Setting up a Ledger Nano S

1. Go to [www.ledger.com](http://www.ledger.com)
   1. Products
      1. Download Ledger Live
   2. Download the app
2. Downloads > Run the Ledger Live installer
3. Run Ledger Live
   1. Get Started
   2. Plug in Ledger and Select Ledger Nano S
   3. Setup a New Nano S
   4. Click through the basics
   5. Click OK, I’m Ready!
      1. Follow Instructions
      2. Set PIN = 1234
      3. Record Seed Phrase
   6. Once your Ledger is setup, Click “My Ledger” in Ledger Live
   7. Update Firmware (if needed)
   8. Install the Bitcoin (BTC) App

Setting Up Trezor

1. Go to [www.trezor.io](http://www.trezor.io)
   1. App
      1. Download for desktop
2. Downloads > Run the Trezor Suite installer
3. Run Trezor Suite
   1. Do not allow data collection
   2. “Have you used this Trezor before?”
      1. This device has already been in prior classes…
      2. So, Click “Yes, set up my Trezor”
         1. If this were your device and you had never used it, you should click no, however in this case, its ok to select yes.
   3. Create new wallet
      1. Standard Seed Backup
      2. Record Seed Phrase
      3. Set PIN = 1234
   4. Update Bitcoin Only Firmware (if needed)

Setting Up ColdCard

1. Go to [www.coldcard.com](http://www.coldcard.com/docs/quick/)
   1. Click on “Docs”
   2. Click on “Users Guide”
   3. Click on “QuickStart! Start Here!”
      1. Our ColdCards are a little different than normal because they have been used for previous classes
      2. Jump down to the section “New Wallet (New Seed)
2. On ColdCard
   1. Enter first Part of PIN = 12; Recognize words? Click [√]; Enter Rest of PIN = 1234
   2. New Seed Words
   3. 24 word (default)
   4. Record Seed Phrase
   5. Pass Test
   6. Enable NFC? [√] (not important for this class)
   7. Disable USB port? [√]
3. Go to [www.Sparrowwallet.com](http://www.Sparrowwallet.com)
   1. Download
   2. Windows Installer (7+): Click on **Sparrow-1.8.2.exe**
4. Downloads > Run the Sparrow Installer
   1. Click More Info
   2. Click “Run Anyway”
5. Click on the windows button in the bottom left corner of your screen
6. Click on Sparrow (should be at the top of the list because it was just installed)
7. Click Next
8. Click Next
9. Click Next
10. Click Configure Server
    1. Leave the default connection to a public server (if you run your own node at home, this is where you would configure it in Sparrow)
    2. Click Test Connection
11. Click Create New Wallet
    1. Enter a name for this wallet: Classroom Test
       1. Policy Type: Multi Signature
       2. Ensure Cosigners shows M of N: 2/3
       3. Ensure Native Segwit
    2. Keystore 1
       1. Click on Connected Hardware Wallet
       2. Plug in Ledger
          1. Enter PIN
          2. Open the Bitcoin App by pressing both buttons with the bitcoin app selected
       3. Go back to Sparrow and under Connect Hardware Wallet click on Scan
       4. Ledger Nano S: Click on Import Keystore
    3. Keystore 2
       1. Click on Connected Hardware Wallet
       2. Plug in Trezor
       3. Under Connect Hardware Wallet click on Scan
       4. Trezor One: Click on “Unlock”
       5. Enter the PIN using the device
       6. Click the down arrow next to Send Passphrase
          1. Toggle Passphrase Off
          2. Confirm on Device
       7. Trezor One: Click on Import Keystore
    4. Keystore 3
       1. Click Airgapped Hardware Wallet
       2. Plug in ColdCard
          1. Enter PIN = 12; Recognize words? Click []; Enter Rest of PIN = 1234
          2. Navigate down and Select Settings
          3. Select Multisig Wallets
          4. Select Export XPUB
          5. Navigate to the end of the text and click [√]
          6. Account Number: Type 0 and click [√]
          7. Type 1 to save multisig XPUB file to SD Card
       3. Take out the microSD card and plug it into the USB adaptor provided
          1. Leave your ColdCard Plugged in
       4. Plug the SD card USB adaptor into your computer
       5. Go back to Sparrow
       6. ColdCard Multisig: Click Import File…
          1. Navigate to your ColdCard SD card using the explorer window
          2. Select the .json file on the drive and click Open
    5. Click Apply
    6. Click No Password
       1. just for this class – for your own Multisig Wallet a password should be used
    7. Backup Multisig Wallet?
       1. Click OK [we will backup multiple formats in the next steps]
    8. Above the Classroom Test Tab, Click File>Export Wallet
       1. BSMS: Click Export File
          1. Save to Desktop
       2. Labels: Click Export File
          1. Save to Desktop
       3. Sparrow: Click Export File
          1. Save to Desktop
       4. ColdCard Multisig: Click Export File
          1. Save to Desktop
          2. Save a second copy on the ColdCard SD Card
    9. Navigate to your ColdCard SD card using the explorer window
       1. Delete the .json file containing your XPUB
       2. Keep the file containing the Sparrow ColdCard Backup File
    10. Remove your SD Card from the computer and put it back into the ColdCard
    11. Scroll back up and select Import from File (Still on the Multisig Wallets Menu)
        1. Scroll down and click [√]
        2. Select the Classroom Test file and click [√]
    12. Congratulations! You just created a multisig wallet 😊
        1. Back in Sparrow Click on Transactions to see your past transactions (none in this case)
        2. Click on Receive to show your first receive address

Resetting Computer

1. Close all windows
2. Click on the windows button in the bottom left corner of your screen
3. Right Click on Sparrow (should be at the top of the list because it was just installed)
   1. Uninstall
4. Select Sparrow
   1. Click Uninstall
5. Select Ledger Live
   1. Click Uninstall
6. Navigate to C:\Program Files
   1. Delete Ledger Live Folder
7. Navigate to C:\Users\user\AppData\Roaming
   1. Delete Sparrow Folder
   2. Delete Ledger Live Folder

Resetting Signing Devices

1. Reset Ledger
   1. Plug in Ledger
   2. Type PIN
   3. Navigate to the Settings Icon
      1. HOLD Both Buttons
      2. When the X and the Lock icons appear, then let go of the buttons
      3. Then Click with both buttons on the settings icon
      4. Navigate down to Security and click both buttons
      5. Navigate down to Reset device and click both buttons
      6. Click right until you get to Reset device and click both buttons
      7. Enter PIN
   4. Unplug Ledger
2. Reset Trezor
   1. Plug in Trezor
   2. Click on the windows button in the bottom left corner of your screen
   3. Click on Trezor Suite (apps are in alphabetical order, just scroll down to Trezor Suite)
      1. Enter PIN
      2. Click on My Trezor
      3. Click on the Settings Gear Icon
      4. Scroll down to Factory Reset
      5. Click both check boxes and click on Factory Reset
      6. Confirm on Device
   4. Unplug Trezor
3. Reset ColdCard
   1. Plug in ColdCard
   2. Enter PIN = 12; Recognize words? Click []; Enter Rest of PIN = 1234
   3. Scroll down to Advanced/Tools and click [√]
   4. Scroll down to Danger Zone and click [√]
   5. Select Seed Functions and click [√]
   6. Select Destroy Seed and click [√]
   7. Are you sure? Scroll down and click [√]
   8. Are you REALLY sure though??? Scroll down and read the message and click [4] to confirm
   9. Unplug ColdCard

For the purpose of this class, we will not be rebuilding the wallets that you all just created.

We will all rebuild a wallet that I made previously that has some transactions on it so you can try to sign a transaction with only a subset of your keys.

First, we will rebuild all of our signing devices with the seed phrases I developed earlier.

Restore Ledger Nano S

1. Downloads > Run the Ledger Live installer
2. Run Ledger Live
   1. Get Started
   2. Plug in Ledger and Select Ledger Nano S
   3. Scroll down to “Already Have a Recovery Phrase?”
      1. Click on: Use an existing recovery phrase to restore your private keys on a new Nano!
   4. Click OK, I’m ready!
   5. Click right until you see “Restore from Recovery phrase” and click both buttons
   6. Choose Pin = 1234
   7. Recovery phrase with 24 words > click both buttons
   8. Enter Word 1 > click both buttons
      1. Navigate through alphabet spelling the first word from the printed out seed phrase
      2. Repeat for Words 2 through 24
   9. Click through remaining menus in Ledger Live
   10. Disconnect your Ledger
   11. Reconnect your Ledger
       1. Type in PIN
   12. Allow ledger manager on device
   13. Click Continue in Ledger Live
   14. Click on My Ledger
       1. Install the Bitcoin App

Restore Trezor

1. Plug in Trezor
2. Click on the windows button in the bottom left corner of your screen
3. Click on Trezor Suite (apps are in alphabetical order, just scroll down to Trezor Suite)
   1. “Have you used this Trezor before?”
      1. Click “Yes, set up my Trezor”
      2. Firmware already installed
      3. Click Recover Wallet
      4. 24 words
      5. Standard recovery [this is only a time saving measure for the class, normally you should not type your seed phrase into a computer]
         1. Confirm on Trezor
      6. Trezor will show which word to type into the computer
      7. Set PIN = 1234
      8. Complete Setup
4. Close Trezor Suite
5. Unplug Trezor

Restore ColdCard

1. Plug in ColdCard
2. Enter PIN = 12; Recognize words? Click [√]; Enter Rest of PIN = 1234
3. Select Import Existing and click [√]
4. 24 Words [√]
5. Use arrows to spell out words
6. Enable NFC? [√] (not important for this class)
7. Disable USB port? [√]

Restore MultiSig Wallet

1. Downloads > Run the Sparrow Installer
2. Click on the windows button in the bottom left corner of your screen
3. Click on Sparrow (should be at the top of the list because it was just installed)
4. Click Next
5. Click Next
6. Click Next
7. Click Configure Server
   1. Leave the default connection to a public server (if you run your own node at home, this is where you would configure it in Sparrow)
   2. Click Test Connection
8. Create Wallet
9. Click Create New Wallet
   1. Close this window
10. Click File > Import Wallet
    1. Sparrow: Click Import File…
    2. Navigate to Desktop\Classroom Restore\Classroom Restore-sparrow.mv.db
    3. Enter a Name for this Wallet: Classroom Restore
    4. No Password
11. Plug your ColdCard SD card into the computer
12. Navigate to Desktop\Classroom Restore\ and copy the ColdCard backup file
13. Paste the ColdCard backup file onto the SD card
14. Remove your SD Card from the computer and put it back into the ColdCard
15. Scroll back up and select Import from File (Still on the Multisig Wallets Menu)
    1. Scroll down and click [√]
    2. Select the Classroom Test file and click [√]

Sign Multisig Transaction

1. In Sparrow, Click on Addresses
   1. Pick an unused receive address (e.g., the 3rd one)
      1. Right click on it, and select Copy Address
2. In Sparrow, Click on Send
   1. Pay to: [Paste]
   2. Label: test
   3. Amount: Max
   4. Fee Rates, etc.: Default
   5. Click Create Transaction
   6. Click Finalize Transaction for Signing
3. Sign Transaction
   1. Sign with Trezor
      1. Plug in Trezor
      2. Click on the Button Labeled “Sign”
      3. Trezor One: Unlock
      4. Unlock with PIN = 1234
      5. Trezor One: Sign
      6. Confirm Spend and Fee on Device
   2. Sign with ColdCard
      1. Remove the SD Card from the ColdCard and Plug it into the computer
      2. In Sparrow Click the Button: Save Transaction
      3. Navigate to the SD Card in the file explorer and click Save
      4. Remove the SD Card from the computer and put it back into the ColdCard
      5. Navigate back to the home screen of the ColdCard and Click on Ready to Sign
         1. If the fee is too high go back to the home screen
         2. Navigate to Settings
         3. Scroll down to max network fee
         4. Change to no limit
         5. Go back to the home screen and Click on Ready to Sign
      6. Read the message and Click [√] to approve
      7. Remove the SD card from the ColdCard and put it back into the computer
      8. In Sparrow, Click on Load Transaction and Navigate to the SD Card
         1. Select the psbt file that includes “-part”
      9. At this point the transaction is signed and could be broadcast into the mempool, however, we will just cancel the transaction to save the fees for another class 😊
      10. Click the [x] in the test transaction tab in Sparrow

Verifying the Software [*Optional, but highly recommended*]

1. Download the Manifest: Click on **sparrow-1.8.2-manifest.txt**
2. Download the Manifest Signature: Click on **sparrow-1.8.2-manifest.txt.asc**
3. Scroll down to “Verifying the Release”
4. Click on the link to the Windows version of gpg
5. Click the Green button “Download Gpg4win 4.2.0”
6. Click on $0 (consider donating in the future – bitcoin accepted)
7. Click on the Blue Download button
8. Downloads > Run the Gpg4win installer
   1. Install all the default options
   2. Uncheck “Run Kleopatra”
9. Next to the windows button in the bottom left corner of your screen click in the “Type here to search” box
   1. Type “CMD” and hit enter on the keyboard
10. Go back to the Sparrow download page in the browser
    1. Select and copy the following text with your cursor:

curl https://keybase.io/craigraw/pgp\_keys.asc | gpg --import

1. Go back to the command line window
2. Simply right click anywhere in the command line window and it will paste in the text copied above
3. Hit Enter on the Keyboard
4. Type “cd downloads” and hit enter on the keyboard
5. Go back to the Sparrow download page in the browser
   1. Select and copy the following text with your cursor:

gpg --verify sparrow-1.8.2-manifest.txt.asc

1. Go back to the command line window
2. Simply right click anywhere in the command line window and it will paste in the text copied above
3. Hit Enter on the Keyboard
4. Go to <https://keybase.io/craigraw>
   1. Click on the link next to the key icon
5. Open the downloaded file: sparrow-1.8.2-manifest.txt.asc
   1. Verify that the 64-bit key from the website matches the file
6. Go back to the Sparrow download page in the browser
   1. Select and copy the following text with your cursor:  
      CertUtil -hashfile Sparrow-1.8.2.exe SHA256 | findstr /v "hash"
7. Go back to the command line window
8. Simply right click anywhere in the command line window and it will paste in the text copied above
9. Hit Enter on the Keyboard
10. Open the downloaded file: sparrow-1.8.2-manifest.txt
    1. Verify that the hash output in the command line window match the hash from the manifest file for your download

Encrypting Your Wallet Backup File(s) [*Optional, but highly recommended*]

1. Go to [www.veracrypt.fr](http://www.veracrypt.fr)
   1. Click on Downloads
   2. Click on the Windows EXE Installer “VeraCrypt Setup 1.26.7.exe”
2. Downloads > Run the VeraCrypt Installer
   1. Leave all defaults and install
   2. Click Finish
   3. Do you want to view the tutorial?
      1. No
   4. Do you want to disable Fast Startup?
      1. No [just for this class, at home you should consider this option]
3. Click on the windows button in the bottom left corner of your screen
4. Click on VeraCrypt (should be at the top of the list because it was just installed)
5. Scroll down and Select Drive Z
6. Click Create Volume
7. Select “Create an encrypted file container” and click Next >
8. Select “Standard VeraCrypt Volume” and click Next >
9. Volume Location
   1. Click Select File…
   2. Navigate to Desktop
   3. Type a File Name: “Container.hc”
   4. Click Next >
10. Encryption Options
    1. Encryption Algorithm: AES
    2. Hash Algorithm: SHA-512
    3. Click Next >
11. Volume Size
    1. 100 MB
    2. Click Next >
12. Volume Password
    1. For this class we will use a simple password [RunningBitcoin]
    2. Type the password and confirm it
    3. Click Next >
    4. Use Short Password?
       1. Yes
13. Move your mouse around the VeraCrypt window until the bar at the bottom turns green
    1. Click Format
    2. Click OK
    3. Click Close
14. Click Select File…
15. Navigate to Desktop and select Container.hc
16. Click Mount (while Drive Z is Selected)
17. Type in the Password [RunningBitcoin] and Click OK
18. Copy your Multisig Wallet Backup Files from the Desktop
19. Navigate to Drive Z
20. Paste your Multisig Wallet Backup Files from the Desktop
21. Close Drive Z
22. Go Back to VeraCrypt
23. Click Dismount
24. Click Exit

Recognizing that different students will have different skill levels and interests in more advanced topics, handouts will be offered on the following more advanced topics or can be shared with the whole class if there is common interest:

- How to verify your software download

- Sparrow

- How to encrypt your wallet configuration files using VeraCrypt

- How to restore your multisig wallet using Nunchuk Desktop

- How to sign a transaction using Nunchuk Desktop if you don’t have your Signing Device (seed phrase only)