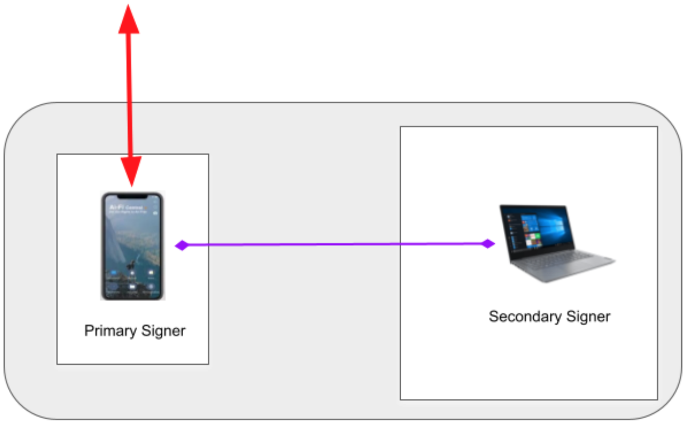
# Ai-Fi Counterseal Wallet

## Background

Ai-Fi Counterseal Wallet is different from all traditional crypto wallets in many important ways. It commits to a highly unconventional approach out of necessity. It requires two independent components to work, each of which is made state-less so that they are invulnerable to any loss events. A separate document offers more historical background and gory details that are required reading if you are risking a large sum of money in the crypto market.

Functionally, the class of hardware wallets exemplified above is what the Counterseal emulates. The difference is that it may utilize only generic devices and accomplish substantially stronger security by applying the Threshold Signature technology. Counterseal splits the hardware wallet, or any wallet, into two interlocking components for the express purpose of eliminating Single Points of Failure. It achieves its security strength through redundancy, the textbook example in reliability enhancing engineering. Through the Counterseal scheme the dedicated hardware is no longer a necessity and many different configurations may be offered. One popular configuration is depicted below:



The red interface path replaces the USB wire in the earlier picture and the signing of crypto transactions now requires the agreement by both the **Primary and Secondary Signers**. All the UI are conducted through the smartphone, which affords us much richer interfaces than the generic hardware wallets, specifically when air-gapped operations are involved between the counterseal wallet (key vault) and the **front-end wallet** (e.g. Electrum or BlueWallet) and further insulates the back-end key vault from any network interference if so configured.

As described, the only difference between the Counterseal wallet and other hardware wallets is the introduction of the Threshold Signature technology to support the key vault through redundant components *and* a highly powerful secret preserving construct of **Crypton** that makes both Primary and Secondary Signers "state-less" such that there is no private keys or recovery seeds maintained within the signers when they are not in session. Each signer is initialized at the start of the transaction signing **session** by retrieving their respective secret preserving Crypton. After the transaction signing session or idle timeout those Cryptons along with all key materials are deleted from memory. Note that the Crypton secret preserving scheme can be made even stronger than your valuable Bitcoin accounts, the public key of which is fully exposed on the blockchain. Your Cryptons may be stored in the Ai-Fi Incognito Cloud pseudonymously, or even in the public IPFS cloud. Unlike traditional service providers or custodian services, you need no Ai-Fi account or surrender your PII (Personally Identifiable Information) in order to work with the Ai-Fi Incognito Cloud.

The Primary Signer is supported on both the iPhone and Android for their obvious superiority in heightened security and portability.

The Secondary Signer is offered as follows:

1. Microsoft Windows 10
2. Apple iPad versions 12 and later releases
3. Live USB stick: This is a dedicated Live Linux, stateless, supporting the Secondary Signer on a USB stick, the code on which is constant with a verifiable code checksum.

> This is the ultimate Secondary Signer which boots from a USB stick on any Wintel PC. It is immune to any viruses, worms and any other hacking attacks. Losing your USB stick is absolutely of no consequence. More on this topic later.

The combination of the Primary Signer and the Secondary Signer installed in various combination of platforms affords us a considerably more secure framework for wallets. Embodying the Secondary in a Live USB stick would make the threshold signature pair practically indestructible. (It does require a dedicated Wintel platform to boot the Live USB from during its operation. Supports for other dedicated or custom hardware are in the works. including installing the Secondary on dedicated hardware.)

Go to the Counterseal website for downloads and installation instructions.

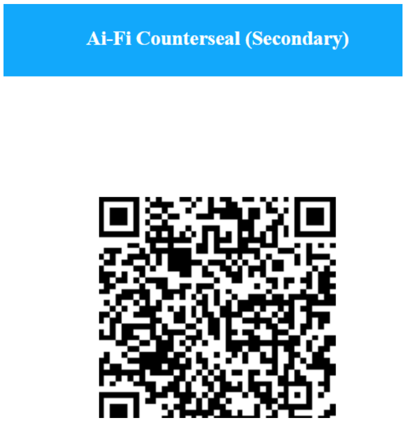
## Pairing of 2 Counterseal Signers/Seals

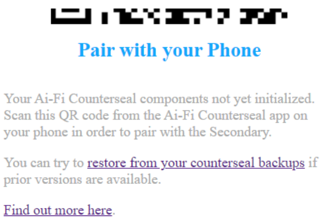
The pairing process described below is specific to the Counterseal framework. Once paired, the signer pairs work with the front-end wallet, e.g. Electrum, in its "watch only" mode with all transactions passed around in an air-gapped interface, which utilizes the cameras on both the Primary Signer and the platform where the Electrum runs on.

The Primary and Secondary Seals work together to support the full Counterseal function set.

Since the Secondary Seal must be securely bound to the Primary, there is a Pairing process at the outset, during which time the Secondary Seal displays a QR code for the Primary to scan, if it is not yet bound to it, to establish the trust relationship based on the principle of TOFU (Trust On First Use) authentication. Once paired, the Primary and the Secondary will be bound to each other internally through two ID key pairs, which are used later for establishing a TLS-strength secure connectivity needed for Threshold Signing. In the case of connectivity loss, the Primary is required to re-connect and re-authenticate itself by repeating the process of the Primary scanning the QR code displayed on the Secondary.

If the Secondary Seal is installed on a Windows 10 platform, its management panel may be found in the Windows system tray. Uninitialized Secondary Seal will display the following pairing QR code to kick off the initialization:





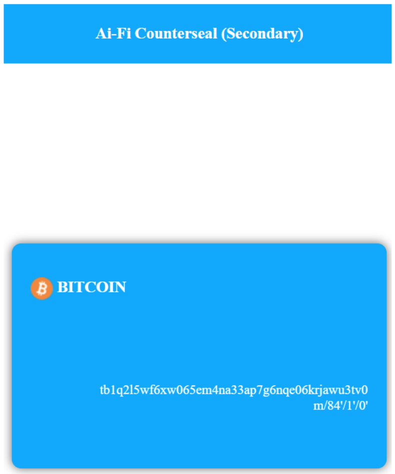
Pair with your Phone

Your Ai-Fi Counterseal components not yet initialized. Scan this QR code from the Ai-Fi Counterseal app on your phone in order to pair with the Secondary.

You can try to restore from your counterseal backups if prior versions are available.

Find out more here.

Once the pairing process completes, the "vault" of the supported crypto coins is represented on both parties as below in the format similar to credit cards:



Ai-Fi Counterseal (Secondary)

BITCOIN

tb1q2l5wf6xw065em4na33ap7g6nqe06krjawu3tv0
m/84'/1'/0'

The "Master Public Key" is displayed on the face of the "wallet card". Before the transaction signature can be carried out, the primary and secondary must be "in sync" in order to operate, under which condition the master public keys displayed on both signers are identical. The upper right icon is for working with the front-end wallet (e.g. Electrum), displaying in QR code the public seed address for the key store of the supported coin type. The "QR scan" icon on the lower left is for scanning the unsigned transactions from a supported front-end wallet in a air-gapped fashion.

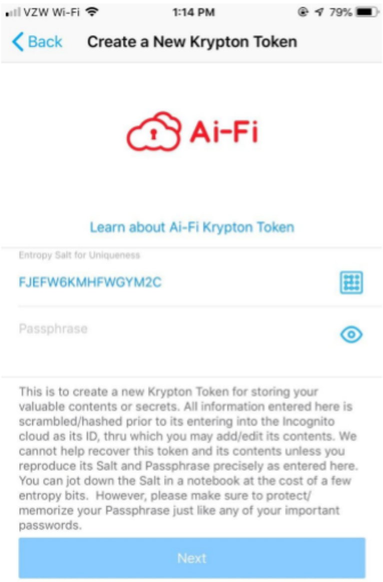
More details on the actual internal steps or the Key Generation of the Threshold Signature Technology conducted during pairing is provided here.

## BIP32 Compatibility and Backup of Seeds

Ai-Fi Counterseal Wallet is BIP32 conformant and follows the BIP32 convention on the account level and supports multiple "accounts" through Extended Key, each of which is composed of a single external keypair chains. The top 4 levels supported are m/84'/0/0.

Internally the Ai-Fi Counterseal Wallet/Vault does not store any private keys and therefore provides no counterpart of standard BIP 32 Master Seed and Master Node in the counterseal scheme. As a consequence, an Ai-Fi Counterseal Wallet may not be exported to traditional wallets and vise versa.

Although not a standard deterministic wallets, Ai-Fi has a customized backup procedure for storing the counterseal "seeds", based on which the Counterseal Vault may be fully recovered. Both the Primary Seal and the Secondary Seal have their own seed for recovery purposes. Due to the complexity of the Threshold Signature scheme that dictates many rounds of cryptographic steps to guarantee its security, the backup data is much more involved and difficult to be condensed into straightforward mnemonic passphrase. For their safekeeping, it is recommended to store them (or one of them) as Cryptons in the Ai-Fi Incognito Cloud, which are based on the Ai-Fi pseudonymous cloud storage design, wherein your files are protected by a cryptographic key pair of similar or stronger strength than that of your Bitcoin accounts recorded in the Bitcoin blockchain. Since your dealings with Ai-Fi.net is account-less and keyless, the Ai-Fi Incognito Cloud is completely pseudonymous like your Bitcoin coins. Please refer to its documentation for more in-depth discussion of this scheme.

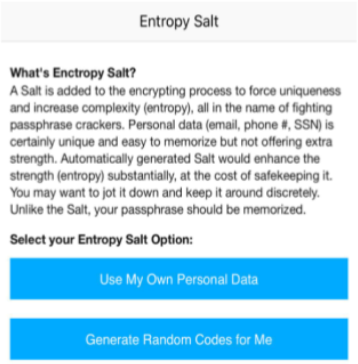


Entropy Salt for Uniqueness

FJEFW6KMHFWGYM2C

Passphrase

This is to create a new Krypton Token for storing your valuable contents or secrets. All information entered here is scrambled/hashed prior to its entering into the Incognito cloud as its ID, thru which you may add/edit its contents. We cannot help recover this token and its contents unless you reproduce its Salt and Passphrase precisely as entered here. You can jot down the Salt in a notebook at the cost of a few entropy bits. However, please make sure to protect/ memorize your Passphrase just like any of your important passwords.



**What's Enctropy Salt?**
A Salt is added to the encrypting process to force uniqueness and increase complexity (entropy), all in the name of fighting passphrase crackers. Personal data (email, phone #, SSN) is certainly unique and easy to memorize but not offering extra strength. Automatically generated Salt would enhance the strength (entropy) substantially, at the cost of safekeeping it. You may want to jot it down and keep it around discretely. Unlike the Salt, your passphrase should be memorized.

**Select your Entropy Salt Option:**

The backup scheme takes advantage of the inbuilt counterseal redundancy and generates two separate backup Cryptons, one of which may be written down on paper (the "paper vault"), which you may rely on the safety of your home or a bank safe deposit box for its protection if so chosen. The other backup seed recovery file may be either maintained privately (in your local storages) or sent to the Ai-Fi Incognito Cloud as a Crypton protected by a strong passphrase. Under this backup arrangement, there is no single points of failure and is completely trustless, eliminating even the possible concern about the involvement of Ai-Fi as a service provider in its management of the Ai-Fi Incognito Cloud.

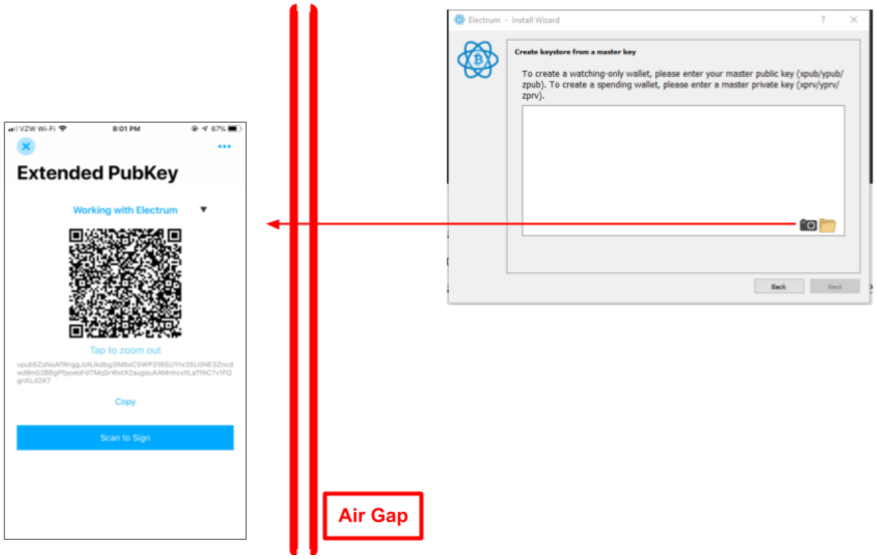
## Air-Gapped Watch-Only Electrum

This section documents the interface to Electrum in its "watch only" mode working with a cold key vault on the backend (Counterseal wallet) in the air-gapped setup. This is a standard interface offered by Electrum, which is summarized here for your quick reference. You may find other similar documents explaining similar steps such as this. We'd strongly suggest a thorough read through this what not to do document.

In the Electrum application, when first creating a wallet:

1. Select "**Standard wallet**" and then,
2. "**Use a master key**" in the Keystore selection screen to indicate that the keys are from an external key vault.

On the next "**Create keystore from a master key**" screen, scan the QR code displayed on the Counterseal Primary Signer (by tapping the "wallet card" on the counterseal app on your mobile phone) in order to initialize the Electrum key store from the air-gapped Counterseal vault, as illustrated below:



vpub5ZsNoAfWrggJsNJkdbg3iMbxC5WP316SUYhr2SLONE3Zncdwd9nG2BBgPfpoeoFdTMqSrWxtX2augsuAAMnhcxtiLaT1AC7v1FQgnXLd2X7

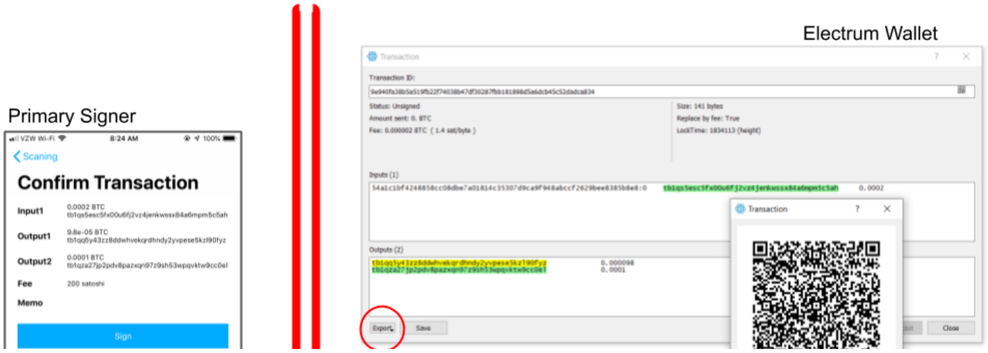
Create keystore from a master key

To create a watching-only wallet, please enter your master public key (xpub/ypub/zpub). To create a spending wallet, please enter a master private key (xprv/yprv/zprv).

Make sure you use the appropriate version of Electrum (Electrum or Electrum Testnet).

## Electrum/Counterseal Transaction Validation

After the keystore is initialized, the normal flow of Bitcoin transactions may commence. For instance, the example "Send" transaction is formulated and "exported" (red circle below) to the Primary Signer through the QR code as illustrated below with the Electrum screen on the right and Primary Signer left:



Confirm Transaction

| | |
|---|---|
| Input1 | 0.0002 BTC<br>tb1qs5esc5fx00u6fj2vz4jenkwssx84a6mpm5c5ah |
| Output1 | 9.8e-05 BTC<br>tb1qq5y43zz8ddwhvekqrdhndy2yvpese5kzl90fyz |
| Output2 | 0.0001 BTC<br>tb1qza27jp2pdv8pazxqn97z9sh53wpqvktw9cc0el |
| Fee | 200 satoshi |
| Memo | |

Transaction ID:
9e940fa38b5a519fb22f74038b47df30287fbb181898d5a6dcb45c52dadca834

Status: Unsigned
Amount sent: 0. BTC
Fee: 0.000002 BTC ( 1.4 sat/byte )

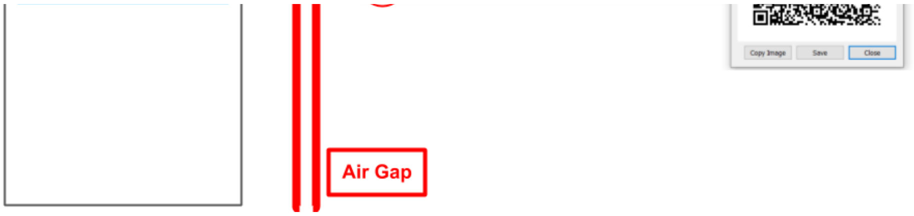
Size: 141 bytes
Replace by fee: True
LockTime: 1834113 (height)

Inputs (1)

```
54a1c1bf4248858cc08dbe7a01814c35307d9ca9f948abccf2629bee8385b8e8:0    tb1qs5esc5fx00u6fj2vz4jenkwssx84a6mpm5c5ah    0.0002
```

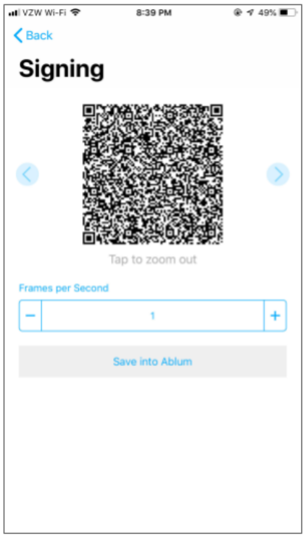
Outputs (2)

```
tb1qq5y43zz8ddwhvekqrdhndy2yvpese5kzl90fyz    0.000098
tb1qza27jp2pdv8pazxqn97z9sh53wpqvktw9cc0el    0.0001
```



The transaction signature request received by the Counterseal app will display its transaction outline (left) for your confirmation. Make sure the highlighted Electrum data (Inputs, Outputs and associated amounts) are identical to those in the confirmation screen of the Counterseal app. **Be sure to verify every single digit displayed on both sides of the air-gap.** This is one of the most important steps in the counterseal process. If successfully validated (visually), all three components (Electrum, Primary Signer, Secondary Signer) must all be compromised for our Counterseal application to be defeated, an extremely unlikely scenario. This is the strongest defense obtainable among all the wallet applications on the market.

The Primary Signer then requests the counterseal signature from the Secondary Signer and displays the QR code below when the countersealed signature is successfully constructed:



Depending on the complexity of the transaction, the counterseal signature may require several steps and trigger multiple frames of QR codes.  After the successful signing of the transaction, Electrum collects this signed transaction (in QR code format) by going to the "Tools" ==> "Load transaction" ==> "From QR code" to read transaction back. Once imported, the transaction is ready to be broadcasted to the Bitcoin Blockchain.

Before the signatures are produced, both the Primary and Secondary Signers independently prompt the user for confirmation. The data crucial to the transaction, such as the amount, sender, recipient, etc., are displayed by both signers separately, each expecting to receive its own button press sanctioning the follow-up signatures.

## Secondary Signer on Live System

In addition to the support on Windows 10, the Secondary Signer may also run on a Live Counterseal platform, which is a bootable, code-only, state-less system with the Electrum and the Secondary Signer built in. Since it is code-only, its checksum may be verified against the constant hash value of the embedded code published on the Counterseal website. Obviously the Secondary Signer can be produced onto a USB stick and carried around on a key chain, or even produced on demand by downloading from Counterseal website when needed.

To be absolutely self-sufficient, you can pull the source code from our Github site and build your own Live USB stick. The next best thing is to download the binary from our website https://counterseal.net, verify its code checksum against what we've published on the same website and produce your own USB Live system. The "production process" is very similar to how one produces a Tails system on a USB stick. Follow the instruction at the Tails web site but plug in our binary instead. This is how we eliminate the Supply Chain attacks once and for all.

This Live Counterseal Signer is mostly used where the crypto transaction involves a large sum of cryptocurrencies under scenarios where any threat of malware on the Windows platform is considered unacceptable.

### Producing Your Own Live System on a USB Stick