Start Here

This is a free sample of the Bitcoin Legacy workbook. It has the Legacy Letter steps for one hardware wallet, and the First 48 Hours and Read This Now pages. Nothing in it was typed into a computer. Tick the boxes, and fill in every line by pen.

How to fill it in

1. Fill in section A of the Legacy Letter for your hardware wallet. If you have two, print that section twice.
2. Fill in the lines on the First 48 Hours and Read This Now pages the same way.
3. Never write recovery words in this workbook, only where they are kept. Keep PINs and any passphrase on a separate sheet, stored apart from the recovery words.
4. Store it with your important papers, never in the same place as your recovery words.
5. Give the Read This Now page to your family today.

What the full kit adds

- Steps for every other common setup: Bitkey, exchange accounts at Coinbase, Kraken, Strike, Cash App, River or Swan, multisig vaults built in Casa, Unchained, Nunchuk or Sparrow, phone wallets including Muun, desktop wallets, Lightning nodes, Liana, and Bitcoin ETFs.
- What to do if the company or exchange is gone, for each one.
- The Security Checklist for PINs and passwords, and a note for your executor or estate attorney.
- A tailored version with only your own steps, checked for gaps before you print.

Instructions checked October 2026. The full kit is at 21vox.com/bitcoin-legacy. This sample is general information, not legal or tax advice.

Legacy Letter

Dear _____,

If you are reading this, I can no longer manage our bitcoin. Everything you need is in this kit. Read the First 48 Hours page before you touch anything. No secrets are written here: where a recovery phrase, PIN or password is needed, this letter says where to find it.

My hardware wallet has its own section below. Go one step at a time.

A. Hardware wallet

Use this section for a hardware wallet: a Trezor, Blockstream Jade, Coldcard, Ledger, BitBox02, Foundation Passport, Keystone or another. If you have two, print this section twice.

Device: ☐ Trezor ☐ Blockstream Jade ☐ Coldcard ☐ Ledger ☐ BitBox02
☐ Passport Core ☐ Passport Prime ☐ Keystone 3 Pro ☐ Other: _____

Uses a passphrase: ☐ Yes ☐ No ☐ Not sure

1. Find the device. Where it is kept: _____.
2. Find the recovery words (a numbered list, usually 12, 20 or 24 words). They are the real key; the device can be replaced. Where they are kept: _____.
3. Never type the recovery words into a website, an email or a phone. Only a hardware wallet should ever see them.
4. With your trusted contact beside you, restore the wallet on this device or on a new one of the same kind, bought directly from the maker, using the maker's official app, downloaded only from the maker's own website.
5. If Yes is ticked for a passphrase, the wallet also uses one, and without it the wallet will look empty. Where to find it: _____. If Not sure is ticked and the restored wallet looks empty, ask your trusted contact before trying anything else.
6. If I wrote this wallet's fingerprint here, the restored wallet should show the same one: _____. Wallet apps may call it the master fingerprint or XFP. If it is different, a word or the passphrase is not right. Stop and check with your trusted contact before sending anything.

The maker's official app

- Trezor: Trezor Suite, downloaded only from trezor.io.
- Blockstream Jade: the Blockstream app, downloaded only from blockstream.com.
- Ledger: Ledger Live, downloaded only from ledger.com.
- Coldcard: follow the instructions on coldcard.com.

The devices below have their own backup and restore steps. Use them instead of steps 2 to 4 above.

If BitBox02 is ticked

Backup: ☐ microSD card ☐ Written words

1. My backup may be a microSD card. The card is kept: _____. It is not locked with any password: anyone who holds it can take the bitcoin, so keep it hidden.
2. Or it may be a list of 12 or 24 words. They are kept: _____.
3. Get a BitBox02 or BitBox02 Nova, bought new from bitbox.swiss. Install the BitBoxApp from bitbox.swiss/download on a computer. The original BitBox02 does not work with an iPhone.
4. Plug in the BitBox and open the app, with your trusted contact beside you. With the card, choose Restore from microSD card, insert it, and pick the backup. With written words, choose Restore from recovery words and type each word on the BitBox itself, never in the app.
5. The BitBox asks you to make a new device password. You do not need my old one. Ten wrong passwords erase a BitBox, so never guess.

If Passport Core is ticked

Backup: ☐ microSD card and 20-digit code ☐ Seed words

If the card is ticked

1. My Passport backup is a microSD card plus a 20-digit Backup Code. You need both. The card is kept: _____. The code is kept: _____.
2. Do not guess the PIN. After 21 wrong tries this Passport stops working for good. If you do not know my PIN, buy a new Passport Core from foundation.xyz.
3. With your trusted contact beside you, turn on the new Passport. At the Create Seed screen choose Restore Backup, insert the card, choose the backup file from the list, and type the 20-digit code.
4. To see and send the bitcoin, install Envoy by Foundation from the App Store or Google Play and connect it to the Passport.
5. The Envoy app on my phone does not hold this bitcoin's key. Do not rely on my phone or my cloud account for it.

If seed words are ticked

1. My 12 or 24 seed words are kept: _____.
2. Do not guess the PIN. After 21 wrong tries this Passport stops working for good. If you do not know my PIN, buy a new Passport Core from foundation.xyz.
3. With your trusted contact beside you, turn on the new Passport. At the Create Seed screen choose Restore Seed, pick 12 or 24 words, and type each word on the Passport.
4. To see and send the bitcoin, install Envoy by Foundation from the App Store or Google Play and connect it to the Passport.

If Passport Prime is ticked

Backup: ☐ Keycards ☐ Seed words

If Keycards are ticked

1. My backup is Keycards: thin cards the Prime reads when you hold them to its back. Any two parts restore it: two Keycards, or one Keycard and the Envoy app on my phone. In the usual setup the third card is a blank spare. The cards are kept: _____.
2. Do not guess the PIN. After 10 wrong tries the Prime erases its key. You can still restore from the backup.
3. With your trusted contact beside you, install Envoy by Foundation on a phone. Turn on a new or erased Prime, follow the screen to connect it to Envoy, and set a new PIN.
4. At the Master Key screen tap Restore, then Restore from Keycards. Hold one card to the back of the Prime until it confirms. Tap the second card when asked.

If seed words are ticked

1. My seed words are kept: _____.
2. Do not guess the PIN. After 10 wrong tries the Prime erases its key. You can still restore from the backup.
3. With your trusted contact beside you, install Envoy by Foundation on a phone. Turn on a new or erased Prime, follow the screen to connect it to Envoy, and set a new PIN.
4. At the Master Key screen tap Restore and choose seed words. Type each word on the Prime.

If Keystone 3 Pro is ticked

Backup: ☐ One list of words ☐ Shamir shares

If one list is ticked

1. My backup is one list of 12 or 24 words. Where it is kept: _____.
2. Never type the recovery words into a website, an email or a phone. Only a hardware wallet should ever see them.
3. This Keystone can hold up to three wallets, each opened by its own passcode. Do not guess: too many wrong tries lock the device, and then it must be wiped.
4. With your trusted contact beside you, use a new or wiped Keystone 3 Pro from keyst.one. Choose Import Wallet, then Single Secret Phrase, and type the words on the Keystone screen only. Set a new passcode when asked.
5. To see the balance and send, connect the Keystone by QR code to Sparrow, BlueWallet or Nunchuk, or to Keystone's own Keystone Nexus app.

If Shamir shares are ticked

1. My backup is several lists of 20 or 33 words, called shares. Lists that belong together start with the same two words. You need _____ of the _____ lists.
2. Share 1 is kept: _____.
3. Share 2 is kept: _____.
4. Share 3 is kept: _____.
5. Any other shares are kept: _____.
6. Shares are pieces of one key. They are not a multisig vault, so skip any multisig steps. Never type them into a website, an email or a phone.
7. This Keystone can hold up to three wallets, each opened by its own passcode. Do not guess: too many wrong tries lock the device, and then it must be wiped.
8. With your trusted contact beside you, use a new or wiped Keystone 3 Pro from keyst.one. Choose Import Wallet, then Shamir Backup and the number of words on each list. Type the lists one at a time on the Keystone screen until the wallet opens. Set a new passcode when asked.
9. To see the balance and send, connect the Keystone by QR code to Sparrow, BlueWallet or Nunchuk, or to Keystone's own Keystone Nexus app.

If my Trezor backup is several lists (shares)

1. My backup is several lists of 20 or 33 words, called shares. Lists that belong together start with the same two words. You need _____ of the _____ lists.
2. Share 1 is kept: _____.
3. Share 2 is kept: _____.
4. Share 3 is kept: _____.
5. Any other shares are kept: _____.
6. Shares are pieces of one key. They are not a multisig vault, so skip any multisig steps. Never type them into a website, an email or a phone.
7. With your trusted contact beside you, use a Trezor Safe 3, Safe 5 or Safe 7, bought new from trezor.io. A Trezor Model One cannot read these lists. Install Trezor Suite from trezor.io on a computer.

8. In Trezor Suite choose Recover wallet. On the Trezor, pick the number of words and type one list on the Trezor itself. It tells you how many more lists it needs. Any order works, and you can unplug it between lists and finish later. Set a new PIN at the end.

Using a passphrase on each device

- Trezor: Turn it on in Trezor Suite under Settings, Device, Passphrase, then type it on the Trezor.
- BitBox02: Turn it on in the BitBoxApp under Settings, Manage device, Expert settings, Passphrase. Unplug the BitBox, plug it back in, and type the passphrase on the BitBox.
- Passport Core: Go to the More menu, choose Enter Passphrase, and type it. Turning the Passport off forgets it.
- Passport Prime: Open the Bitcoin Wallet app and choose Apply Passphrase.
- Keystone 3 Pro: Go to the "..." menu, then Device Settings, Wallet Settings, Passphrase, and type it. The Keystone forgets it when it restarts.

Before you move any bitcoin

1. Use a hardware wallet you trust. If you need a new one, buy it new, directly from the maker's own website. Never use a second-hand device, one from a marketplace or reseller, or one someone sends you.
2. Send a small test amount first. Wait until it arrives before you send the rest.
3. Check the whole receiving address, every character, before you confirm. On a hardware wallet, check it on the device's own screen. Do not check only the first and last few characters: malware can swap a copied address for a lookalike that matches at both ends.
4. Never move bitcoin because someone is rushing you. There is no deadline.

What I would like

- ☐ I would like the bitcoin kept, not sold in a hurry.
- ☐ I would like the bitcoin sold slowly over time, not all at once.
- ☐ What to do with the bitcoin is your decision.

Who gets what _____

_____

A note to you _____

_____

With love,

_____

First 48 Hours

Bitcoin does not disappear if it sits untouched. There is no deadline in the first days. The real danger is acting fast, or trusting a stranger.

STOP. Never do these:

× Do not contact anyone offering "bitcoin recovery" help. They are almost always scammers.

× Do not share the recovery words with anyone, including people who say they work for an exchange or wallet company.

× Do not send bitcoin anywhere to "verify" or "unlock" access. No legitimate service asks for that.

× Do not type recovery words into a website, an email, a chat or a photo.

× Do not reply to messages that arrive after a death announcement asking about crypto.

× Do not trust anyone who contacts you about this kit or my bitcoin. No company, and not 21VOX (the site this kit was made on), will ever reach out to you or ask for these words.

People to call

Trusted contact who understands bitcoin _____

Phone or email _____

Backup contact _____

Phone or email _____

Estate attorney or executor _____

Do this first

1. Put this kit, every hardware wallet and every recovery backup somewhere locked. Do not move bitcoin yet.
2. Call your trusted contact, written under People to call. If you cannot reach them, call the backup contact.
3. Talk to an estate attorney before selling or transferring anything.
4. Work through the Legacy Letter one holding at a time, with your trusted contact.

Taxes

In the US, inherited bitcoin generally takes a new cost basis equal to its value on the date of death. Confirm this with a tax professional before you sell.

This kit is general information, not legal or tax advice.

Read This Now

Dear _____,

This page is for you to read now, while I can still answer your questions. It holds no secrets. The full kit, with step-by-step instructions, is kept separately.

Where the full kit is kept _____

Your trusted contact _____

What I have

Tick each one I have.

☐ A hardware wallet: a small device that keeps the keys offline.

☐ Other places I hold bitcoin: _____

What will happen

- There is no rush. Bitcoin does not disappear if it sits untouched for months.
- You will not do this alone. The trusted contact written above understands bitcoin and can help you.
- Talk to an estate attorney before anything is sold or moved.

Words you will meet

- Recovery words: a numbered list of words, usually 12, 20 or 24, that can rebuild a wallet on a new device. Whoever has them controls the bitcoin. Never type them into a website, a phone, an email or a chat.
- Passphrase: an extra word or phrase added to the recovery words. A different passphrase opens a different wallet, so a wrong one shows an empty wallet, not an error.
- Hardware wallet: a small device that keeps the keys offline and asks you to confirm every payment on its own screen.
- Wallet fingerprint: an 8-character code that names one wallet. It is not a secret. It lets you check you restored the right wallet.

Scams to expect

- People who offer to "recover" bitcoin for a fee.
- Messages that claim to be from an exchange, a wallet company or 21VOX and ask for recovery words or a payment.
- Anyone who rushes you. Real processes are slow.

Practice now, if you like

Ask your trusted contact to help you set up a small wallet of your own, then restore it from its recovery words. It is the same skill you will need later, and nothing of mine is involved.

Keep this page. When I update the kit, I will give you a new one.

With love,

_____