CUVEX

CUVEX ACADEMY · 0.1

Learn. Understand. Take control.

Bitcoin and self-custody, explained step by step. The course, manual, glossary and exercises are free and require no registration. Choose where to start.

Free · no registration

All sections

1. Prepare your learning space
2. Digital money and the problem of trust
3. Bitcoin’s history and limits
4. Working accurately with satoshis
5. Your threat model
6. Nodes, mining and consensus
7. UTXOs and transaction change
8. The mempool, confirmations and reorganizations
9. Fees, virtual size and replacement
10. Networks, addresses and invoices
11. Hashes, signatures and encryption
12. Seed, passphrase and password
13. Derivation, xpubs and descriptors
14. Choosing a wallet and a custody model
15. Backups you can recover from
16. Getting to know Original and BIT
17. Creating a seed with physical entropy
18. Encrypting and decrypting a secret with Cuvex
19. Encryption thresholds and biometrics
20. Cloning, storing and verifying copies
21. Installing and securing Cuvex Desk
22. Linking cryptograms and organizing WOW
23. Pairing Mirror with Desk
24. NFC via Mirror, USB-C and reading QR codes
25. Public providers and your own node
26. Receiving bitcoin and checking the address
27. Labeling, freezing and selecting UTXOs
28. Preparing and reviewing a payment
29. Signing with Original and BIT
30. Finalizing, broadcasting and troubleshooting
31. What can be observed on Bitcoin
32. Separating contexts and managing change
33. Network privacy, Tor and VPNs
34. CoinJoin, Payjoin and their current limits
35. Lessons from real incidents

36. Creating a chat identity and verifying contacts
37. Requesting and paying satoshis in chat
38. Sharing cryptograms deliberately
39. Recovering chat and understanding its metadata
40. Everyday settings and reviewing permissions
41. Designing a multisignature wallet
42. Creating invitations and contributing keys
43. Verifying policies with Mirror in any order
44. Coordinating signatures and broadcasting a multisignature transaction
45. Recovering and changing a multisignature wallet
46. Updating firmware without guesswork
47. Loss, device failure and emergency recovery
48. Phishing, support and voice scams
49. Privacy, legal obligations and personal records
50. Inheritance, continuity and the annual drill
51. Price, saving and fundamental analysis
52. Choosing where to acquire bitcoin
53. Accounts, orders and execution costs
54. Candlesticks, indicators and biases in technical analysis
55. Margin, futures and automation
56. Lightning and other layers
57. Taproot, MuSig2 and a post-quantum future
58. Interoperability and moving away from the manufacturer
59. Technical lab with regtest
60. Final project and continuity plan
61. Student manual
62. Bitcoin and self-custody glossary
63. Check what you have learned

M01

Prepare your learning space

Objective

Set up the course, distinguish the three devices and agree on what information you should never share with the tutor.

Understanding the topic

You will learn to receive, hold, spend and recover bitcoin using your own judgment. By the end, you should be able to explain a decision before authorizing it. You can read the course on your own. The voice tutor offers explanations, questions and guidance. It does not need to see your holdings or control your devices.

Cuvex is the device that protects secrets and lets you authorize operations on its screen. Desk organizes cryptograms, watch-only wallets, payments and coordination on your computer. Mirror is a local bridge for supported operations and a tool for comparing data. It is neither the signer nor a standalone wallet. Your version and model determine which workflow you can use.

Set aside one screen for the course and another for Desk. Keep your phone and Cuvex within reach. If you have only one screen, switch between them without sharing the screen on a video call while entering secrets. A call can end before you finish an exercise. Taking a break is fine. Save only the lesson ID, the step you reached and the difficulty you encountered.

Neither a human instructor nor an AI should receive your seed phrase, BIP39 passphrase, passwords, Chat Key, PIN, private files or full purchase codes. They do not need your xpub, real descriptor or address either. Although these do not allow spending, they reveal activity. Describe error messages and use the lab’s fictitious data.

Practice

1. Identify your computer, phone and Cuvex model. Write down their versions in your private notebook.
2. Keep your learning environment free of funds and separate from your real holdings. Never import a production seed for practice.
3. Open this lesson and find the pause control, help and glossary. If anyone asks for a secret, end that interaction.

Show what you know

Explain who signs, who queries the network and who transports the data. You are ready to move on when you can distinguish these roles without help.

Common question

Do I have to speak to the tutor every day? No. You can study on your own, repeat a session or ask for help with a specific procedure. Access to the course and your balance for the voice service are separate entitlements.

Pause point

L01 complete. Devices identified. No secrets recorded in the course.

The tutor asks for your seed phrase to check that you wrote it down correctly. What do you do?

1. Read it out slowly.
2. Stop the request and check the seed phrase only in my own secure environment.
3. Send just the first few words.

> **Show answer: Stop the request and check the seed phrase only in my own secure environment.**
> No part of a secret belongs in the training service.

M01

Digital money and the problem of trust

Objective

Understand the problem Bitcoin seeks to solve before you open a wallet.

Understanding the topic

A bank balance is an entry managed by an institution. The institution authenticates customers, decides which transfers to process and keeps the books. An ordinary digital file is easy to copy. Sending someone a photo does not stop you keeping another copy. For a digital unit to work as money, it must be possible to prevent it being spent twice.

Bitcoin combines validation rules, signatures and a shared transaction history. Instead of entrusting the entire record to a single organization, it lets independent participants verify whether a transaction follows the rules. Scarcity depends on those rules continuing to be checked and accepted. It does not come from the image of a coin or the price an exchange quotes.

Self-custody changes your responsibilities. You can retain the ability to spend without a custodian’s permission, but you can lose it by destroying every backup or signing the wrong payment. The freedom to act still requires security, coordination, connectivity to broadcast a transaction and compliance with applicable obligations.

Distinguish Bitcoin, the network and protocol, from BTC, its monetary unit. Other networks use the word blockchain and may offer different properties. A company’s promise denominated in “bitcoin” is also different from controlling a Bitcoin output with your own keys.

Practice

1. Compare three situations: a bank balance, an exchange balance and a UTXO controlled by your keys.
2. For each one, write down who can stop you moving the balance and who can help if you forget how to access it.
3. Describe what would happen if you copied a photo and what would happen if you tried to spend the same output twice.

Show what you know

Explain in your own words how a balance differs from the ability to sign. You do not need to memorize technical terms.

Common question

Does self-custody remove all intermediaries? You can choose services for buying, querying information or communicating. What matters is how much power those services retain and which data they receive.

Pause point

Save your comparison of responsibilities without naming real accounts.

Which monetary problem does a digital signature by itself fail to solve?

1. Preventing an attempt to spend the same output twice.
2. Proving authorization with a key.
3. Detecting a change to the signed message.

> **Show answer: Preventing an attempt to spend the same output twice.**
> Signatures authorize spending. Rules and consensus determine the order of conflicting spends.

M01

Bitcoin’s history and limits

Objective

Place Bitcoin’s origins in context and distinguish historical facts from marketing claims.

Understanding the topic

Satoshi Nakamoto circulated the Bitcoin paper in 2008, and the network started in 2009. The paper proposed peer-to-peer electronic cash, building on earlier work in cryptography, proof of work and digital money. You do not need to know Satoshi’s legal identity to verify the software or a transaction.

Bitcoin has evolved without a single company unilaterally replacing its rules. Developers propose and review changes, operators choose software, miners build blocks, and users and services decide what to accept. This distribution of roles can lead to disagreement. A fork and an application update are different things.

A node can reject a block that breaks its rules even when a great deal of work went into producing it. Consensus is more than a simple vote by number of computers. Running thousands of copies of a node does not automatically grant more decision-making power. Likewise, a majority of miners does not thereby obtain a user’s private key.

Bitcoin has deliberate limits and trade-offs, including block capacity, verification costs, variable confirmation times and a public record. It provides neither administrative payment reversals nor comprehensive confidentiality by default. Layers and applications address particular use cases at the cost of new dependencies.

Practice

1. Place the initial paper, the start of the network, SegWit adoption and Taproot activation on a timeline. Check the dates against sources before publishing them.
2. Classify “a company guarantees the price,” “a node validates” and “a miner proposes a block” as marketing promises or technical functions.
3. Explain one benefit and one cost of having no administrator who can reverse payments.

Show what you know

Distinguish a consensus rule, a local policy and a business decision. The application you use represents only part of the network.

Common question

Does the latest software always change monetary rules? No. Releases also fix bugs, improve performance or change local policies. Read the release and compatibility notes.

Pause point

Write down one verifiable property and one claim that would need further evidence.

A block includes a spend without valid authorization. Can a majority of miners make it valid?

1. Yes, if it exceeds 51%.
2. Only if the exchange announces it.
3. Not for a node enforcing the rules that reject it.

> **Show answer: Not for a node enforcing the rules that reject it.**
> Accumulated work is compared among histories that are valid under the node’s rules.

M01

Working accurately with satoshis

Objective

Convert between BTC and satoshis and check amounts without relying on an exchange rate.

Understanding the topic

One BTC equals 100,000,000 satoshis. A “sat” is a unit of bitcoin. On the base chain, amounts are recorded as whole numbers of satoshis. 0.001 BTC equals 100,000 sat, and 0.00001000 BTC equals 1,000 sat. The decimal separator shown by an interface depends on the language. Never add zeros by eye.

A price quote converts BTC into a currency such as EUR or USD at a given time. It does not change how many satoshis you control. If you have 100,000 sat and the price changes, you still have the same number of satoshis. Desk displays a reference price with a source and date. An old quote can lead to a poor financial decision even if the BTC balance is correct.

Distinguish the amount the recipient will receive, the network fee and the total spent. If you send 50,000 sat with a 600 sat fee, 50,600 sat leaves your wallet, apart from any outputs that return to you. “Send all” normally results in the recipient receiving less than the available balance because the fee must be covered.

The course examples are arithmetic exercises. They do not quote market prices or recommend fee rates. Before signing, verify the unit, network, recipient and total cost on the relevant screen. The voice interface can say “fifty thousand satoshis” while displaying “50,000 sat.” It should never choose an amount based on an uncertain transcription.

Practice

1. Convert 250,000 sat to BTC: 0.0025 BTC. Convert 0.00025000 BTC to satoshis: 25,000 sat.
2. Calculate the cost of sending 75,000 sat with a 900 sat fee: 75,900 sat in total.
3. In the simulator, start with 120,000 sat, send 70,000 and set a fee of 1,000. Check that the change is 49,000 sat.

Show what you know

Read an amount in BTC and in sat, and explain which figure includes the fee. If you are unsure, pause the operation.

Common question

Do I need to buy a whole bitcoin? No. You can buy a fraction, subject to the provider’s minimums and fees.

Pause point

Keep only your exercise results.

You have 80,000 sat and want to send the entire balance with a fee of 1,200 sat. How much does the recipient receive?

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

> **Show answer: 78,800 sat.**
> With no other outputs in this example, the recipient receives the spendable balance minus the fee.

M01

Your threat model

Objective

Choose proportionate measures against loss, theft, deception and data exposure.

Understanding the topic

Security means retaining the ability to act as you intend. Privacy means controlling who knows your data and relationships. Availability means having access when you need it. A box that nobody can open might also lock you out. A very convenient copy might expose too much information.

Identify assets, adversaries and accidents. Assets include keys, backups, transaction history, backup locations and contacts’ identities. Risks include malware, phishing, fire, forgetting information, coercion, equipment failure, death and your own mistakes. No single tool reduces all these risks.

Use a simple matrix with estimated likelihood, impact and a specific measure. A long password makes guessing harder. It cannot correct a fraudulent destination that you authorize yourself. Two backups in the same bag do not protect against losing that bag. A multisignature setup whose devices and backups one person controls can still have a common point of failure.

The course and the tutor are part of your model, too. Purchases, calls, connection times and progress can create metadata. The course site should not ask for addresses or balances to personalize a lesson. The fact that Desk or Mirror does not require conventional registration says nothing about what the store, a voice provider or a third-party query may reveal about your activity.

Practice

1. Write down your three most important risks without listing amounts held or exact locations.
2. For each risk, choose measures for prevention, detection and recovery. For example, address the loss of a card through two separate copies, an inventory and a restoration test.
3. Identify which person or system can observe a purchase, a call, a balance query and a public transaction.

Show what you know

Explain how your next measure addresses a particular risk. Avoid complexity that you cannot maintain or explain to your heirs.

Common question

Do more devices always mean greater security? Only if they reduce shared dependencies and you can test recovery. Extra devices also mean more maintenance and more opportunities for confusion.

Pause point

Keep the plan in your private records. Record only “threat model reviewed” in the course.

Which measure best reduces the risk of losing every backup in a fire at one location?

1. Change the card’s color.
2. Put two copies in the same drawer.
3. Keep tested copies in locations exposed to independent risks.

> **Show answer: Keep tested copies in locations exposed to independent risks.**
> The backup arrangement must survive the same incident that threatens the original.

M02

Nodes, mining and consensus

Objective

Explain what nodes validate and what mining contributes.

Understanding the topic

A full node receives blocks and transactions, verifies the rules and maintains a view of the chain. It need not trust the balance a website reports. Mining is the process of proposing blocks through proof of work. Miners select valid transactions and compete to find an acceptable block.

Proof of work makes rewriting history expensive. When valid alternatives exist, accumulated work matters. Counting blocks alone ignores difficulty. Intervals between blocks vary. Ten minutes is a target average, not a scheduled time for your next payment.

The mining reward combines the block subsidy and transaction fees. The subsidy decreases according to a schedule based on block height. Fees depend on the transactions included. A higher payment fee cannot make an invalid signature valid. Economic security and attack costs do not make a recent payment mathematically irreversible.

Running your own node allows verification and reduces the need to send queries to outside providers. You still need to protect its operating system, access and connection. A node that is running but unsynchronized, or an app configured to query a different server, does not automatically give you these benefits.

Practice

1. Assign responsibility for checking a signature, choosing transactions for a block, safeguarding your seed and deciding whether to accept a payment.
2. Explain why “the miner holds my bitcoins” is incorrect.
3. In a lab network, observe block height and synchronization. Never publish RPC credentials.

Show what you know

Describe the difference between verifying and proposing. You can use an analogy, but finish by describing the actual technical function.

Common question

Must I mine to use Bitcoin? No. You can also start without your own node, although you need to understand how much trust you are placing in your provider.

Pause point

Record the type of lab provider without its private URL.

What can a properly configured full node do for its user?

1. Verify that the chain it accepts follows the rules.
2. Recover any lost key.
3. Guarantee that the price will rise.

> **Show answer: Verify that the chain it accepts follows the rules.**
> Validation and custody are different functions.

M02

UTXOs and transaction change

Objective

Read a transaction in terms of the outputs it spends and creates.

Understanding the topic

A UTXO is an output of a previous transaction that remains unspent. A wallet calculates its balance by identifying the outputs it can control. There is no universal account that gets debited like a bank ledger. An input refers to a previous output by transaction ID and output position.

A UTXO is spent in full. To pay less than its value, you typically create an output for the recipient and a change output you control. With an input of 120,000 sat, a payment of 70,000 and a fee of 1,000, the change is 49,000. The input total must equal the output total plus the fee.

An address is distinct from a UTXO. It can receive several outputs and does not necessarily represent one person. A transaction ID may already be public, but linking it to your identity or explaining who owns each output adds information the chain alone does not provide.

This structure matters for privacy. Combining inputs can suggest common control, and change can link future payments. Collaborative transactions exist, so that inference is not universally valid. Coin control means choosing the outputs to spend while understanding the effects of combining them.

Practice

1. Draw three fictitious inputs of 40,000, 60,000 and 200,000 sat. Use only the first two to pay 70,000 with a fee of 1,000.
2. Check that the change is 29,000 sat and that the third input is unused.
3. Repeat using only the 200,000 sat input. The change would be 129,000. Compare potential costs and links without assuming equal transaction sizes.

Show what you know

Locate the input, recipient, change and fee in the course diagram. If you cannot identify an output, do not sign a real transaction.

Common question

Is everything that returns to my wallet change? No. It might be a transfer to a different address of your own. Classification requires knowing the policy and derivation. The amount alone is insufficient.

Pause point

Keep the fictitious diagram. Never keep a screenshot of your holdings for this exercise.

An input of 100,000 sat produces outputs of 30,000 and 69,200 sat. What is the fee?

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

> **Show answer: 800 sat.**
> 100,000 minus 99,200 equals 800 sat.

The mempool, confirmations and reorganizations

Objective

Distinguish a prepared transaction from one that has been broadcast or confirmed.

Understanding the topic

A mempool is the local set of unconfirmed transactions that a node keeps under its policies. Nodes do not share one identical worldwide mempool. If an explorer shows your payment, that service knows about it. This guarantees neither acceptance by all nodes nor confirmation within a particular time.

Preparing a PSBT does not broadcast anything. Signing produces authorization. Finalizing creates the transaction that can be broadcast. Broadcasting attempts to transmit it. Confirmation means it was included in a block of the chain accepted by your verification source. A second confirmation means another block has been built on top, not that the recipient signed again.

A reorganization can change part of the chain, causing a transaction to lose confirmations or become pending again. The parties to higher-exposure payments usually require more confirmations. No single number removes every risk for every amount and situation.

If Desk displays a saved status, check the synchronization date. “Confirmed” in an old snapshot may no longer describe the current state. If a payment is missing, keep its local ID and check its broadcast status and history before preparing it again. An impatient retry can create a second valid payment.

Practice

1. Put these cards in order: draft, PSBT, signature, final transaction, broadcast, inclusion in a block.
2. Simulate a disconnection after broadcasting. Decide what to check before paying again.
3. Explain to a merchant why a chat message saying “paid” cannot replace verification on the network.

Show what you know

State the transaction status, the source and the date of that information without treating it as a guarantee.

Common question

Does closing Desk cancel a broadcast transaction? No. Other nodes and participants may retain it. Canceling a local draft has a different scope.

Pause point

Record the state of the simulation. Do not give the tutor real transaction identifiers.

Your computer disconnects just after you press Broadcast. What do you do first?

1. Prepare the same payment again from scratch.
2. Delete the wallet.
3. Reconnect and check the transaction and its inputs.

> **Show answer: Reconnect and check the transaction and its inputs.**
> A missing response does not prove that broadcasting failed.

M02

Fees, virtual size and replacement

Objective

Estimate costs, interpret sats per vbyte and understand RBF and CPFP.

Understanding the topic

The network fee is the difference between the value of the inputs and outputs. Fee competitiveness is usually expressed in sat/vB, satoshis per virtual byte. It does not depend directly on the monetary value sent. Many inputs can make a small payment expensive, while a large payment with few inputs can take less space.

For example, 200 vB at 5 sat/vB costs 1,000 sat. Before signing, the fee may only be an estimate because the final size can depend on the signatures and structure. Desk offers estimated speeds and a manual fee rate. A “fast” label does not promise confirmation by a particular time.

RBF is a policy for replacing unconfirmed transactions under certain conditions. It allows a conflicting spend with a higher fee to be proposed. Node policies have evolved, so a signal that a transaction is not replaceable is no guarantee of payment. A replacement requires a fresh review and the necessary signatures.

CPFP spends an output of a pending transaction to make confirming parent and child together attractive. It requires control of a spendable output, compliance with applicable policies and payment of its cost. This is a Bitcoin technique. Do not assume the student’s Cuvex version offers a CPFP button.

“Dust” is an output considered too small under the applicable policies and estimated spending costs. The threshold varies with script type and other conditions. Do not teach one fixed figure as a consensus rule. If a change output is impractical, review the amount, selected inputs or sweep, and the effective fee.

Practice

1. Calculate the fee for 180 vB at 8 sat/vB: 1,440 sat. Check it against your lab budget.
2. Compare one input with ten inputs. Explain why the amount sent is insufficient for estimating the cost.
3. Simulate a pending transaction and choose whether to wait, use RBF or investigate CPFP. Check actual support before relying on a feature.

Show what you know

Justify the fee rate, the absolute fee and its cost relative to the payment. Reject a fee you cannot explain.

Common question

Does RBF guarantee cancellation of an earlier payment? No. The competing versions remain in play until confirmation, and propagation matters. Do not release goods on the promise of cancellation.

Pause point

Save your decision and the reason for it.

What fee results from 250 vB at 4 sat/vB?

1. 1,000 sat.
2. 254 sat.
3. 4% of the amount sent.

> **Show answer: 1,000 sat.**
> Virtual size multiplied by the fee rate gives the estimated fee.

M02

Networks, addresses and invoices

Objective

Recognize the network, address format and payment instructions before copying or scanning them.

Understanding the topic

Mainnet transfers bitcoin with real economic value. Test networks support development and learning, but they are not interchangeable. Regtest is a local network controlled by the lab operator. Signet and testnet each have their own rules and ecosystems. Single-signature support on signet does not establish that the Cuvex multisignature profile supports that network.

Addresses encode receiving conditions. On mainnet you will encounter formats beginning with 1, 3, bc1q or bc1p. A prefix helps identify a family. It does not verify the recipient, guarantee that the signer is compatible or replace validation of the complete format.

A QR code is a visual container. It can carry an address, an invoice, a descriptor or malicious text. Scanning it does not authenticate its author. A bitcoin: link can also specify an amount and message. BIP321 is the modern reference that supersedes BIP21. The reviewed Desk implementation retains BIP21 terminology and compatibility. An updated standard does not by itself expand what an app understands.

A Lightning invoice differs from an on-chain address. It may contain an expiry time and other fields. Never paste it into an on-chain payment if the application does not offer a compatible workflow. A token called BTC on another network is not automatically native bitcoin either.

Practice

1. Classify the labeled course samples without using spendable addresses: an address, a bitcoin: URI, a Lightning invoice and a descriptor.
2. Identify the selected network in the lab. The reviewed Cuvex multisignature profile supports mainnet/regtest.
3. Before a real transaction, compare the complete text the recipient requested through an authenticated channel.

Show what you know

Decline a request if you do not recognize its network or payment method, and explain what you need to verify.

Common question

Can I send BTC over any network an exchange lists? No. The withdrawal network must match the actual receiving method. Do not choose on fee alone.

Pause point

Record only the type of network used for learning.

A bc1 receiving address alone does not authorize a BTC withdrawal on a different token network. What is missing?

1. Change the recipient’s alias.
2. Confirm that the withdrawal uses Bitcoin on-chain and that all details match.
3. Enter the seed on the exchange.

> **Show answer: Confirm that the withdrawal uses Bitcoin on-chain and that all details match.**
> The asset, network and receiving method must be compatible.

M03

Hashes, signatures and encryption

Objective

Distinguish integrity, authorization and confidentiality.

Understanding the topic

A hash transforms data into a fixed-length fingerprint. Comparing it with a known fingerprint helps detect changes. It does not encrypt the file or identify its publisher by itself. If you download both the file and its hash from a compromised page, an attacker may have replaced both.

A private key can create signatures. The corresponding public key can verify them. A signature binds an authorization to a specific message under the algorithm and its rules. It does not conceal what was signed. In Bitcoin, a valid signature can be one of the conditions required to spend an output.

Encryption aims to make content readable only to someone with the appropriate capability. Authenticated encryption also detects alterations. In Cuvex, cryptograms protect secrets, signed transactions authorize spending and encrypted channels transport messages. All three use cryptography for different purposes.

A human-entered password usually passes through a derivation function before use as a cryptographic key. “AES-256” describes the algorithm and key size. It cannot turn a predictable password into a strong choice. Generation, implementation, storage, display and recovery all contribute to overall security.

A complex-looking QR code is no assurance of safety. Understand what it contains, who created it and how the application will use it. Before accepting an action, ask the tutor to explain its purpose without asking for the private data.

Practice

1. Match “detecting a file change,” “hiding a seed” and “authorizing a payment” to a hash, encryption and a signature.
2. Change one letter in fictitious text and observe the change in its hash. Use no secrets for this demonstration.
3. Explain how a transaction can be both public and signed.

Show what you know

Describe the property you need and which mechanism provides it. Avoid using “encrypted” to describe every kind of security.

Common question

Does a firmware hash certify that the firmware has no bugs? No. It identifies bytes if the reference is reliable. An audit, a manufacturer’s signature and a physical test answer different questions.

Pause point

Save the three matches from the exercise.

Which mechanism conceals the content of a secret?

1. Publishing its filename.
2. Signing it without encrypting it.
3. Encrypting it correctly with a protected key.

> **Show answer: Encrypting it correctly with a protected key.**
> Neither a signature nor a fingerprint provides confidentiality on its own.

M03

Seed, passphrase and password

Objective

Avoid confusing the system’s different credentials.

Understanding the topic

A BIP39 mnemonic represents entropy and a checksum using words from a wordlist. The standard lengths are 12, 15, 18, 21 or 24 words. Choosing a memorable expression, song lyrics or words that seem random to a person does not reproduce secure generation. The checksum detects some mistakes. It does not prove who created the seed or that nobody else knows it.

The BIP39 passphrase participates in deriving the binary seed. A different passphrase can open a completely different, apparently empty wallet. You may never see a “wrong passphrase” warning. The passphrase need not be a word from the list and is not literally a twenty-fifth word.

The Cuvex cryptogram password protects the stored secret. The Desk password protects local storage on the computer. A pairing PIN authorizes a communication session. The Chat Key recovers a messaging identity. Each differs from the seed. Knowing one does not let you reconstruct all the others.

Keeping a seed and its passphrase together in one cryptogram may simplify recovery, but anyone able to decrypt it gains access to both. Separating them places greater demands on you and your heirs. Document and test your decision. Do not choose an option because a tutor calls it “more advanced.”

Practice

1. Make five paper cards labeled seed, passphrase, Cuvex password, Desk password and Chat Key. Do not write actual secret values on them.
2. Write what each one recovers and what you would lose if you forgot it.
3. Design a test using an empty wallet. Enter the words and the passphrase privately. Tell the tutor only the result.

Show what you know

Explain why the course should never request a password to “validate” your learning. Identify which secret your recovery procedure requires.

Common question

Can my email address reset my passphrase? BIP39 has no such mechanism. A custodial provider may offer account recovery, which is a different model.

Pause point

Record “credentials distinguished” without writing down any of their values.

You change one letter in a BIP39 passphrase and see a zero balance. Which explanation is correct?

1. It may be another valid wallet derived from the different passphrase.
2. The network erased your funds.
3. Desk must guess the original passphrase.

> **Show answer: It may be another valid wallet derived from the different passphrase.**
> A different passphrase can produce another wallet without generating an error.

M03

Derivation, xpubs and descriptors

Objective

Understand how to describe a wallet without giving away the ability to spend.

Understanding the topic

A hierarchical wallet derives many keys from a root. A path identifies the branch in use. On mainnet, BIP84 commonly uses m/84'/0'/0' for the first single-signature SegWit account. BIP48 P2WSH uses m/48'/0'/0'/2' for the first multisignature account. The apostrophe marks hardened derivation. Changing the account, network or script type can produce different addresses from the same mnemonic.

An xpub is an extended public key that can derive certain descendant public keys. It is not a spending password, but it can reveal a family of addresses. A master fingerprint is a short identifier useful for associating records. By itself it cannot guarantee identity or prevent collisions.

A descriptor specifies how to construct scripts and addresses, including the script type, keys, origins and derivation paths. A watch-only descriptor containing public keys enables monitoring without signing. The word “descriptor” does not guarantee that all its contents are public. Some formats can include private keys. Never upload a real descriptor to the course.

Recovering a multisignature wallet normally requires the full policy in addition to one signer’s words. Preserve the threshold, participants, xpubs, paths, network, script type and discovery data. The descriptor checksum helps catch transcription errors. It does not authenticate the participants.

Practice

1. Read a fictitious path and explain its purpose, coin, account and branch. Do not enter real keys.
2. Distinguish a receiving address, a participant’s xpub and a complete descriptor.
3. Prepare a private recovery form with empty field labels and a separate place to keep the documentation.

Show what you know

Explain why an empty wallet after restoration does not prove loss. Check the network, passphrase, script, account, path and discovery settings.

Common question

Can an xpub be published without consequences? It does not normally allow spending on its own, but it exposes private information and may increase other risks in particular cryptographic combinations.

Pause point

Keep the form in the course without any sensitive values.

What information might be missing if you try to recover a multisignature wallet with just one seed?

1. The device’s color.
2. The policy and the other participants’ public keys.
3. A social media password.

> **Show answer: The policy and the other participants’ public keys.**
> Reconstructing the scripts requires the full policy as well as the threshold number of private keys.

M03

Choosing a wallet and a custody model

Objective

Compare tools by their functions, trust requirements and recovery procedures.

Understanding the topic

A wallet is a set of tools for describing and monitoring funds and, where applicable, authorizing spending. A hot wallet can sign in a connected environment. An isolated signer aims to keep secrets separate from the device querying the network. A watch-only wallet holds enough public information to monitor activity and prepare transactions but needs another system to sign.

Under third-party custody, an account may represent a claim against a company. In self-custody, you retain the technical ability to spend, alone or jointly. Email recovery and the power to block a withdrawal usually indicate the first model. Assess the two arrangements using the responsibilities specific to each.

Compare supported networks and script types, on-screen verification, backups, updates, interoperability, maintenance, provider queries and the clarity of error messages. A list of coins or a polished case is insufficient. A signing device cannot stop you approving an incorrect address if you fail to check it.

Cuvex separates secrets protected in cryptograms from organization and network queries in Desk. You must retain both the cryptogram and the means to unlock it. Protection against losing the device does not ensure recovery if all copies or passwords are lost as well. Learn the whole procedure before moving funds.

Practice

1. Compare Cuvex, a hot wallet and an exchange in a table. Identify who signs, who sees the queries, who can recover access and what happens if the company closes.
2. Choose two criteria that require evidence beyond advertising.
3. Verify that the practice environment and your actual savings use separate keys.

Show what you know

Justify your choice for one specific case without declaring any tool invulnerable.

Common question

Does a hardware wallet make every transaction private? No. It primarily protects signing capability and parts of the review. The blockchain, network queries and counterparties still generate information.

Pause point

Keep the comparison table without including account names.

What can a watch-only wallet properly configured with public keys do?

1. Monitor activity and prepare transactions without being able to sign them on its own.
2. Change a lost seed.
3. Guarantee anonymity.

> **Show answer: Monitor activity and prepare transactions without being able to sign them on its own.**
> Monitoring and authorizing can be separate capabilities.

M03

Backups you can recover from

Objective

Design a complete backup and demonstrate recovery before relying on it.

Understanding the topic

A useful backup restores a capability, not simply a file. For single-signature use, this may require the mnemonic, passphrase and derivation details. Multisignature recovery also requires the policy and enough signers. Desk may need an encrypted backup and its password. In chat, recovering the identity does not mean recovering old messages.

Redundancy protects against accidental loss. Separation protects against several components being compromised together. Two copies on different media and in different locations can reduce correlated failures. Every extra copy also needs access controls, inventory and review. Filenames and labels should neither reveal your holdings nor make every component easy to locate.

Test against an address you previously verified. In a learning environment, also test the ability to sign a controlled transaction. Opening a file does not prove it belongs to the right wallet. Never test a backup by entering your production seed on an arbitrary computer.

Document what each backup includes and excludes. Changing the current password does not automatically change older copies. If a previous password was exposed, backups protected with it remain affected. Deleting a file from modern storage also does not guarantee removal of all its copies or versions.

Practice

1. Complete a private table with the object, contents, associated password, independent location, test date and responsible person.
2. Restore a learning backup in a separate environment. Verify the network, first address and derivation.
3. Simulate losing the computer and then losing the device. Identify which part of the procedure changes.

Show what you know

Recover your test scenario without improvised assistance and explain what would still be missing in a different scenario.

Common question

Is a full Desk backup a copy of everything? Do not assume so. The reviewed implementation excludes chat history and chat sessions. The multisignature policy and private keys also serve different functions.

Pause point

Record the test date and outcome. Never record the backup’s contents in the course.

You change the Desk password. What happens to a previous backup?

1. It updates itself.
2. It automatically loses its encryption.
3. It retains the protection and password used when it was created.

> **Show answer: It retains the protection and password used when it was created.**
> Previous backups are independent objects.

M04

Getting to know Original and BIT

Objective

Choose the right workflow for the device and its version.

Understanding the topic

Original uses NFC cards to transport cryptograms and supported operations. It uses Bluetooth for updates and, in the documented model, USB-C for power. BIT uses USB-C for file exchange and provides biometrics for cryptograms that require them. Do not apply Original’s NFC or Bluetooth instructions to BIT.

The device offers encryption, decryption, wallet creation, signing and settings. Original can clone cards. BIT works with files on its USB medium. Labels, languages and entry points may vary by version. BIT’s new “Verify policies” entry opens the supported workflow without changing who authorizes it.

The editorial references are Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 and Mirror beta.12.12. These are source references. Signing, distribution and physical acceptance of each combination need to be verified with the team. Never replace your firmware with an unsigned binary from an engineering package.

Before use, check provenance, seals, appearance and version. Traceability and an update signature help address particular threats but cannot replace every check. If you see tampering or an unexpected version, pause initialization and contact support through a channel you have verified.

Practice

1. Identify the model and record the visible version without photographing secrets.
2. Locate encrypt, decrypt, create wallet, PSBT and settings. Do not start an erase or an update just to explore menus.
3. Choose the Original or BIT branch of the course and keep that selection throughout the exercise.

Show what you know

Explain how an operation enters and leaves your model and which medium needs protection against overwriting.

Common question

Is BIT automatically safer for everyone? The models offer different operating choices. The answer depends on threats, recovery and correct use.

Pause point

Keep the model and version in your local notes. The course only needs the model you selected.

You have a BIT, but a guide says the device itself must write to an NFC card. What do you do?

1. Check which model the guide covers and use the supported USB workflow.
2. Force the Original update.
3. Send the seed to the phone.

> **Show answer: Check which model the guide covers and use the supported USB workflow.**
> The instructions must match the model’s actual transport method.

M04

Creating a seed with physical entropy

Objective

Understand generation and practice the workflow without turning course data into keys you use.

Understanding the topic

Entropy means unpredictability. Dice can provide it if the dice are suitable, you set their order before rolling and the conversion algorithm is correct. Repeat rejected results exactly as the procedure specifies. Substituting the maximum value or choosing another word would introduce bias.

The reviewed Cuvex workflow combines a coin and four dice. It calculates the coin value times 1,296 plus the base-six number formed from each die result minus one. Indices from 0 through 2,047 are accepted. If the result falls outside the wordlist, flip the coin and roll all four dice again. Keeping the coin result and rerolling only the dice would introduce bias. This describes the reviewed source. The screen and complete workflow must be validated for each distributed firmware version.

This differs from choosing favorite words. Never use a public demonstration to generate material for securing money. Treat every seed shown in training materials as known. The device’s complete algorithm must produce the final word and its check. Do not complete a mnemonic by hand.

Prepare a space without cameras, nearby active voice assistants, screen recording or observers. The tutor should stop while you enter and review the secret. It may explain beforehand and assess your understanding afterward without hearing roll results or words.

After generation, verify the backup, encrypt it as the model requires and test recovery of an empty wallet. A verification address helps check consistency without exposing the seed to the computer. If the workflow accepts values that contradict the instructions or shows unexpected words, stop and record only the version, screen and error.

Practice

1. Follow the device steps with material that holds no funds. Fix the order of the dice and never change results.
2. Repeat rejected inputs according to the screen. Do not adjust them to make them fit.

3. Review the contents privately, make a copy and confirm that you can reconstruct the same learning wallet.

Show what you know

Explain why physical entropy, correct conversion and keeping the result secret are three separate requirements.

Common question

Can I tell the AI my rolls so it can check the algorithm? Not for a seed you intend to use. Assistance uses separate synthetic examples.

Pause point

Leave the device in a secure state. Do not leave a seed on screen during a break.

The firmware rejects a dice input. Which action follows the procedure?

1. Pick a word manually.
2. Repeat as instructed by the device without biasing the result.
3. Reduce the number until it is accepted.

> **Show answer: Repeat as instructed by the device without biasing the result.**
> Rejections are part of entropy conversion. Do not replace rejected results arbitrarily.

Encrypting and decrypting a secret with Cuvex

Objective

Create a learning cryptogram and verify that you can recover it.

Understanding the topic

Select the correct content type, such as BIP39, SLIP39, Monero or text when available in your workflow. These are distinct formats. Encrypting SLIP39 text does not make Cuvex a signer for every network that might use it. Secret storage and signing protocol support have different scopes.

To keep the contents off connected equipment, enter them directly on the device. Importing from a phone or PC may already have exposed the secret at its source, even if it is encrypted afterward. Use the review screen to catch incorrect words, word order, capitalization and fields.

The cryptogram password should be long, unique and recoverable under your plan. The reviewed creation keyboard accepts up to 40 characters. The validator requires at least 12, including uppercase and lowercase ASCII letters, a number and a recognized symbol. Desk’s 12-to-1,024-character policy is different and does not apply automatically to the Cuvex keyboard. Other recovery fields may have different limits. Check the workflow and version.

On Original, write to a suitable blank card and keep it in position until confirmation. On BIT, retain the files created by the USB workflow, including any required biometric components. Do not rename or combine files by guesswork. Then test reading and decrypting on the device without giving the tutor the secret.

Practice

1. Encrypt training text created for this exercise, with no credentials or monetary value.
2. Identify the medium and resulting object. Privately record its alias and purpose.
3. Restart the decryption workflow, verify the text on the trusted display and close the display when finished.

Show what you know

Distinguish correct contents, a successful write and successful recovery. A “file copied” message cannot prove all three.

Common question

Is a card alias a password? No. It is organizational information. Avoid balances or descriptions that make your holdings easier to identify.

Pause point

Never leave decrypted content visible. Record only whether the exercise succeeded or failed.

What best demonstrates that a test cryptogram can recover its contents?

1. It has an attractive name.
2. The file exists in two folders.
3. Read and decrypt it using the correct workflow, then check the contents privately.

> **Show answer: Read and decrypt it using the correct workflow, then check the contents privately.**
> A copy’s existence does not prove that it works or that it corresponds to the expected data.

M04

Encryption thresholds and biometrics

Objective

Distinguish shared protection of a secret from Bitcoin multisignature.

Understanding the topic

A cryptogram protected by multiple passwords controls who can decrypt its contents. A Bitcoin multisignature wallet controls which keys must authorize a spend on the network. A jointly protected secret can belong to a single-signature wallet, and each signer of a multisignature wallet can have a separate individual cryptogram.

If several people jointly unlock one seed that can spend alone, the on-chain threshold remains one key. Once revealed, someone could retain that seed. Do not present this setup as requiring several signatures for every payment.

BIT biometrics add an access condition for the formats that use them. A finger is neither a seed nor a universal password replacement. Plan for injury, fingerprint changes, equipment failure, device availability and inheritance. Keep and test the cryptogram’s documented recovery method before relying on it.

A recovery export may reveal a secret on a computer precisely to resolve an emergency. That capability does not make the PC equivalent to the device. Normal use should maintain isolation. Consider local recovery deliberately and plan a subsequent migration if exposure occurred.

Practice

1. Draw two policies: “two passwords to open one seed” and “two keys out of three to spend.”
2. In a test with no funds, identify the files needed for a biometric backup and where recovery is checked.
3. Simulate one person being unavailable. Determine whether your threshold still allows you to proceed.

Show what you know

Explain who can learn the secret and who can authorize a spend after decryption.

Common question

Can I remove a participant by changing a label? No. Distinguish organizational changes from new protection for the secret and from a new spending policy.

Pause point

Keep the diagram without real names or biometric data.

Three people use two passwords to open a cryptogram containing a single-signature seed. How many keys does Bitcoin require to spend?

1. One, if that is the wallet policy.
2. Two, because the file required two passwords.
3. Three, because there are three people.

> **Show answer: One, if that is the wallet policy.**
> The encryption threshold does not alter the script controlling the coins.

M04

Cloning, storing and verifying copies

Objective

Build redundancy without destroying the only valid copy.

Understanding the topic

Cloning a cryptogram copies encrypted data. It does not create another balance or seed, or remove dependence on an exposed password. Identical copies protect against losing a storage medium but do not repair compromise of the original secret. This is why restoration and migration to new keys address different situations.

On Original, distinguish the cryptogram card from the PSBT transport card. An operations card may be reused as the workflow permits. A card holding your backup should never become that transport medium. If an operation rejects a card containing a cryptogram, do not bypass its protection or erase its header manually.

On BIT, a backup must preserve the complete required set of files and their relationship. A file manager may show a completed transfer before the device has validated the contents or finished its operation. Wait for the specified states and test a copy through controlled recovery.

Keep a private inventory with discreet identifiers, format version and the date and result of the latest test. Separate at least two copies against the incidents in your threat model. Do not upload backups to support channels for diagnosis. Provide sanitized metadata and error codes.

Practice

1. Copy your training cryptogram to another medium through the correct workflow.
2. Disconnect the original medium and recover the test text from the copy.
3. Document how you would handle loss, file damage and password exposure. Each calls for a different procedure.

Show what you know

Identify the copy you tested and explain why the original remains intact.

Common question

Can I erase the original once I see a second file? Verify recovery and coverage first. Deletion should follow a plan, not simply a count of copies.

Pause point

Store the media before ending the session. Keep backup cards separate from cards used for payment tests.

Someone knows the password and obtains a copy of the cryptogram. What does making three more clones achieve?

1. It revokes the attacker’s copy.
2. It adds redundancy without revoking that access.
3. It automatically changes the Bitcoin seed.

> **Show answer: It adds redundancy without revoking that access.**
> Duplication cannot undo an existing compromise.

M05

Installing and securing Cuvex Desk

Objective

Open an installation from a verified source and protect its local storage.

Understanding the topic

Select the package for your system and architecture. Depending on the distribution available, this may be macOS Intel or Apple Silicon, Windows x64 or ARM64, or Linux x64 or ARM64. A source ZIP, a Manager package and a client installer are different distributions. The course should never direct a student to a private signing package.

Check the source and the operating system’s verification results. A Windows engineering signature alone does not establish public trust in the publisher. On Mac, application signing, notarization and assessment when opening are separate controls. Never disable system-wide protections on the instructions of someone claiming to be support. If a release produces an unexpected warning, retain its text and use the official channel.

Desk creates password-protected encrypted local storage. In the reviewed implementation, new passwords may contain 12 to 1,024 characters. Where confirmation is requested, both fields must match. Length alone does not guarantee strength. Use a unique phrase and avoid reuse. Where available, computer biometrics offer convenient access and need their own configuration.

Set a lock after inactivity and, where appropriate, when the app goes into the background. The manual covers delays after failures and optional erasure. Do not enable automatic erasure during a demonstration. The app can work without an ordinary user account, but network queries, chat and download services have their own requirements and communications.

Practice

1. Verify the platform, visible version and source of the package without giving the tutor private identifiers.
2. Create a learning store, lock it and reopen it. Enter its password privately.
3. Plan an encrypted backup and keep its password according to your plan. Do not test repeated lockouts on your real setup.

Show what you know

Distinguish the local password, the commercial account and credentials for services you add.

Common question

Does changing my Desk password change my cards’ passwords? No. They are independent protections. Older backups do not change automatically either.

Pause point

Lock Desk and save the lesson ID without credentials.

The installer does not match your computer architecture. What should you do first?

1. Disable safeguards to force it to run.
2. Obtain the correct official package and check its requirements.
3. Import the seed into a website to continue.

> **Show answer: Obtain the correct official package and check its requirements.**
> Establish compatibility and provenance before using custody material.

Linking cryptograms and organizing WOW

Objective

Link an encrypted copy and distinguish it from a watch-only account.

Understanding the topic

Desk organizes cryptograms linked through NFC, USB or a compatible backup file. A visual design and alias help you recognize them but provide no cryptographic proof of identity. The details view shows the source and properties interpreted by the app, including format, size and access characteristics.

Linking imports or organizes a supported object. It does not decrypt it on the PC or verify the secret. WOW is a watch-only wallet associated through compatible public information. One set of secrets can have different accounts or derivation paths. Make sure the association is for the wallet you intend to manage.

Activate or import the account using the descriptor or public information exported by the device workflow. Review the network, script type, fingerprint, path and verification address. The account name is organizational. An identifier derived from a predictable name can be guessed and does not provide strong anonymization.

The reviewed Desk implementation retains accounts awaiting association and offers functions to export backups, clone objects and delete local records. Deleting a card in the interface neither destroys outside copies nor moves funds. “No backup” means the app cannot verify a copy under its criteria. A backup could still exist elsewhere.

Practice

1. Link the training cryptogram through the chosen transport and review its details.
2. Import a compatible learning account and check its network and verification address without showing keys to the tutor.
3. Distinguish the cryptogram record, the WOW account and the physical medium. Identify what local deletion would remove.

Show what you know

Explain which data Desk needs for monitoring and which data should usually remain off the computer.

Common question

Does linking a .bin file guarantee that it holds my seed? No. Verify its provenance and recovery. A file extension does not certify the contents.

Pause point

Keep only the status “test link verified.”

Does deleting a WOW account locally move its bitcoins?

1. No. It removes local information according to the workflow without spending UTXOs.
2. Yes. It sends them to the manufacturer.
3. It cancels any signature someone else has retained.

> **Show answer: No. It removes local information according to the workflow without spending UTXOs.**
> Local state and blockchain state are distinct.

M05

Pairing Mirror with Desk

Objective

Establish and end an authorized local connection without confusing its codes.

Understanding the topic

Mirror supports local operations with Desk through the pairing, PIN and QR workflow shown in the applications. The six-digit PIN belongs to that session. It is separate from the Desk password, cryptogram password and recovery words. Check which screen generates it and where it should be entered. Do not use a code sent by a stranger.

Start in the correct Desk context. Linking, reading a QR code, transporting a PSBT and updating firmware serve different purposes. The window reports search, connection, discovery, PIN, QR and action on a card or file. A device appearing in the search results does not mean the operation has finished.

Grant the permissions the system requires, such as camera access for optical reading and Bluetooth or NFC for workflows that need them. Software cannot add missing physical capabilities to a phone. Adapter and validation details differ on iOS. A project that compiles must not be presented as already distributed and tested on every iPhone.

If an operation fails, identify the precise stage. The device may be absent, found but unable to connect, the PIN rejected, the QR unreadable, the card unread or the response missing. Close old sessions, verify compatible versions and permissions, then retry in a controlled way. An incorrect PIN is no reason to change firmware or enter seed words elsewhere.

Practice

1. Start a test read in Desk and connect Mirror using the local screens.
2. Check the purpose before presenting a training QR code or card.
3. Cancel the session and confirm that a late reading from the previous context is not applied. Open a fresh session.

Show what you know

Describe the failed stage and the devices involved without disclosing active codes or sensitive contents.

Common question

Must Mirror stay connected at all times? It depends on the operation. Do not treat it as a permanent service or assume a session remains authorized after closure or backgrounding.

Pause point

Close the pairing session and lock applications you are not using.

What should the tutor do if pairing fails before the PIN appears?

1. Ask for the seed.
2. Check discovery, permissions, session and versions before proceeding.
3. Assume the connection succeeded.

> **Show answer: Check discovery, permissions, session and versions before proceeding.**
> Diagnosis should follow the observed stage. It should never assume a successful connection.

NFC via Mirror, USB-C and reading QR codes

Objective

Use each transport method for its intended purpose and carry out the required checks.

Understanding the topic

Cuvex Desktop’s NFC workflows require Cuvex Mirror on a compatible smartphone paired with the computer over Bluetooth. Cuvex Desktop does not support external USB NFC readers. The card, its format and its capacity must also be compatible. A small card that holds a cryptogram may not fit a PSBT containing previous transactions. The effective limit depends on the complete contents, not just the number of recipients. Never use a backup card as a transport card.

With Original, Mirror can write a request to an operations card. Original processes it and writes a response, which Mirror returns to Desk. Confirmation that the card was written does not confirm that Desk received the response. Hold the card steady until the device reports the result. If the system refuses an operation to protect a recognized cryptogram, respect that refusal.

BIT exchanges files through a USB volume or folder. During the exchange the volume may disappear and be presented again. Desk must select the right medium, validate the response and acknowledge it as the protocol requires. Copying a file to a PC folder with the same name does not deliver it to the device.

Focus, glare, size, movement or code density can keep a camera from reading a QR code. Enlarge the displayed data and adjust the lighting and distance. Do not shorten a long identifier to its first few letters or accept a partial transcription. A successful scan is only the start of validating what the data means.

Practice

1. Using the course materials, identify the request, medium and response for Original and BIT in the diagram.
2. Try canceling a QR scan without retaining any value that arrives late. Repeat with a different purpose.
3. Simulate a file that is too large. Explain how to simplify the transaction or select a compatible medium while retaining all validation checks.

Show what you know

State which device confirmed each stage: reading, writing, validation, receipt or acknowledgment.

Common question

Does a hash or a successful copy message prove that the Bitcoin recipient is correct? No. Review the transaction and its outputs on the signing device.

Pause point

Remove and store backup cards. Clearly identify the transport medium.

Original reports that it wrote the response to the card. What still needs to happen before you can say Desk received it?

1. Paint the card a different color.
2. Create a new seed.
3. Read the response and validate it through the relevant Desk workflow.

> **Show answer: Read the response and validate it through the relevant Desk workflow.**
> A successful write and successful receipt are different events.

Public providers and your own node

Objective

Choose a source for network queries and understand its disclosures and limitations.

Understanding the topic

Desk can query supported public providers or a user-configured Bitcoin Core node. A provider can see the queries it receives, their sequence and connection data. Keeping a complete xpub private reduces one kind of exposure, but scripts and their hashes may still be linked.

Desk 9.21 explicitly offers Blockstream Electrum over TLS in addition to REST alternatives and a personal node. TLS protects the channel from certain network observers. The provider itself still receives the queries. No silent provider rotation guarantees anonymity. Understand the trade-off between privacy and convenience.

For Core, configure the endpoint, authentication and watch-only wallet according to its guide. Do not publish the RPC port or expose it to the internet so the app can “see” it. Restrict access to trusted environments and use appropriate protected transport. Never read an RPC password to the tutor.

Initial synchronization and a rescan can take time. A progress indicator reports work in progress, not an early success. Desk continues background work. Closing a view does not stop the node. The documented minimum lookback window cannot guarantee discovery of earlier activity. For an older wallet, verify the import date and the actual scan range.

Discovery depends on transaction history, not a positive balance. An address spent down to zero is still used. In the reviewed multisignature implementation, the gap is 20 consecutive addresses without history per branch and participant, with address-issuance limits. Do not extrapolate a global limit to every wallet.

Practice

1. Select a learning provider and explain what information it can see.
2. Check last synchronization time, network and progress. If HTTP 429 appears, respect the pause and make a deliberate decision before changing providers.
3. Simulate a wallet with a zero balance and old transactions. Check why “zero” differs from “unused.”

Show what you know

Determine whether your source meets your verification and privacy needs and recognize an incomplete state.

Common question

Does my own node make me anonymous? No. It reduces reliance on outside queries. You still need to consider your connection, counterparties, broadcasting and other metadata.

Pause point

Record only the provider type and whether the scan is complete.

An address has a zero balance but previously received and spent funds. How should wallet discovery treat it?

1. As an address with history.
2. As an address that has never been used.
3. As an invalid address.

> **Show answer: As an address with history.**
> History determines whether the address has been used, regardless of its current balance.

Receiving bitcoin and checking the address

Objective

Create a receiving request and verify it before giving it to someone.

Understanding the topic

Open the correct WOW account and confirm its network and policy. Generate or retrieve a receiving request. You can add a reason, observer and expected amount for your own records. These are local details. An expected amount does not prevent someone sending a different one.

Verify the address using the device workflow and correct wallet context. If physical testing has not validated the workflow for your combination, keep the exercise simulated and escalate before receiving substantial funds. Two screens fed from the same source do not provide independent verification.

Where the workflow permits, use a new address for a new payment relationship. In the reviewed multisignature implementation, addresses already displayed are never reassigned and do not expire, since a payer may use them later. If you reach the limit for consecutive new addresses without history, retrieve the appropriate earlier request and understand the limit. Never rewind the indices.

After sharing the request, watch for the payment through your verification source. An email, exchange receipt or payer’s screenshot cannot prove settlement. Check the network, txid, output, amount and required confirmations for your exposure. Do not open your address in a public explorer for convenience if your plan requires keeping those queries private.

Practice

1. Generate a request in the lab, review the account and network, and explain how you would verify the address.
2. Record a fictitious label and retrieve the same request after closing the view.
3. Simulate receipt of a different amount. Decide how to reconcile it without changing the history.

Show what you know

Distinguish a generated address, verified address, shared request and confirmed receipt.

Common question

Does an old address stop working when I create another? Normally no. Maintaining discovery and the record of requests keeps late payments visible.

Pause point

Keep the status of the lab request. Do not give its contents to the tutor.

The payer sends a screenshot marked “withdrawal complete.” What should you check before accepting payment?

1. Only the quality of the screenshot.
2. The corresponding output and required confirmations through a reliable network source.
3. The payer’s password.

> **Show answer: The corresponding output and required confirmations through a reliable network source.**
> A commercial receipt or screenshot cannot replace payment verification.

Labeling, freezing and selecting UTXOs

Objective

Prepare inputs without accidentally mixing different sources.

Understanding the topic

Labels preserve context that is absent from the chain, such as origin, counterparty, purpose and restrictions on use. In Desk, UTXO labels and address notes can have different lengths and functions. “Client A” can be useful. A legal name or identity document may create an unnecessarily sensitive record.

Freezing a UTXO in Desk excludes it from certain local selections. It does not block spending on Bitcoin, change the script or stop another application with the keys from using it. This can also cause total and spendable balances to differ. Check whether a coin is frozen, reserved by a draft or actually spent.

Automatic selection optimizes according to its algorithm and context. It does not necessarily know your private relationships. For a particular payment, consider choosing an output from the same context instead of combining savings, salary and business activity. Useful separation requires consistent choices later as well as clear labels now.

Exporting labels in BIP329 format helps preserve or migrate them. The format itself does not encrypt. Desk offers an encrypted wrapper for export. Distinguish a protected file from compatible plaintext. Before importing over existing information, check the wallet match and how frozen outputs are handled.

Practice

1. Label three synthetic UTXOs as savings, business activity and donation.
2. Freeze one and check the difference between the observed balance and the amount available for selection.
3. Export the lab labels with a password, import them into a copy and review the results without using actual private data.

Show what you know

Justify the selected inputs in terms of cost and exposure. Recognize that freezing is a local preference.

Common question

Does a label travel to the recipient when I pay? Its existence as a local label does not transmit it. Exporting, sharing files, using another service or adding it to a message can expose it.

Pause point

Save the practice labels and freeze status.

What is the effect of freezing a UTXO in Desk?

1. It creates a network-wide consensus lock.
2. It transfers the UTXO to a special account.
3. The app applies a local selection restriction.

> **Show answer: The app applies a local selection restriction.**
> It does not revoke the spending ability of other copies of the keys.

M06

Preparing and reviewing a payment

Objective

Build a PSBT you can explain and identify every cost and output.

Understanding the topic

Choose the account, spendable inputs, recipients and amounts. Verify the source of the request. After pasting or scanning, check the complete address and network because clipboard contents or an image can be replaced. When full verification is available, do not rely on just the first and last characters.

Choose a fee rate and review the absolute fee, estimated size, total and change. With “Send all,” Desk subtracts the fee from the available amount. If the action starts in chat and the net amount falls short of the request, make a partial payment only deliberately. The original request does not change to hide the difference.

Check for a small change output or no change output at all. Verify any output labeled as your own against the policy, independently of the coordinator’s label. If change is impractical, reconsider sweeping or add a compatible input. Do not let the remainder silently turn into a disproportionate fee.

A PSBT transports information and signatures. It does not inherently provide privacy or authenticity of origin. It may contain previous transactions, public keys, derivation paths and metadata. In the reviewed Final firmware, the multisignature profile uses PSBT v0/BIP174. “Transaction version 2” does not mean “PSBT version 2.”

Practice

1. In the simulator, build a payment with an input of 120,000 sat, a recipient amount of 70,000 sat and a fee of 1,000 sat.
2. List all outputs and explain the 49,000 sat change. Repeat with a sweep.
3. Cancel the draft and explain what you canceled locally. Do not use this simulator to sign or broadcast anything.

Show what you know

Before exporting, explain what goes in, what comes out, who receives it, what it costs and which authorization is still missing.

Common question

Can I send the full displayed balance? Only if the app can calculate a viable net payment and cover the fees. The balance may include unavailable coins.

Pause point

Save or cancel a learning draft. Never store an actual PSBT in the course portal.

A screen says “transaction version 2.” Does this prove the file is a PSBT v2?

1. No. These are separate version fields.
2. Yes, always.
3. It proves that it uses Taproot.

> **Show answer: No. These are separate version fields.**
> BIP370 distinguishes the container version from the transaction version.

Signing with Original and BIT

Objective

Complete the signing workflow for each model and receive a response linked to the correct transaction.

Understanding the topic

For Original, deliver the PSBT on the transport card using the supported Cuvex Mirror workflow. On the device, read the request, supply the cryptogram and unlock it privately. Review every output and amount, the change and the fee. The device writes its response to the card. It must then be read and validated in Desk. A successful card write does not replace that return step.

For BIT, select the correct volume and deliver the request over USB-C. Desk’s local service handles the expected exchange while you operate the device. Supply the cryptogram as directed and review the transaction on BIT. “Receive from BIT” imports the response. Desk validates and records it before confirming acknowledgment. After a disconnection, resume the same operation. Do not choose another because it looks similar.

For multisignature signing in the Final firmware, review the mandatory summary and outputs, applicable warnings and all three final “Sign PSBT” confirmations. The optional extended review lets you examine additional parameters. Choosing “No” does not remove the mandatory checks. Independent policy verification follows a different workflow and applies only to that particular review.

Signing requires a compatible cryptogram whose authenticity can be verified. An older copy may still recover the secret without being eligible for signing. If the device warns that an old copy lacks verified authenticity, recover and check the secret and create a new copy before signing. Never edit headers or bypass the rejection.

Cancel if an address differs, a fee is unexpected, information is missing, a different network appears or the device rejects the policy. Do not allow pressure to finish a call to become an approval. The AI does not press buttons, perform the final confirmation or declare something signed before you have verified it.

Practice

1. Follow the workflow for your model with a wallet containing no funds or a lab that has passed physical acceptance testing.

2. Simulate stopping before the final confirmations and explain why this does not constitute authorization.
3. Check the returned response, its link to the draft and, on BIT, the receipt and acknowledgment status.

Show what you know

Describe the workflow without revealing credentials. Distinguish device approval, an imported response and a broadcast transaction.

Common question

Does an offline device know whether my inputs remain unspent? It cannot check current chain state on its own. The app must check the final transaction against its network source.

Pause point

If you interrupt signing, cancel or leave an identified pending transaction according to the workflow, with no secrets visible.

BIT signs but Desk does not confirm receipt. What status should you assume?

1. The payment has definitely been broadcast.
2. The response still needs to be received or validated. Resume the same operation.
3. The wallet is lost.

> **Show answer: The response still needs to be received or validated. Resume the same operation.**
> Signing, receiving and broadcasting are separate stages.

Finalizing, broadcasting and troubleshooting

Objective

Complete the payment without duplicating it and diagnose failures by stage.

Understanding the topic

After importing a signature, Desk must verify it belongs to the draft and preserves the intended transaction. A multisignature threshold may still be unmet. Importing a single-signature authorization does not remove the need for review either. Once the conditions are met, finalizing produces the transaction ready to broadcast.

Broadcast only after the final review. A server response or txid gives a result for the request. Follow-up still needs to confirm acceptance and chain status. If the app received no response, check before retrying. Do not create another payment to solve a display problem.

For a pending payment, review the fee rate, validity, conflicts and actual support for RBF. A change of policy or recipient requires appropriate new signatures on the new proposal. Local cancellation neither destroys a signature or transaction already retained by another party nor revokes a confirmed transaction.

Diagnose preparation, transport, unlocking, review, signing, return, validation, finalization, broadcast and confirmation separately. Record system, version, model, stage, approximate time and error code. The app’s diagnostics are designed to exclude sensitive data, but review them before sharing. Do not attach backups, QR codes, your Chat Key or credentials.

Practice

1. Order the states of a fictitious payment and identify where you could safely pause.
2. Work through insufficient funds, a missing USB response and a disconnection during broadcast.
3. Write a support ticket using synthetic data and a verifiable expected result.

Show what you know

Decide whether the student, device, coordinator or network still needs to act, and avoid making an unnecessary second payment.

Common question

Should I respond to FIRMWARE_CAPABILITY_REQUIRED by changing firmware blindly? No. In the documented Desk incident, recognition of the Final build required a correction to Desk’s catalog. Check version and profile before changing devices.

Pause point

Save the status and next action. If you broadcast a real transaction outside the lab, keep its record in your private documentation.

Which action can, on its own, revoke an already confirmed transaction?

1. Delete the local draft.
2. Close Mirror.
3. Neither action.

> **Show answer: Neither action.**
> Local deletion does not rewrite the chain or withdraw authorizations already in circulation.

M07

What can be observed on Bitcoin

Objective

Identify public data, inferences and information you add outside the chain.

Understanding the topic

Bitcoin’s on-chain data is public. Scripts and addresses that can be represented, values, relationships between inputs and outputs, and positions in blocks can all be analyzed. Your name need not appear, but an identified purchase, published invoice or shared address can connect you to that history.

Pseudonymity means using identifiers that do not themselves name you. Anonymity would require a set of participants and conditions under which an observer cannot distinguish you. Installing an app does not provide that by itself. Privacy depends on context. A merchant knows about your payment, an exchange may know about your withdrawal, a server sees queries and a person may observe your devices.

Separate facts from inferences. “This output was spent in that transaction” is verifiable on-chain. “All these inputs belong to one person” is a heuristic that can fail. Off-chain identification can strengthen a hypothesis without making every interpretation certain.

Address reuse makes aggregating activity easier. Combining UTXOs from different contexts may link them. Revealing an xpub enables broader observation than sharing one address. A txid can also expose other outputs and relationships the recipient did not need to know.

Practice

1. In a fictitious transaction, mark the public data and the labels that belong to you.
2. Add a named invoice and describe the new link it creates.
3. Write a support request that resolves an error without disclosing an address, descriptor or balance.

Show what you know

State “this is observable” or “this is inferred” and explain which evidence is missing.

Common question

Am I anonymous if I never reuse an address? No. Input selection, change, queries, counterparties and other metadata still matter.

Pause point

Keep a map of observers without real identities or transactions.

What information typically lets someone observe a family of addresses belonging to an account?

1. The icon’s color.
2. Its xpub and enough derivation context.
3. The cable brand.

> **Show answer: Its xpub and enough derivation context.**
> Extended public information is privacy-sensitive even though it cannot authorize spending on its own.

Separating contexts and managing change

Objective

Make spending decisions that take account of the origins of your UTXOs.

Understanding the topic

Separating contexts starts before payment. Decide whether an incoming amount relates to savings, business, everyday spending or a particular relationship. Keep that context in private labels so a future selection does not erase a distinction accidentally.

A label does not cryptographically separate outputs. Spending UTXOs from two contexts together publishes a connection. Consolidation reduces the number of inputs needed for future payments but strengthens the link among the consolidated outputs. Doing it when fees are low may be efficient and still conflict with your privacy objective.

Change is a new output controlled by the same policy, not “invisible money.” Spending it later may extend earlier relationships. Do not label an address as change because the amount looks unusual. During a real review the device must verify it belongs to the wallet.

Avoid turning privacy practices into rigid patterns of amounts, timings or repeated transfers. These patterns can also be recognized and can generate extra fees. Assess what each party knows and what the proposed transaction would publish. No sequence erases history already published.

Practice

1. Create five fictitious UTXOs from three contexts. Prepare a payment that uses as few contexts as necessary.
2. Identify the resulting change and decide how to label it.
3. Compare the cost and exposure of consolidating all outputs with keeping them separate.

Show what you know

Justify or reject consolidation for a specific reason without applying an absolute rule to every case.

Common question

Does moving everything to another address of my own break the history? No. That transfer publishes an additional connection and can add cost without addressing your threat.

Pause point

Keep your lab reasoning and chosen selection policy.

What can happen when you consolidate salary and donation funds in one transaction?

1. A connection between those inputs can become visible.
2. Their public origin is erased.
3. They become guaranteed anonymous cash.

> **Show answer: A connection between those inputs can become visible.**
> Reducing the number of UTXOs can increase observable connections.

M07

Network privacy, Tor and VPNs

Objective

Distinguish connection privacy from blockchain privacy.

Understanding the topic

A query server may associate requests with a connection. Depending on the transport, your internet provider can see destinations or patterns. A VPN shifts some trust to its operator. It neither removes Bitcoin’s public information nor prevents an identified account from recognizing you.

Tor routes traffic through a network to reduce certain links between source and destination. It does not make a Bitcoin address private or protect an application whose traffic does not pass through Tor. Opening Tor Browser does not automatically configure Desk, Bitcoin Core or every other service on the computer.

Verify the route and configuration before saying a connection is protected. Do not assume the reviewed Desk version has a built-in Tor toggle. A deployment using a node or proxy needs engineering guidance and validation of actual traffic. Another wallet having a setting is no reason to invent a matching field in Desk.

DNS, account synchronization, explorer links and price services can also leak information. A setup may protect balance queries but reveal activity when you open a public explorer. Define each measure’s scope and what happens on connection failure. Avoid silent fallback to a less private provider.

Practice

1. Draw the route from the computer through the connection provider and any proxy to the node or service and the Bitcoin network.
2. Identify who receives the queries and who sees your commercial identity.
3. Simulate an unresponsive private node. Decide whether to pause or deliberately switch sources with an understanding of the exposure.

Show what you know

Explain which threat your setup reduces and which threats remain.

Common question

Does Tor guarantee that nobody can link a payment to me? No. Counterparties, commercial identification, patterns and operating mistakes may still link it.

Pause point

Record the design’s scope without private endpoints or passwords.

Does opening Tor Browser force Desk to send its queries through Tor?

1. Yes, because they share a computer.
2. Yes, if the icon is visible.
3. No. Configure and verify the network route for each application.

> **Show answer: No. Configure and verify the network route for each application.**
> Other applications do not automatically inherit one application’s protection.

CoinJoin, Payjoin and their current limits

Objective

Understand collaborative tools without attributing anonymity or unsupported capabilities to them.

Understanding the topic

CoinJoin combines contributions from several people in one transaction, making some inferences about inputs and outputs harder. It differs from handing coins to a custodial service that promises to return others. For each design, examine coordination, custody, fees, resistance to malicious participants and how outputs are used afterward.

Payjoin includes inputs from both payer and payee in a collaborative payment, weakening some common-ownership heuristics. It requires compatible support at both ends and a specific protocol. This is technical background. The reviewed sources do not establish that Cuvex Desk has an integrated, operating Payjoin or CoinJoin workflow.

Availability and legal context change. Wasabi’s documentation records the closure of the zkSNACKs coordinator on June 1, 2024. A historical button should never be taught as a guarantee of service today. In 2025, the US Department of Justice announced the guilty pleas and subsequent sentences of Samourai’s founders. This case does not establish that every privacy technique is illegal in every jurisdiction.

A tool can reduce one inference and leave others intact. An identified origin remains in a counterparty’s records. Subsequent recombination, metadata and failures within the participant set can erode privacy. Some services may also apply different commercial policies to coins with particular histories.

Practice

1. Compare an ordinary transaction, a collaborative transaction and a service that takes custody without executing real operations.
2. Before proposing a particular tool, find its version, maintainer, service status and current documentation.
3. Identify technical, custody and legal risks separately. The tutor should never design ways to evade controls or promise “untraceable funds.”

Show what you know

Explain one limited benefit and at least two requirements or risks of a privacy technique.

Common question

Does Cuvex need a mixer to provide privacy-conscious custody? No. Controlling queries, data, keys and UTXO selection already addresses particular risks without promising complete concealment.

Pause point

Record a tool as “studied.” Mark it “compatible” only when evidence supports that conclusion.

Which statement can be justified?

1. CoinJoin guarantees permanent anonymity.
2. A collaborative technique can make certain inferences harder, subject to requirements and limitations.
3. Any service called a mixer preserves self-custody.

> **Show answer: A collaborative technique can make certain inferences harder, subject to requirements and limitations.**
> Its properties depend on the protocol, implementation, participants and subsequent use.

Lessons from real incidents

Objective

Turn documented incidents into decisions you can verify without attacking competitors or exaggerating protection.

Understanding the topic

Mt. Gox. A 2023 US Department of Justice indictment describes unauthorized access to servers and keys and the subsequent disappearance of customer funds. An indictment contains allegations rather than a judgment. For custody, ask who really controls the keys and what happens if the company fails.

Ledger Connect Kit, December 2023. Ledger documented a malicious release of a library used by decentralized applications after a former employee’s access was compromised. The incident affected software distribution and deceived EVM DApp users into signing. It does not establish a compromise of Ledger hardware or Bitcoin consensus.

Bybit, February 2025. The FBI attributed theft of approximately $1.5 billion in virtual assets to North Korea. This incident involved an exchange and assets on other networks. It is not presented as a break in Bitcoin cryptography. Verify what a signature authorizes and avoid having several people blindly trust the same screen.

Coinbase, May 2025. The company reported data theft by bribed support agents to facilitate social engineering. It said passwords and private keys were not exposed. A scammer may know true details about you and still be a scammer.

Bitcoin Core also publishes software issues. The CVE-2024-35202 advisory described a possible remotely triggered shutdown in versions before 25.0. Enforcing rules does not remove the need to maintain software. The advisory does not imply that keys were stolen.

In January 2026, The Register reported exposure of Ledger buyers’ order and contact data through Global-e. It attributed confirmations to both companies, whose statements said recovery keys were unaffected. A purchase can reveal that you own a device even if the hardware has not been compromised.

In April 2026, The Record reported the attack on Drift and the platform’s announced suspension of deposits and withdrawals. Drift is a decentralized finance protocol on Solana. The incident did not break Bitcoin. Do not present initial loss estimates as final or later recovery efforts as guaranteed reimbursement.

Practice

1. Classify each incident by custody, interface or distribution, personal data, protocols on other networks and availability.
2. For each, propose one prevention measure and identify a limit to that measure.
3. Rehearse a fraudulent call: “I know about your purchase. Move your funds to this safe address.” Hang up and verify through a channel you initiate.

Show what you know

Explain why none of these incidents proves another brand is invulnerable. Each item of evidence supports a particular scope.

Common question

Are these the latest hacks in existence? No. This selection was verified for the November 17, 2026 edition. It is neither an exhaustive inventory nor live monitoring.

Pause point

Write down the practice you will change and how you will check that you maintain it.

A caller knows about your purchase and asks you to transfer funds to a “rescue wallet.” What does knowing about the purchase establish?

1. The information may have leaked. It authenticates neither the caller nor the address.
2. The caller must be legitimate support.
3. You should share the seed.

> **Show answer: The information may have leaked. It authenticates neither the caller nor the address.**
> Accurate information can be used to construct a convincing scam.

M08

Creating a chat identity and verifying contacts

Objective

Activate a chat identity without exposing its key, and verify the other person.

Understanding the topic

In Desk, chat is linked to a cryptogram through a Chat Key generated in Cuvex. It may look like an xpub, but it is secret and must never be treated as a WOW account’s public key. The tutor never needs to read it or see its QR code.

The workflow distinguishes creating a new alias from moving or recovering an existing one. In the reviewed implementation, select the corresponding iOS or Android mobile profile. Do not assume historically derived identities are interchangeable. DEV and Production are separate environments. Switching between them does not automatically migrate aliases or conversations.

Adding an alias does not verify identity. Check the fingerprint over an independent, authenticated channel. If the app offers recognition questions, use nonpublic information and avoid answers that disclose passwords. Familiar voices can be mimicked. In higher-risk situations, combine methods agreed in advance.

If a contact’s identity changes, pause payments and coordination until you understand why. It may be legitimate recovery or malicious substitution. End-to-end encryption protects a channel according to its protocol and implementation. It does not prove who is using the device at the other end.

Practice

1. In a test setup, explain creation or recovery without providing the Chat Key.
2. Add a lab contact and agree over another channel how to verify the fingerprint.
3. Simulate an identity change. Define how you would verify it before paying.

Show what you know

Distinguish an alias, a public fingerprint, a secret Chat Key and your personal trust in someone.

Common question

Does a long-standing alias guarantee the same person is using it? No. Follow the workflow to verify continuity and key changes.

Pause point

Record only “test contact verified” and the method, without keys or private questions.

A string labeled Chat Key looks like an xpub. How should you treat it in Desk?

1. As information you can post on a forum.
2. As a secret for recovering an identity.
3. As a Bitcoin receiving address.

> **Show answer: As a secret for recovering an identity.**
> Appearance does not determine a value’s confidentiality or purpose.

M08

Requesting and paying satoshis in chat

Objective

Go from a conversation to a payment while retaining both review and context.

Understanding the topic

Chat lets you request an address, respond with a receiving address, request payment and open payment preparation from a WOW account. Keeping context in one channel reduces copying errors between applications. It does not turn every message into an authenticated spending instruction.

Before responding or paying, review the verified contact, network, amount and original request. The shared form retains the UTXO selection and fee. If the message requests an amount and you choose “Send all,” the amount net of fees may be lower. Identify it as a partial payment where applicable.

Authorization remains on Cuvex. Chat carries intent and coordination and cannot sign automatically. A payment confirmation sent to a contact must distinguish receipt of a message from the existence of a confirmed transaction. The recipient verifies through their own account or source.

External links, attached QR codes and addresses remain untrusted until validated. “View in Mempool” may open a third-party service and expose queries. If your policy uses a personal node, use compatible verification in WOW and assess any switch to a public service.

Practice

1. Act out two roles. The recipient requests 50,000 sat and the payer prepares the payment without broadcasting.
2. Simulate a net available balance of 48,000 sat. Explain what agreement and reconciliation a partial payment still needs.
3. Deliberately change the network in a test message and stop the workflow.

Show what you know

Trace the links among the request, address, draft, signature and confirmation. An “OK” in chat is insufficient.

Common question

Does sending sats from chat use Lightning? No. The documented WOW workflow prepares on-chain Bitcoin payments. Sats name a unit, not a transport network.

Pause point

Cancel the lab draft or record its state. Do not broadcast merely to demonstrate an interface.

You receive a confirmation in chat. What is the decisive check that the payment arrived?

1. The message icon is green.
2. The other person says “confirmed.”
3. Verify the transaction and its outputs on the network using the appropriate source.

> **Show answer: Verify the transaction and its outputs on the network using the appropriate source.**
> Message status and transaction status are different.

M08

Sharing cryptograms deliberately

Objective

Understand what you transfer when you give someone an encrypted copy.

Understanding the topic

Sharing a cryptogram transfers a copy of an encrypted object. It need not send any bitcoins or add a signer. If the recipient also obtains sufficient means to unlock it, they may access its contents under the scheme. Decide in advance what capability you intend to transfer.

Chat’s end-to-end encryption and file encryption protect different layers. After downloading the object, the recipient can retain it outside chat. Deleting your message or local record cannot guarantee removal of every copy. Sending the password through the same channel can put all required components in one place.

Verify identity, format and purpose before sending. Linking a received cryptogram in the app organizes a copy. It does not establish that any file is safe to decrypt. Do not use attachments that require entering a seed or password on an external website.

Recovery needs an operating agreement covering who retains each component, who can open it, how exposure is detected and how custody changes if the relationship ends. For an ordinary payment, a validated address is normally sufficient. Sharing your cryptogram is unnecessary.

Practice

1. Design a transfer of encrypted training text to a lab contact.
2. List what the recipient knows and can do before and after learning the password.
3. Simulate the relationship ending. Explain why deleting the message revokes neither the copy nor the keys.

Show what you know

Distinguish “I shared data,” “I shared access to a secret” and “I signed a spend.”

Common question

Can an encrypted file circulate without consequences? It may reveal metadata, enable password-guessing attempts and be retained indefinitely. Assess whether sharing it is necessary.

Pause point

Do not leave custody attachments in the course. Record only your conclusion.

Is sharing a cryptogram in chat the same as sending bitcoins?

1. No. It transfers an object whose contents and access have a different scope.
2. Yes, as long as the filename ends in .bin.
3. It automatically activates a new multisignature wallet.

> **Show answer: No. It transfers an object whose contents and access have a different scope.**
> Transporting secrets and moving UTXOs are different operations.

M08

Recovering chat and understanding its metadata

Objective

Plan a device change and distinguish identity recovery from message recovery.

Understanding the topic

Desk states that history and sessions are encrypted locally and excluded from its full backup. The Chat Key allows recovery of the identity but does not guarantee recovery of all earlier conversations. The app has states and actions for pending activation, key maintenance and local recovery when compatible material is available.

The guide for the reviewed implementation says to use each alias on only one device at a time. Do not activate it on two devices at once to “test synchronization” when that use is unsupported. Move it through the documented procedure and verify continuity with your contacts.

“Pending,” “accepted by server,” “received” and “could not decrypt” describe different stages. Do not blindly resend a message whose delivery is unconfirmed. Establish whether it arrived first. If a session key is missing or the identity changes, retaining a pending message does not mean it was read.

Encrypted contents do not necessarily hide timing, size, delivery relationships, aliases or connection data from every system involved. Voice has a similar limitation. Transport encryption does not make a conventional call suitable for secrets. Use the minimum information needed to learn or diagnose a problem.

Practice

1. Simulate losing your PC and explain what each available item can recover.
2. Classify message states and decide when a payment request should not be resent.
3. Prepare a notice about changing devices that contacts can verify through an independent channel.

Show what you know

Explain which conversation would be lost and which identity could be restored without promising more than the backup covers.

Common question

Does deleting local chat also remove messages at the other end? Do not assume so. The recipient may separately retain messages and files.

Pause point

Keep a transfer plan with empty field labels and no Chat Key.

According to the reviewed guide, what does the Chat Key provide on its own?

1. Every past conversation on any PC.
2. The ability to recover the identity through the supported workflow, without a guarantee of recovering all old messages.
3. Automatic access to contacts’ Bitcoin keys.

> **Show answer: The ability to recover the identity through the supported workflow, without a guarantee of recovering all old messages.**
> Recovering an identity and recovering a message archive are different capabilities.

Everyday settings and reviewing permissions

Objective

Manage Desk settings while distinguishing convenience from protection.

Understanding the topic

Desk offers Night, Day and System themes, automatic synchronization and 3- or 5-minute intervals, transaction sounds, a chat background, language and reference currency. These preferences affect appearance or query frequency. They neither modify a Bitcoin signature nor add anonymity.

The reviewed security settings include inactivity locking, a background lock, a maximum delay after failures and optional erasure. The inactivity schema accepts 30 to 86,400 seconds, while the interface may offer narrower choices. Check defaults in the version you are running instead of assuming they match a recorded class.

The bitcoin: link integration opens a request to unlock, choose an account and review. It does not authorize automatic payment. On Linux, the guide distinguishes an integrated installation from an AppImage for registering links. A Lightning invoice needs a different supported workflow. Making Desk the default application is insufficient.

Quotes, price charts and information links may query external services. They provide information, not buy signals. Check date and source before converting amounts. Dark mode or a small window must not hide final controls, the address or the fee. If something is hidden, pause and report the layout problem.

Practice

1. Adjust appearance and locking in the learning store. Verify you can unlock it again.
2. Review the automatic features you enable. Synchronization, sounds and firmware checks have different effects.
3. Open a fictitious bitcoin: link request and cancel before preparing any real operation.

Show what you know

Explain each setting’s effect and identify settings that involve network queries or sensitive actions.

Common question

Do PC biometrics replace my recovery backup? No. They may depend on that computer and its secure system storage. Keep an independent recovery method.

Pause point

Lock Desk and record only which preferences you changed.

What changes when you select synchronization every three minutes?

1. The intended frequency of queries when the feature is running.
2. The on-chain signing policy.
3. The device seed.

> **Show answer: The intended frequency of queries when the feature is running.**
> This is an operational preference. It does not change custody.

M09

Designing a multisignature wallet

Objective

Choose a threshold that can withstand plausible loss and compromise.

Understanding the topic

In an M-of-N policy, N is the number of participants with distinct keys and M is the number of required signatures. A 2-of-3 policy survives one key becoming unavailable, but two compromised keys can authorize a spend. Keeping all three seeds in one place or exposing them together reduces their independence.

The reviewed Cuvex multisignature profile uses native P2WSH with sortedmulti and BIP48 derivation. Original structurally supports up to six policy keys, and BIT up to fifteen. If both participate, observe the more limited model and the actual transport size. Structural maximums do not guarantee that a policy with many keys and inputs will fit.

The app accepts thresholds that satisfy the policy constraints, but a 1-of-N policy allows spending without cooperation. The firmware retains specific warnings about this risk. Larger numbers do not improve everything. They increase coordination, costs, recovery material and the possibility of lockout.

MuSig2 is a different Schnorr signature aggregation scheme. On its own it is N-of-N, not an arbitrary 3-of-5 threshold. The studied Final firmware does not implement signing of Taproot inputs, MuSig2 or Miniscript. Accepting a P2TR recipient does not demonstrate the ability to sign spends from a Taproot wallet.

Practice

1. Design a fictitious 2-of-3 policy with independent risks for each participant.
2. Simulate losing one key and compromising one key. Explain what remains possible in each case.
3. Check the limits for each model before choosing a larger policy.

Show what you know

State your design’s tolerance for loss, attack threshold and shared dependencies.

Common question

Does multisignature require participants to know each other’s seeds? No. Each should retain private signing capability while sharing the public information needed to build and recover the policy.

Pause point

Keep the design with fictitious participants and their responsibilities.

In a 2-of-3 policy with independent keys, how many private keys suffice to authorize a valid spend under that policy?

1. One.
2. Two.
3. Always all three.

> **Show answer: Two.**
> The threshold requires two. The other conditions and validation checks must also be satisfied.

Creating invitations and contributing keys

Objective

Build a policy with verified participants without sharing seeds.

Understanding the topic

The creator chooses the name, network, M, N, contacts, their own public information and operational invitation conditions. The reviewed schema accepts mainnet and regtest, 2 to 15 participants before applying device limits and an operational expiry of 1 to 720 hours. Those limits never authorize skipping a capacity check.

Each participant reviews and accepts or rejects the invitation, then supplies their extended public key with the fingerprint and BIP48 path through the compatible workflow. They do not supply a seed, private key, isolated address or another wallet’s entire descriptor. A key with incorrect context can produce a different policy even if it looks like a valid xpub.

The creator coordinates. Each signer remains responsible for validation. Before receiving funds, everyone should be able to reconstruct and verify the same parameters and a verification address. Accepting a contact in chat does not automatically approve every policy the contact sends.

An invitation expiry is an application coordination rule. It does not change an already funded script, delete signatures others retained or serve as a consensus timelock. Canceling a proposal and withdrawing funds from an existing policy are distinct actions.

Practice

1. In a prepared regtest lab, create a 2-of-3 proposal with test contacts.
2. Act out acceptance, rejection and a contribution on the wrong network. Verify that the last one is stopped.
3. List what everyone must retain before funding: network, threshold, public keys, origins, script and verified address.

Show what you know

Identify an incomplete invitation and explain whose approval is missing without inferring approval from a chat connection.

Common question

Does an expiry date make later spending impossible? Not when it is merely an invitation field. A Bitcoin time restriction requires specific script or transaction conditions and actual support.

Pause point

Keep the training proposal ID and the outstanding approval.

What does the documented workflow request when you contribute your part of a multisignature wallet?

1. Every participant’s seed.
2. Any receiving address.
3. Your extended public key with a compatible fingerprint and BIP48 origin.

> **Show answer: Your extended public key with a compatible fingerprint and BIP48 origin.**
> The correct public material allows the policy to be built without disclosing private keys.

Verifying policies with Mirror in any order

Objective

Compare complete fields and understand precisely what a match establishes.

Understanding the topic

Independent verification presents the threshold, network, profile, SIGHASH, policy ID, first address, user position and data for each participant. It checks intent and consistency. It does not assume that the device has permanently registered a policy. The documented scope is “this review.”

In Mirror 12.12, you can read the Cuvex or Desk QR code first and choose any field. You need not start at step 1, scan every field or follow a fixed order. If you review text manually and skip its scan, Mirror does not mark it as independently checked.

The comparator shows the full literal text. Spaces, line breaks, case and Unicode differences count. “Match” means the two values in that pair are equal. It does not authenticate their origin, prove they belong to the same policy or activate the wallet. Final approval and its correlated response still use the Cuvex and Desk workflow.

Current Desk QR codes carry only the value, without a step number or session. Mirror cannot always infer the step. “Specify Desk step” adds manual context and should be displayed as such. With N participants, the documented map has 7 + 4N fields. For k starting at zero, 8+4k is the fingerprint, 9+4k the path, 10+4k the xpub and 11+4k the key ID. With N=2, step 15 is the second key’s ID and may be compared first.

Practice

1. Use synthetic data and first compare an ID labeled step 15. Then compare network and threshold.
2. Introduce a single-character difference. Verify “No match” and start another pair without carrying over the result.
3. Compare “2 / 3” and explain why the text alone cannot always tell you whether this is the threshold or user position.

Show what you know

Describe which field you checked, how you identified its context and what remains to approve. Do not treat partial matches as overall approval.

Common question

Must I scan every QR code to continue learning? No. You may compare in any order. Mandatory signer reviews and authorizations have their own workflow.

Pause point

Close the comparator. Under the reviewed design, leaving it or putting it in the background should clear the values.

Mirror compares two QR codes for step 15 and displays “Match.” What does that establish?

1. The two values are literally equal, in the context identified or specified.
2. The whole policy has been approved.
3. The origin of both QR codes is authentic.

> **Show answer: The two values are literally equal, in the context identified or specified.**
> Comparison does not replace authentication, overall review or the hardware response.

Coordinating signatures and broadcasting a multisignature transaction

Objective

Bring a proposal to its signing threshold without losing sight of intent or control.

Understanding the topic

A multisignature operation specifies inputs, recipients, amounts, fee rate, replacement behavior and operational notes. The creator can request signatures from compatible participants. Each signer independently reviews network, policy, inputs, every output and the fee before authorizing on their own device.

A partial signature alone does not move funds if the threshold is unmet. Once it is met, the coordinator can combine signatures and finalize according to the workflow. Reports from other participants or the coordinator are coordination information. They are distinct from checks you carried out locally, and the app should identify their sources.

The reviewed implementation supports retrying, receiving and acknowledging signatures, rejection and handover of coordination. Handover changes neither the keys nor the on-chain threshold. Correlate a saved response with its request and the actual profile used. Never choose a different policy because it looks similar or appears first in the catalog.

If someone changes recipients or other relevant conditions, review a new proposal and obtain the appropriate signatures. Never manually delete security data from a PSBT to make it fit on NFC. The firmware requires supported profiles and validations and sets limits on inputs, outputs and size.

Before broadcasting, verify that this is the agreed transaction and that no version has already been broadcast. Then track confirmations through your chosen source. Rejecting in your app does not automatically revoke signatures others retained or prevent every action still allowed by the remaining threshold.

Practice

1. Act out a 2-of-3 scenario with three fictitious roles. One signs, another rejects and the third asks for clarification.
2. Change the test payment’s address and explain why an earlier verbal approval cannot be reused.

3. Simulate a failed acknowledgment after saving a signature. Resume the same job without duplicating the payment or switching profiles.

Show what you know

Identify who coordinates, signs and finalizes, and the evidence for each stage.

Common question

Do two “OK” messages in chat count as two signatures? No. The threshold requires valid cryptographic authorizations under the policy.

Pause point

Record the status, pending signatures and next responsible person, excluding private contents.

A 2-of-3 transaction has one valid signature and two messages saying “I agree.” Has it met the threshold?

1. Yes, because three people participated.
2. No. It still needs another valid cryptographic signature.
3. Yes, if the coordinator announces it.

> **Show answer: No. It still needs another valid cryptographic signature.**
> Agreement in conversation and a valid signature are different kinds of evidence.

M09

Recovering and changing a multisignature wallet

Objective

Recover the policy and plan for losing or replacing participants.

Understanding the topic

Recovery needs two kinds of material: data that reconstructs the policy and sufficient private signing capabilities to spend. A policy backup containing xpubs may reveal history without containing seeds. Encryption protects the backup file but creates a need to retain its password. The .cuvexms extension alone is no proof of encryption. Check the actual format and export.

In Desk 9.21, recovery requests the participant’s extended public key with fingerprint and BIP48 path exported by their device. Supported workflows allow reading by webcam or Mirror. Do not substitute a receiving address or send a seed to support.

If one key is lost in a 2-of-3 policy, the other two may still allow spending. The original policy remains in force. Effectively removing a participant and establishing new keys normally requires creating a new policy and moving funds with the necessary authorizations. Changing an alias or deleting a wallet in Desk does not change existing UTXOs.

Backups should enable reconstruction of both branches and discovery of history. Retain indices, issued requests and the context needed to avoid address reuse or misreading a wallet as empty after an incomplete scan. Restoring and resuming a pending operation must use the profile saved when it was created.

Practice

1. Export and restore a lab policy through the documented function. Verify the network and a known address.
2. Simulate losing one participant and prepare a rotation plan without moving real funds.
3. Simulate losses that leave fewer signers than the threshold. Recognize that neither support nor AI can manufacture the missing signatures.

Show what you know

Recover the test scenario and distinguish restoring information from changing control over coins.

Common question

Does deleting the multisignature wallet in Desk disable it for everyone? No. The workflow removes local state. Other people and copies may retain capabilities compatible with the policy.

Pause point

Keep the tested backup and private plan. Record only the result in the course.

You want to remove a person from a policy that already controls funds. Is deleting their name in Desk enough?

1. Yes.
2. Yes, if you also delete the chat.
3. No. Plan a new policy and an authorized transfer of funds when appropriate.

> **Show answer: No. Plan a new policy and an authorized transfer of funds when appropriate.**
> Editing local records does not change the scripts of existing UTXOs.

M10

Updating firmware without guesswork

Objective

Prepare a compatible update and verify the outcome on the device.

Understanding the topic

An update changes trusted software. Verify the model, hardware revision, version, source and the manufacturer’s authentication method. A completed download or a matching hash from a webpage cannot replace checks of the signature and compatibility. Never install an unsigned engineering firmware application as if it were a customer release.

In the documented workflow, Original updates through Bluetooth and BIT uses USB-C. Mirror provides compatible preparation and transport workflows. A particular combination of PC, phone and device cannot be promised to work until it passes physical acceptance testing. The historical Original update issue on Windows requires specific diagnosis. Pretending an update succeeded at 99% does not resolve it.

Before starting, verify recoverable backups, stable power and the absence of other operations. Prepare the official file or a previously verified copy as directed by the app. Distinguish transfer, validation, installation, reboot and version check. A progress bar is not final proof.

Afterward, check the version displayed on the device and record the date and result. Desk’s compatibility catalog does not measure firmware remotely. firmwareAttestation remains false. Selecting a Final profile does not prove which bytes are actually installed. If the update fails, follow documented recovery and preserve the stage and error without blindly disconnecting during a critical step.

Practice

1. Review a preparation checklist without starting a real update in the exercise.
2. Order the states and explain why “transferred” and “installed” are different.
3. Write a fictitious 99% failure report including model, version, system, stage and final message.

Show what you know

Identify the appropriate artifact, transfer method and final success criterion.

Common question

Should I update just to clear a Desk error? Identify its origin first. A catalog incompatibility may require fixing Desk while retaining the validated firmware.

Pause point

Pause a real update only at a point the procedure explicitly identifies as safe. The end of a call is not such a criterion.

What can Desk’s explicit catalog verify on its own?

1. Supported compatibility references, without remotely measuring the installed firmware.
2. Physical attestation of every connected device.
3. That no vulnerabilities exist.

> **Show answer: Supported compatibility references, without remotely measuring the installed firmware.**
> Compatibility, signature, measurement and physical acceptance are different kinds of evidence.

Loss, device failure and emergency recovery

Objective

Choose recovery steps proportionate to the incident and preserve useful evidence.

Understanding the topic

First classify what was lost or exposed: computer, device, card, file, password, seed, passphrase or policy. “I cannot get in” does not necessarily mean “I have been robbed.” If compromise is suspected, stop entering secrets on the suspect device.

Loss of a device may be recoverable with compatible media and recovery credentials. Losing the computer may require restoring Desk storage and reconstructing watch-only access. If all means of unlocking are lost or fewer than the required keys survive, there may be no technical solution. No AI can guarantee recovery of nonexistent keys.

Desk provides local recovery for supported formats and export of the corresponding recovery material. Decrypting on a PC can expose the secret to its operating system or malware. This is an exceptional decision. Use a prepared environment, compatible material and a plan to move to new keys if the secret may have been compromised. This differs from Cuvex’s usual isolation.

If a seed leaked, changing the Desk password does not revoke it. Assess an authorized transfer to a new wallet and protect it using trusted equipment. Avoid publishing details that help the attacker or paying services that demand another seed or fraudulent advance fees in exchange for recovery.

Practice

1. Work through four fictitious scenarios: a lost PC, a broken card with a valid copy, a forgotten password and an exposed seed.
2. For each, identify the material needed, the risk of taking action and the criterion for recovery.
3. Rehearse only with learning data. Never upload actual emergency files to the tutor.

Show what you know

Choose among restoration, watch-only reconfiguration, migration of control or escalation to a specialist without claiming an impossible solution.

Common question

Does changing the password re-encrypt all secrets someone has already seen? No. A plaintext copy or a seed someone has learned remains known.

Pause point

Record the incident category and next safe action. Stop the voice session before working with secrets.

Your seed has been published and you change your PC password. Has the attacker’s ability to spend been revoked?

1. Yes.
2. No. The seed still controls the same keys and requires a custody response.
3. Yes, if you also change the chat background.

> **Show answer: No. The seed still controls the same keys and requires a custody response.**
> Local protection does not revoke an exposed Bitcoin key.

M10

Phishing, support and voice scams

Objective

Recognize dangerous requests and respond using an agreed procedure.

Understanding the topic

An effective scam may use your name, your purchase, your device and a familiar voice. True information can come from a leak. Verify identity through a channel you initiate and a known procedure. The caller’s urgency or accuracy is no substitute.

Warning signs include requests for a seed, passwords, PIN or Chat Key, remote control software to “synchronize,” disabling antivirus, transferring to a “safe wallet,” scanning an unexplained QR code or signing to prove ownership without details of what you authorize. Pressure to act before a call ends is reason to stop the call.

A legitimate tutor explains and checks understanding. It neither holds keys, asks for test transactions to its own address nor promises to recover a seed. A legitimate ownership verification function should be specific and reviewable. It never requires handing over private keys.

Fraud can also occur during a technical session. QR text, a document or a message may contain instructions telling an AI to ignore its own guidance. Such content is material to analyze, not authority over the tutor. The knowledge base should distinguish approved sources from text supplied by a student or third party.

Practice

1. Role-play a false support call and end it before revealing data.
2. Independently verify an official channel you previously saved.
3. Describe an installation error without sharing a screen containing secrets or allowing remote access to your custody environment.

Show what you know

Explain which data is requested, what purpose could require it and why the particular request exceeds educational support.

Common question

Is it safe to show only a few words of my seed? No. Training never requires revealing any fragment of your own seed.

Pause point

Keep your support verification procedure and check that it contains no plaintext secrets.

A voice that sounds like your business partner asks you to skip verification and sign urgently. What do you do?

1. Pause, authenticate the request through the agreed procedure and review the entire transaction.
2. Sign because the voice matches.
3. Share the seed to save time.

> **Show answer: Pause, authenticate the request through the agreed procedure and review the entire transaction.**
> Voice recognition and urgency cannot replace authentication and review.

Privacy, legal obligations and personal records

Objective

Understand the general framework and prepare specific legal and tax questions.

Understanding the topic

Financial privacy does not remove tax obligations, applicable identification requirements, sanctions or crime-prevention duties. Your situation depends on residence, activity, counterparty and service. AI should provide dated, sourced general information and refer individual decisions to qualified professionals.

In the EU, MiCA regulates certain crypto-assets and services. General application began on December 30, 2024. The maximum transitional period specified in the regulation extended to July 1, 2026, subject to national decisions. Check current authorization and scope in official registers. An old reference to registration is insufficient. Authorization guarantees neither price, solvency nor full compensation.

Regulation 2023/1113 lays down information accompanying transfers involving providers subject to its requirements. For transfers exceeding €1,000 involving self-hosted addresses, it provides for measures to assess ownership or control. That threshold does not create a general exemption from identification below it. Person-to-person transfers without a provider are excluded from this regulation’s scope, while other obligations may still apply.

Retain sufficient documentation of purchases, sales, fees and sources of funds for your situation, and protect it from unnecessary access. You do not need to publish your whole history to keep private records. The course does not teach splitting transactions to evade controls, falsifying information or hiding income.

Where voice recordings or transcripts and identifiable progress are involved, the service must define purpose, legal basis, retention, access, processors and applicable rights. The commercial privacy configuration must be validated before sale, not improvised during a call.

Practice

1. Draft a fictitious case for an adviser that specifies residence, activity and transactions without keys.
2. Identify where to check the provider’s authorization and the date of that information.
3. Design a private transaction record and a minimal student-data policy.

Show what you know

Distinguish a legal rule, an exchange policy and a technical capability of Bitcoin.

Common question

Is all self-custody prohibited in the EU? That conclusion does not follow from the cited rules. Avoid absolute headlines and check the exact provision and its scope.

Pause point

Keep outstanding questions for your adviser without providing personal documents to the tutor.

Does the €1,000 threshold cited for certain address-control checks remove every obligation below that amount?

1. Yes.
2. Only if you split the transaction.
3. No. It is not a general exemption from identification or other obligations.

> **Show answer: No. It is not a general exemption from identification or other obligations.**
> Interpret the rule according to the measure in question and its scope. A threshold is not a universal exemption.

Inheritance, continuity and the annual drill

Objective

Create a plan that lets authorized people act without exposing everything in advance.

Understanding the topic

Inheritance combines legal authority, the ability to locate materials and technical capability. A person may have the right to inherit without knowing how to reconstruct a wallet. Another may possess a key without authorization to use it. Address both dimensions with appropriate advice.

Separate shareable instructions from access to secrets. The inventory can describe what exists, whom to contact and what to verify without putting every key and password in a widely accessible document. Avoid writing seeds in wills or files that could circulate outside your control.

For multisignature, decide who keeps the policy and backups, what threshold remains available after a loss and what happens if a key participant dies. A single custodian controlling enough components could become a single point of abuse. Excessive complexity can make assets unrecoverable.

Include recovery of cryptogram passwords, the passphrase if used, derivation data, device compatibility and a procedure for the manufacturer ceasing operations. Do not assume a proprietary file or biometric fingerprint will be usable without preparation. Test interoperability with practice data and documented formats.

Review after changes in family, address, policy, software or participants, and run periodic drills. Test whether a trusted person understands the instructions without disclosing holdings or unnecessarily moving money.

Practice

1. Complete a private template for responsibilities, components, authorized access and substitutes.
2. Give someone lab instructions without explaining them aloud and see where they get stuck.
3. Correct ambiguities and record a review date. The course does not automatically create reminders.

Show what you know

Explain what happens if you are unavailable and what information each role needs at each stage.

Common question

Does a 2-of-3 wallet replace an inheritance plan? No. It is a technical tool. Heirs still need context, materials, coordination and legal authority.

Pause point

Keep the plan outside the course and mark only “drill reviewed.”

What is a useful criterion for evaluating an inheritance plan?

1. An authorized person can complete a documented drill without improvising or receiving secrets prematurely.
2. The plan has many pages.
3. It depends solely on remembering a password.

> **Show answer: An authorized person can complete a documented drill without improvising or receiving secrets prematurely.**
> Recovery and access control must be tested in practice.

Price, saving and fundamental analysis

Objective

Analyze investment arguments separately from verifiable technical properties.

Understanding the topic

Price results from trades on specific markets and may vary between platforms. Liquidity, quote currency, market depth, banking providers’ opening hours and demand affect the trade you can actually execute. A displayed quote does not guarantee an offer for your order size.

Fundamental analysis examines factors such as adoption, demand, competition, economic security, regulation and supply. A known issuance schedule alone does not determine future prices. Assessments of monetary utility or “intrinsic value” depend on assumptions. There is no objective number AI can present as universally certain.

Regular buying spreads entry times but does not guarantee a profit or prevent prolonged losses. Long-term saving also requires liquidity for obligations, tolerance for volatility and a custody plan. The course does not prescribe a percentage of your assets or make decisions for you.

Ask three separate questions. Do I understand the asset? Can I protect and recover it? Can I bear its economic risk? Mastery of keys does not automatically answer the third. Training does not turn a price projection or historical chart into a personal recommendation.

Practice

1. Write a fictitious investment thesis, its assumptions and facts that would invalidate it.
2. Simulate a 50% fall at the same time you need liquidity without entering your actual holdings.
3. Identify which parts of the argument are verifiable and which are expectations.

Show what you know

Discuss investment without promising returns or confusing conviction with evidence.

Common question

Does scarcity ensure the price rises? No. Demand and other conditions remain decisive for the market price.

Pause point

Keep the lab assumptions, without creating an automatic buying instruction.

What does buying at regular intervals guarantee?

1. A long-term profit.
2. No return is guaranteed. It spreads purchases over time according to a chosen rule.
3. Protection against losing keys.

> **Show answer: No return is guaranteed. It spreads purchases over time according to a chosen rule.**
> Spreading out purchases does not remove economic or operational risk.

M11

Choosing where to acquire bitcoin

Objective

Evaluate a provider’s authorization, cost, withdrawal options, privacy and custody risk.

Understanding the topic

Compare verifiable criteria: legal entity and jurisdiction, authorized services, withdrawal network, fees, price spread, limits, support, authentication and data handling. A trade name or sponsorship does not establish authorization for a particular service.

Total cost may include deposit, conversion, spread, trading fee, withdrawal and bank charges. A “fee-free” trade may have a wider spread. Check net amounts and reference currency. If self-custody is your goal, include the withdrawal in the budget.

While holding a custodial balance, you depend on the provider. Proof of reserves alone does not establish all liabilities, ownership of funds or future solvency. Check restrictions and make a small withdrawal you can afford before relying on a new process.

Commercial identification can associate your identity with a withdrawal. Protecting that information afterward does not erase what the provider already knows. Never falsify data or use the course to evade obligations. Purchasing a training code also creates a commercial record separate from your wallet.

Practice

1. Build a fictitious comparison of two providers covering total cost, network, minimum withdrawal, authorization and required data.
2. Calculate the net amount for a learning transaction with all specified charges.
3. Design a test withdrawal to a previously verified address without executing it through this course site.

Show what you know

Justify a choice for your situation and identify outdated or unverified information.

Common question

Does the course recommend one exchange as best for everyone? No. Permissions, fees, countries served and conditions change. A comparison needs a date and a use case.

Pause point

Keep the table without credentials or identity documents.

Which comparison is more useful than looking only at the trading fee?

1. The total cost through receipt of BTC on the desired network and address.
2. The provider’s follower count.
3. The color of its application.

> **Show answer: The total cost through receipt of BTC on the desired network and address.**
> The final cost includes items that may be absent from the advertised trading fee.

Accounts, orders and execution costs

Objective

Understand basic orders and protect your account without turning the course into a trading terminal.

Understanding the topic

A market order prioritizes available execution and exposes you to slippage. A limit order sets a maximum purchase price or minimum sale price but may not fill, or may fill only partially. A stop order triggers another action according to the provider’s rules. It does not by itself guarantee the final price.

The order book shows available offers, without guaranteeing that every volume will remain. During a drop or in low liquidity, execution may differ from the last quote. Stop-market and stop-limit orders have different risks: execution at a worse price or possible non-execution.

Protect access with a unique password, phishing-resistant authentication where supported, session reviews and appropriate withdrawal controls. Keep second-factor recovery independently. An automation API key may carry more dangerous permissions than a data query needs. Never enter it in the tutor or the course site.

Before withdrawing, check the asset and Bitcoin network, your wallet address and the net amounts. A platform may use the same symbols for different products. Keep purchase, execution, fee and withdrawal records as appropriate. A withdrawal to your own wallet is different from a new purchase.

Practice

1. Simulate an order book with one unit at 100 and another at 102. Explain why buying two at market does not guarantee an average price of 100.
2. Design a limit order and describe a scenario in which it does not fill.
3. Audit permissions for a fictitious API and remove withdrawal permission if it only needs to read data.

Show what you know

Describe priority, price and non-execution risk for each order.

Common question

Does a stop-loss always limit loss to an exact amount? No. Gaps, liquidity, slippage and provider rules can prevent that.

Pause point

Keep the exercise result without real orders or API keys.

What risk remains with a limit buy order at 100?

1. It may never execute or may only fill partially.
2. It must execute at any price.
3. It automatically creates a backup.

> **Show answer: It may never execute or may only fill partially.**
> Control over the price comes with the risk of non-execution.

M11

Candlesticks, indicators and biases in technical analysis

Objective

Read charts as historical data and evaluate strategies without mistaking patterns for predictions.

Understanding the topic

A candlestick shows a period’s open, high, low and close. Volume depends on the source. Changing platform, currency, time zone or interval can change what you see. A candle does not show the complete order of price moves within its interval.

A moving average smooths past prices. A momentum indicator transforms observed data under a formula. Neither knows the future. Two indicators derived from the same series may convey highly correlated information despite different names and colors.

Before looking at results, define entry, exit, invalidation, costs, size and data. Avoid selecting only winners, adjusting parameters until they fit or using future data to make a past decision. Distinguish training data from validation on a later period.

A backtest should account for spread, fees, slippage, data availability and feasible execution. Gross return, hit rate, maximum loss and the loss distribution answer different questions. A strategy with frequent wins can lose money if its losses are large. Never teach a buy or sell signal as a certainty.

Practice

1. Read a fictitious candlestick and explain what timing information it omits.
2. Write a rule before evaluating ten synthetic outcomes, including costs and a failure criterion.
3. Compare nine gains of 1 with one loss of 15. The gross result is -6 despite a 90% hit rate.

Show what you know

Critique an attractive result on the basis of selection, costs or risk without having to trade.

Common question

Does combining many indicators guarantee a better signal? No. It can increase overfitting and complexity without providing independent information.

Pause point

Save the rule and lab results without creating a market order.

Nine trades gain 1 each and one loses 15. What is the result before costs?

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

> **Show answer: -6.**
> Nine units gained minus fifteen lost gives a loss of six.

M11

Margin, futures and automation

Objective

Recognize exposure, liquidation and automation failure before considering complex products.

Understanding the topic

Leverage increases exposure relative to the capital contributed. In a simplified example, 100 of margin supports exposure of 1,000. An adverse 5% move in the underlying asset loses 50 before costs, half the initial margin. Actual maintenance, liquidation, collateral and fee rules may worsen the outcome and trigger earlier than expected.

Futures and perpetual contracts may involve expiry, cash settlement of differences, funding rates and reference prices different from the last trade. They are distinct from withdrawing native bitcoin to Cuvex. Safeguarding a seed does not protect a position from liquidation or counterparty failure.

A bot automates rules, errors included. It needs position limits, minimum permissions, idempotent orders, reconciliation, loss controls, emergency stopping and oversight. Repeating a request after a timeout can double exposure if the previous result is unknown.

AI can explain concepts and detect inconsistencies in a fictitious case. It should never receive API keys, enable trading or promise a profitable strategy. For this course, understanding the risks lets you decide against products you do not understand.

Practice

1. Work through the exposure and margin example without assuming liquidation occurs at exactly 10%.
2. Simulate an API that executes an order but loses the response. Explain why reconciliation must precede a retry.
3. Design a stop control that prevents new orders and checks outstanding ones, without connecting to a broker.

Show what you know

Describe a risk that remains despite a stop order, one that remains despite a bot and one that remains despite self-custody of external funds.

Common question

Does removing emotion through automation guarantee results? No. Automation may reduce impulsive intervention while multiplying design or execution mistakes.

Pause point

Mark this extension as understood without enabling complex products.

With exposure of 1,000 and margin of 100, a loss of 5% on the exposure amounts, before costs, to:

1. A loss of 5.
2. A loss of 50, or 50% of the margin.
3. No loss if a bot is used.

> **Show answer: A loss of 50, or 50% of the margin.**
> Leverage and costs cause the return on margin to differ from the asset’s price movement.

M12

Lightning and other layers

Objective

Understand channel-based payments and recognize features outside the reviewed Cuvex workflow.

Understanding the topic

Lightning uses channels and updates to make payments without recording every exchange individually on the base chain. Opening and closing channels and some recovery scenarios may require on-chain transactions. Availability, inbound and outbound liquidity, and monitoring depend on wallet design and the services used.

An invoice may include an amount, description and expiry. Depending on context, amounts may be in satoshis or millisatoshis. Millisatoshis do not imply sub-satoshi outputs on the base chain. Paying an invoice requires compatible support and an available route. A QR code does not guarantee payment through any application.

Custodial and noncustodial services have very different models. Typical speed does not prove the absence of risks. Do not present Lightning as completely anonymous. Observers, routes, counterparties and metadata remain relevant.

Cuvex chat can coordinate requests for sats paid on-chain through a WOW account. This edition does not attribute a Lightning node, channel management or Lightning invoice signing to Desk. If a request includes several payment methods, verify which you understand and which your application will execute.

Practice

1. Classify training examples of an on-chain address, a bitcoin: URI and a Lightning invoice.
2. Compare on-chain and channel payments in terms of confirmation, liquidity, custody and recovery.
3. Explain why an expired invoice should be checked with the recipient instead of being reinterpreted as an address.

Show what you know

Decline an incompatible payment method without exposing keys or incorrectly attributing a failure to Cuvex.

Common question

Are all payments in sats Lightning payments? No. Satoshis express value. The method depends on the protocol used.

Pause point

Record the exercise’s payment method without saving real invoices.

How can you tell that a request is payable over Lightning?

1. It uses the word “sats.”
2. It arrived in chat.
3. It has a compatible format and payment method. The unit and message channel alone are insufficient.

> **Show answer: It has a compatible format and payment method. The unit and message channel alone are insufficient.**
> The unit of account and the payment network are distinct.

Taproot, MuSig2 and a post-quantum future

Objective

Distinguish standards, proposals and implemented capabilities.

Understanding the topic

Taproot allows spending conditions with key and script paths. Schnorr signatures and aggregation can improve some constructions, but the privacy outcome depends on configuration and spending. A bc1p address does not show that there are no other participants or reveal all hidden conditions.

MuSig2 allows a set of signers to aggregate keys and interact to produce a compatible Schnorr signature. The base standard is N-of-N. An arbitrary M-of-N threshold requires another construction or additional protocol. Nonce and session management are critical and cannot be implemented by informal exchanges of messages.

PSBT v2 reorganizes information relative to v0. A file containing a version 2 transaction is not automatically upgraded to PSBT v2. For the multisignature profile, this edition’s Final firmware retains PSBT v0, P2WSH/sortedmulti and SIGHASH_ALL. Future capabilities require their own specification and validation.

NIST published its first finalized post-quantum standards in 2024. Their publication does not itself change Bitcoin signatures. Using a post-quantum algorithm to authenticate firmware would protect that layer. It would not automatically convert ECDSA or Schnorr signatures for a UTXO into post-quantum signatures. The tutor also cannot guarantee a date for a future attack.

Practice

1. Classify five claims as a standard, verified implementation, proposal or advertising.
2. Explain why “accepts a Taproot recipient” does not prove “signs a Taproot input.”
3. Draw separate layers for firmware signing, secret encryption, chat and Bitcoin spending authorization.

Show what you know

Request evidence for a particular layer without transferring guarantees between protocols.

Common question

Should I move my funds because of a quantum computing headline? An actual decision requires current technical evidence, verifiable support, risk assessment and a secure migration plan. The course does not direct fund movements on the basis of headlines.

Pause point

Record technical questions without creating an automatic spending plan.

If implemented and validated, would a post-quantum signature in the bootloader change the signing conditions of an existing UTXO?

1. No. These are separate layers.
2. Yes. It switches the whole network to another algorithm.
3. It removes the need for backups.

> **Show answer: No. These are separate layers.**
> Authenticating an update does not rewrite Bitcoin spending conditions.

Interoperability and moving away from the manufacturer

Objective

Plan for continuity if the software, device or provider changes.

Understanding the topic

A list of acronyms is insufficient to establish interoperability. The network, script, derivation, keys, policy, transaction format and signature semantics must be preserved. Two applications may understand BIP174 without supporting the same fields, sizes or input types.

To avoid dependence on an interface, keep documented recovery information and practice with learning wallets. A standard mnemonic may allow key derivation, but multisignature recovery requires the complete policy. BIP329 labels add privacy-sensitive context. Chat history has a different scope.

Do not expose a real seed to test compatibility. Start with public descriptor export and watch-only recovery. If an emergency requires reconstructing keys, use an environment designed for that purpose and consider migrating afterward. An incompatible wallet showing zero does not prove the funds were lost.

Keep verifiable copies of the documentation, course version and tools needed. Application signing, expired certificates and system changes can affect installation. Available open-source code does not guarantee that someone can build it years later without its dependencies and the necessary knowledge.

Practice

1. Design an exit test with an empty account. Reproduce the same network, policy and verification address in two compatible implementations.
2. List which components follow standards and which need a converter or Cuvex format documentation.
3. Define what result establishes compatibility and what still needs hardware or real signing tests.

Show what you know

Describe a recovery path that does not depend on one company continuing to provide the same service.

Common question

Does open source mean the manufacturer no longer matters? No. Distribution, maintenance, physical components and operational experience still matter. Open source enables inspection and possible continuity without guaranteeing them automatically.

Pause point

Save the lab results with the versions and observed limitations.

Which is stronger evidence of interoperability?

1. Both apps say “Bitcoin.”
2. Reconstructing and checking the same policy and address in a lab using identified software versions.
3. The icons look similar.

> **Show answer: Reconstructing and checking the same policy and address in a lab using identified software versions.**
> A test must retain the relevant conditions and produce a verifiable result.

Technical lab with regtest

Objective

Understand a reproducible lab without confusing synthetic testing with physical use.

Understanding the topic

Regtest lets you create a controlled local chain, generate blocks and test transactions with no economic value. Use separate directories and credentials and never import real material. Its results alone do not demonstrate USB, NFC, Bluetooth or camera compatibility on physical equipment.

A complete lab records versions, network configuration, policy, test inputs, PSBT, signatures, final transaction and acceptance result. It can verify that amounts balance, an altered signature is rejected and a valid payment enters a local block. Include failures as well as the successful path.

Desk 9.21 validation reports tests with Bitcoin Core 31 regtest and automated engine and simulated UI tests. This edition uses the reports as documentary evidence. It does not claim that the tests were repeated or that device operations were performed. Checking a package likewise does not prove installation on every system.

Before a technical class, the engineer should provide a working lab and a procedure compatible with the student’s version. Never expose RPC to the internet for the tutor to control. AI may guide interpretation of synthetic results but should receive neither credentials nor administrative permissions.

Practice

1. With the lab ready, observe a valid transaction and one with an altered signature. Record acceptance or rejection.
2. Check one case of incorrect change and another with an incompatible network.
3. Distinguish “engine test,” “simulated interface” and “physical hardware” in your report.

Show what you know

Describe exactly what was tested and what remains outstanding without presenting a simulation as certification.

Common question

If regtest works, can I sell the course as validated for every device? No. Physical workflows, installation, accessibility, recovery and the commercial service still need testing.

Pause point

Stop and save the lab according to its instructions, retaining only synthetic data.

Does a regtest engine test demonstrate actual NFC reading on a particular phone?

1. Yes, because both use Bitcoin.
2. Yes, if the PSBT is small.
3. No. A separate physical test is required.

> **Show answer: No. A separate physical test is required.**
> Validation environments have different scopes.

Final project and continuity plan

Objective

Demonstrate independence from preparation through recovery and privacy.

Understanding the topic

The outcome is the ability to explain intent, verify a result and stop an operation you do not understand. Memorizing a menu is insufficient. Assessment combines concepts, guided practice and an independent case. It never depends on revealing seeds, holdings or personal addresses to an evaluator.

Case A. Set up a learning environment, identify models and versions, protect Desk, link a training cryptogram and reconstruct a watch-only account. Explain which backups are necessary and what data the provider may observe.

Case B. Design a payment using fictitious UTXOs from different contexts. Justify the selection, verify recipient, change and fee, and describe the signing workflow for your device. Resolve an interruption during return of the response and another during broadcast without duplicating the payment. Without physically accepted hardware, record this part as simulated and still awaiting physical completion.

Case C. Design a 2-of-3 policy, act out invitation and verification, compare a field of your choice in Mirror in any order and explain exactly what “OK” establishes. Recover the learning policy, simulate the loss of a participant and plan for continuity and inheritance.

The proposed passing standard requires at least 80% on knowledge and every critical control correct: keep secrets private, check network and outputs, distinguish stages and retain recovery capability. A critical error requires review and new practice. Correct market answers cannot offset it. Any commercial certificate issued should specify what was assessed and whether the evidence involved physical observation or simulation only.

Practice

1. Complete all three cases with synthetic data and your own explanation.
2. Complete the final assessment in the appendix and review each incorrect answer.
3. Submit only a results sheet with no secrets, documenting the scope of the evidence and outstanding work.

Show what you know

Stop on your own initiative when an operation lacks sufficient evidence, and identify what you need in order to proceed.

Common question

Does reading every page mean I am ready to safeguard any amount? No. Demonstrate capability and assess risk according to your circumstances. Reading and exercises do not guarantee future outcomes.

Pause point

Keep your review plan and outstanding exercises. You can return to the chapter you need without repeating the whole course.

What is a critical requirement for completing practical training?

1. Having opened every page.
2. Demonstrating recovery and transaction review within a documented scope, without revealing secrets.
3. Predicting next month’s price.

> **Show answer: Demonstrating recovery and transaction review within a documented scope, without revealing secrets.**
> Learning is demonstrated by verified capabilities and limits, rather than browsing activity or prediction.

Student manual

Cuvex operating manual

This manual accompanies the lessons. Each procedure describes the workflow found in the reviewed sources, its checks and its stopping point. This is a pilot candidate edition. It does not attest to independent physical tests with Original, BIT, phones or every desktop platform. Before teaching with real funds, the team must complete the acceptance matrix and adjust any labels or screens that differ.

References: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 and Mirror 1.0.0-beta.12.12. Selecting a profile in Desk declares compatibility. It does not remotely measure firmware. The included Mirror screenshots come from the Android emulator for package 12.12. The product photographs are corporate materials and do not prove which version a current device displays.

P01 | Check provenance and version | Cuvex | L16,L21 | C01,C02

Preparation: Have the purchase details and an official channel you can verify independently. Do not enter any secrets yet.

1. Inspect the packaging and seals. If you see signs of tampering, stop setup and retain nonsensitive evidence.
2. Use the integrity and seal-check workflow in the app compatible with your delivery. Enter codes only there, never with the tutor.
3. Identify whether you have Original or BIT and which revision is available. Check the versions displayed by the device and applications.
4. Compare them with the team’s published matrix. Neither a catalog nor a hash replaces firmware authentication or physical acceptance.

Result: The model and versions have been identified and the source checked without exposing secrets. If the codes are invalid or the interface differs, do not use a historical guide to force operation.

Pause: Stop before loading custody material. Commercial traceability alone cannot guarantee the absence of sophisticated tampering.

P02 | Update Original over Bluetooth | Original | L46 | C01,C02,C03

Preparation: Have recoverable backups, stable power, a compatible official package and an accepted workflow for your system. This course does not establish complete physical availability on every platform.

1. In the app’s devices or firmware section, select Original and the official download or corresponding authentic local file.
2. Use the device menu to enter update mode and connect through the application workflow. Stay nearby and avoid competing sessions.
3. Enter the code shown by Original in the specified field. It is separate from the cryptogram password.
4. Follow transfer, validation, installation and reboot. A percentage alone does not prove installation.
5. Check the final version on Original and record it in the app if the corresponding field exists.

Result: The device screen confirms the version after reboot and the workflow confirms completion. If it fails before the PIN, during packet transfer or at the end, record the stage and code. Do not improvise a disconnection or software change to “get past 99%.”

P03 | Update BIT over USB | BIT | L46 | C01,C02,C03

Preparation: Identify BIT’s actual storage medium, power supply and compatible official package. Retain backups before changing software.

1. Select BIT in the compatible Desk or Mirror firmware workflow.
2. Connect the device using the appropriate data cable and adapter. Authorize volume or folder access when requested.
3. Select authentic firmware for the model. Check the version and compatibility details before transferring it.
4. Wait through transfer and device validation. A volume may disappear and be mounted again as the protocol proceeds.
5. After reboot, check the version on BIT and the final result in the app.

Result: Installation has been checked on the device itself. If the volume does not appear, check device mode, data cable, permissions, mounting and competing active sessions. A PC folder with the same name cannot substitute for it. Recovery after a failed update requires the official procedure for that hardware.

P04 | Generate a wallet with a coin and dice | Cuvex | L17 | C01

Preparation: Use a private space, suitable dice and a coin, with the tutor microphone off and no cameras. Use a learning wallet.

1. Open wallet creation and the firmware’s entropy workflow. Fix the order of the four dice before starting.
2. Enter the coin result and each die as the screen directs. Never change a result to suit a preference.
3. The reviewed source computes index = coin × 1,296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). It accepts only indices 0 through 2,047.
4. On rejection, flip the coin and roll all the dice again. The warning retains the previous words and asks for a new complete set.
5. Complete the device algorithm including final validation, protect the mnemonic and test recovery privately.

Result: The wallet was generated through the full procedure without manually selecting words. Stop if the screen and source disagree. Never adopt a public example of dice, seed or key as your own material.

P05 | Encrypt a secret | Cuvex | L18,L19 | C01

Preparation: Choose model, content format and protection. Entering a secret on a PC or phone exposes it at the source even when the destination is encrypted.

1. Select encryption and a supported type: BIP39, SLIP39, Monero or text. Do not interchange wordlists. The reviewed plaintext keyboard accepts up to 500 characters. Storing another format does not imply support for signing on its network.
2. Enter the content directly on the device to maintain isolation. Review order, characters and additional fields on its screen.
3. Choose individual or shared protection according to the workflow, and biometrics on BIT if appropriate. Distinguish this threshold from the Bitcoin threshold.
4. Privately enter and confirm the passwords according to the firmware validator. Do not automatically apply Desk’s rules.
5. On Original, write to a compatible blank card. On BIT, retain the export objects created by the USB workflow. Wait for confirmation.
6. Start a test recovery to verify the contents, then close the secret display.

Result: The cryptogram has been checked through recovery. If a read or write fails, protect the original and follow the screen’s retry procedure. Do not delete headers or force overwrites.

P06 | Decrypt on the device | Cuvex | L18 | C01,C02

Preparation: Ensure physical privacy and sufficient unlocking components. Turn off nearby microphones and screen capture when working with the secret.

1. Start decryption on the correct model and supply the cryptogram through NFC on Original or the BIT USB workflow.
2. Check the alias and object identification before entering credentials.
3. Supply the required passwords and biometrics if the format requires them. Avoid repeated automatic retries after failures. Access controls and lockouts apply.
4. Verify the contents only on the intended display. A QR code representing the secret is just as sensitive as its text.
5. Close or end the process as the device directs, and store the medium and credentials separately according to your plan.

Result: The contents have been recovered privately and the session has ended. If the format is unrecognized, authentication fails or the contents are unexpected, do not “fix” them using an unknown app. Give support the version, format and error without attaching the secret.

P07 | Prepare recovery of a biometric cryptogram | BIT | L19,L47 | C01,C02

Preparation: Use a learning cryptogram and documentation for its format. A .bin copy alone does not establish recoverability.

1. In the Desk details view, identify any biometric components and the available recovery export.
2. Retain the full set of files associated by the workflow and an independent copy, using discreet identifiers.
3. Test normal unlocking on BIT and document the passwords and conditions it requires.
4. Study the exceptional local recovery method and its supported formats. Verify the necessary material exists before you need it.
5. Use data with no funds to rehearse device failure or an unavailable fingerprint.

Result: You have a tested plan with defined limits for that specific format. This does not imply that any biometric requirement can be bypassed or that a fingerprint replaces backups. If a secret is recovered on a PC, assess its exposure and whether control should be moved afterward.

P08 | Create and check a cryptogram backup | Cuvex and Desk | L20 | C01,C02

Preparation: Identify the original and choose a compatible destination without data you need to retain.

1. On Original, use the device’s clone function or the compatible Desk function. Present source and destination in the specified order.
2. Hold cards steady and respect rejection of media that already hold cryptograms.
3. For BIT or a file, export the complete set of components and preserve the required names or associations.
4. Isolate the original copy and test reading and recovery from the new one.
5. Privately record the date, format and result. Store the copies where they face independent physical risks.

Result: A second copy has passed testing. It is not another wallet, does not revoke passwords and provides no protection against an already leaked seed. If the destination fails, retain the original without trying to “repair” it to make the copies match.

P09 | Create and unlock Desk storage and change its password | Desk | L21,L40 | C02

Preparation: Use a verified installer and the correct architecture. Have a backup plan for the store.

1. Create the store with a unique password of 12 to 1,024 characters and matching confirmation.
2. Lock and reopen it to verify access. Enter the password only in Desk.
3. Under Security and Access and Locking, review inactivity and background behavior. Keep optional erasure off during a demonstration.
4. To change the password, enter the current one and confirm the new one through the appropriate workflow.
5. If you used PC biometrics, configure them again as instructed. Make a current backup and retain the relationship to prior copies.

Result: Access is confirmed. Earlier copies retain their original password and encryption. PC biometrics and BIT biometrics are distinct. If access fails, stop repeated attempts and review recovery without asking the tutor to store credentials.

P10 | Link and review a cryptogram in Desk | Desk | L22 | C02

Preparation: Use a test cryptogram of known origin and an available transport method.

1. Open Cryptograms or Cards and choose to link via NFC, USB or a compatible backup.
2. Select the design and source. For NFC, use Cuvex Mirror paired with the computer over Bluetooth. Alternatively, use the volume of a Cuvex BIT connected by USB-C. Cuvex Desktop does not support external USB NFC readers.
3. Review alias, source, size, format and interpreted access conditions in the details view. These are metadata, not decrypted contents.
4. Check for retained accounts awaiting association and link only the verified account.
5. Export a copy if backup coverage is incomplete and test recovery separately.

Result: The object is organized locally. “Linked” proves neither seed authenticity nor balance. For an unrecognized object, check format and version. Do not change its extension or delete data to force acceptance.

P11 | Activate a watch-only WOW account | Desk and Cuvex | L13,L22 | C01,C02

Preparation: Have the public information obtained through the device workflow and privately verify its origin.

1. Open Activate WOW or Add Account from the correct cryptogram.
2. Import the supported descriptor or public material through file, webcam or Mirror as the function permits.
3. Review network, script, origin, fingerprint, path and checksum where applicable. Never enter a seed or xprv.
4. Name the account and make an informed choice of query source.
5. Check a verification address and the scope of discovery before interpreting the balance.

Result: The watch-only wallet is associated. A zero balance calls for checking network, original passphrase, derivation, account, provider and scan before concluding that coins disappeared. Networks supported by a general interface may not be supported by the multisignature profile. Respect the context.

P12 | Configure the node and synchronization | Desk | L25,L33 | C02

Preparation: Decide what privacy you need. If using Core, have access to a protected, synchronized node.

1. Under Security and Privacy and Nodes, select the WOW account and review its provider.
2. Explicitly choose a supported public provider or Core. For Core, enter endpoint, wallet and credentials only in the application.
3. Authorize the query after considering what data each service receives. TLS does not hide the query from the provider.
4. Synchronize and review date, chain tip, progress and completion state. For a rescan, check the period covered and continuity of the work.
5. On HTTP 429, respect the pause. If the provider fails, do not assume another node took over. The configuration does not rotate silently.

Result: You know the source and its state. Do not expose RPC to the internet, share the password or restrict discovery to addresses with a balance. An empty history may be only a partial result.

P13 | Generate and retrieve a receiving request | Desk and Cuvex | L26 | C01,C02

Preparation: Verify the account, network and policy.

1. Open Receive and generate or retrieve the appropriate request.
2. Add observer, reason and expected amount only if you need those local metadata.
3. Verify the address through the compatible device workflow before receiving a significant payment. Where physical acceptance is outstanding, stop the exercise at simulation.
4. Share only the necessary data over the recipient’s authenticated channel.
5. Check receipt, amount and confirmations through your network source.

Result: The payment has been reconciled, beyond merely issuing a request. Multisignature addresses already displayed are kept for late payments and never reassigned. If you reach the limit for new addresses without history, retrieve previous requests. Do not force indices manually.

P14 | Labels, freezing and BIP329 | Desk | L27 | C02,B13

Preparation: Use a lab account with UTXOs and a password for protected export.

1. Label an input with its context, omitting unnecessary personal information.
2. Freeze or unfreeze deliberately and review the spendable balance. The restriction is local.
3. Export labels using the protected function. Distinguish the BIP329 format from file encryption.
4. Import into a compatible copy and check that references, labels and freeze states match.
5. Keep a current backup of the metadata with its associated password according to your plan.

Result: The context is preserved and selection understood. Never let an import automatically unfreeze coins without review. Do not send the tutor the label file. It may reveal counterparties and relationships without containing spending keys.

P15 | Prepare a payment and send the entire balance | Desk | L28 | C02

Preparation: Have a verified request and an account with sufficient spendable inputs.

1. Open Pay from WOW, UTXOs or chat and confirm the account and network.
2. Select inputs, recipients and amounts. Review which contexts you are connecting.
3. Choose the fee rate and review the absolute fee, change and warnings. If there is dust, consider alternatives without accepting a hidden fee.
4. To send all, check the net amount after fees. In chat, explicitly confirm a partial payment if it does not cover the request.
5. Prepare a draft and review every detail before exporting for signing.

Result: The intent is clear and the PSBT belongs to that transaction. A general form may accept more inputs or recipients than the hardware. Apply the effective limits of signer and transport. A change to outputs or conditions starts a new review.

P16 | Sign and return a PSBT with Original | Original and Mirror | L29 | C01,C02,C03

Preparation: Have the correct draft, compatible transport card, compatible authenticated cryptogram and a private way to unlock it. An older copy without verified authenticity may require verified recovery and creation of a new copy before signing. Editing its header does not fix it.

1. Export the request through the compatible NFC workflow from Desk/Mirror.
2. Take it to Original. Supply the cryptogram when requested and unlock it without dictating credentials.
3. Review network, summary, complete outputs, fee, change and mandatory warnings.
4. For Final multisignature, decide whether to examine extended parameters. Complete the three final confirmations only if everything matches.
5. Wait for the response to be written to the card and read back.
6. Read the response with Cuvex Mirror and validate it in the corresponding Desk operation.

Result: The signature has been received and linked to the draft. It has not yet been broadcast. If writing fails, retain the state and follow the retry process. Never use a backup card as disposable payment transport.

P17 | Sign, receive and acknowledge with BIT | BIT and Desk | L29 | C01,C02

Preparation: Have the correct draft, a compatible authenticated cryptogram and the actual BIT volume selected. If an older copy is rejected for signing, follow the indicated recovery and renewal procedure without forcing the format.

1. Deliver the request over USB-C through Desk’s service. Follow the device screen for the cryptogram.
2. Unlock privately and review the summary, every output, the fee and the warnings.
3. For Final multisignature, optionally inspect the extended details. Authorize with the mandatory final confirmations.
4. In Desk, use Receive from BIT to import and validate the response for that job.
5. Check that the response is saved and acknowledged. If acknowledgment fails after receipt, retry the same operation. Do not allow the model to select a different one.

Result: The signature is verified and exchange state is consistent. If disconnection occurs before receipt or after saving, retain the request’s profile. Never switch to another firmware entry in the catalog to make a pending response fit.

P18 | Finalize, broadcast and monitor a transaction | Desk | L30,L44 | C02

Preparation: Have verified signatures and a sufficient threshold where applicable.

1. Review the intent, inputs, outputs, fee and network again.
2. Use the appropriate action to finalize and verify that no signatures or conditions are missing.
3. Authorize broadcast and retain the local result. If the network response is lost, check before retrying.
4. Track the mempool and confirmations through the selected provider, noting the synchronization date.
5. If considering RBF, review the new transaction and obtain the required signatures. Do not assume built-in CPFP support.

Result: Chain state has been checked against its source. Canceling a draft does not revoke exported signatures or rewrite confirmed payments. A chat message or screenshot cannot replace monitoring.

P19 | Compare two policy QR codes in any order | Mirror | L43 | C03,C02

Preparation: Have the field visible in Desk and Cuvex. During practice, use only the course’s synthetic samples.

1. Open Compare Policies and scan either side first.
2. Choose whichever field you want to check. You may begin at step 15 and skip fields you reviewed manually.
3. Scan the counterpart and review both complete texts. If the step is ambiguous, use Specify Desk Step and remember that this context is entered manually.
4. Interpret Match or No Match only for that literal pair. Spaces, capitalization and encoding count.
5. Start another pair in any order. Exit or move to the background to finish according to the reviewed clearing behavior.

Result: This is a local check of one pair. It does not establish origin, session, overall approval or activation. Clarify any discrepancy with the sources. Do not normalize the text to force an OK.

P20 | Activate, recover and move chat | Desk and Cuvex | L36,L39 | C02

Preparation: Choose DEV or Production. Have an alias and Chat Key on the device, never in the course.

1. Open chat activation or recovery from the cryptogram context.
2. Choose a new alias or transfer an existing one. Select the compatible mobile profile specified by the app.
3. Enter or read the Chat Key exclusively through the private workflow. Do not use a seed, PIN or WOW key.
4. Check activation with the service. If it is pending, use the completion or verification action rather than assuming success.
5. Verify continuity with contacts after a transfer. Avoid using one alias on several devices simultaneously.

Result: The identity is activated or recovered in the correct environment. Neither the Chat Key nor the full Desk backup automatically recovers past history and sessions. Respect the limits of the available material.

P21 | Verify a contact’s identity | Desk | L36,L48 | C02

Preparation: Have an independent channel agreed in advance with the person.

1. Add the alias and inspect its public identity through the app.
2. Compare the fingerprint through the authenticated channel, not just inside the newly created conversation.
3. If using recognition questions, avoid public information and secrets reused on other services.
4. Confirm only after all discrepancies are resolved. Suspend payments and coordination after an identity change until it is verified.
5. Document the verification method without storing sensitive answers in the course.

Result: You have contextual trust in the contact, without a guarantee covering every future request. A voice can be imitated and a legitimate device compromised. Each operation still needs review.

P22 | Request an address, request payment and pay through chat | Desk and Cuvex | L37 | C02,C01

Preparation: Have a verified contact and a compatible WOW account.

1. Choose Request Address, Reply with Address or Request Payment according to your intent.
2. Review the original request, network, amount and note before sending it.
3. To pay, start preparation from the correct account, select UTXOs and fee rate and review the net amount.
4. Authorize on Cuvex following the procedure for your model. Chat never signs automatically.
5. Track broadcast and confirmation through your source. Reconcile any explicitly agreed partial payment against the original request.

Result: Chat has provided coordination while preserving custody review. Message status and transaction status are distinct. An explorer link may send information to a third party. Assess it before opening it.

P23 | Share and link a received cryptogram | Desk | L38 | C02

Preparation: Identify a concrete reason for sharing, verify the contact and define which means of access the contact will receive.

1. Choose Share Cryptogram from the chat action and review the object.
2. Do not attach passwords, a seed or a Chat Key as a comment.
3. The recipient checks provenance and links the supported object through the receiving action.
4. Consider what capability the recipient obtains immediately and what they could obtain with sufficient unlocking credentials.
5. Keep a realistic revocation plan. Deleting messages does not remove external copies or revoke known keys.

Result: An encrypted object has been deliberately transferred. This does not make a payment or independently add a key to a multisignature wallet. If the attachment directs you to an unknown webpage for decryption, stop the workflow.

P24 | Make and restore a full Desk backup | Desk | L15,L21 | C02

Preparation: Use a learning store and a controlled backup destination.

1. Open the store backup function and set the requested password. Keep track of which password belongs to this particular backup.
2. Store the backup away from your only working device. Follow the workflow to check provenance and integrity.
3. Restore it in a separate test environment and verify the covered accounts, settings and data.
4. Review exclusions. Do not assume chat, its sessions and history are included. A multisignature policy and private keys are not interchangeable.
5. Repeat after major changes and retain recovery instructions.

Result: You know the backup’s scope and password. Older backups retain older passwords. When access changes or a secret is exposed, assess those copies as well as the current store.

P25 | Create and accept a multisignature wallet | Desk and Cuvex | L41,L42 | C01,C02

Preparation: Have independent participants, verified contacts and agreement on the network and effective limits.

1. The creator chooses the name, M/N, network, participants and operational validity period.
2. Supply the correct extended public key with fingerprint and BIP48 path through the supported workflow.
3. Each participant reviews, accepts or rejects and supplies their public material. No participant shares a seed.
4. Build the complete policy and prepare to verify it on each device.
5. Keep policy backups before funding. Check a verification address and the ability to recover.

Result: The proposal is complete and verifiable. Accepting an invitation cannot replace hardware review. If Original participates, apply its six-key maximum and the NFC size limit. BIT does not increase other participants’ capabilities.

P26 | Verify a policy and receive confirmation | Desk and Cuvex | L43 | C01,C02,C03

Preparation: Give everyone the same complete policy. Use the correct firmware profile and a device without competing operations.

1. Start Verify Policies in the supported context. Original requires explicit selection of the installed profile. BIT negotiates capabilities under its specification.
2. Deliver the request by NFC/Mirror or USB-C according to the model.
3. Review the policy fields on the device. You may use Mirror to compare selected pairs in any order.
4. Complete device confirmation and return the response through the appropriate transport.
5. In Desk, validate the response for this request. A visual OK from the comparator cannot replace that step.

Result: The response is correlated and applies to this review. The catalog does not remotely attest firmware, and the device is not presented as a persistent policy store. On FIRMWARE_CAPABILITY_REQUIRED, first check the Desk version and model/build combination.

P27 | Request and receive signatures and hand over coordination | Desk and Cuvex | L44 | C01,C02

Preparation: Have a verified policy, an identified transaction and agreed recipients.

1. Prepare inputs, outputs, fee and notes and request signatures from compatible participants.
2. Each participant reviews and signs on their device through its transport workflow.
3. Receive, validate and save each signature. Resolve pending acknowledgments without changing the saved profile.
4. On handover, the recipient accepts the coordination workflow and checks its state. This changes neither M/N nor key ownership.
5. Once the threshold is reached, review and finalize before broadcasting. Track the transaction on the network.

Result: You have separate evidence for each coordination step. A coordinator’s progress report is distinct from your own local check. Canceling or rejecting in one app need not destroy signatures already retained by others.

P28 | Export, restore and locally delete a multisignature wallet | Desk | L45 | C02

Preparation: Have a known policy and a backup encrypted with a unique password.

1. Use Desk’s recovery export. The current workflow uses an authenticated CVXMSBK1 container for this export.
2. Keep the copy and password exposed to independent risks. Do not infer encryption from the extensions of older files.
3. To restore, supply the backup, password and participant public key with the correct origin, using webcam or Mirror if applicable.
4. Check policy, network, address and discovery before operating.
5. For local deletion, read the scope and confirmation. Keep a backup if you want to retain recovery. A later restore is an explicit action.

Result: The policy can be recovered, or local state was deliberately removed. Deletion does not move funds, erase other signers’ keys or automatically cancel operations retained by others.

P29 | Perform exceptional recovery on a PC | Desk | L47 | C02

Preparation: Have supported-format material, a prepared clean environment and a backup. This operation may reveal a secret to the PC. Use learning data during the course.

1. Start local recovery from the correct context and read the format restrictions and warnings.
2. Consciously accept the risk and disconnect the network as the workflow requires. The window checks connection state before allowing you to proceed.
3. Enter only the required credentials in the private window. Do not dictate them, paste them into the course or share them with support.
4. Enable viewing only in a space free of cameras and listening assistants. Respect the timer and closing behavior.
5. Finish, consider the exposure that may have occurred and plan migration to new keys if necessary.

Result: This is exceptional recovery. It does not guarantee forensic erasure or equivalence to isolated hardware. If authentication, format compatibility or access material is missing, do not test internet tools on the real backup.

P30 | Review preferences, biometrics and locking | Desk | L40 | C02

Preparation: Know the password and verify a tested backup before changing security.

1. Under Access and Locking, review password, available biometrics, inactivity and locking when the app goes into the background.
2. Understand the delay after failures and the configured maximum before changing it.
3. Keep optional erasure disabled until you understand its conditions, threshold and recovery. Never test it in production.
4. Under Preferences, adjust language, theme, currency, 3- or 5-minute synchronization and sounds.
5. If you register bitcoin: links, verify that opening a request still requires unlocking, selection and review. Opening the link does not pay by itself.

Result: You understand the configuration. Operating-system biometrics depend on the device and replace neither the password nor the backup. Visual preferences do not modify Bitcoin policy.

P31 | Delete records with a clear understanding of scope | Desk | L22,L45 | C02

Preparation: Identify whether you are deleting a local cryptogram, account, WOW record, chat or multisignature wallet and which backup you will keep.

1. Read the selected object and its warning. Confirm the exact alias or explicit condition when the app asks.
2. Export and test a backup if you need to recover that state later.
3. Delete only the intended object and check which associations the workflow keeps or removes.
4. Check for outstanding operations or outside participants. Do not assume messages, signatures or files disappear from other devices.
5. Document the change in your private inventory without adding sensitive data to the course.

Result: Local state has been deliberately managed. None of these actions alone changes the scripts of funded UTXOs, destroys a seed known to others or reverses confirmed transactions.

P32 | Diagnose problems without exposing secrets | Desk and Mirror | L23,L30,L48 | C02,C03

Preparation: Note the approximate time, system, architecture, version and stage. Avoid repeatedly triggering a sensitive operation whose state is unknown.

1. Identify whether the failure involves search, pairing, reading, writing, validation, signing, return, network or display.
2. Copy the error code and text without QR codes or private data. Use the app’s diagnostics where appropriate.
3. Review the file before sharing it. Do not attach a store backup, cryptogram, seed, Chat Key, descriptor or RPC credential.
4. For an interface issue, record window size, zoom and hidden controls using a synthetic scene.
5. Send the expected result and reproducible steps through the official channel. The course does not automatically send messages to support.

Result: The report allows investigation with minimal data. Record a stage lacking evidence as “pending” rather than “completed.” Voice assistance does not need remote access to your custody device.

Bitcoin and self-custody glossary

Bitcoin

A network and set of rules for transferring value and verifying its history without a single administrator of the ledger.

BTC

Bitcoin’s monetary unit. One BTC equals one hundred million satoshis.

Satoshi

A unit on the base chain equal to one hundred-millionth of a BTC.

Blockchain

A history of linked blocks verified against a set of rules. The term alone does not describe every property of a network.

Block

A data set that includes transactions and a header that can be validated.

Full node

Software that verifies the rules of the blocks and transactions it accepts.

Mining

Building blocks by means of proof of work under the rules of the network.

Proof of work

A mechanism that requires verifiable computational work to propose a block.

Consensus

Agreement among participants on the rules and the valid history they accept.

Mempool policy

Local acceptance and relay rules that need not be the same as consensus rules.

Mempool

A node’s local set of unconfirmed transactions.

Confirmation

Inclusion in a block of the accepted chain and the subsequent depth of that block.

Reorganization

A change to part of the accepted chain that can affect confirmations.

UTXO

An unspent transaction output that can be spent under its specified conditions.

Input

A reference to a previous output and the data needed to authorize its spending.

Output

An amount and spending condition created by a transaction.

Change

An output that returns part of the inputs to your control after the payment and the fee.

Fee

The difference between the total value of a transaction’s inputs and outputs.

vbyte

A unit of virtual size used to express the relative cost of a transaction.

sat per vbyte

A fee rate expressed in satoshis per unit of virtual size.

Dust

An output considered small under applicable policies and spending costs. The threshold depends on the context and script.

RBF

Replacement of an unconfirmed transaction under compatible policies. Cancellation is not guaranteed.

CPFP

Use of a child transaction to increase the incentive to include it and its parent together.

Hash

A data fingerprint useful for checking integrity. It does not encrypt the data or identify its author on its own.

Private key

The cryptographic capability to produce authorizations under the relevant scheme.

Public key

Data used to verify signatures and construct certain spending conditions without exposing the private key.

Digital signature

Cryptographic proof authorizing a particular message. It does not hide that message’s content.

Encryption

Protection of confidentiality using a key and an algorithm.

Authenticated encryption

Encryption that also checks for alterations according to its design.

AES GCM

An authenticated encryption family used in formats within the ecosystem. Its properties depend on implementation and key handling.

Mnemonic

A sequence of words representing generation and verification material according to a given format.

Seed

Material from which keys are derived. In everyday usage the term may also refer to the words, so the context matters.

Entropy

Unpredictability in the material used for generation. Picking memorable words does not provide it.

Checksum

A value that detects certain errors. It does not authenticate the author.

BIP39

A specification for mnemonics and for deriving a seed with an optional passphrase.

BIP39 passphrase

An additional input to derivation. A different one may produce another valid wallet that appears empty.

BIP32

A specification for hierarchical key derivation.

Derivation path

The sequence of branches used to obtain keys from a root.

Hardened derivation

A derivation step usually marked with an apostrophe or h, with properties different from ordinary public derivation.

xpub

An extended public key with derivation context. It is sensitive from a privacy standpoint.

xprv

An extended private key. Never share it or import it into a course.

Master fingerprint

A short root identifier useful for association. By itself it is insufficient proof of identity.

Descriptor

An expression describing how to construct scripts using keys and derivation paths. It may be public or contain private material.

Watch-only

A wallet for monitoring that lacks sufficient private signing capability to sign on its own.

WOW

The name for watch-only accounts and wallet management in the Cuvex ecosystem.

Hot wallet

A tool that can sign in a connected environment.

Self-custody

A model in which the user retains the technical ability to spend, individually or jointly, under their own policy.

Custodian

An entity that controls spending capability on behalf of a customer and applies its own access conditions.

Cuvex cryptogram

An encrypted object that protects a secret. It does not itself constitute a transaction or a balance.

Desk password

Protects access to local storage. It is distinct from the seed and the cryptogram password.

Chat Key

A secret used to recover a chat identity. Its appearance may suggest that it is public, even though it is private.

Pairing PIN

A temporary code for a connection session, distinct from a custody password.

Air gap

Operational separation of environments. Data transferred between them still needs validation.

NFC

A short-range communication technology used with compatible cards and readers.

USB Mass Storage

The BIT model’s file-based exchange interface, with its own protocol, validation and acknowledgments.

PSBT

A container for information and signatures used to coordinate construction and authorization of transactions.

PSBT v0

The format version defined in BIP174 and used by the reviewed Final multisignature profile.

PSBT v2

The version defined in BIP370. A version 2 transaction does not establish that the PSBT is version 2.

SIGHASH ALL

The signature commitment mode used by the reviewed profile. Checking what it commits to is part of validating the transaction.

P2WPKH

A single-key SegWit spending condition commonly associated with BIP84 accounts.

P2WSH

A SegWit condition committing to a script, used by the reviewed Final multisignature profile.

P2TR

A Taproot output type. Supporting it as a destination does not imply support for signing spends from it.

sortedmulti

A multisignature construction using deterministic key ordering to generate scripts.

M-of-N threshold

The number M of authorizations needed from N participants under a specific policy.

MuSig2

A Schnorr aggregation protocol whose basic scheme is N-of-N, distinct from an arbitrary threshold.

Taproot

A set of Bitcoin spending and commitment mechanisms with key and script paths.

Miniscript

A language for describing and analyzing certain script policies. The reviewed Final profile does not implement it.

Regtest

A local test network controlled by whoever sets up the lab, with no economic value.

Signet

A test network with its own characteristics. It is not interchangeable with regtest by default.

Mainnet

The Bitcoin network used for real economic activity.

Gap limit

The number of consecutive unused addresses a wallet uses as a discovery criterion. Its scope depends on the wallet.

Coin control

Deliberately selecting the UTXOs to spend.

Consolidation

Combining outputs to reduce fragmentation, with implications for cost and privacy.

Pseudonymity

Use of identifiers other than a person’s legal name, without automatic anonymity.

Anonymity

A contextual property of being indistinguishable to specified observers. An app label cannot guarantee it.

Metadata

Information about communications or activity, such as timing, sizes and relationships, distinct from the content.

CoinJoin

A collaborative construction that makes certain inferences harder, without guaranteeing permanent anonymity.

Payjoin

A collaborative payment using inputs from both payer and payee under a compatible protocol.

Tor

A network and tools for protecting connections. Its use must be configured and verified for each application.

VPN

A channel that shifts part of the trust in a connection to the operator. It does not obscure the blockchain.

Lightning

A channel-based payment system with requirements and risks different from those of an on-chain transaction.

Invoice

A structured payment request whose format and payment method must be identified.

RPC

An interface for calling a service such as Bitcoin Core. It requires authentication and protection.

TLS

Transport protection against certain threats. The receiving server can still see the requests.

SRTP

Audio protection on certain VoIP segments. It does not automatically keep the conversation secret from the operator.

Idempotency

A property that prevents an effect from being duplicated when an identified request is repeated.

Webhook

An event sent between servers whose authenticity and possible replay must be checked.

RAG

Retrieval of knowledge excerpts to ground a response in the relevant context and version.

Teach-back

Checking learning by asking a student to explain what they understood in their own words.

Phishing

Deception using impersonation and a convincing context to obtain access or induce someone to act.

Social engineering

Manipulation of human decisions that may use genuine information and a sense of urgency.

Notarization

An Apple distribution control, distinct from a product audit or physical testing of all workflows.

Attestation

Evidence of state under a specific mechanism. Desk’s compatibility catalog is not a remote measurement.

MiCA

A European framework for certain crypto-assets and services. It guarantees neither returns nor full compensation.

Travel Rule

Information requirements for transfers within its scope. Using self-custody does not exempt a transfer from them.

Checkpoint

A place to resume learning, recorded with minimal data and no wallet information.

Check what you have learned

Practice without real funds. The assessment is open to everyone and does not require an account.

Who authorizes spending during normal use of Cuvex?

1. The device, after the user reviews the operation
2. The voice tutor
3. The course server

> **Show answer: The device, after the user reviews the operation**
> Authorization takes place on Cuvex.

How many satoshis are there in 0.001 BTC?

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

> **Show answer: 100,000**
> One BTC equals 100,000,000 sat.

The inputs total 120,000 sat and the outputs total 119,000 sat. What is the fee?

1. 1,000 sat
2. 119,000 sat
3. 1 sat/vB, without needing any more information

> **Show answer: 1,000 sat**
> The difference in value gives the absolute fee.

A signed transaction that has yet to be broadcast is:

1. Confirmed
2. Irreversible because it has been signed
3. Authorized but not necessarily broadcast

> **Show answer: Authorized but not necessarily broadcast**
> Signing and broadcasting are separate steps.

What does 200 vB at 6 sat/vB cost?

1. 206 sat
2. 1,200 sat
3. 6% of the amount sent

> **Show answer: 1,200 sat**
> Multiply virtual size by the fee rate.

Before withdrawing from an exchange, what should you check?

1. Only the lowest fee
2. That the asset, network, address and net amount are compatible
3. The counterparty’s seed

> **Show answer: That the asset, network, address and net amount are compatible**
> Some networks use a BTC symbol without being Bitcoin on-chain.

What does a digital signature do on its own?

1. Hide the entire message
2. Authorize a message that can be verified under its signature scheme
3. Erase published data

> **Show answer: Authorize a message that can be verified under its signature scheme**
> Confidentiality requires a separate mechanism.

Changing a BIP39 passphrase can:

1. Produce a different, valid wallet that appears empty
2. Always be reversed by email
3. Change the public record of past payments

> **Show answer: Produce a different, valid wallet that appears empty**
> The passphrase participates in derivation.

How should you treat an account xpub?

1. As data with no consequences
2. As identical to the private seed
3. As privacy-sensitive information

> **Show answer: As privacy-sensitive information**
> It can allow more of your activity to be observed.

Why might one seed be insufficient for multisignature recovery?

1. The policy and the authorizations needed to meet the threshold are missing
2. Bitcoin does not allow anything to be recovered
3. You need the app’s original color

> **Show answer: The policy and the authorizations needed to meet the threshold are missing**
> Keeping the policy and retaining private signing capability are separate requirements.

If a roll is rejected by the reviewed Final algorithm, what should you do?

1. Flip only the coin until it is accepted
2. Flip the coin and roll all four dice again
3. Pick a familiar word

> **Show answer: Flip the coin and roll all four dice again**
> Repeating only part of the set can bias the mapping.

What do two passwords used to unlock a single-signature seed imply?

1. Two mandatory on-chain keys
2. A Taproot multisignature wallet
3. An access threshold for the secret that is separate from the Bitcoin spending threshold

> **Show answer: An access threshold for the secret that is separate from the Bitcoin spending threshold**
> Encryption does not change the script.

When evaluating a full Desk backup, what should you remember?

1. It necessarily includes the entire chat
2. Its scope has exclusions and you should not assume it includes chat
3. It updates every old backup

> **Show answer: Its scope has exclusions and you should not assume it includes chat**
> Recovering an identity and recovering messages are different tasks.

What does a properly configured personal node do?

1. Eliminate every information leak
2. Reduce reliance on third-party queries and allow independent verification
3. Recover lost keys

> **Show answer: Reduce reliance on third-party queries and allow independent verification**
> It guarantees neither anonymity nor recovery of secrets.

What happens when you freeze a UTXO in Desk?

1. The app applies a local restriction
2. The consensus condition changes
3. Other copies of the seed are revoked

> **Show answer: The app applies a local restriction**
> Freezing it locally does not prevent spending everywhere.

If you lose your connection just as you broadcast a transaction, what should you do?

1. Immediately pay again
2. Delete the wallet
3. First check whether the payment has already been broadcast

> **Show answer: First check whether the payment has already been broadcast**
> A timeout does not prove that nothing happened.

What can reusing addresses or combining UTXOs from different contexts do?

1. Make connections between activities easier to observe
2. Erase the history
3. Guarantee anonymity

> **Show answer: Make connections between activities easier to observe**
> Privacy depends on the context and on subsequent use.

Does opening Tor Browser automatically configure Desk?

1. Yes
2. No
3. Only if dark mode is enabled

> **Show answer: No**
> Each application’s network route must be checked.

What is a Chat Key that looks like an xpub?

1. Something you can publish
2. A receiving address
3. A secret that controls an identity

> **Show answer: A secret that controls an identity**
> Sensitivity depends on the key’s purpose.

What does a chat message marked “paid” tell you?

1. It replaces confirmations
2. The payment still needs to be checked independently on the network
3. It changes the network of the request

> **Show answer: The payment still needs to be checked independently on the network**
> The status of a message is distinct from the status of a payment.

What does the reviewed Final multisignature profile use?

1. MuSig2 and PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Any Bitcoin script

> **Show answer: P2WSH sortedmulti BIP48 PSBT v0**
> A desired feature or a product name does not establish support.

Where can you start a comparison in Mirror 12.12?

1. Only at step 1
2. With any chosen field, including step 15
3. Only at the last step, after completing every other one

> **Show answer: With any chosen field, including step 15**
> You may compare pairs independently in any order.

What does “Match” in Mirror establish?

1. Overall approval
2. The authenticity of the source of both QR codes
3. Literal equality of the two values

> **Show answer: Literal equality of the two values**
> The rest of the review and the response are still pending.

If a seed has been exposed, what does changing the Desk password do?

1. Revoke the attacker’s access
2. Leave the keys derived from that seed valid
3. Erase all copies

> **Show answer: Leave the keys derived from that seed valid**
> A safe transfer of control needs to be assessed.

What must the final practical training record identify?

1. Which work was reading, simulation and physical testing, and what remains outstanding
2. Only the hours sold
3. A promise of invulnerable custody

> **Show answer: Which work was reading, simulation and physical testing, and what remains outstanding**
> Each kind of evidence has a different scope.