“Pleb” is an everyday Bitcoiner. “Dominium” is Latin for absolute ownership. This guide is for the Bitcoiner who wants to build a secure, self-custody Bitcoin wallet from the ground up, bypassing the need for a company, an app, or a custodian to manage or store access to the funds.

What this guide instructs

This guide instructs users how to generate entropy with dice, import it into verified software, and create a 2-of-3 multisig wallet stamped into titanium. Hardware wallets and signers are completely optional.

The process leaves no trace. It utilizes Tails OS, an operating system run entirely from a USB drive that is designed to forget all activity upon shutdown.

Plebum Dominium is a goal, not a product. This is an educational tool designed to guide more people toward true, homemade self-custody.

This guide walks a Bitcoiner through the work in order. A company, an app, and a custodian are not part of that order. Verification comes before the computer is taken offline.

1 **Why**

2 **Offline**

3 **Verify**

4 **Dice**

5 **Spend**

6 **Metal**

The order

Why comes first. One seed, one app, one house, one company, or one photo is enough to lose the coins. The long-term fund needs any two of three keys.

Offline comes next. Each key is made on a computer that is not on the internet. Tails is installed on one USB drive, and networking is set to Disabled before the desktop appears.

Verify is the stop. Tails, Sparrow 2.5.5, Electrum, the Ian Coleman page, and the dice converter are downloaded from their own sources and checked before anything is copied onto a drive. A failed check means the file is deleted.

Dice is how the keys are made. Faces 1 through 4 are kept. Faces 5 and 6 are rolled again. The work is done three times, with a full shutdown between keys. Two offline programs have to print the same 24 words.

Spend is a small amount, both ways, before any savings move. The payment file walks between the computers. The seed stays on the offline computer.

Metal is last. Once all three keys can be reproduced offline, they are stamped into titanium and kept in three places. If two keys share a house, the setup has a single point of failure again.

One vendor, one phone, one tool, one house, or one seed. Lose that one thing and the coins are gone. A hardware wallet does not remove that threat, because a device does not create the key.

What this guide is built to remove

One seed that can spend by itself is a leak, a fire, or one demand away from an empty wallet.

An app or an exchange holding the keys is not custody. A login is not a key. The company can freeze it, lose it, or be ordered to hand it over.

One place holding every copy means a fire, a flood, or a theft at that address takes all of them.

One device from one company means a failed maker is the whole fund. Firmware, a factory, or a shop can fail, and the coins fail with it.

A photo, a note, a password manager, or an email is one hacked account away from the seed. The words go on metal. They do not go on a screen that can be copied.

The same computer is used twice. The first boot stays on the network. It watches the wallet. It never holds a seed.

BOOT 1

Network on

BOOT 2

Networking off

What this boot is allowed to do

The everyday boot holds the wallet map, and only the map. It can see the balance. It cannot spend.

It builds the payment, sets the fee, and reads the address against a note that was written down before the file is exported. An unsigned payment file is copied to the data USB.

It broadcasts the payment only after both signatures have been added on the offline computer.

A seed is never typed, pasted, or photographed on this boot. A networked machine with a seed loaded is treated as burned.

The process leaves no trace. Tails OS is an operating system run entirely from a USB drive, and it is designed to forget all activity upon shutdown. That boot is the offline computer. It borrows the hardware and leaves the hard disk alone.

BOOT 1

Network on

BOOT 2

Networking off

How the boot is made

The computer is shut down fully before Tails is booted. Networking is set to Disabled on the welcome screen, before the desktop appears. Turning the network off after a program has already opened does not count.

Persistent Storage is not created, and it is not unlocked. Ethernet is never plugged. The Tails file comes from tails.net only, and the signature is checked before the drive is written.

Exactly one seed is loaded. The session converts the dice, restores one seed, signs one payment, or exports the map. The result is copied back to the data USB. The screen goes dark before the drive is unplugged.

The second seed is a new boot, after another full shutdown. Two seeds are never loaded in one session. The only secret that crosses the USB is a signature file, not a seed.

These files must be downloaded from their original sources. A compromised file compromises the funds. If the fingerprint or the signature fails, the file is deleted and the work does not continue with it.

The files

- Tails, from tails.net.
- Sparrow 2.5.5, the required version. The Tails file is sparrowwallet-2.5.5-x86_64.tar.gz.
- Electrum, from electrum.org.
- The Ian Coleman page, saved and opened only while offline.
- The dice converter. It is the one file this site provides.

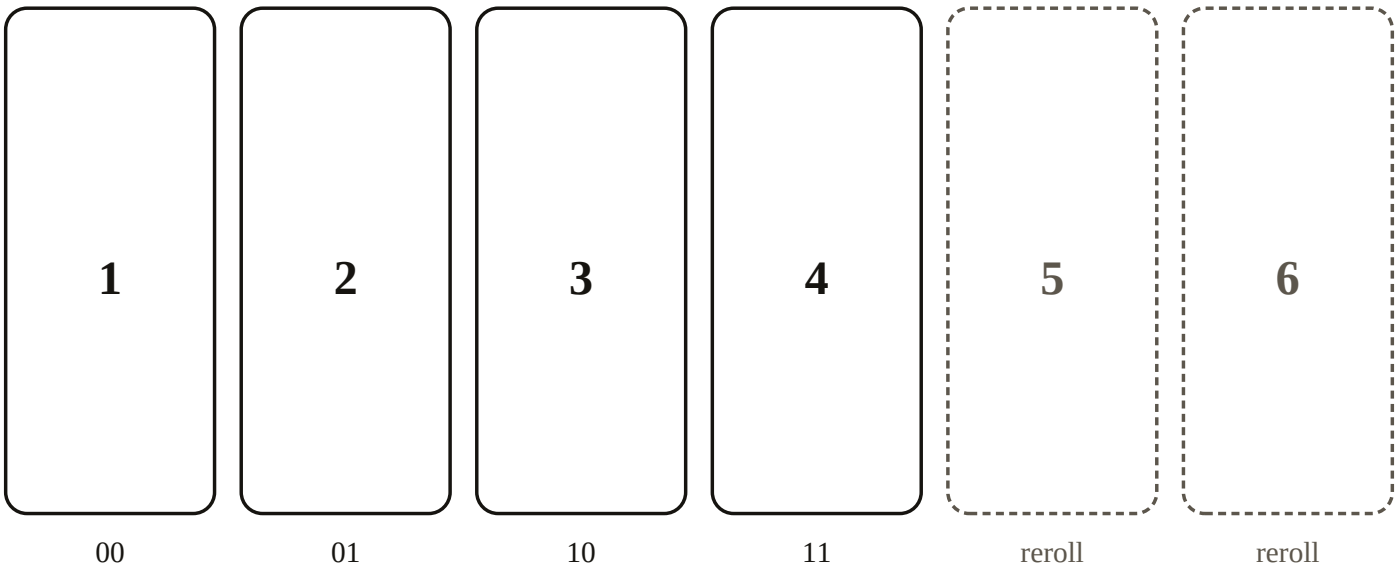
What a check is

The Windows installer and the Mac installer do not go on the Tails drive. Sparrow is not downloaded from inside Tails.

A newer download that does not match the pinned version is a stop, not an upgrade. The kit checks Tails 7.13, Sparrow 2.5.5, and Electrum 4.8.2.

The dice converter is checked against the fingerprint printed on this site, under Verify the dice converter. The same fingerprint is written in VERIFY.md. If the lines do not match in every character, the file is deleted.

This starts after Tails has booted with networking set to Disabled, and before any plate is stamped. Five casino dice are required, and every face has to be readable.



The faces that are kept

A six-sided die is not used as a raw bit. Faces 1 through 4 are two fair bits each. 1 is 00. 2 is 01. 3 is 10. 4 is 11.

The dice are read left to right, the same way every shake. Only 0 and 1 are written down. At least 256 bits are required. More is fine.

Example: 4, 6, 1, 3, 2 becomes 11, the 6 is skipped, then 00, 10, 01.

There cannot be a camera in the room. The work is done in an established private setting.

Faces 5 and 6 are not written down. Those dice are rolled again. Using all six faces as bits would bias the result.

Three keys, not one sitting

The work is done three times. Each key is a new set of rolls. A list is never continued from the previous boot.

Between keys, Tails is shut down. The screen goes dark. The next key is a new boot, with networking set to Disabled again.

Three lists of 24 words are the result. They are not three copies of one list.

One program can be wrong. Two programs printing the same words from the same bits is the check. If the results differ, the work stops. The prettier list is not chosen.

Still offline

The checked converter and the Ian Coleman page are copied from the data USB to the Desktop. Nothing is downloaded from inside Tails.

The bits are pasted into the converter. It prints 24 words. The Ian Coleman page is opened offline, with entropy type set to Binary and the word count set to 24. The same bits are used.

The two lists have to match in every word. Word 24 is not changed to force a match.

Sparrow and Electrum are later given the same seed, still offline. The first addresses have to match. The wallet map, imported with no seed, has to show those same addresses. The map can watch. It cannot spend.

The 24 words are not 24 free choices. The last word carries a short check so a copying mistake is caught before metal is stamped.

What that means

Word 24 is produced by the program. It is not invented, and it is not picked from the list because it looks familiar.

Changing word 24 to force a wallet to open destroys the key. The plate would then hold words that do not open the fund.

If the two programs disagree on word 24, the bits are checked for a copying mistake. If the bits are right and the words still differ, the work stops and the rolls are done again.

The long-term fund needs any two of three keys. One key by itself cannot move it. That is the whole point of the lock.

KEY A

Home

THE FUND

Any two

KEY B

Off-site

Where the keys sit

Key A is seed 1, on the plate at home. Seed 2 and seed 3 are not kept there.

Key B is seed 2, off-site, in a different building.

Key C is seed 3, in another town or with a trusted party.

Any pair can spend. A stolen plate, or a lost plate, is one key. The fund still needs a second plate from a second place.

The wallet is native SegWit, 2 of 3, on the path m/48'/0'/0'/2'. Sparrow 2.5.5 is the required version. Signing happens on offline Tails. The output descriptor is the map.

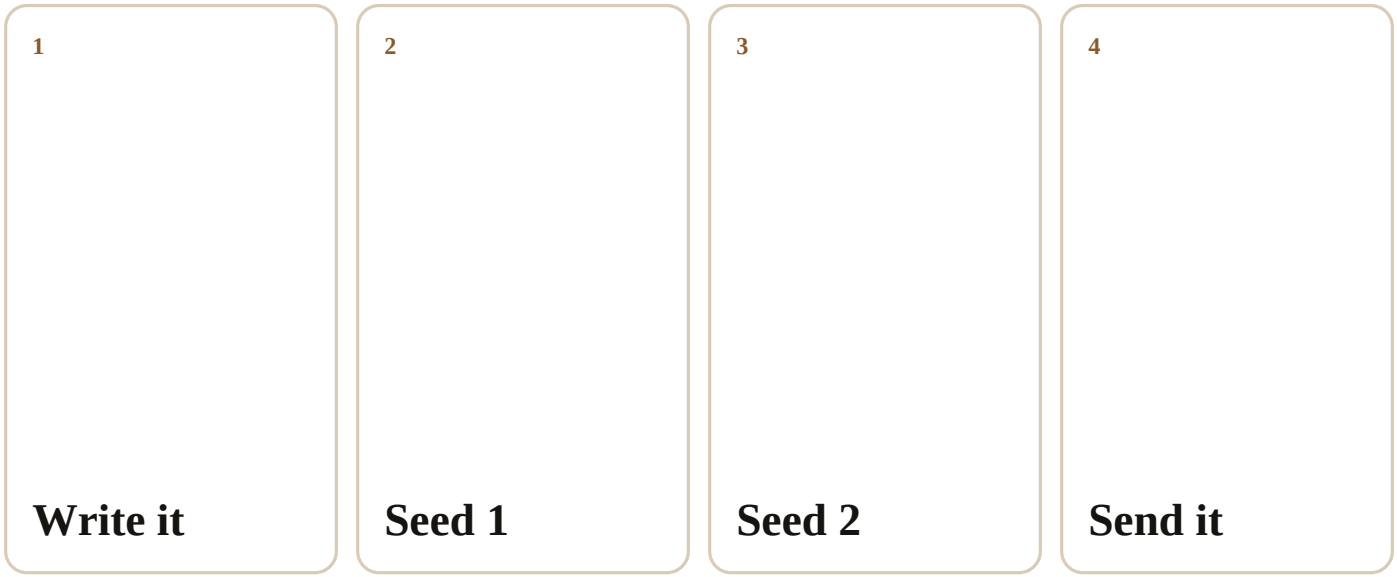
Why not the other setups

One key is the classic single point of failure. One leak, one fire, or one seed empties the wallet. That is the setup this guide is built to avoid.

Three of three means one lost plate locks the coins forever. That setup is too brittle for real life, and it is too brittle for an heir.

Two of three survives one loss and one compromise. The fund still moves with the other two plates. Heirs can be told a clear story: find two plates, in two places, and the map.

A small amount moves before any savings. The payment file walks. The seed stays seated. Savings stay where they are until a small amount has gone out and come back.



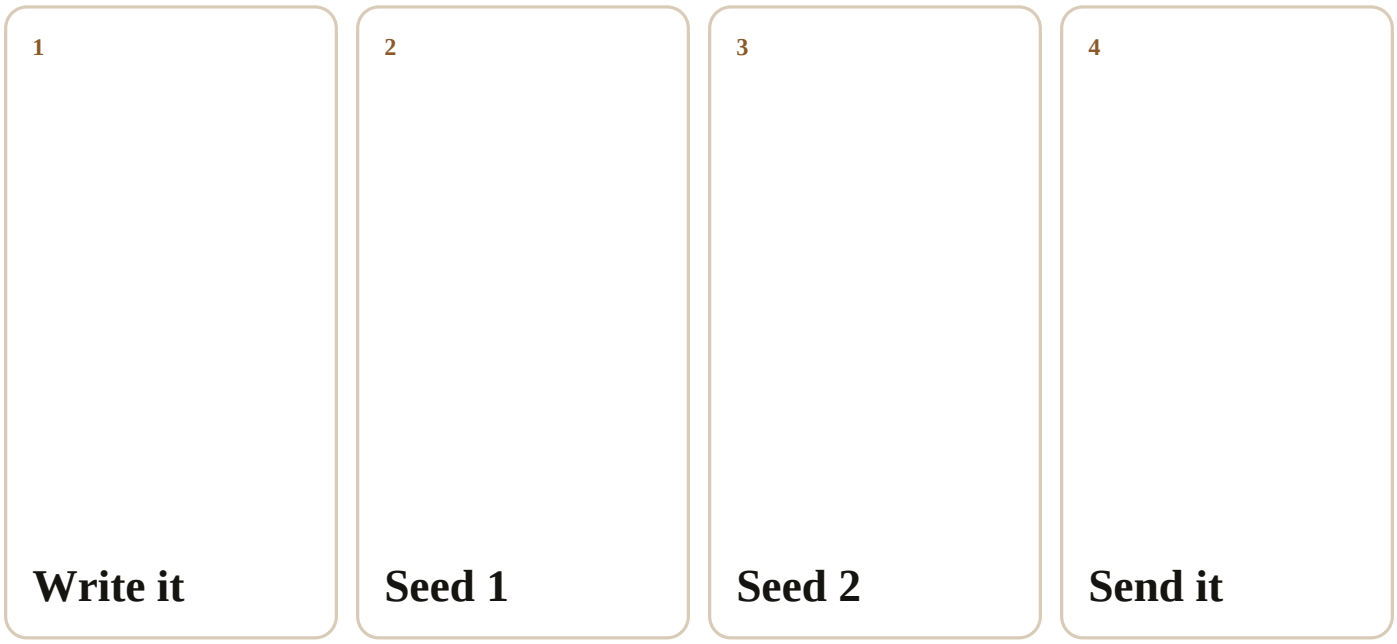
Build, then sign once

The wallet is built only after no seed is loaded. One public key is copied per boot. A public key is not the 24 words. The path has to read m/48'/0'/0'/2'. If it shows anything else, the work stops.

The map is exported. It watches. It cannot spend. The everyday computer imports that map as watch-only.

The destination, the amount, and the fee are written on paper before the unsigned file is exported. The first seed signs that file on Tails, with networking off. Then the computer is shut down fully. The screen goes dark before the drive is unplugged.

The second signature is a new boot. Seed 1 is not still in memory. Seed 3 is not loaded unless one of the other keys is gone.



Then the payment can move

Tails is booted again, with networking set to Disabled. Seed 2 is the only seed loaded. The partially signed file is opened, the second signature is added, and the finished file is copied out.

The everyday computer opens that file and broadcasts it only after both signatures are present. The destination and the amount are checked against the note that was written down before the first signature.

Seed 3 stays boxed. It is used only if seed 1 or seed 2 is gone. Two seeds are never loaded in one session.

A plate is not stamped until a small payment has gone out and come back, and until all three keys can be reproduced in an offline, air-gapped environment.

PLACE 1	PLACE 2	PLACE 3
Plate A	**Plate B**	**Plate C**

One seed on each plate

Three titanium plates are required. StampSeed is the recommended kit. Only one plate is included in the kit. Two more plates will have to be purchased additionally.

Cryptotag is the other option. It punches the word numbers, and the kit includes two plates, so one more plate has to be purchased. One method is used on a plate, and the two methods are not mixed.

Plate A is seed 1 only, in the home safe or fire box. Plate B is seed 2 only, in a second place. Plate C is seed 3 only, in a third place. If two keys are stored in the same house, the separation is gone.

The plate is read back against the paper, then restored on offline Tails. The paper is destroyed only after that restore has passed.

The words on the home plate, alone, open a small wallet. That balance is not the long-term fund. The long-term fund still needs a second plate.

PLATE ALONE

A small balance

PLATE + PASSPHRASE

Spending

TWO PLATES

The long-term fund

Three ways the home plate is used

The plate alone is what a thief sees. A little bitcoin. That is the decoy. It is not the savings.

The same words, plus a passphrase, open a modest spending wallet. The passphrase is not stamped on the plate, and it is not kept in the same drawer. A passphrase is not a plate, and it cannot replace the second key.

The home plate plus one plate from another place opens the long-term fund. That is savings and inheritance. Any two of the three plates can do it. The third plate stays somewhere else.

These are the limits of the method. A convenience is not allowed to break one of them.

RULE

No photos

RULE

Network off

RULE

One seed

RULE

Stop

RULE

Later

The limits

No photos are taken of seeds, plates, or screens that show the words. A camera in the room means the sitting is over.

A seed is never loaded on a computer that had the network up in that session. Networking is set to Disabled before the desktop appears.

Only one seed is loaded in a Tails boot. The computer is shut down fully before the next seed. Persistent Storage is not created on the Tails USB, and it is not unlocked.

If a fingerprint or a signature fails, the file is deleted. The work does not continue with that file, and a newer unmatched download is not treated as an upgrade.

A hardware signer is not required to begin. If more than one key is later loaded onto a device, the devices come from more than one maker. All three keys are not put on hardware. The plates are the backup.

These have to be in the room before the first die is rolled. A hardware signer is not required to begin.

On the table

Five casino dice are required, and every face has to be readable. A pencil is required, along with extra copies of the recording grid. An established private setting is required, and there cannot be a camera in the room.

The computer and the drives

One computer is used twice. The first boot stays on the network and only watches. The second boot is a Tails USB on that same computer, with networking turned off. A second USB drive carries only files that have already been checked, and later the payment files.

Three titanium plates are required, with one seed stamped on each plate. StampSeed is the recommended kit. Only one plate is included. Two more plates are purchased. Three places are required, far enough apart that losing one place does not lose all three keys.

Hardware wallets and signers are completely optional. The keys are generated with dice, on a computer that is not on the internet. The device stays in the drawer until the plates exist and a small payment has moved.

Signing only

A finished seed can later be loaded onto a signer, for signing only. The words still live on titanium. The device is a tool, not the backup.

If more than one key goes onto hardware, the devices come from different makers. All three keys are not put on hardware. One failed maker is one lost key. The plates and the three places still hold the wallet.

The inheritance letter is not a hardware-wallet guide. Heirs are told to put one plate in one device and the other plate in a device from a different maker, bought from the official shops.

These are the places the work usually stops. The answer is to stop, not to improvise.

The download is newer than the version on the sheet

Stop. This kit checks Tails 7.13, Sparrow 2.5.5, and Electrum 4.8.2. The Sparrow file for Tails has to be named sparrowwallet-2.5.5-x86_64.tar.gz. A newer file will not match. That is a stop, not an upgrade. The file is deleted.

The two word lists do not match

Stop. The list that looks nicer is not chosen. Word 24 is not changed to force a wallet to open. The bits are checked for a copying mistake. If they are right and the words still differ, the rolls are done again. A fixed word is a destroyed key.

A password manager, a note, or a photo

No. A photo, a note, a password manager, or an email is one hacked account away from the whole seed. The words go on metal. The map is encrypted. The passphrase for the map is on paper, away from the plates.

The map is lost, or its passphrase is lost

The coins are not gone. That passphrase hides the map. It does not spend. Two plates can rebuild the map. The path is 2-of-3, native SegWit, m/48'/0'/0'/2'. That path is written on the inheritance sheet. It is not a secret.

A hardware wallet is already in the house

The device stays in the drawer until the plates exist and a small payment has moved. A signer does not create the key. If a key is later loaded onto a device, a second key goes onto a device from a different maker. All three keys are not put on hardware. The plates are the backup.

This is for a spouse who has never used Bitcoin. It is read before a plate is touched. One plate cannot spend the long-term fund. The fund needs any two plates and the wallet map. The words are never typed into a phone.

Do not

The words are not typed into a phone, and they are not typed into a website. The plates are not photographed. Both plates are not put into one device. Devices are not bought from a marketplace listing or from a link in a message.

Do this

Two plates are found in two places. The third is left where it is. The map is found. If it asks for a passphrase, that paper is stored away from the plates. The map is not the words.

A Jade is bought from Blockstream’s own shop. A BitBox is bought from BitBox’s own shop. Two makers. Not two of the same box. Plate A goes into one device. Plate B goes into the other. Never both plates in one device.

The map is loaded so the devices are looking at the same fund. The path is m/48'/0'/0'/2'. That line is not a secret. A small test is sent first. If the test arrives, the fund can move. If the devices disagree, the work stops and it is not forced.

The words on the home plate, alone, open a small wallet. That is not the long-term fund. The long-term fund still needs a second plate. The home balance is not treated as the whole savings.

Three keys, made at home. Any two can spend. No company has to agree. Plebum Dominium is a goal, not a product. The plates do not share a house.

What is left

The computer that watched the wallet never held a seed. The computer that signed forgot the session. The paper is gone after the plates have been read back and restored.

Hardware wallets remain optional. The backup is titanium, in three places. Plebum Dominium is a goal, not a product.