짜를 기록하세요. 강좌가 알림을 자동 생성하지는 않습니다.

이해 확인

자신이 부재하면 무슨 일이 생기고 각 단계에서 각 역할에 어떤 정보가 필요한지 설명하세요.

자주 묻는 질문

3명 중 2명이 상속 계획을 대체하나요? 아니요. 기술 도구일 뿐입니다. 상속인에게는 맥락, 자료, 조율, 정당한 권한이 여전히 필요합니다.

잠시 멈추기

계획은 강좌 밖에 보관하고 '모의 훈련 검토 완료'만 표시하세요.

상속 계획을 평가하는 유용한 기준은 무엇인가요?

1. 권한 있는 사람이 임기응변이나 성급한 비밀 공개 없이 문서화한 훈련을 수행할 수 있다.
2. 페이지가 많다.
3. 비밀번호 기억에만 의존한다.

> **정답 보기: 권한 있는 사람이 임기응변이나 성급한 비밀 공개 없이 문서화한 훈련을 수행할 수 있다.**
> 복구 가능성과 접근 통제는 실제로 점검해야 합니다.

M11

가격, 저축과 기본적 분석

학습 목표

투자 논거를 검증 가능한 기술적 속성과 구별해 분석합니다.

이해하기

가격은 특정 시장의 거래 결과이며 플랫폼마다 다를 수 있습니다. 유동성, 호가 통화, 시장 깊이, 은행 운영 시간, 수요가 실제 체결에 영향을 줍니다. 화면 시세는 원하는 수량 전부에 대한 보장된 제안이 아닙니다.

기본적 분석은 채택, 수요, 경쟁, 경제적 보안, 규제, 공급 등을 살펴봅니다. 발행 일정이 알려져 있어도 미래 가격은 정해지지 않습니다. 화폐 효용이나 '내재 가치' 평가는 가정에 따라 달라지며 AI가 보편적 확실성으로 제시할 객관적 수치는 없습니다.

정기 매수는 매수 시점을 분산하지만 수익을 보장하거나 장기 손실을 막지는 않습니다. 장기 저축에도 의무 이행을 위한 유동성, 변동성 감내 능력, 수탁 계획이 필요합니다. 강좌는 자산 비율을 정하거나 대신 결정하지 않습니다.

'자산을 이해하는가', '보관하고 복구할 수 있는가', '경제적 위험을 감당할 수 있는가'를 구별하세요. 키를 잘 다룬다고 세 번째 질문의 답까지 얻지는 못합니다. 교육을 받아도 가격 전망이나 과거 차트가 개인 맞춤 권고로 바뀌지 않습니다.

실습

1. 가상 투자 가설, 전제, 이를 무효화할 사실을 적으세요.
2. 실제 자산을 입력하지 않고 50% 하락과 현금 필요가 동시에 발생한 상황을 모의로 분석하세요.
3. 논거에서 검증 가능한 데이터와 기대에 해당하는 부분을 구별하세요.

이해 확인

수익을 약속하거나 확신을 증거와 혼동하지 않고 투자에 관해 논의하세요.

자주 묻는 질문

희소하면 가격이 반드시 오르나요? 아니요. 수요와 다른 조건도 시장 가격에 결정적입니다.

잠시 멈추기

자동 매수 지시가 아닌 실습 가정을 보관하세요.

정기 매수는 무엇을 보장하나요?

1. 장기 수익.
2. 수익률은 보장하지 않으며 선택한 규칙으로 매수 시점만 분산한다.
3. 키 분실 방지.

> **정답 보기: 수익률은 보장하지 않으며 선택한 규칙으로 매수 시점만 분산한다.**
> 매수 시점을 분산해도 경제적·운영 위험은 남습니다.

M11

비트코인 구매처 선택

학습 목표

인가, 비용, 출금, 프라이버시 및 수탁 위험을 기준으로 제공자를 평가합니다.

이해하기

법인과 관할, 인가 서비스, 출금망, 수수료, 가격 차이, 한도, 지원, 인증, 데이터 처리 등 검증 가능한 기준으로 비교하세요. 상호나 후원만으로 특정 서비스 인가를 증명하지 않습니다.

총비용에는 입금, 환전, 스프레드, 매매 수수료, 출금, 은행 비용이 포함될 수 있습니다. '수수료 무료' 거래의 가격 차이가 더 클 수도 있습니다. 순수령액과 기준 통화를 확인하고 자기 수탁이 목적이면 출금 비용까지 예산에 넣으세요.

수탁 잔액을 맡겨 두면 제공자에 의존합니다. 준비금 증명 하나로 모든 부채, 자금 소유권, 미래 지급 능력을 입증할 수 없습니다. 제한을 확인하고 새 절차에 의존하기 전에 감당할 수 있는 소액으로 출금해 보세요.

사업자의 본인 확인으로 신원과 출금이 연결될 수 있습니다. 나중에 보호해도 제공자가 아는 정보는 사라지지 않습니다. 허위 정보를 내거나 의무 회피에 강좌를 쓰지 마세요. 학습 코드 구매도 지갑과 별개인 상거래 기록을 만듭니다.

실습

1. 가상 제공자 두 곳의 총비용, 망, 최소 출금액, 인가, 요구 데이터를 표로 만드세요.
2. 지정한 모든 비용을 포함해 실습 거래의 순수령액을 계산하세요.
3. 미리 검증한 주소로 시험 출금을 설계하되 이 사이트에서 실행하지 마세요.

이해 확인

해당 사례에서의 선택을 설명하고 오래되거나 검증되지 않은 정보를 식별하세요.

자주 묻는 질문

강좌가 모두에게 최적인 거래소를 추천하나요? 아니요. 인가, 요금, 서비스 국가, 조건은 변합니다. 비교에는 날짜와 용도가 필요합니다.

잠시 멈추기

인증 정보와 신분 서류 없이 표를 보관하세요.

거래 수수료만 보는 것보다 유용한 비교는 무엇인가요?

1. 원하는 망과 주소로 BTC를 받을 때까지의 총비용.
2. 제공자의 팔로워 수.
3. 앱 색상.

> **정답 보기: 원하는 망과 주소로 BTC를 받을 때까지의 총비용.**
> 최종 비용에는 표시 수수료 밖의 항목도 있을 수 있습니다.

M11

계정, 주문 및 체결 비용

학습 목표

기본 주문과 계정 보호를 배우되 강좌를 실거래 단말기로 사용하지 않습니다.

이해하기

시장가 주문은 가능한 체결을 우선해 슬리피지 위험이 있습니다. 지정가는 매수 최고가나 매도 최저가를 정하나 미체결·부분 체결될 수 있습니다. 스톱 주문은 제공자 규칙에 따라 다음 동작을 발동하며 최종 가격 자체는 보장하지 않습니다.

호가창은 현재 주문을 보여 줄 뿐 모든 물량이 남는다는 약속은 아닙니다. 하락장이나 낮은 유동성에서는 체결 결과가 직전 시세와 달라질 수 있습니다. 스톱 시장가는 더 나쁜 가격에 체결될 위험, 스톱 지정가는 미체결 위험이 있습니다.

고유 비밀번호, 지원되는 경우 피싱 방지 인증, 세션 점검, 적절한 출금 제어로 계정을 보호하세요. 2차 인증 복구 수단은 별도 보관합니다. 자동화용 API 키는 데이터 조회에 필요한 것보다 위험한 권한이 있을 수 있으므로 튜터나 사이트에 입력하지 마세요.

출금 전 자산과 비트코인 망, 본인 지갑 주소, 순수령액을 확인하세요. 플랫폼이 다른 상품에 같은 기호를 쓸 수 있습니다. 종료 후 상황에 맞춰 구매·체결·수수료·출금 자료를 보관하세요. 자기 지갑 출금은 새 구매와 다릅니다.

실습

1. 100에 1단위, 102에 1단위인 가상 호가창을 만들고 2단위 시장가 매수의 평균가가 100임을 보장하지 않는 이유를 설명하세요.
2. 지정가 주문을 설계하고 체결되지 않을 상황을 설명하세요.
3. 가상 API 권한을 점검하고 조회만 필요하면 출금 권한을 제거하세요.

이해 확인

각 주문의 우선순위, 가격, 미체결 위험을 설명하세요.

자주 묻는 질문

손절 주문은 항상 손실을 정확히 제한하나요? 아니요. 가격 갭, 유동성, 슬리피지, 제공자 규칙 때문에 그렇지 않을 수 있습니다.

잠시 멈추기

실제 주문이나 API 키 없이 연습 결과를 보관하세요.

100에 낸 지정가 매수 주문에 남는 위험은?

1. 체결되지 않거나 일부만 체결될 수 있다.
2. 어느 가격에든 반드시 체결된다.
3. 백업이 자동 생성된다.

> **정답 보기: 체결되지 않거나 일부만 체결될 수 있다.**
> 가격을 제한하는 대신 체결되지 않을 수 있습니다.

M11

캔들, 지표와 기술적 분석의 편향

학습 목표

차트를 과거 데이터로 읽고 패턴을 예측으로 오해하지 않으면서 전략을 평가합니다.

이해하기

캔들은 일정 기간의 시가, 고가, 저가, 종가를 요약합니다. 거래량은 출처에 따라 다릅니다. 플랫폼, 통화, 시간대, 기간이 바뀌면 보이는 값도 달라집니다. 한 캔들은 구간 안의 모든 가격 움직임 순서를 보여 주지 않습니다.

이동평균은 과거 가격을 평활하고 모멘텀 지표는 관측 데이터를 공식으로 변환합니다. 어느 것도 미래를 알지 못합니다. 같은 계열에서 파생한 두 지표는 색과 이름이 달라도 높은 상관 정보를 줄 수 있습니다.

규칙 평가는 결과를 보기 전에 진입, 청산, 무효 조건, 비용, 규모, 데이터를 정합니다. 성공 사례만 고르거나 결과에 맞을 때까지 조정하거나 과거 결정에 미래 데이터를 쓰지 마세요. 훈련 데이터와 시간 기준 검증 데이터를 구별하세요.

백테스트는 스프레드, 수수료, 슬리피지, 데이터 가용성, 실제 체결 가능성을 고려합니다. 비용 전 수익률, 승률, 최대 손실, 손실 분포는 서로 다른 질문에 답합니다. 적중이 많아도 한 번의 손실이 크면 돈을 잃을 수 있습니다. 매매 신호를 확실한 예측으로 가르치지 않습니다.

실습

1. 가상 캔들을 읽고 어떤 시간 순서 정보가 빠져 있는지 설명하세요.
2. 합성 결과 열 개를 평가하기 전에 비용과 실패 기준을 포함한 규칙을 적으세요.
3. 1씩 얻은 거래 9건과 15를 잃은 1건을 비교하세요. 승률 90%여도 비용 전 결과는 −6입니다.

이해 확인

실제 거래 없이 매력적인 결과를 사례 선택, 비용, 위험 측면에서 비판적으로 검토하세요.

자주 묻는 질문

지표를 많이 합치면 신호가 반드시 좋아지나요? 아니요. 독립 정보 없이 과적합과 복잡성만 커질 수 있습니다.

잠시 멈추기

시장가 주문 대신 규칙과 실습 결과를 보관하세요.

아홉 거래에서 각각 1을 벌고 한 거래에서 15를 잃었습니다. 비용 전 결과는?

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

> **정답 보기: -6.**
> 9단위 이익에서 15단위 손실을 빼면 6단위 손실입니다.

M11

증거금, 선물과 자동화

학습 목표

복잡한 상품을 고려하기 전에 위험 노출, 청산, 자동화 실패를 파악합니다.

이해하기

레버리지는 투입 자본 대비 익스포저를 늘립니다. 단순 예로 증거금 100에 익스포저 1,000이면 기초자산이 불리하게 5% 움직일 때 비용 전 손실은 50으로 초기 증거금의 절반입니다. 실제 유지·청산·담보·수수료 규칙은 결과를 악화시키거나 예상보다 일찍 작동할 수 있습니다.

선물·무기한 계약에는 만기, 차액 결제, 펀딩 비율, 직전 거래와 다른 기준 가격 등이 있을 수 있습니다. 네이티브 비트코인을 Cuvex로 출금하는 것과 다릅니다. 시드를 보관해도 포지션의 청산이나 상대방 부도는 막지 못합니다.

봇은 오류까지 포함해 규칙을 자동화합니다. 포지션 한도, 최소 권한, 주문 멱등성, 대조, 손실 통제, 긴급 중지, 감독이 필요합니다. 이전 결과를 모르고 시간 초과 뒤 요청을 중복하면 익스포저도 두 배가 될 수 있습니다.

AI는 개념을 설명하고 가상 사례의 모순을 찾을 수 있습니다. API 키를 받거나 거래를 켜거나 수익 전략을 약속해서는 안 됩니다. 위험을 이해하고 모르는 상품을 쓰지 않기로 결정할 수 있는 것이 강좌의 주목적에 맞습니다.

실습

1. 청산 수준을 정확히 10%라고 가정하지 말고 익스포저와 증거금 예제를 풀어 보세요.
2. 주문은 실행했지만 응답을 잃은 API를 모의로 재현하고 재시도 전에 대조해야 하는 이유를 설명하세요.
3. 브로커에 연결하지 않고 새 주문을 차단하고 이미 열린 주문을 확인하는 정지 버튼을 설계하세요.

이해 확인

스톱 주문 후, 봇 사용 후, 외부 자금을 자기 수탁한 뒤에도 남는 위험을 하나씩 설명하세요.

자주 묻는 질문

자동화가 감정을 없애 결과를 보장하나요? 아니요. 충동적인 개입을 줄여도 설계나 실행 오류를 증폭할 수 있습니다.

잠시 멈추기

복잡한 상품을 활성화하지 않고 이 심화 내용을 이해했다고 표시하세요.

익스포저 1,000, 증거금 100에서 익스포저의 5%를 잃으면 비용 전 손실은?

1. 손실 5.
2. 손실 50, 증거금의 50%.
3. 봇을 쓰면 손실 없음.

> **정답 보기: 손실 50, 증거금의 50%.**
> 레버리지와 비용으로 인해 증거금 대비 결과는 자산 가격 변동률과 다릅니다.

M12

Lightning과 기타 계층

학습 목표

채널 결제를 이해하고 검토한 Cuvex 절차가 제공하지 않는 기능을 구별합니다.

이해하기

Lightning은 채널과 상태 갱신을 이용해 모든 교환을 기본 체인에 기록하지 않고 결제합니다. 채널 개설·종료와 일부 복구에는 온체인 거래가 필요합니다. 가용성, 인바운드·아웃바운드 유동성, 감시는 지갑 설계와 사용하는 서비스에 달려 있습니다.

인보이스에는 금액, 설명, 만료 시각이 포함될 수 있습니다. 맥락에 따라 사토시 또는 밀리사토시로 표시해도 기본 체인에 1사토시 미만 출력이 있다는 뜻은 아닙니다. 결제하려면 호환성과 경로가 필요하며 QR이 모든 앱 결제를 보장하지 않습니다.

수탁형과 비수탁형 서비스의 모델은 크게 다릅니다. 대개 빠르다고 위험이 없는 것은 아닙니다. 관찰자, 경로, 상대, 메타데이터가 관련되므로 Lightning을 완전한 익명으로 설명하지 마세요.

Cuvex 채팅은 WOW 계정에서 온체인으로 지급하는 sat 요청을 조율할 수 있습니다. 이 판에서는 Desk에 Lightning 노드, 채널 관리, Lightning 인보이스 서명 기능이 있다고 하지 않습니다. 여러 결제 방식이 있는 요청은 이해한 방식과 앱이 실행할 방식을 확인하세요.

실습

1. 교육용 온체인 주소, bitcoin: URI, Lightning 인보이스를 분류하세요.
2. 체인 결제와 채널 결제를 확인, 유동성, 수탁, 복구 측면에서 비교하세요.
3. 만료 인보이스를 주소로 재해석하지 말고 수취인과 검토해야 하는 이유를 설명하세요.

이해 확인

키를 노출하거나 Cuvex 고장으로 단정하지 않고 호환되지 않는 방식을 거절할 수 있어야 합니다.

자주 묻는 질문

sat로 표시된 결제는 모두 Lightning인가요? 아니요. 사토시는 가치 단위이고 결제 방식은 사용하는 프로토콜에 따라 다릅니다.

잠시 멈추기

실제 인보이스 없이 실습 방식만 기록하세요.

Lightning으로 지불하는 요청임을 구별하는 정보는?

1. sats라는 단어.
2. 채팅으로 도착함.
3. 호환되는 형식과 결제 방식. 단위나 메시지 채널만으로는 부족하다.

> **정답 보기: 호환되는 형식과 결제 방식. 단위나 메시지 채널만으로는 부족하다.**
> 회계 단위와 결제 네트워크는 별개입니다.

M12

Taproot, MuSig2와 양자 내성의 전망

학습 목표

표준, 제안, 구현된 기능을 구별합니다.

이해하기

Taproot는 키 경로와 스크립트 경로를 이용한 지출 조건을 허용합니다. Schnorr 서명과 집계로 일부 구성을 개선할 수 있지만 프라이버시는 설정과 지출 방식에 달려 있습니다. bc1p 주소만으로 다른 참여자가 없음을 증명하거나 숨은 조건 전체를 드러낼 수는 없습니다.

MuSig2는 서명자들이 상호 작용으로 키를 집계하고 호환 Schnorr 서명을 생성하게 합니다. 기본 표준은 N명 중 N명입니다. 임의의 N명 중 M명 임계치에는 다른 구성이나 추가 프로토콜이 필요합니다. 논스와 세션 관리가 중요하며 비공식 메시지 교환으로 구현하지 않습니다.

PSBT v2는 v0와 정보 구성이 다릅니다. 버전 2 거래가 든 파일이 자동으로 PSBT v2가 되지는 않습니다. 이 판의 Final 펌웨어 멀티시그는 PSBT v0, P2WSH/sortedmulti, SIGHASH_ALL을 유지합니다. 향후 기능에는 별도의 명세와 검증이 필요합니다.

NIST는 2024년에 처음 확정된 양자 내성 표준을 발표했습니다. 그 자체로 비트코인 서명이 달라지지는 않습니다. 양자 내성 알고리즘으로 펌웨어를 인증하면 해당 계층을 보호하나 UTXO의 ECDSA나 Schnorr가 자동으로 양자 내성 서명이 되지는 않습니다. 튜터가 미래 공격 날짜를 확실히 약속할 수도 없습니다.

실습

1. 다섯 주장을 표준, 검증된 구현, 제안, 홍보로 분류하세요.
2. ‘Taproot 수취처를 허용한다’가 ‘Taproot 입력에 서명한다’는 증거가 아닌 이유를 설명하세요.
3. 펌웨어 서명, 비밀 암호화, 채팅, 비트코인 지출 서명을 별개 계층으로 그리세요.

이해 확인

특정 계층의 증거를 요청하고 한 프로토콜의 보장을 다른 곳에 적용하지 마세요.

자주 묻는 질문

양자컴퓨터 기사 제목을 보고 자금을 이전해야 하나요? 실제 판단에는 최신 기술 증거, 검증 가능한 지원 상황, 위험 평가, 안전한 이전 계획이 필요합니다. 강좌는 제목만 보고 자금 이동을 지시하지 않습니다.

잠시 멈추기

자동 지출 계획을 만들지 않고 기술적 질문을 기록하세요.

부트로더에 양자 내성 서명을 구현하고 검증했다고 가정하면 기존 UTXO의 서명 조건이 바뀌나요?

1. 아니다. 서로 다른 계층이다.
2. 그렇다. 전체 망의 알고리즘이 바뀐다.
3. 백업이 필요 없어지게 된다.

> **정답 보기: 아니다. 서로 다른 계층이다.**
> 업데이트 인증은 비트코인 지출 조건을 다시 쓰지 않습니다.

M12

상호 운용성과 제조사 의존에서 벗어나기

학습 목표

소프트웨어, 기기 또는 제공자가 바뀌어도 운영을 계속할 수 있게 계획합니다.

이해하기

상호 운용성은 약어 목록으로 검증할 수 없습니다. 망, 스크립트, 파생, 키, 정책, 거래 형식, 서명의 의미를 유지해야 합니다. 두 앱이 BIP174를 이해해도 지원 필드, 크기, 입력 유형은 다를 수 있습니다.

특정 인터페이스 의존에서 벗어나려면 문서화된 복구 정보를 보관하고 실습 지갑으로 시험하세요. 표준 니모닉으로 키를 파생해도 멀티시그 복구에는 전체 정책이 필요합니다. BIP329 라벨은 프라이버시 맥락을 보완하며 채팅 이력의 범위는 다릅니다.

호환성 시험을 실제 시드의 노출로 만들지 마세요. 공개 디스크립터 내보내기와 관찰 전용 복구부터 확인합니다. 긴급히 키 재구성이 필요하면 이를 위해 준비한 환경을 쓰고 이후 이전도 검토하세요. 호환되지 않는 지갑이 0을 표시해도 자금 손실의 증거는 아닙니다.

문서, 강좌 버전, 필요한 도구의 검증 가능한 사본을 유지하세요. 앱 서명, 인증서 만료, 시스템 변경은 설치에 영향을 줍니다. 공개 소스가 있어도 의존성과 지식 없이 수년 후 누구나 빌드할 수 있다는 보장은 없습니다.

실습

1. 빈 계정으로 이탈 시험을 설계해 호환 구현 두 곳에서 같은 망, 정책, 확인 주소를 검증하세요.
2. 표준 요소와 변환기 또는 Cuvex 형식 문서가 필요한 요소를 열거하세요.
3. 호환성을 말할 수 있는 결과와 실물 기기나 실제 서명이 더 필요한 부분을 정하세요.

이해 확인

회사가 같은 서비스를 계속 제공하는 것에 의존하지 않는 복구 경로를 설명하세요.

자주 묻는 질문

오픈 소스면 제조사가 더는 중요하지 않나요? 아니요. 배포, 유지보수, 물리 부품, 운영 경험은 여전히 중요합니다. 검사와 연속성 가능성을 제공할 뿐 자동으로 보장하지 않습니다.

잠시 멈추기

버전과 관찰한 한계를 포함해 실습 결과를 보관하세요.

상호 운용성을 더 확실히 뒷받침하는 증거는?

1. 양쪽 앱에 ‘Bitcoin’이라 적혀 있다.
2. 버전을 특정한 실습 환경에서 동일한 정책과 주소를 재구성해 검증한다.
3. 아이콘이 비슷하다.

> **정답 보기: 버전을 특정한 실습 환경에서 동일한 정책과 주소를 재구성해 검증한다.**
> 시험은 관련 조건을 유지하고 검증 가능한 결과를 내야 합니다.

M12

regtest 기술 실습

학습 목표

합성 시험과 실물 기기 사용을 구별하고 재현 가능한 실습 환경을 이해합니다.

이해하기

regtest에서는 통제하는 로컬 체인을 만들어 블록을 생성하고 경제적 가치 없는 거래를 연습할 수 있습니다. 별도 디렉터리와 인증 정보를 쓰고 실제 자료는 가져오지 마세요. 결과만으로 실물 기기의 USB, NFC, Bluetooth, 카메라 호환성을 증명하지는 못합니다.

완전한 실습은 버전, 망 설정, 정책, 시험 입력, PSBT, 서명, 최종 거래, 수용 결과를 기록합니다. 합계 일치, 변조 서명 거부, 유효한 결제의 로컬 블록 포함을 확인할 수 있습니다. 성공 경로뿐 아니라 실패 사례도 시험해야 합니다.

Desk 9.21 검증 자료는 Bitcoin Core 31 regtest 시험과 엔진·모의 UI 자동 시험을 보고합니다. 이 판은 이를 문서 증거로 쓰며 시험을 반복하거나 실물 기기를 조작했다고 주장하지 않습니다. 패키지 검사도 모든 시스템에 설치됐음을 입증하지 않습니다.

기술 수업 전 담당자가 학습자 버전에 맞는 구축된 실습 환경과 절차를 제공해야 합니다. 튜터가 조종하도록 RPC를 인터넷에 공개하지 마세요. AI는 합성 결과의 해석을 도울 수 있지만 인증 정보나 관리 권한을 받아서는 안 됩니다.

실습

1. 준비한 환경에서 유효 거래와 서명이 변조된 거래를 관찰해 수용 또는 거부를 기록하세요.
2. 거스름돈이 잘못된 경우와 망이 호환되지 않는 경우를 확인하세요.
3. 보고서에서 ‘엔진 시험’, ‘모의 인터페이스’, ‘실물 하드웨어’를 구별하세요.

이해 확인

시뮬레이션을 인증으로 제시하지 않고 확인한 사항과 남은 사항을 정확히 설명하세요.

자주 묻는 질문

regtest가 작동하면 모든 기기 검증 완료로 강좌를 팔 수 있나요? 아니요. 실물 절차, 설치, 접근성, 복구, 상용 서비스 시험이 남습니다.

잠시 멈추기

지침에 따라 실습 환경을 중지·저장하고 합성 데이터만 남기세요.

엔진 regtest로 특정 휴대전화의 실제 NFC 읽기를 증명할 수 있나요?

1. 둘 다 비트코인을 쓰므로 그렇다.
2. PSBT가 작으면 그렇다.
3. 아니다. 별도의 실물 시험이 필요하다.

> **정답 보기: 아니다. 별도의 실물 시험이 필요하다.**
> 검증 환경마다 확인할 수 있는 범위가 다릅니다.

M12

최종 과제와 연속성 계획

학습 목표

준비부터 복구와 프라이버시까지 스스로 판단하고 수행할 수 있음을 보여 줍니다.

이해하기

목표는 메뉴 암기가 아니라 의도를 설명하고 결과를 검증하며 이해하지 못한 작업을 멈출 수 있는 것입니다. 평가는 개념, 안내 실습, 독립 사례를 결합합니다. 평가자에게 시드, 자산, 개인 주소를 공개할 필요는 없습니다.

사례 A에서는 실습 환경 설정, 모델과 버전 식별, Desk 보호, 실습 암호문 연결, 관찰 전용 계정 재구성을 수행하세요. 필요한 백업과 제공자가 볼 수 있는 데이터를 설명하세요.

사례 B에서는 맥락이 다른 가상 UTXO로 결제를 설계하고 선택 이유를 밝히며 수취처, 거스름돈, 수수료를 검토하고 모델별 서명 경로를 설명하세요. 반환과 전파 중 중단을 중복 결제 없이 해결합니다. 실물 인수 검증된 장비가 없으면 모의로 기록하고 실제 시험은 미완으로 둡니다.

사례 C에서는 3명 중 2명을 설계해 초대와 검증을 재현하고 Mirror에서 순서와 관계없이 원하는 필드를 대조해 OK의 범위를 설명하세요. 실습 정책을 복구하고 참여자 한 명 상실을 가정해 연속성과 상속을 준비하세요.

제안된 통과 기준은 지식 평가 80% 이상과 비밀 미공개, 망·출력 확인, 단계 구별, 복구 수단 보존 등 핵심 검사 전부 정답입니다. 핵심 오류는 재검토·재실습이 필요하고 시장 문제 정답으로 상쇄하지 않습니다. 상업적 인증서가 발급된다면 평가 내용과 실물 관찰 여부 또는 모의만 했는지 밝혀야 합니다.

실습

1. 합성 데이터와 자신의 설명으로 세 사례를 완료하세요.
2. 부록 최종 평가를 풀고 틀린 답을 하나씩 검토하세요.
3. 비밀 없이 확인 범위의 증거와 남은 사항을 기재한 결과지만 제출하세요.

이해 확인

증거가 부족한 작업을 스스로 중단하고 계속하기 위해 필요한 것을 말할 수 있어야 합니다.

자주 묻는 질문

모든 페이지를 마치면 어떤 금액이든 보관할 준비가 됐나요? 아니요. 능력을 시험하고 상황에 맞게 위험을 평가해야 합니다. 읽기와 연습은 미래 결과를 보장하지 않습니다.

잠시 멈추기

검토 계획과 남은 실습을 보관하세요. 전 과정을 반복하지 않고 필요한 장으로 돌아갈 수 있습니다.

실습 종료의 핵심 요건은 무엇인가요?

1. 모든 페이지를 열었다.
2. 비밀을 노출하지 않고 문서화된 범위에서 복구와 거래 검토를 입증한다.
3. 다음 달 가격을 예측한다.

> **정답 보기: 비밀을 노출하지 않고 문서화된 범위에서 복구와 거래 검토를 입증한다.**
> 학습 성과는 페이지 이동이나 예측이 아닌 검증된 능력과 한계로 평가합니다.

수강생 설명서

Cuvex 운용 설명서

이 설명서는 강의를 보완합니다. 각 절차는 검토한 소스의 흐름과 확인 사항, 중단 지점을 설명합니다. 시범 운영 후보판으로 Original, BIT, 휴대전화, 각 데스크톱 플랫폼에 대한 자체 실물 시험을 입증하지 않습니다. 실제 자금으로 가르치기 전 담당팀은 인수 검증표를 완성하고 다른 표시 문구나 화면을 수정해야 합니다.

참고 버전 Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21, Mirror 1.0.0-beta.12.12. Desk의 프로필 선택은 명시된 호환성이며 펌웨어 원격 측정이 아닙니다. 수록된 Mirror 화면은 12.12 패키지 Android 에뮬레이터에서 얻었습니다. 제품 사진은 기업 자료이며 현재 기기의 표시 버전을 입증하지 않습니다.

P01 | 출처 및 버전 확인 | Cuvex | L16,L21 | C01,C02

준비 구매 자료와 독립적으로 확인 가능한 공식 채널을 준비하세요. 아직 비밀을 입력하지 마세요.

1. 포장과 봉인을 검사하세요. 조작 흔적이 있으면 초기 가동을 멈추고 민감하지 않은 증거를 보관하세요.
2. 배송품에 맞는 앱에서 무결성과 봉인을 확인하세요. 코드는 그곳에만 입력하고 튜터에게 주지 마세요.
3. Original 또는 BIT 모델과 확인 가능한 리비전을 파악하고 기기 및 앱의 표시 버전을 확인하세요.
4. 팀이 공개한 호환 표와 비교하세요. 목록이나 해시는 펌웨어 인증 또는 실물 인수 검사를 대신하지 않습니다.

결과 비밀을 노출하지 않고 모델과 버전, 출처를 확인했습니다. 코드가 무효이거나 화면이 다르면 옛 지침으로 사용을 강행하지 마세요.

중단 지점 수탁 자료를 넣기 전에 멈추세요. 유통 이력만으로 정교한 조작이 없었다고 보장할 수 없습니다.

P02 | Bluetooth로 Original 업데이트 | Original | L46 | C01,C02,C03

준비 복구 가능한 사본, 안정된 전원, 호환 공식 패키지, 해당 시스템에서 인수 검증된 절차를 준비하세요. 강좌는 모든 플랫폼의 실물 작동을 입증하지 않습니다.

1. 앱의 기기 또는 펌웨어 화면에서 Original과 공식 다운로드 또는 해당하는 진짜 로컬 파일을 선택하세요.
2. 기기 메뉴에 따라 업데이트 모드로 두고 앱 절차로 연결하세요. 가까이 두고 경쟁 세션을 피하세요.
3. Original 화면의 코드를 지정란에 입력하세요. 암호문 비밀번호와 혼동하지 마세요.
4. 전송, 검증, 설치, 재시작을 지켜보세요. 진행률을 설치의 증거로 삼지 마세요.
5. Original에서 최종 버전을 확인하고 앱에 해당란이 있으면 기록하세요.

결과 재시작 후 화면에서 버전을 확인하고 최종 절차를 확인했습니다. PIN 전, 패키지 전송 중, 마지막 중 어느 단계에서 실패했는지와 코드를 기록하세요. ‘99%를 넘기려고’ 임의로 연결을 끊거나 소프트웨어를 바꾸지 마세요.

P03 | USB로 BIT 업데이트 | BIT | L46 | C01,C02,C03

준비　실제 BIT 매체와 전원, 호환 공식 패키지를 확인하세요. 소프트웨어 변경 전 사본을 보관하세요.

1. 호환되는 Desk 또는 Mirror 펌웨어 절차에서 BIT를 선택하세요.
2. 적절한 데이터 케이블과 어댑터로 기기를 연결하세요. 요청이 표시되면 볼륨 또는 폴더 접근을 허용하세요.
3. 모델에 맞는 진짜 펌웨어를 고르고 보내기 전 버전과 호환 정보를 검토하세요.
4. 기기의 전송·검증 단계를 기다리세요. 프로토콜에 따라 볼륨이 사라지거나 다시 마운트될 수 있습니다.
5. 재시작 후 BIT의 버전과 앱의 최종 결과를 확인하세요.

결과　기기 자체에서 설치를 확인했습니다. 볼륨이 안 보이면 기기 모드, 데이터 케이블, 권한, 마운트, 다른 활성 세션을 확인하세요. PC에 동명 폴더를 만들어 대체하지 마세요. 업데이트 실패 복구에는 해당 하드웨어의 공식 절차가 필요합니다.

P04 | 동전과 주사위로 지갑 생성 | Cuvex | L17 | C01

준비　비공개 장소, 적합한 주사위와 동전, 학습용 지갑을 준비하세요. 튜터 마이크와 카메라를 끄세요.

1. 지갑 생성과 펌웨어의 엔트로피 절차를 열고 주사위 네 개의 순서를 미리 정하세요.
2. 원하는 값으로 바꾸지 말고 화면 지시에 따라 동전과 각 주사위 결과를 입력하세요.
3. 검토한 소스의 계산식은 인덱스 = 동전 값 × 1,296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1)입니다. 0~2,047만 허용합니다.
4. 거부되면 동전과 주사위 전부를 다시 던지세요. 경고는 앞의 단어를 유지하고 한 묶음을 다시 던지도록 합니다.
5. 최종 검증을 포함해 기기 알고리즘을 마치고 니모닉을 보호한 뒤 비공개로 복구를 확인하세요.

결과　단어를 수동으로 고르지 않고 전체 절차로 지갑을 생성했습니다. 화면과 소스가 다르면 사용을 멈추세요. 공개된 주사위 예시나 시드·키를 자신의 자료로 쓰지 마세요.

P05 | 비밀 정보 암호화 | Cuvex | L18,L19 | C01

준비　모델, 콘텐츠 형식, 보호 방식을 고르세요. 대상이 암호화되어도 PC나 전화에 입력하면 원본 환경에 노출됩니다.

1. 암호화와 BIP39, SLIP39, Monero, 호환 텍스트 중 유형을 선택하세요. 사전을 서로 바꾸지 마세요. 검토한 평문 키보드는 최대 500자이며 다른 형식의 저장이 해당 망의 서명 지원을 의미하지 않습니다.
2. 격리를 유지하도록 기기에 직접 입력하고 화면에서 순서, 문자, 보조 필드를 확인하세요.
3. 절차에 따라 개인 또는 공동 보호를 고르고 해당하면 BIT 생체 인증을 선택하세요. 이 임계치와 비트코인 임계치를 구별하세요.
4. 펌웨어 검증 조건에 맞춰 비공개로 비밀번호를 입력하고 확인하세요. Desk 규칙을 그대로 적용하지 마세요.
5. Original은 호환 빈 카드에 기록하고 BIT는 USB 절차에서 내보낸 객체를 보관하세요. 확인을 기다리세요.
6. 시험 복구를 열어 내용을 확인한 뒤 비밀 표시를 닫으세요.

결과　복구를 검증한 암호문이 만들어졌습니다. 읽기나 쓰기가 실패하면 원본을 보호하고 화면의 재시도 절차를 따르세요. 헤더를 지우거나 강제로 덮어쓰지 마세요.

P06 | 기기에서 복호화 | Cuvex | L18 | C01,C02

준비　사생활이 지켜지는 공간과 충분한 해제 요소를 마련하고 비밀 근처의 마이크와 화면 캡처를 끄세요.

1. 해당 모델에서 복호화를 시작하고 Original은 NFC, BIT는 USB 절차로 암호문을 전달하세요.
2. 인증 정보를 입력하기 전에 객체의 별명과 식별 정보를 확인하세요.
3. 필요한 비밀번호와 형식이 요구하는 생체 인증을 제공하세요. 접근 통제와 잠금이 있으므로 실패 시 무작정 반복하지 마세요.
4. 지정된 화면에서만 내용을 확인하세요. 비밀 QR은 텍스트와 똑같이 민감합니다.
5. 기기 절차에 따라 닫거나 종료하고 계획에 맞게 매체와 인증 정보를 분리 보관하세요.

결과　비공개로 내용을 복구하고 세션을 종료했습니다. 형식 인식이나 인증이 실패하거나 예상 밖의 내용이 나타나면 모르는 앱으로 '수정'하지 마세요. 비밀을 첨부하지 않고 버전, 형식, 오류를 지원팀에 설명하세요.

P07 | 생체 인증 암호문 복구 준비 | BIT | L19,L47 | C01,C02

준비　실습 암호문과 해당 형식 문서를 준비하세요. .bin 사본 하나가 있다고 복구 가능하다고 추정하지 마세요.

1. Desk 정보 화면에서 생체 인증 구성 요소와 사용 가능한 복구용 내보내기를 확인하세요.
2. 절차에 연결된 파일 전체와 독립 사본을 눈에 띄지 않는 식별자로 보관하세요.
3. BIT에서 일반 잠금 해제를 시험하고 필요한 비밀번호와 조건을 기록하세요.
4. 예외적인 로컬 복구 경로와 지원 형식을 익히고 필요해지기 전에 자료가 갖춰졌는지 확인하세요.
5. 자금 없는 데이터로 기기 고장이나 지문을 사용할 수 없는 상황을 연습하세요.

결과　해당 형식에 대해 한계를 포함한 계획을 시험했습니다. 모든 생체 인증을 생략할 수 있거나 지문이 사본을 대체한다는 뜻은 아닙니다. PC에서 비밀을 복구했다면 노출과 이후 통제권 이전 필요성을 평가하세요.

P08 | 암호문 사본 생성 및 검증 | Cuvex 및 Desk | L20 | C01,C02

준비　식별된 원본 사본과 보존할 데이터가 없는 호환 대상을 준비하세요.

1. Original에서는 기기의 복제 또는 Desk의 호환 기능을 사용해 지정 순서대로 원본과 대상을 제시하세요.
2. 카드를 움직이지 말고 이미 암호문을 담은 매체가 거부되면 그대로 따르세요.
3. BIT 또는 파일 방식은 요소 전체를 내보내고 필요한 이름과 연결 관계를 유지하세요.
4. 원본 사본을 분리하고 새 사본에서 읽기와 복구를 시험하세요.
5. 날짜, 형식, 결과를 비공개로 적고 물리적 위험이 독립적인 곳에 사본을 보관하세요.

결과　시험한 두 번째 사본이 생겼습니다. 별도 지갑 생성, 비밀번호 취소, 이미 유출된 시드 보호를 뜻하지 않습니다. 대상이 실패하면 원본을 '수리'해 맞추려 하지 말고 보관하세요.

P09 | Desk 생성, 잠금 해제 및 비밀번호 변경 | Desk | L21,L40 | C02

준비　검증된 설치 파일, 맞는 아키텍처, 저장소 백업 계획을 준비하세요.

1. 재사용하지 않는 12~1,024자 비밀번호로 저장소를 만들고 확인란 값을 일치시키세요.
2. 잠갔다 다시 열어 접근이 유지되는지 확인하세요. 비밀번호는 Desk에만 입력합니다.
3. ‘보안’의 ‘접근 및 잠금’에서 비활동 및 백그라운드 전환을 검토하세요. 시연 중 선택적 삭제를 켜지 마세요.
4. 비밀번호 변경 시 현재 값을 제공하고 해당 절차에서 새 값을 확인하세요.
5. PC 생체 인증을 썼다면 지시에 따라 재설정하세요. 현재 사본을 만들고 이전 사본과의 관계를 보관하세요.

결과　접근을 확인했습니다. 이전 사본에는 원래 비밀번호와 암호화가 유지됩니다. PC와 BIT의 생체 인증은 별개입니다. 접근 실패 시 반복 시도를 멈추고 튜터에게 인증 정보를 보관해 달라고 하지 말고 복구 방법을 검토하세요.

P10 | Desk에서 암호문 연결 및 검토 | Desk | L22 | C02

준비　출처를 아는 실습 암호문과 사용 가능한 전송 수단을 준비하세요.

1. 암호문 또는 카드 화면을 열고 NFC, USB, 호환 사본 중 연결 방법을 고르세요.
2. 디자인과 출처를 고르세요. NFC는 컴퓨터와 Bluetooth로 연결한 Cuvex Mirror를 쓰고 BIT는 USB-C로 연결한 Cuvex BIT의 볼륨을 사용합니다. Cuvex Desktop은 외장 USB NFC 리더기를 지원하지 않습니다.
3. 세부 화면에서 별명, 출처, 크기, 형식, 해석된 조건을 검토하세요. 복호화한 내용이 아니라 메타데이터입니다.
4. 보관 중인 연결 대기 계정이 있는지 확인하고 검증한 계정만 연결하세요.
5. 백업이 부족하면 사본을 내보내고 따로 복구를 시험하세요.

결과　객체를 로컬에서 정리했습니다. ‘연결됨’은 시드 인증이나 잔액의 증거가 아닙니다. 인식되지 않으면 형식과 버전을 확인하고 앱이 받도록 확장자를 바꾸거나 데이터를 지우지 마세요.

P11 | 관찰 전용 WOW 계정 활성화 | Desk 및 Cuvex | L13,L22 | C01,C02

준비　기기 절차에서 얻은 공개 정보와 출처를 비공개로 확인할 수단을 준비하세요.

1. 해당 암호문에서 WOW 활성화 또는 계정 추가를 여세요.
2. 기능에 따라 파일, 웹캠, Mirror로 지원 디스크립터나 공개 자료를 가져오세요.
3. 망, 스크립트, 기원, 지문, 경로 및 해당하는 체크섬을 확인하세요. 시드나 xprv를 입력하지 마세요.
4. 계정 이름을 정하고 동의한 조회 출처를 고르세요.
5. 잔액을 해석하기 전 확인 주소와 탐색 범위를 검토하세요.

결과　관찰 전용 지갑을 연결했습니다. 0이면 자금이 사라졌다고 단정하지 말고 망, 원래 패스프레이즈, 파생, 계정, 제공자, 검색을 확인하세요. 화면이 일반적으로 지원하는 망이라도 멀티시그 프로필이 지원하지 않을 수 있으니 각 상황을 따르세요.

P12 | 노드 및 동기화 설정 | Desk | L25,L33 | C02

준비　프라이버시 방침을 정하고 Core를 쓰면 보호되고 동기화된 노드에 접근할 수 있게 하세요.

1. ‘보안’의 ‘프라이버시와 노드’에서 WOW 계정을 고르고 제공자를 검토하세요.
2. 호환 공개 제공자 또는 Core를 명시적으로 선택하세요. Core의 엔드포인트, 지갑, 인증 정보는 앱에만 입력하세요.
3. 각 서비스가 받는 정보를 이해하고 조회를 승인하세요. TLS는 제공자에게 조회를 숨기지 않습니다.
4. 동기화 후 시각, 체인 끝, 진행률, 완료 상태를 확인하세요. 재검색 범위의 과거 시점과 작업 지속 여부도 보세요.
5. 429이면 대기 시간을 지키세요. 실패해도 다른 노드가 활성화됐다고 가정하지 마세요. 설정은 몰래 전환되지 않습니다.

결과　출처와 상태를 확인했습니다. RPC를 인터넷에 공개하거나 비밀번호를 공유하거나 탐색을 잔액 있는 주소로 한정하지 마세요. 빈 이력은 일부 결과일 수 있습니다.

P13 | 입금 요청 생성 및 다시 불러오기 | Desk 및 Cuvex | L26 | C01,C02

준비　계정, 망, 정책을 검증하세요.

1. 받기 화면을 열어 알맞은 요청을 만들거나 다시 불러오세요.
2. 로컬 메타데이터가 필요할 때만 관찰자, 목적, 예상 금액을 추가하세요.
3. 중요한 입금 전 기기의 호환 절차로 주소를 검증하세요. 실물 인수 시험이 없다면 시뮬레이션에서 멈추세요.
4. 수취인의 인증된 채널로 꼭 필요한 데이터만 공유하세요.
5. 네트워크 출처에서 입금, 금액, 확인 수를 검증하세요.

결과　요청 발급뿐 아니라 입금 대조까지 마쳤습니다. 멀티시그에서 표시한 주소는 늦은 결제를 위해 보관하며 재할당하지 않습니다. 이력 없는 새 주소 한도에 이르면 이전 요청을 불러오고 인덱스를 수동으로 강제하지 마세요.

P14 | 라벨, 동결 및 BIP329 | Desk | L27 | C02,B13

준비　UTXO가 있는 실습 계정과 보호된 내보내기용 비밀번호를 준비하세요.

1. 불필요한 개인정보 없이 입력 맥락을 라벨로 표시하세요.
2. 의도에 따라 동결 또는 해제하고 가용 잔액을 확인하세요. 제한은 로컬입니다.
3. 보호 기능으로 라벨을 내보내세요. BIP329 형식과 파일 암호화를 구별하세요.
4. 호환 사본에 가져오고 참조, 라벨, 동결 상태가 일치하는지 확인하세요.
5. 계획에 따라 메타데이터의 최신 백업과 해당 비밀번호를 보관하세요.

결과　맥락을 보존하고 선택 방식을 이해했습니다. 가져오기로 검토 없이 동결된 코인을 자동 해제하지 마세요. 라벨 파일은 지출 키가 없어도 상대와 관계를 드러낼 수 있으므로 튜터에게 보내지 마세요.

P15 | 결제 준비 및 전액 송금 | Desk | L28 | C02

준비　검증된 요청과 충분한 지출 가능 입력이 있는 계정을 준비하세요.

1. WOW, UTXO 또는 채팅에서 결제를 열고 계정과 망을 확인하세요.
2. 입력, 수취인, 금액을 고르고 서로 연결될 맥락을 확인하세요.
3. 수수료율을 고르고 절대 수수료, 거스름돈, 경고를 보세요. 더스트가 있으면 숨은 수수료를 받아들이지 말고 대안을 검토하세요.
4. 전액 송금은 수수료 차감 후 금액을 확인하세요. 채팅 요청을 충족하지 못하면 부분 결제를 명시적으로 확인하세요.
5. 초안을 만들고 서명용 내보내기 전 모든 데이터를 검토하세요.

결과　의도가 분명한 거래와 PSBT가 준비됐습니다. 일반 양식은 하드웨어보다 많은 입력이나 수취인을 받을 수 있으므로 서명기와 전송의 실제 한도를 적용하세요. 출력이나 조건이 바뀌면 새로 검토합니다.

P16 | Original에서 PSBT 서명 및 반환 | Original 및 Mirror | L29 | C01,C02,C03

준비　정확한 초안, 호환 전송 카드, 인증된 호환 암호문, 비공개 해제 수단을 준비하세요. 진위 미검증 구형 사본은 서명 전 검증된 복구와 새 사본 생성이 필요할 수 있습니다. 헤더 편집으로 고치지 마세요.

1. Desk/Mirror에서 지원되는 NFC 절차로 요청을 내보내세요.
2. Original로 옮기고 요청될 때 암호문을 제시해 인증 정보를 읽어 주지 않고 해제하세요.
3. 망, 요약, 전체 출력, 수수료, 거스름돈, 필수 경고를 검토하세요.
4. Final 멀티시그에서 확장 항목을 볼지 정하고 전부 일치할 때만 마지막 세 차례 확인을 마치세요.
5. 카드에 응답을 쓰고 다시 읽기를 마칠 때까지 기다리세요.
6. Cuvex Mirror로 응답을 읽고 Desk의 해당 작업에서 검증하세요.

결과　서명을 받아 초안에 연결했으며 아직 발행과는 다릅니다. 쓰기가 실패하면 상태를 보존하고 재시도 절차를 따르세요. 백업 카드를 소모성 결제 매체로 쓰지 마세요.

P17 | BIT에서 서명 후 수신 및 확인 응답 | BIT 및 Desk | L29 | C01,C02

준비　정확한 초안, 인증된 호환 암호문, 선택한 실제 BIT 볼륨을 준비하세요. 옛 사본이 서명에서 거부되면 형식을 강제하지 말고 안내된 복구·갱신을 따르세요.

1. Desk 서비스로 USB-C를 통해 요청을 전달하고 암호문은 기기 화면을 따르세요.
2. 비공개로 해제하고 요약, 모든 출력, 수수료, 경고를 확인하세요.
3. Final 멀티시그에서 선택적으로 확장 세부 정보를 보고 필수 최종 확인으로 승인하세요.
4. Desk의 ‘BIT에서 받기’로 해당 작업의 응답을 가져와 검증하세요.
5. 저장과 수신 확인을 점검하세요. 수신 후 확인 응답이 실패하면 같은 작업을 재시도하고 모델이 고른 다른 새 작업은 사용하지 마세요.

결과　서명이 검증되고 교환 상태가 일치합니다. 수신 전이나 저장 후 연결이 끊기면 요청의 프로필을 유지하세요. 대기 응답을 맞추려고 목록의 다른 펌웨어로 바꾸지 마세요.

P18 | 거래 최종화, 전파 및 추적 | Desk | L30,L44 | C02

준비　검증된 서명을 확보하고 해당하는 경우 임계치를 충족하세요.

1. 의도, 입력, 출력, 수수료, 망을 다시 검토하세요.
2. 해당 동작으로 최종화하고 서명이나 조건이 부족하지 않은지 보세요.
3. 전파를 승인하고 로컬 결과를 보관하세요. 망 응답이 사라지면 반복 전에 조회하세요.
4. 선택한 제공자에서 동기화 시각을 확인하며 멤풀과 확인 수를 추적하세요.
5. RBF를 고려하면 새 거래를 검토해 필요한 서명을 받으세요. CPFP 내장을 전제하지 마세요.

결과　출처를 확인하고 체인 상태를 검증했습니다. 초안 취소는 내보낸 서명을 철회하거나 확인된 결제를 바꾸지 않습니다. 채팅이나 화면 캡처는 추적을 대신하지 않습니다.

P19 | 정책 QR 두 개를 자유로운 순서로 비교 | Mirror | L43 | C03,C02

준비　Desk와 Cuvex에 필드를 표시하세요. 실습에는 강좌의 합성 예시만 사용합니다.

1. 정책 비교를 열고 양쪽 중 어느 쪽이든 먼저 읽으세요.
2. 검토할 항목을 고르세요. 단계 15에서 시작하고 수동 검토한 다른 항목은 생략해도 됩니다.
3. 대응 값을 읽고 두 텍스트 전체를 확인하세요. 단계가 불명확하면 ‘Desk 단계 지정’을 사용하며 수동 맥락임을 이해하세요.
4. ‘일치’와 ‘불일치’는 해당 쌍의 원문 비교에만 적용하세요. 공백, 대소문자, 인코딩도 구별합니다.
5. 원하는 순서로 다른 쌍을 시작하세요. 검토된 삭제 동작에 따라 나가거나 백그라운드로 전환해 종료합니다.

결과　해당 항목을 로컬에서 비교했습니다. 출처, 세션, 전체 승인, 활성화를 증명하지 않습니다. 차이가 있으면 출처에서 규명하고 억지로 OK를 얻으려 텍스트를 정규화하지 마세요.

P20 | 채팅 활성화, 복구 및 이전 | Desk 및 Cuvex | L36,L39 | C02

준비　DEV 또는 운영 환경을 선택하고 기기에 별명과 채팅 키를 준비하세요. 강좌에는 입력하지 마세요.

1. 암호문 화면에서 채팅 활성화 또는 복구를 여세요.
2. 새 별명 또는 기존 별명 이전을 고르고 앱이 지정하는 호환 모바일 프로필을 선택하세요.
3. 비공개 절차에서만 채팅 키를 입력하거나 읽으세요. 시드, PIN, WOW 키를 사용하지 마세요.
4. 서비스에서 활성화를 확인하세요. 대기 중이면 완료 또는 확인 기능을 사용하고 성공했다고 가정하지 마세요.
5. 이전 후 연락처와 연속성을 확인하고 여러 기기에서 같은 별명을 동시에 사용하지 마세요.

결과　올바른 환경에서 신원을 활성화하거나 복구했습니다. 이전 이력과 세션은 채팅 키나 Desk 전체 백업으로 자동 복구되지 않습니다. 가진 자료의 한계를 고려하세요.

P21 | 연락처 신원 확인 | Desk | L36,L48 | C02

준비　상대와 미리 합의한 독립 채널을 준비하세요.

1. 별명을 추가하고 앱을 통해 공개 신원을 조회하세요.
2. 방금 만든 대화에만 의존하지 말고 인증된 채널에서 지문을 비교하세요.
3. 본인 확인 질문을 쓰는 경우 공개 정보나 다른 서비스에서 재사용한 비밀은 피하세요.
4. 차이가 해소된 뒤에만 확인하세요. 신원이 바뀌면 검증까지 결제와 조율을 중단하세요.
5. 검증 방법을 기록하되 민감한 답변을 강좌에 저장하지 마세요.

결과　해당 맥락에서 상대에 대한 신뢰를 확인했습니다. 향후 모든 요청의 보장은 아닙니다. 목소리는 모방할 수 있고 정상 기기도 침해될 수 있습니다. 매 거래를 검토하세요.

P22 | 채팅으로 주소 요청, 결제 요청 및 지급 | Desk 및 Cuvex | L37 | C02,C01

준비　검증된 연락처와 호환 WOW 계정을 준비하세요.

1. 의도에 따라 주소 요청, 주소로 응답, 결제 요청 중 고르세요.
2. 보내기 전 원래 요청, 망, 금액, 메모를 확인하세요.
3. 결제하려면 맞는 계정에서 준비 화면을 열고 UTXO와 수수료율을 고른 뒤 순수령액을 검토하세요.
4. 모델별 절차로 Cuvex에서 승인하세요. 채팅은 자동 서명하지 않습니다.
5. 자신의 출처에서 발행과 확인을 추적하고 명시한 부분 결제를 원래 요청과 대조하세요.

결과　수탁 검토를 유지하며 조율했습니다. 메시지와 거래의 상태는 다릅니다. 탐색기 링크가 제삼자에게 정보를 보낼 수 있으므로 열기 전에 판단하세요.

P23 | 암호문 공유 및 수신한 암호문 연결 | Desk | L38 | C02

준비　구체적인 공유 필요성, 확인된 연락처, 상대가 받을 접근 수단을 정하세요.

1. 채팅 동작에서 암호문 공유를 고르고 대상을 검토하세요.
2. 댓글에 비밀번호, 시드, 채팅 키를 첨부하지 마세요.
3. 수취인이 출처를 확인하고 수신 기능으로 호환 객체를 연결합니다.
4. 상대가 지금 얻는 능력과 충분한 해제 인증 정보를 확보할 때 얻게 될 능력을 평가하세요.
5. 현실적인 철회 계획을 유지하세요. 메시지를 삭제해도 외부 사본이나 이미 알려진 키를 회수하지 못합니다.

결과　암호화 객체를 의미를 알고 전송했습니다. 결제도 아니고 멀티시그에 키를 자동 추가하는 것도 아닙니다. 첨부물에서 모르는 페이지로 가서 복호화하라고 하면 멈추세요.

P24 | Desk 전체 백업 및 복원 | Desk | L15,L21 | C02

준비　실습용 저장소와 통제 가능한 백업 대상을 준비하세요.

1. 저장소 백업 기능을 열어 지정된 비밀번호를 설정하고 이 사본과의 대응 관계를 보관하세요.
2. 평소 쓰는 유일한 기기 밖에 보관하고 절차로 출처와 무결성을 확인하세요.
3. 분리한 시험 환경에서 복원하고 포함된 계정, 설정, 데이터를 확인하세요.
4. 제외 항목을 확인하세요. 채팅, 세션, 이력이 포함된다고 가정하지 마세요. 멀티시그 정책과 개인 키는 서로 대체할 수 없습니다.
5. 중요 변경 후 반복하고 복구 지침을 보관하세요.

결과　범위와 비밀번호가 확인된 백업을 만들었습니다. 옛 사본은 예전 비밀번호를 유지합니다. 접근 변경이나 노출 시 현재 저장소만 바꾸지 말고 그 사본들도 평가하세요.

P25 | 멀티시그 생성 및 수락 | Desk 및 Cuvex | L41,L42 | C01,C02

준비　독립 참여자와 검증된 연락처, 합의한 망과 실제 한도를 준비하세요.

1. 생성자가 이름, M/N, 망, 참여자, 운영 유효 기간을 선택합니다.
2. 호환 절차로 올바른 확장 공개 키와 지문, BIP48 경로를 제공하세요.
3. 각 참여자는 검토해 수락 또는 거절하고 자신의 공개 자료를 제공합니다. 시드는 공유하지 않습니다.
4. 전체 정책을 구성하고 각 기기에서 검증할 준비를 하세요.
5. 자금을 넣기 전에 정책 사본을 보관하고 확인 주소와 복구 능력을 검증하세요.

결과　완전하고 검증 가능한 제안이 만들어졌습니다. 초대 수락은 실물 검토를 대신하지 않습니다. Original이 참여하면 키 6개 한도와 NFC 크기를 적용하세요. BIT가 있다고 다른 참여자의 기능이 늘지 않습니다.

P26 | 정책 검증 및 확인 응답 수신 | Desk 및 Cuvex | L43 | C01,C02,C03

준비　모두에게 동일하고 완전한 정책, 올바른 펌웨어 프로필, 경쟁 작업 없는 기기를 준비하세요.

1. 호환 화면에서 정책 검증을 시작하세요. Original은 설치된 프로필을 명시적으로 골라야 하고 BIT는 명세에 따라 기능을 협상합니다.
2. 모델에 따라 NFC/Mirror 또는 USB-C로 요청을 전달하세요.
3. 기기에서 정책 필드를 검토하세요. Mirror는 고른 쌍을 자유로운 순서로 대조하는 선택적 도구입니다.
4. 기기 확인을 마치고 해당 전송 수단으로 응답을 반환하세요.
5. Desk에서 요청에 연결된 응답을 검증하세요. 비교기의 시각적 OK로 이 단계를 대신하지 마세요.

결과　이번 검토 범위 내에서 요청과 응답을 대조했습니다. 목록은 펌웨어를 원격 증명하지 않으며 기기를 영구 정책 저장소로 설명하지 않습니다. FIRMWARE_CAPABILITY_REQUIRED이면 먼저 Desk 버전과 모델·빌드 조합을 확인하세요.

P27 | 서명 요청 및 수신, 조율 역할 인계 | Desk 및 Cuvex | L44 | C01,C02

준비　검증된 정책, 식별한 거래, 합의한 수취처를 준비하세요.

1. 입력, 출력, 수수료, 메모를 준비하고 호환 참여자에게 서명을 요청하세요.
2. 각 참여자가 자신의 전송 경로와 기기로 검토하고 서명합니다.
3. 각 서명을 수신·검증·저장하고 기존 프로필을 바꾸지 않으면서 대기 중인 확인 응답을 해결하세요.
4. 조율을 인계하면 받는 사람이 절차를 수락해 상태를 검증합니다. M/N이나 키 소유권은 바뀌지 않습니다.
5. 임계치에 도달하면 검토·최종화한 뒤 발행하고 망에서 거래를 추적하세요.

결과　증거 출처를 구분해 조율했습니다. 조율자의 진행 보고는 자신의 로컬 검증과 다릅니다. 한 앱에서 취소·거절해도 타인이 이미 보관한 서명이 지워지는 것은 아닙니다.

P28 | 로컬 멀티시그 내보내기, 복원 및 삭제 | Desk | L45 | C02

준비　내용을 아는 정책과 고유 비밀번호로 암호화한 사본을 준비하세요.

1. Desk의 복구 내보내기 기능을 쓰세요. 현행 절차에서는 이 내보내기에 인증 컨테이너 CVXMSBK1을 사용합니다.
2. 사본과 비밀번호를 서로 독립적인 위험 환경에 보관하세요. 예전 파일의 확장자로 암호화를 추정하지 마세요.
3. 복원 시 사본, 비밀번호, 올바른 기원 정보의 참여자 공개 키를 제공하고 해당하면 웹캠 또는 Mirror를 사용하세요.
4. 작업 전 정책, 망, 주소, 탐색을 확인하세요.
5. 로컬 삭제 전 범위와 확인 내용을 읽고 복구가 필요하면 사본을 보관하세요. 이후 복원은 명시적 작업입니다.

결과　복구 가능한 정책 또는 의미를 알고 실행한 로컬 삭제가 완료됐습니다. 삭제는 자금을 옮기거나 다른 서명자의 키를 지우지 않으며 타인이 보관하는 거래를 단독으로 취소하지 않습니다.

P29 | 예외적인 PC 복구 | Desk | L47 | C02

준비　지원 형식 자료, 준비된 깨끗한 환경, 백업을 마련하세요. 이 작업에서 PC에 비밀이 노출될 수 있으므로 강좌에서는 학습용 데이터만 쓰세요.

1. 알맞은 화면에서 로컬 복구를 시작하고 형식 제한과 경고를 읽으세요.
2. 위험을 이해해 수락하고 절차에 따라 네트워크를 끊으세요. 창은 계속하기 전 상태를 확인합니다.
3. 비공개 창에 필요한 인증 정보만 입력하세요. 읽어 주거나 강좌에 붙여 넣거나 지원팀과 공유하지 마세요.
4. 카메라나 듣고 있는 음성 비서가 없는 곳에서만 표시를 켜고 타이머와 종료 절차를 따르세요.
5. 종료하고 가능한 노출을 검토해 필요하면 새 키 이전을 계획하세요.

결과　예외적 복구를 수행했습니다. 포렌식 삭제나 격리 기기와 동등함을 보장하지 않습니다. 인증, 형식, 접근 자료가 부족하면 인터넷 도구에 실제 사본을 넣어 시험하지 마세요.

P30 | 기본 설정, 생체 인증 및 잠금 점검 | Desk | L40 | C02

준비　보안을 바꾸기 전에 비밀번호를 확인하고 백업 복구를 시험하세요.

1. ‘접근 및 잠금’에서 비밀번호, 사용 가능한 생체 인증, 비활동 및 백그라운드 전환 잠금을 검토하세요.
2. 변경 전 실패 후 지연과 설정된 최댓값을 이해하세요.
3. 조건, 임계치, 복구를 이해하기 전까지 선택적 삭제는 꺼 두세요. 운영 환경에서 시험하지 마세요.
4. ‘기본 설정’에서 언어, 테마, 통화, 3분 또는 5분 동기화, 소리를 조정하세요.
5. bitcoin: 링크를 등록한다면 요청을 열어도 해제, 선택, 검토 단계가 유지되고 저절로 결제되지 않는지 확인하세요.

결과　설정을 이해했습니다. 운영체제 생체 인증은 기기에 의존하며 비밀번호나 백업을 대체하지 않습니다. 시각 설정은 비트코인 정책을 바꾸지 않습니다.

P31 | 적용 범위를 구분하며 기록 삭제 | Desk | L22,L45 | C02

준비　삭제 대상이 로컬 암호문, 계정, WOW, 채팅, 멀티시그 중 무엇이고 어떤 사본을 유지할지 확인하세요.

1. 선택 객체와 경고를 읽고 앱이 요구하면 정확한 별명이나 명시적 조건을 확인하세요.
2. 나중에 이 상태를 복구해야 하면 사본을 내보내고 검증하세요.
3. 의도한 객체만 삭제하고 어떤 연결을 유지하거나 제거하는지 확인하세요.
4. 외부 작업이나 참여자가 남는지 확인하세요. 다른 기기의 메시지, 서명, 파일까지 없어졌다고 가정하지 마세요.
5. 변경을 개인 목록에 기록하고 강좌에는 민감한 정보를 남기지 마세요.

결과　로컬 상태를 이해하고 관리했습니다. 이들 작업만으로 자금이 있는 UTXO의 스크립트 변경, 타인이 아는 시드 삭제, 확인된 거래 취소가 이루어지지 않습니다.

P32 | 비밀을 노출하지 않고 진단 | Desk 및 Mirror | L23,L30,L48 | C02,C03

준비　대략의 시각, 시스템, 아키텍처, 버전, 단계를 기록하세요. 상태를 모른 채 민감한 작업을 반복하지 마세요.

1. 검색, 연결, 읽기, 쓰기, 검증, 서명, 응답 반환, 망, 표시 중 실패 단계를 찾으세요.
2. QR이나 비공개 데이터를 빼고 오류 코드와 문구를 복사하세요. 해당하면 앱 진단 기능을 쓰세요.
3. 공유 전에 파일을 확인하고 저장소 사본, 암호문, 시드, 채팅 키, 디스크립터, RPC 인증 정보를 첨부하지 마세요.
4. 화면 문제는 합성 화면으로 창 크기, 확대율, 숨겨진 조작 요소를 기록하세요.
5. 기대 결과와 재현 단계를 공식 채널로 보내세요. 강좌가 지원팀에 메시지를 자동 발송하지는 않습니다.

결과　최소 정보로 조사 가능한 보고서를 만들었습니다. 단계의 증거가 없으면 ‘완료’가 아닌 ‘대기’로 기록합니다. 음성 지원에 수탁 기기 원격 접근은 필요하지 않습니다.

비트코인과 자기 수탁 용어집

비트코인

장부를 관리하는 단일 주체 없이 가치를 옮기고 그 이력을 검증하는 네트워크와 규칙의 집합.

BTC

비트코인의 화폐 단위. 1 BTC는 1억 사토시다.

사토시

기본 체인의 단위로 1 BTC의 1억분의 1이다.

블록체인

규칙에 따라 연결하고 검증한 블록의 이력. 이 명칭만으로 망의 모든 특성을 설명할 수는 없다.

블록

거래와 검증 가능한 헤더를 포함한 데이터 집합.

풀 노드

수용할 블록과 거래가 규칙을 따르는지 검증하는 소프트웨어.

채굴

네트워크 규칙에 따라 작업 증명으로 블록을 구성하는 일.

작업 증명

블록을 제안하려면 검증 가능한 계산 작업을 요구하는 장치.

합의

참여자들이 수용하는 규칙과 유효한 이력이 서로 양립하는 상태.

멤풀 정책

거래 수용 및 재전파에 관한 로컬 규칙. 반드시 합의 규칙과 같은 것은 아니다.

멤풀

각 노드가 로컬에 보관하는 미확인 거래 집합.

확인

수용한 체인의 블록에 포함된 사실과 이후 그 블록 위에 쌓인 깊이.

체인 재구성

수용한 체인의 일부 구간이 바뀌어 확인 수가 달라질 수 있는 현상.

UTXO

정해진 조건을 충족하면 쓸 수 있는 미사용 거래 출력.

입력

이전 출력에 대한 참조와 그 지출 승인에 필요한 데이터.

출력

거래가 생성하는 금액과 지출 조건.

거스름돈

지불액과 수수료를 제외한 입력의 일부를 자신의 통제 아래로 돌려주는 출력.

수수료

거래의 입력 총액과 출력 총액의 차이.

가상 바이트(vbyte)

거래의 상대적 비용을 나타내는 가상 크기 단위.

가상 바이트당 사토시

단위 가상 크기당 사토시로 표시한 수수료율.

더스트

정책과 지출 비용에 비해 지나치게 작은 출력. 기준은 상황과 스크립트에 따라 다르다.

RBF

호환되는 정책에서 미확인 거래를 대체하는 방법. 취소를 보장하지 않는다.

CPFP

자식 거래를 이용해 부모와 자식 거래를 함께 블록에 넣을 유인을 높이는 방법.

해시

데이터 무결성 확인에 쓰이는 지문. 그 자체로 암호화하거나 작성자를 식별하지 않는다.

개인 키

해당 암호 방식에서 승인을 생성할 수 있게 하는 비밀 정보.

공개 키

개인 키를 드러내지 않고 서명을 검증하고 특정 조건을 구성하는 데이터.

전자 서명

특정 메시지를 승인했음을 보이는 암호학적 증거. 내용을 숨기지는 않는다.

암호화

키와 알고리즘을 이용해 기밀성을 보호하는 것.

인증 암호

설계된 방식으로 변조 여부도 확인하는 암호화 방식.

AES GCM

이 생태계의 형식에 쓰이는 인증 암호 계열. 특성은 구현과 키 관리에 따라 달라진다.

니모닉

생성에 쓰이는 자료와 검사용 정보를 정해진 형식의 단어로 표현한 것.

시드

키를 파생하는 원자료. 일상적으로 단어열도 이렇게 부르므로 문맥을 밝혀야 한다.

엔트로피

생성 자료의 예측 불가능성. 기억하기 쉬운 단어를 골라서는 얻지 못한다.

체크섬

특정 오류를 검출하는 검삿값. 작성자를 인증하지 않는다.

BIP39

니모닉과 선택적 패스프레이즈를 사용한 시드 파생의 규격.

BIP39 패스프레이즈

파생 과정의 추가 입력. 다르면 비어 있는 다른 유효한 지갑이 생길 수 있다.

BIP32

계층적 키 파생을 규정한 규격.

파생 경로

루트에서 키를 얻기 위해 거치는 분기들의 순서.

강화 파생

보통 작은따옴표 또는 h로 표시하며 일반 공개 파생과 성질이 다른 파생 단계.

xpub

파생 맥락을 포함한 확장 공개 키. 프라이버시에 민감한 정보다.

xprv

확장 개인 키. 공유하거나 강좌에 가져와서는 안 된다.

마스터 지문

루트의 짧은 식별자. 연계에는 유용하지만 그 자체로 충분한 신원 증거는 아니다.

디스크립터

키와 파생 정보로 스크립트를 구성하는 표현식. 공개 정보만 있거나 비밀 자료를 포함할 수 있다.

관찰 전용 지갑

스스로 서명하기에 충분한 비밀 정보를 갖지 않은 관찰용 지갑.

WOW

Cuvex 생태계에서 지갑을 관찰하고 관리하는 계정의 명칭.

핫 월렛

연결된 환경에서 서명할 수 있는 도구.

자기 수탁

이용자가 자신의 정책 아래 단독 또는 공동 지출의 기술적 능력을 유지하는 방식.

수탁자

고객을 대신해 지출 능력을 통제하고 자체 접근 조건을 적용하는 주체.

Cuvex 암호문

비밀을 보호하는 암호화 객체. 그 자체가 거래나 잔액인 것은 아니다.

Desk 비밀번호

로컬 저장소 접근을 보호한다. 시드나 암호문 비밀번호와는 다르다.

채팅 키

채팅 신원을 복구하는 비밀. 공개 정보처럼 보여도 공개 정보가 아니다.

연결 PIN

연결 세션의 임시 코드. 자산 보관 비밀번호가 아니다.

에어갭

환경을 운영상 분리하는 것. 전달한 데이터는 여전히 검증해야 한다.

NFC

호환 카드와 리더기에서 사용하는 근거리 통신 기술.

USB Mass Storage

BIT가 파일로 데이터를 교환하는 인터페이스. 고유한 프로토콜, 검증, 수신 확인이 필요하다.

PSBT

거래 구성과 승인을 조율하는 정보와 서명을 담는 컨테이너.

PSBT v0

BIP174에서 정의한 형식 버전. 검토한 Final 멀티시그 프로필에 쓰인다.

PSBT v2

BIP370에서 정의한 버전. 거래 자체가 버전 2라고 해서 PSBT v2인 것은 아니다.

SIGHASH ALL

검토한 프로필에서 쓰는 서명의 커밋 방식. 그 기술적 범위도 거래 검증의 일부다.

P2WPKH

보통 BIP84 계정과 연결되는 단일 키 SegWit 지출 조건.

P2WSH

스크립트에 커밋하는 SegWit 조건. 검토한 Final 멀티시그에서 사용한다.

P2TR

Taproot 출력 형식. 수취처로 지원해도 그 출력에서 지출하는 거래에 서명할 수 있다는 뜻은 아니다.

sortedmulti

키를 결정적 순서로 정렬해 스크립트를 생성하는 멀티시그 구성.

N명 중 M명 임계치

해당 정책에 따라 N명의 참여자 중 필요한 승인 수 M.

MuSig2

Schnorr 서명 집계 프로토콜. 기본 방식은 N명 중 N명이며 임의 임계치 방식과 다르다.

Taproot

키 경로와 스크립트 경로가 있는 비트코인 지출 및 커밋 메커니즘의 집합.

Miniscript

특정 스크립트 정책을 기술하고 분석하는 언어. 검토한 Final 프로필에는 구현되지 않았다.

regtest

환경을 구축한 사람이 통제하며 경제적 가치가 없는 로컬 실습망.

signet

고유한 특성의 시험망. 기본적으로 regtest와 상호 교환되지 않는다.

mainnet

실제 경제적 거래에 쓰는 비트코인 네트워크.

갭 리밋

주소 탐색에서 이력이 없는 연속 주소의 수를 기준으로 삼는 값. 적용 범위는 지갑에 따라 다르다.

코인 컨트롤

지출할 UTXO를 의식적으로 선택하는 것.

UTXO 통합

출력을 합쳐 파편화를 줄이는 것. 비용과 프라이버시에 영향을 준다.

가명성

실명을 직접 나타내지 않는 식별자를 사용하는 것. 자동 익명성을 뜻하지 않는다.

익명성

정해진 관찰자가 대상을 구별할 수 없는 맥락적 성질. 앱의 명칭만으로 보장되지 않는다.

메타데이터

통신이나 활동의 시각, 크기, 관계 등 내용 자체와 구별되는 정보.

CoinJoin

일부 추론을 어렵게 하는 협업 거래 구성. 영구적인 익명성을 보장하지 않는다.

Payjoin

호환 프로토콜에서 지급인과 수취인이 모두 입력을 제공하는 협업 결제.

Tor

연결을 보호하는 네트워크와 도구. 앱마다 사용 경로를 설정하고 검증해야 한다.

VPN

연결에 대한 신뢰 일부를 운영자에게 옮기는 통신 경로. 체인 기록을 숨기지는 않는다.

Lightning

채널을 통한 결제 시스템. 온체인 송금과 요건 및 위험이 다르다.

인보이스

형식과 방식을 식별해야 하는 구조화된 결제 요청.

RPC

Bitcoin Core 등의 서비스를 호출하는 인터페이스. 인증과 보호가 필요하다.

TLS

특정 위협으로부터 전송 구간을 보호하는 장치. 수신 서버는 여전히 요청을 본다.

SRTP

일부 VoIP 구간에서 음성을 보호하는 방식. 운영자에게까지 비밀이라는 뜻은 아니다.

멱등성

식별된 요청을 반복해도 효과가 중복되지 않는 성질.

Webhook

서버 간에 보내는 이벤트. 진위와 중복 전송 여부를 확인해야 한다.

RAG

지식 조각을 검색해 맥락과 버전에 근거한 답변을 만드는 기법.

티치백

학습자가 이해한 내용을 자신의 말로 설명하도록 해 학습 정도를 확인하는 방법.

피싱

사칭과 그럴듯한 정황으로 접근 권한을 얻거나 행동을 유도하는 사기.

사회공학

사실인 정보나 긴박감을 이용할 수도 있는 인간의 의사결정 조작.

공증(Notarization)

Apple의 배포 단계 검사. 제품 감사나 모든 흐름의 실물 시험과 다르다.

증명(Attestation)

특정 메커니즘을 통해 얻은 상태의 증거. Desk의 호환성 목록은 원격 측정이 아니다.

MiCA

특정 암호자산과 서비스에 적용되는 유럽 규제 체계. 수익이나 전액 보상을 보장하지 않는다.

트래블 룰

적용 대상 이전 거래에 관한 정보 제공 의무. 자기 수탁을 이용해도 면제되지 않는다.

체크포인트

지갑 정보를 제외하고 최소 데이터만으로 남기는 학습 재개 지점.

배운 내용 확인하기

실제 자금 없이 연습하세요. 누구나 자유롭게 평가에 참여할 수 있으며 계정은 필요하지 않습니다.

Cuvex를 일반적으로 사용할 때 지출은 누가 승인하나요?

1. 사용자가 검토한 뒤 기기가 승인한다
2. 음성 튜터
3. 강좌 서버

> **정답 보기: 사용자가 검토한 뒤 기기가 승인한다**
> 승인은 Cuvex에서 정해진 절차를 거칩니다.

0.001 BTC는 몇 사토시인가요?

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

> **정답 보기: 100,000**
> 1 BTC는 100,000,000 sat입니다.

입력이 120,000 sat이고 출력이 119,000 sat이면 수수료는 얼마인가요?

1. 1,000 sat
2. 119,000 sat
3. 추가 정보 없이도 1 sat/vB

> **정답 보기: 1,000 sat**
> 입력과 출력 총액의 차이가 절대 수수료입니다.

서명을 마쳤지만 아직 전파하지 않은 거래의 상태는 무엇인가요?

1. 블록에서 확인됨
2. 서명했으니 취소 불가능함
3. 승인되었지만 네트워크에 발행되었다고 볼 수 없음

> **정답 보기: 승인되었지만 네트워크에 발행되었다고 볼 수 없음**
> 서명과 발행은 별개 단계입니다.

200 vB에 6 sat/vB를 적용하면 얼마인가요?

1. 206 sat
2. 1,200 sat
3. 송금액의 6%

> **정답 보기: 1,200 sat**
> 가상 크기에 수수료율을 곱합니다.

거래소 출금 전에 무엇을 확인해야 하나요?

1. 최저 수수료만
2. 자산, 네트워크, 주소, 순수령액의 적합성
3. 상대방의 시드

> **정답 보기: 자산, 네트워크, 주소, 순수령액의 적합성**
> BTC 기호가 있는 모든 망이 비트코인 온체인인 것은 아닙니다.

전자 서명만으로 할 수 있는 것은 무엇인가요?

1. 메시지 전체를 숨긴다
2. 해당 서명 방식으로 검증할 수 있는 메시지를 승인한다
3. 공개된 데이터를 지운다

> **정답 보기: 해당 서명 방식으로 검증할 수 있는 메시지를 승인한다**
> 기밀성에는 별도의 장치가 필요합니다.

BIP39 패스프레이즈를 바꾸면 어떻게 될 수 있나요?

1. 비어 있는 것처럼 보이는 다른 유효한 지갑이 생긴다
2. 항상 이메일로 재설정할 수 있다
3. 이전 결제의 공개 기록이 바뀐다

> **정답 보기: 비어 있는 것처럼 보이는 다른 유효한 지갑이 생긴다**
> 패스프레이즈는 파생 과정에 쓰입니다.

계정의 xpub를 어떻게 취급해야 하나요?

1. 아무 영향도 없는 데이터
2. 비공개 시드 그 자체
3. 프라이버시에 민감한 정보

> **정답 보기: 프라이버시에 민감한 정보**
> 관찰할 수 있는 활동 범위가 넓어질 수 있습니다.

멀티시그에서 시드 하나만으로 부족할 수 있는 이유는 무엇인가요?

1. 정책과 임계치만큼의 승인이 부족하기 때문
2. 비트코인은 아무것도 복구할 수 없기 때문
3. 앱의 원래 색상이 필요하기 때문

> **정답 보기: 정책과 임계치만큼의 승인이 부족하기 때문**
> 정책 보관과 개인 키를 사용할 수 있는 상태 유지는 별개 요건입니다.

검토한 Final 알고리즘에서 주사위 결과가 거부되면 어떻게 하나요?

1. 허용될 때까지 동전만 다시 던진다
2. 동전과 주사위 네 개를 모두 다시 던진다
3. 아는 단어를 고른다

> **정답 보기: 동전과 주사위 네 개를 모두 다시 던진다**
> 일부만 다시 던지면 값의 대응에 편향이 생길 수 있습니다.

단일 서명 시드를 열기 위해 비밀번호 두 개를 쓰는 것은 어떤 의미인가요?

1. 온체인 지출에 키 두 개가 필요하다
2. Taproot 멀티시그다
3. 비밀 접근 임계치가 비트코인 지출 임계치와 별개다

> **정답 보기: 비밀 접근 임계치가 비트코인 지출 임계치와 별개다**
> 암호화는 스크립트를 바꾸지 않습니다.

Desk 전체 백업에 관해 알아야 할 점은 무엇인가요?

1. 반드시 전체 채팅이 포함된다
2. 포함·제외 범위가 있으며 채팅이 포함된다고 전제하지 않는다
3. 모든 예전 사본을 갱신한다

> **정답 보기: 포함·제외 범위가 있으며 채팅이 포함된다고 전제하지 않는다**
> 신원 복구와 메시지 복구는 다릅니다.

제대로 설정한 자체 노드의 기능은 무엇인가요?

1. 모든 정보 유출을 없앤다
2. 제삼자 조회 의존도를 줄이고 직접 검증할 수 있다
3. 잃어버린 키를 되찾는다

> **정답 보기: 제삼자 조회 의존도를 줄이고 직접 검증할 수 있다**
> 익명성이나 비밀 복구를 보장하지 않습니다.

Desk에서 UTXO를 동결한다는 뜻은 무엇인가요?

1. 해당 앱 안의 로컬 제한이다
2. 합의 조건을 바꾼다
3. 다른 시드 사본을 무효화한다

> **정답 보기: 해당 앱 안의 로컬 제한이다**
> 네트워크 전체의 지출을 막지는 않습니다.

발행을 누르자마자 연결이 끊기면 어떻게 해야 하나요?

1. 즉시 다시 결제한다
2. 지갑을 삭제한다
3. 먼저 이미 결제가 전파되었는지 확인한다

> **정답 보기: 먼저 이미 결제가 전파되었는지 확인한다**
> 시간 초과는 작업이 반영되지 않았다는 증거가 아닙니다.

주소를 재사용하거나 서로 다른 맥락의 UTXO를 합치면 어떤 일이 일어날 수 있나요?

1. 관계를 더 쉽게 관찰할 수 있다
2. 이전 이력이 지워진다
3. 익명성이 보장된다

> **정답 보기: 관계를 더 쉽게 관찰할 수 있다**
> 프라이버시는 맥락과 이후 사용법에 따라 달라집니다.

Tor Browser를 열면 Desk도 자동으로 설정되나요?

1. 예
2. 아니요
3. 다크 테마일 때만

> **정답 보기: 아니요**
> 앱별로 연결 경로를 확인해야 합니다.

xpub처럼 보이는 채팅 키는 무엇인가요?

1. 공개해도 되는 정보
2. 수금 주소
3. 신원에 관한 비밀

> **정답 보기: 신원에 관한 비밀**
> 민감도는 용도로 결정됩니다.

채팅 메시지에 '결제 완료'라고 쓰여 있다면?

1. 네트워크 확인을 대신한다
2. 실제 결제를 네트워크에서 별도로 검증해야 한다
3. 요청의 네트워크가 바뀐다

> **정답 보기: 실제 결제를 네트워크에서 별도로 검증해야 한다**
> 메시지 상태와 결제 상태는 다릅니다.

검토된 Final 멀티시그 프로필은 무엇을 사용하나요?

1. MuSig2와 PSBT v2
2. P2WSH, sortedmulti, BIP48, PSBT v0
3. 모든 비트코인 스크립트

> **정답 보기: P2WSH, sortedmulti, BIP48, PSBT v0**
> 기대나 상품명으로 지원 범위가 늘어나지는 않습니다.

Mirror 12.12에서 어떤 항목부터 비교할 수 있나요?

1. 1단계만
2. 15번을 포함해 원하는 항목
3. 나머지를 모두 마친 뒤 마지막 항목만

> **정답 보기: 15번을 포함해 원하는 항목**
> 비교는 항목 쌍별로 독립적이며 순서가 자유롭습니다.

Mirror의 '일치'가 입증하는 것은 무엇인가요?

1. 전체 승인
2. 두 QR 모두의 출처가 진짜임
3. 비교한 두 값이 글자 그대로 같음

> **정답 보기: 비교한 두 값이 글자 그대로 같음**
> 나머지 검토와 응답은 여전히 필요합니다.

시드가 노출된 뒤 Desk 비밀번호를 바꾸면 어떻게 되나요?

1. 공격자의 권한이 철회된다
2. 그 시드에서 파생된 키는 취소되지 않는다
3. 모든 사본이 지워진다

> **정답 보기: 그 시드에서 파생된 키는 취소되지 않는다**
> 통제권을 안전하게 옮기는 방법을 검토해야 합니다.

실습을 마칠 때 기록해야 할 것은 무엇인가요?

1. 읽기, 시뮬레이션, 실물 시험에서 확인한 내용과 남은 사항
2. 판매한 시간만
3. 절대 뚫리지 않는 수탁이라는 약속

> **정답 보기: 읽기, 시뮬레이션, 실물 시험에서 확인한 내용과 남은 사항**
> 증거마다 뒷받침하는 범위가 다릅니다.