R109-bg-Open Source Multisig Bitcoin routine.

P018>Seminars>resources>R109

10/5/2022

Revised: 10/4/2022
Previous revision: 9/23/2022

Start of Your Procedure

Part 1

1. This is open source, plain English, trust based, documentation. Open source means users help each other to keep the documentation current by emailing changes and suggestions to jeff@Loquate.tv.
    a. No person is responsible.
    b. Any person is free to use or propose upgraded documentation.
    c. You and any user of this open source documentation absolves, indemnifies and holds harmless Loquate from any matter which you may dispute.
2. This version includes 2 of 3 Bitcoin wallets: 2 of yours from Ledger brand, Ledger Nano S Plus ("Ledger") and 1 by processor 1.
    a. One is loaned by you to processor 1. You still own it. You can always get it back.
    b. Another is always held by you in your possession.
    c. Processor 2 owns a third Ledger.
    d. 2 of 3 multi sig means sending Bitcoin can only be executed from your private Bitcoin address when 2 of the 3 Ledgers are present.
3. What is a **wallet**? A wallet is a multi-signature address where your Bitcoin is stored. Processor 2 holds a third private key. The wallet is yours. Your wallet requires 2 of 3 private keys to access your address where your Bitcoin is stored. Since you control two Ledgers, at any time you may remove your Bitcoin from your wallet and store it in any other wallet you so choose subject to conditions of a processor agreement.
4. What is **2 Factor Authentication (2FA)**? 2FA is:
    a. An additional layer of security to protect your account
    b. Uses your mobile phone to log in to a service like Coinbase
    c. 2FA is used when:
        i. You buy bitcoin
        ii. You sell bitcoin
        iii. You move bitcoin to cold storage
        iv. You move bitcoin from cold storage to Coinbase

Purchase Ledger Nano S Plus devices

5. Open Google Chrome browser
6. Navigate Google Chrome browser to https://shop.ledger.com/products/ledger-nano-s-plus
7. Click the black tile to select the "Matte Black" Nano S
8. Click the Add to Cart button
9. Click the orange tile to select the "BTC Orange" Nano S
10. Click the Add to Cart button
11. Click the black Checkout button
12. Enter your email address and shipping address
13. Click the black Continue button
14. Click the black Continue button
    a. Hint: there is only one Shipping option available
15. Enter your credit card information
16. Click the black Complete Order button

You have now purchased two Ledger Nano S Plus devices. You will receive emails from Ledger regarding approximate delivery.

Set Up Ledger Nano S Plus devices

(Hint: Be prepared. Initial set up is hard. Here is why initial set up is hard. It is necessary to protect your bitcoin. Multisig and cold storage of bitcoin is superior protection against loss or theft. That is why you go through the trouble to establish initial set up. This is a detailed list of steps to be done step by step.)

17. Print out this write-up
    a. Enter a check on each completed step using a good black pen.
    b. Hint: gives confidence you did each step and allows you to step away and resume precisely where you left off.
    c. Hint: you will use the same pen to record "Your personal recovery seed."
18. Start with black Ledger Nano S Plus device
    a. Hint: the orange Ledger Nano S Plus device will have an orange dot on the

back of its package, so choose the box without the orange dot

19. Remove Ledger Nano S Plus device from package
20. Remove the envelope labeled "Secret Recovery Sheet" from the package
21. Open the envelope and set all three "Confidential My 24-word recovery phase" cards to the side
22. Remove the "Ledger.com/Start" envelope from the package and set aside.
23. Remove the USB cable from the package, found in the black envelope.
24. Flip open the Ledger Nano S Plus to expose the USB port and connect the USB cable
25. Connect the other end of the USB cable to your computer
    a. Hint: the screen on the Ledger Nano S Plus will light up when connected
26. Open Google Chrome browser
27. Navigate Google Chrome browser to https://www.ledger.com/start
28. Click the Download button and select your computer type (Windows, Mac, or Linux)
29. Click the "ledger-live-deskto….exe" button that appears in the bottom left corner of Google Chrome
    a. Hint: this will install version 2.39.2 or greater of Ledger Live
30. Click on the .exe file to open.
31. Click Yes to allow this app to make changes to your computer
32. Click the Install button
    a. Hint: Ledger Live software will install itself on your computer
33. Check the box next to "Run Ledger Live"
34. Click the Finish button
    a. Hint: the Ledger Live app will appear
35. Click the Get started button
36. Check the box next to "I have read and accept the Terms of service and Privacy policy"
37. Click the Enter Ledger app button
38. Click the "Nano S Plus" device
39. Click the image that says "First use: Set up a new Nano S"
40. Click the right chevron ">" button
    a. You will click this right chevron ">" button three more times
41. Click the Let's do this! Button
    a. Hint: if you did not get a pen in the beginning of this routine, get one now because you will need it
42. Click the OK, I'm ready! button
43. Click the Next step > button
44. Check the box next to "I understand that I must choose my PIN code myself and keep it private"
45. Click the Set up PIN code > button
46. Pick up your Ledger Nano S Plus device
    a. Hint: there are two buttons on the device
    b. Hint: Assume that these buttons are on the top and when flipped open the silver shield is on the right and the black body with screen is on the left
    c. Hint: the button further to the right will be called "right button" and the button further to the left will be called "left button"
47. Push the right button until the screen reads "Set up as new device"
48. Push both buttons at the same time
49. The screen will now say "Choose PIN"
50. Push both buttons at the same time again
51. You will now enter a PIN of your choosing
    a. Hint: this PIN must be between 4 and 8 digits long
    b. Hint: do not use an obvious combination that an attacker could find like your birthday or the last four digits of your phone number
52. Use the right button to increment the number and the left button to decrement
53. When you have incremented / decremented to the first number you want for your PIN, push both buttons to move on to the second number
    a. Repeat until you have entered at least four numbers
54. Once you have at least four numbers, a check mark will appear in the number space, if you are finished with your PIN push both buttons with the check mark to signal that you have completed entering your PIN or keep incrementing / decrementing until you reach 8 digits
55. Your Ledger Nano S Plus screen will now read "Write down your recovery phrase","
56. Switch back to your computer and click the Next step > button
57. Check the box next to "I understand that if I lose this recovery phrase, I will not be able to access my crypto in case I lose access to my Nano."
58. Click the Recovery phase > button
59. Pick up your Ledger Nano S Plus again

    a. Push both buttons, device will say “Your device will generate 24 words, they are your Recovery Phrase”
60. Push the right button
    a. Push the right button four more times as the screens describe the next step, which is writing down the 24-word recovery phrase
61. Push both buttons
62. Grab all three “My 24-word recovery phrase” cards from the envelope included in the Ledger Nano S Plus package as you will fill them all out in the next step
63. The Ledger Nano S Plus screen is now displaying the first word of your 24-word recovery phrase
64. Write this word down carefully and clearly on each of your three “My 24-word recovery phrase” cards
    a. Prove that you wrote the word down with the correct spelling and in the correct # space for each card
65. Once you have proven that the word is correctly ordered and correctly spelled, push the right button to receive the next word
66. Repeat this process for each of the 24 words
67. Once you have written down all 24 words in order on each of the three cards, use the left and right buttons to cycle through all 24 words again one last time for each card
    a. Hint: this 24-word recovery phrase is the only way to recover your Bitcoin in case you lose your Ledger Nano S Plus, so this extra diligence and care is worth the time
68. Push the right button until your screen says “Confirm your Recovery phrase”
69. Push both buttons
70. Confirm your 24-word recovery phrase one last time by using card you just filled out:
    a. Push both buttons on top of ledger
    b. The Ledger Nano S Plus screen will prompt you to select the first word
    c. Read the first word from your card
    d. Push the right / left buttons until you find that first word
    e. When you find the first word, push both buttons
    f. Repeat for each of the 24 words in order
71. Your recovery phrase is set.
72. Push the right button and read the prompts on your Ledger Nano S Plus
    a. Push the right button 3 times
73. When the Ledger Nano S Plus screen reads “Press both buttons to continue”, push both buttons
74. Switch back to your computer
75. Click the Next step > button
76. Click the Next step > button again
77. Click the OK, I’m done! button
78. Click the Let’s take the quiz button
79. Answer the three questions by clicking the right answers, remembering that:
    a. Your Bitcoin is stored on the blockchain, not on the Ledger Nano S Plus: the Ledger Nano S Plus protects your Bitcoin from attackers
    b. If your 24-word recovery phrase is no longer secure or private, that your Bitcoin is no longer safe and you need to transfer them to a secure place
    c. When you connect your Nano Ledger S Plus to your computer and open the Ledger app, your private key is still offline and does not connect to the internet
80. Click the Finish Quiz button
81. Click the Next step > button
82. Click the Check my Nano > button
83. Pick up your Ledger Nano S Plus and push both buttons
    a. Hint: this allows the Ledger Live app on your computer to verify your Ledger Nano S Plus device
84. Click the Continue > button
85. Click the Add account button
86. Choose Bitcoin from the drop-down menu
87. Pick up your Ledger Nano S Plus and enter your PIN
88. Switch back to your computer and click the Continue button
89. The Ledger Live app will update your Ledger Nano S Plus
90. Pick up your Ledger Nano S Plus and verify that the screen reads “Open app Bitcoin”
91. Push both buttons on your Ledger Nano S Plus
92. Your Ledger Nano S Plus screen should read “Bitcoin is ready”
93. Switch back to your computer
94. The Ledger Live app will synchronize for approximately one minute
95. Click the Add account button
96. Click the Done button

97. Your Ledger Nano S Plus device is now ready for use with Bitcoin
98. Repeat this routine for your second Nano Ledger S Plus device (the orange one that you will loan to processor 1)
    a. Hint: installing the Bitcoin app on your Ledger Nano S Plus is slightly different the second time
    b. Eject the black Ledger Nano S Plus
    c. Plug in your Orange Ledger Nano S Plus
    d. With your orange Ledger Nano S Plus device connected to your computer, in the Ledger Live app
    e. Click My Ledger, receive message "Your device is not ready to use yet"
    f. Click Setup Device button
    g. Choose Ledger Nano S Plus
    h. Setup a New Nano S Plus
    i. Continue through all steps as above until the step where you enter your PIN (step 87 above), then continue below
    j. Click My Ledger
    k. Click the Install button next to Bitcoin
    l. The Ledger Live app on your computer will display Bitcoin
99. Eject the Orange Ledger Nano S Plus
100. Close out of Ledger Live app on your computer
101. Mail your orange Ledger to processor 1

Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate

Your Black Ledger Subroutine – results in a master public key for the black Ledger.

(Hint: The master public key is used to ensure you are the owner of an address that can receive funds. The public key is also mathematically derived from your private key. Your private key is for you alone to know. Source: https://www.dummies.com.)

(Hint: The master public key can be recreated. If an error occurs, do Ledger Subroutine again.)

End of Your Procedure Part 1.

Part 2

Hint: virtual meeting of you, processor 1, and processor 2 occurs up to one hour
Hint: these steps must be completed while you, processor 1, and processor 2 are working at computers

Download and Install Electrum Wallet Software (free, open-source software)

102. Toggle to Google Chrome browser
103. Navigate to https://electrum.org/#download
104. Click the link associated with your computer
    a. For Windows, click the "Standalone Executable" link
    b. For mac, click the "Executable for OS X" link
    c. Hint: you will be installing version 4.1.5 or later of Electrum
105. When the file finishes downloading, click "electrum…" in the bottom left corner of Google Chrome
106. Click the Install button
    a. Hint: installation will begin

Start Ledger Subroutine
Hint: the following step 105 and onward can be done remotely

107. Open Electrum
    a. On Windows: Start > Electrum
    b. On Mac: upper-right Spotlight, search "Electrum", click Electrum icon
108. Click the Next button
    a. Hint: leave "default_wallet", you are not going to create a wallet in this subroutine
109. Click the button next to "Multi-signature wallet" then click the Next button
110. Slide the "From X cosigners" up from 2 to 3
111. Slide the "Require Y signatures" down from 3 to 2
112. Click Next
113. Click the button next to "Use a hardware device" then click the Next button
114. Plug your black Ledger Nano S Plus into your computer
115. Enter the black Nano PIN into the black Ledger Nano S Plus

116. Push the right button until the Bitcoin screen appears
117. There are two buttons on the black Ledger Nano S Plus, push both buttons to open the Bitcoin app
    a. Hint: screen will read “Bitcoin is ready” when the Bitcoin app is running
118. Switch back to Electrum on computer
119. Click the Next button
120. Click the button next to “[Ledger Nano S Plus, initialized, hid]” then click the Next button
121. Click the button next to “native segwit multisig (p2wsh)”
    a. Hint: do not make any changes to the derivation path
122. Click the Next button
123. Highlight the text in the box
124. Right-click and select “Copy”
125. Open email
126. Compose new message
127. Paste text into body
128. Subject: “Your Name”, for example “John Smith”
129. Send email to processor 1
    a. Hint: This master public key will allow processor 1 and processor 2 to create a 2 of 3 multisignature (“multisig”) wallet using your black Ledger
    b. Hint: even if an evil person were to gain access to a master public key, he cannot steal the bitcoin without also successfully stealing 2 of 3 Ledgers undetected, statistically highly unlikely.
130. Click Cancel
131. Exit Electrum

End Ledger Subroutine

Part 2 End

Processor 1 orange Ledger Subroutine – results in a master public key for the orange Ledger.

132. Processor 1 repeats Ledger subroutine as above, mentally replacing Ledger color as orange
133. Processor 1 sends email to processor 2

Processor 2 creates 2 of 3 multisig wallet using master public keys one from each Ledger. Neither processor 1 nor processor 2 will ever know the private key of your Black Ledger.

Hint: each Ledger has its own independent master public key.

Processor 2 steps:

134. Open Electrum
    a. On Windows: Start > Electrum
    b. On Mac: upper-right Spotlight, search “Electrum”, click Electrum icon
135. Enter a name for your wallet, for example “wagdaj02” where “wag” are the first three letters of your last name, “da” are the first two letters of your first name, and “02” is which number wallet you are creating
136. Click the Next button
137. Click the button next to “Multi-signature wallet” then click the Next button
138. Slide the “From X cosigners” up from 2 to 3
139. Slide the “Require Y signatures” down from 3 to 2
140. Click Next
141. Select “Use a master key” then click Next
142. Copy the black Ledger master key into box then click Next
143. Click Next
144. Select “Enter cosigner key” then click Next
145. Copy processor 1’s orange Ledger master key into box then click Next
146. Select “Cosign with hardware device”
147. Plug your blue Ledger Nano S Plus into your computer
148. Enter the blue Nano PIN into the blue Ledger Nano S
149. Push the right button until the Bitcoin screen appears
150. There are two buttons on the blue Ledger Nano S Plus, push both buttons to open the Bitcoin app
    a. Hint: screen will read “Bitcoin is ready” when the Bitcoin app is running
151. Switch back to Electrum on computer
152. Click the Next button
153. Click the button next to “[Ledger Nano S Plus, initialized, hid]” then click the Next button
154. Click the button next to “native segwit multisig (p2wsh)”
    a. Hint: do not make any changes to the derivation path
155. Click the Next button
156. Enter a password for this wallet
157. Confirm the password
158. Click Next

End Processor 2 steps

You Open a Coinbase Account

Hint: you will need your checking account routing number, driver's license, and camera-enabled smartphone to complete these steps so have these materials ready.

159. In Google Chrome browser navigate to https://www.coinbase.com/
160. Click Sign up button
161. Enter the following fields:
    a. First name
    b. Last name
    c. Email
    d. Password
    e. State of driver's license
162. Check the box verifying that you are 18 years of age or older and agree to the User Agreement and Privacy Policy
163. Click Continue button
164. Click Continue button on next screen
165. Open a new tab in Google Chrome browser
166. Navigate to your email account
167. Open email from Coinbase titled "Please Verify Your Email Address"
168. Click Verify Email Address button in email
    a. Hint: click this link confirms your email address to Coinbase
169. Toggle back to Coinbase tab in Google Chrome
170. Enter your mobile phone number in the Phone number field
171. Click Send code button
    a. Hint: you will receive a 7-digit code in a text message from Coinbase
172. Open the text message you just received on your smartphone
173. Enter the 7-digit code into the Coinbase field where it says "Enter authentication code"
174. Click Submit button
175. Select the country of your citizenship
    a. Hint: if you are a citizen of multiple countries, pick only one
176. Click Submit button
177. Enter the following fields:
    a. Date of birth
    b. Street Address
    c. What will you use Coinbase for? Pick "Investing"
    d. What is your source of funds? Pick "Occupation" if your primary source is your job, pick "Savings" if your primary source is your savings, etc.
    e. Employment status
    f. Last 4 digits of Social Security Number
178. Click Continue button
179. Select answer to question "How much crypto do you expect to trade per year?" from drop-down, for example "$10,000 - $99,999"
180. Select answer to question "What industry do you work in?" for example "Transportation"
181. Click Submit button
182. Navigate Google Chrome browser to https://www.coinbase.com/dashboard
183. Click "Send & receive crypto / Verify your ID" link
184. Click Enable send receive button
185. Click Driver's License button
186. Click Mobile Camera button
187. Open the text message you just received on your smartphone
188. Tap the link in the text message to navigate to a Coinbase website for confirming your identity
189. Tap the top button to take a photo of the front of your driver's license
    a. This will open your camera app, use the camera to take a picture of the front of your driver's license
190. Tap the bottom button to take a photo of the back of your driver's license
    a. This will open your camera app again, use the camera to take a picture of the back of your driver's license
191. Tap Complete verification button
192. You can now close the Coinbase page on your smartphone
193. Back to Google Chrome browser, you may see a "Verifying identity" window with a spinning icon
    a. Hint: this will complete within 5 minutes as Coinbase verifies your driver's license
194. Once verification is complete a new screen will pop up, click the Continue button
195. Navigate Google Chrome browser to https://www.coinbase.com/settings/linked-accounts
196. Click Add a payment method button
197. Click Bank Account link

198. Click Continue button
199. Search for your bank account, for example "PNC", then click on your bank
200. The next step depends on your bank:
    a. For PNC, enter your user ID and Password
    b. Click Continue and Google Chrome will navigate you to your Chase login page
    c. Enter your username and password
    d. Click Submit button
    e. Select the button next to "Text"
    f. Click Continue button
    g. Open the text message you just received on your smartphone
    h. Enter the code from the text message into the field labeled "Code"
    i. Click Submit
    j. Select the button next to the account you wish to connect, for example "Everyday Checking"
    k. Click Continue button
    l. Enter your checking account routing number
    m. Click Continue button
    n. Click Continue button
201. Follow the steps for your bank if different than PNC

You call processor 1 when you want to:

- Buy bitcoin
- Sell bitcoin
- Make a transaction with bitcoin

Caution: you must be available to accommodate 2FA with your mobile phone and seek to execute transaction expeditiously so as to avoid hot wallet theft of bitcoin.

Processor 1 calls processor 2 to complete these steps. Transactions will be processed on a pre-arranged day and time.

Buy Bitcoin on Coinbase

202. Navigate Google Chrome browser to https://www.coinbase.com/dashboard
203. Click Buy / Sell button
    a. "Buy" set to Bitcoin
    b. "Pay With" set to your bank account
    c. Enter the amount of USD you would like to purchase Bitcoin with, for example $500
    d. Click Preview Buy button
        i. Hint: you will be charged a "taker" fee based on the size of your order, the amount and ranges can be found here: https://help.coinbase.com/en/exchange/trading-and-funding/exchange-fees
    e. Click Buy Now button
204. The bitcoin purchase is complete and can now be sent to cold storage wallet
    a. (Technically, you will have sent bitcoin from the Coinbase address on the blockchain to the cold storage address on the blockchain)

Processor 2 collects all the data on the Coinbase transaction.

Find Your Coinbase Transactions

Hint: you can use your Coinbase transactions to keep track of your Bitcoin cost basis

205. Navigate Google Chrome browser to https://www.coinbase.com/dashboard
206. Click "Bitcoin"
207. Click "Wallet"
208. This screen shows you the date and amount purchased for all transactions

You tell processor 1 you want to sell your bitcoin.
Caution: you want to execute your transactions as fast as possible to avoid hacking.

Processor 2 steps:

Send Bitcoin from Coinbase to Your 2 of 3 Multisig Wallet using Electrum

209. Open Electrum
210. Click Tools > Preferences in Electrum
211. Select "BTC" from the dropdown menu labeled "Base unit:"
    a. Hint: BTC means full Bitcoin, compared to mBTC (1 / 1,000 of a Bitcoin) or sats (1 / 100,000,000 of a Bitcoin)

    b. Hint: this routine assumes full Bitcoin
212. Click Close
213. Click the "Receive" tab in the Electrum
    a. Optional: add a description, for example "Bitcoin on 3/15/2022 from Coinbase"
    b. Optional: enter the amount of Bitcoin you will be receiving into the "Requested amount" field, for example "0.001"
    c. Hint: entering the requested amount allows you to quickly see how much Bitcoin in USD you will be receiving, but this is not required
214. Click the New Address button
215. In the "Address" window that pops up, click the blue icon with two pieces of paper on it to copy the address
216. Open Google Chrome and navigate to https://www.coinbase.com/
217. Click "Sign in" link
218. Enter your email and password
219. Check your smartphone for a text message from Coinbase
220. Enter the code from the text message into the Coinbase field
221. Click the Login button
222. Click the Send / Receive button
223. Click the "Pay with" field and select Bitcoin
224. Enter a small amount, for example $20
225. Place cursor in "To" field (text says "Mobile, email, or address"
226. Right-click select Paste
    a. Caution: Toggle back to Electrum to confirm that the text pasted into the Coinbase screen matches what appears in Electrum
227. Click Continue button
228. Confirm that the "To" address ends with the four digits you wrote down, for example "0km5"
    a. Hint: a network fee in Bitcoin will be charged to complete this transaction, and the fee is set by the Bitcoin network
    b. Hint: Coinbase does not take any of this fee, it is paid to Bitcoin miners who are enabling the transaction
229. Click Send now button
230. Check your mobile phone for a text message from Coinbase
231. Enter the code from your mobile phone into the Coinbase prompt in Google Chrome
232. Click Confirm button
    a. Hint: it may take up to a half hour to appear in Electrum while the Bitcoin network processes the transaction
    b. Hint: this transaction took less than two minutes during the writing of this routine
    c. Hint: as soon as Electrum sees that a transaction has taken place, it will highlight the Address section red
    d. Hint: this is meant to warn you that you have already used this address
    e. Hint: it may take up to a half hour for the transaction to be confirmed and added to your total Bitcoin holdings

First buy complete.

Scenarios:
Send Bitcoin from Your Multisig Wallet to Coinbase using Electrum – all Ledgers are in different locations

Processor 1 creates and partially signs transaction

233. Open Google Chrome
234. Navigate to https://www.coinbase.com/signin
235. Enter your email address and password
236. Check your smartphone for a text message from Coinbase
237. Enter the code from the text message into the field on Coinbase then click the Verify button
238. Click the Send / Receive button
239. Click the Receive tab
240. Click the "Asset" text and select Bitcoin
241. Click the small dark grey boxes to copy the address
242. If Electrum is open, close it
243. Connect your orange Ledger to the computer
244. Enter the orange Nano PIN into the orange Ledger
245. Push the right button until you arrive at the Bitcoin app
246. There are two buttons on the orange Ledger, push both buttons to open the Bitcoin app
    a. Hint: screen will read "Bitcoin is ready" when the Bitcoin app is running
247. Re-open Electrum
    a. Hint: Must close and re-open wallet to clear cache of previously-used devices
248. Enter Password then click Next

249. Click “No” two times
    a. Hint: these prompts are for the other two Ledgers associated with this wallet, clicking “No” does not harm this process
250. Click the “Send” tab
251. Paste the address from Coinbase into the “Pay to” field
252. Enter a description of the transaction, for example “Send 1 bitcoin to Coinbase for sale per request on 2022-0606”
253. Enter the amount of bitcoin to be sent to Coinbase in the “Amount” field
254. Click “Pay…”
255. Prove
    a. Confirm the amount of bitcoin to be sent matches what you expect
256. Click “Send”
257. Pick up orange Ledger
258. Push the right button three times on the orange Ledger to see “Approve”
    a. Hint: Ledger device is warning that this transaction is unusual, but nothing is wrong
259. Push both buttons on the orange Ledger to approve
260. Push right button once on orange Ledger
261. Prove: confirm that the amount of Bitcoin displayed on the Ledger screen matches what you typed into the Electrum screen
    a. After proven, push right button once on orange Ledger
262. Prove: confirm the address displayed on the screen matches what is shown on Coinbase site
    a. After proven, push right button twice on orange Ledger
263. Push both buttons on orange Ledger to accept
264. Push right button five times on orange Ledger
    a. Hint: this screen displays the full Extended Public Key, shortened “XPub”, for this transaction
265. Push both buttons on orange Ledger to accept
266. Push right button two times on orange Ledger
    a. Hint: this screen shows the fees in Bitcoin associated with this transaction
267. Push both buttons on orange Ledger to “Accept and send”
268. Toggle back to Electrum on your computer
269. Click “No” twice
    a. Hint: Electrum expects one of the other Ledgers to sign this transaction, but we need the Processor to complete this from the Processor’s computer
270. Click the “Export” button in the bottom left corner
271. Select “For hardware device; include xpubs” > “Export to file”
272. Save the file with the exact name created by Electrum to your desktop
    a. Hint: should be wallet-ID, for example wagdaj02-1234abcd.psbt
273. Click “OK”
274. Open email
275. Compose new message
276. Attach the saved file, for example wagdaj02-1234abcd.psbt
277. Attach the wallet file associated with this transaction, for example wagdaj02
    a. Hint: wallet files can be found at C:\Users\<your_user_name>\AppData\Roaming\Electrum\wallets\wagdaj02
278. Subject: Transaction
279. Send email to Processor

Processor 2 second signature on transaction

280. Processor 2 receives email and downloads files to desktop
    a. Hint: two files, wagdaj02-1234abcd.psbt (the transaction) and wagdaj02 (the wallet, has no file extension)
281. If Electrum is open, close it
282. Connect your blue Ledger to the computer
283. Enter the blue Nano PIN into the blue Ledger
284. Push the right button until you arrive at the Bitcoin app
285. There are two buttons on the blue Ledger, push both buttons to open the Bitcoin app
    a. Hint: screen will read “Bitcoin is ready” when the Bitcoin app is running
286. Re-open Electrum
    a. Hint: Must close and re-open Electrum to clear cache of previously used devices
287. Click “Choose…” button
288. Select the downloaded file, for example wagdaj02, then click OK
289. Call processor 1 for password, before hanging up get the amount of bitcoin to be sent for proof
290. Enter Password then click Next
291. Click “No” twice

    a. Hint: Electrum expects the other Ledgers to be connected but you will only need the blue Ledger
292. Tools > Load Transaction > From File
293. Select downloaded file, for example wagdaj02-1234abcd.psbt, then click OK
294. Click “Sign”
295. Pick up blue Ledger
296. Push the right button three times on the blue Ledger to see “Approve”
    a. Hint: Ledger device is warning that this transaction is unusual, but nothing is wrong
297. Push both buttons on the blue Ledger to approve
298. Push right button once on blue Ledger
299. Prove: confirm that the amount of Bitcoin displayed on the screen matches what Processor 1 told you
    a. After proven, push right button once on orange Ledger
300. Prove: confirm the address displayed on the screen matches what is shown on Coinbase site
    a. After proven, push right button twice on orange Ledger
301. Push both buttons on blue Ledger to accept
302. Push right button five times on blue Ledger
    a. Hint: this screen displays the full Extended Public Key, shortened “XPub”, for this transaction
303. Push both buttons on blue Ledger to accept
304. Push right button two times on blue Ledger
    a. Hint: this screen shows the fees in Bitcoin associated with this transaction
305. Push both buttons on blue Ledger to “Accept and send”
306. Toggle back to Electrum on your computer
307. Click “Broadcast”
308. Click “OK” on screen that says “Payment Sent”
309. The Bitcoin has been sent to your Coinbase account.
    a. Hint: it may take up to a half hour to appear in Coinbase while the Bitcoin network processes the transaction
    b. Hint: this transaction took less than five minutes during the writing of this routine

Recovery – You lose black Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2
Warning: assume an evil person has access to the black Ledger
Warning: assume this evil person also has the PIN code to the black Ledger
Hint: Bitcoin is still safe since evil person does not have access to 2 of 3 multisig wallet in Electrum
Hint: Even if evil person were to gain access to 2 of 3 multisig wallet in Electrum, Bitcoin is still safe because evil person must have 2 Ledgers to send bitcoin.

310. You purchase new black Ledger
311. You receive new black Ledger
312. Follow the steps in “Set Up Ledger Nano S Plus devices” for the new black Ledger
313. You, processor 1, and processor 2 meet with Ledgers
    a. Hint: processor 1 still has the original orange Ledger and processor still has the original blue Ledger
314. Create a new 2 of 3 multisig wallet in Electrum following the steps in “Create a Multisignature (“Multisig”) 2 of 3 Wallet with Electrum – Ledgers separate”
    a. Hint: use your new black Ledger, processor 1 original orange Ledger, and processor 2 original blue Ledger to create a new 2 of 3 multisig Electrum wallet
315. Follow the steps in “Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum”, using an address from the new 2 of 3 multisig wallet in Electrum instead of the Coinbase address, to send all bitcoin from the old 2 of 3 multisig wallet to the new 2 of 3 multisig wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows processor 1’s original orange Ledger and processor 2’s original blue Ledger to be used together to send bitcoin
316. You destroy all “My 24-word recovery phrase” cards for old black Ledger
    a. Hint: this is an extra safety precaution

Recovery – Processor 1 loses orange Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to the orange Ledger
Warning: assume this evil person also has the PIN code to the orange Ledger
Hint: Bitcoin is still safe since evil person does not have access to 2 of 3 multisig wallet in Electrum
Hint: Even if evil person were to gain access to 2 of 3 multisig wallet in Electrum, Bitcoin is still safe because evil person must have 2 Ledgers to send bitcoin.

317. Processor 1 purchases new orange Ledger
318. Processor 1 receives new orange Ledger
319. Follow the steps in "Set Up Ledger Nano S Plus devices" for the new orange Ledger
320. You, processor 1, and processor 2 meet with Ledgers
    a. Hint: you still have original black Ledger and processor 1 still has original blue Ledger of yours on loan to the processor.
321. Create a new 2 of 3 multisig wallet in Electrum following the steps in "Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate"
    a. Hint: use your original black Ledger, processor 1's new orange Ledger, and processor 2's original blue Ledger to create a new 2 of 3 multisig Electrum wallet
322. Follow the steps in "Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum", using an address from the new Electrum wallet instead of the Coinbase address, to send all bitcoin from the old Electrum wallet to the new Electrum wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows original your black Ledger and processor 1's original blue Ledger to be used together to send bitcoin
323. Processor 1 destroys all "My 24-word recovery phrase" cards for old orange Ledger
    a. Hint: this is an extra safety precaution

Recovery – Processor 2 loses blue Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to the blue Ledger
Warning: assume this evil person also has the PIN code to the blue Ledger
Hint: Bitcoin is still safe since evil person does not have access to 2 of 3 multisig wallet in Electrum
Hint: Even if evil person were to gain access to 2 of 3 multisig wallet in Electrum, Bitcoin is still safe because evil person must have 2 Ledgers to send bitcoin.

324. Processor 2 purchases blue Ledger
325. Processor 2 receives new blue Ledger
326. Follow the steps in "Set Up Ledger Nano S Plus devices" for the new blue Ledger

Warning: the processor 2's original blue Ledger was used to create every Electrum wallet, so the following steps must be taken for every Electrum wallet managed by processor 2.

327. You, processor 1, and processor 2 meet with Ledgers
    a. Hint: you still have original black Ledger and processor 1 still has original orange Ledger
328. Create a new 2 of 3 multisig wallet in Electrum following the steps in "Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate"
    a. Hint: use your original black Ledger, processor 1's original orange Ledger, and processor 2's new blue Ledger to create a new 2 of 3 multisig wallet in Electrum
329. Follow the steps in "Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum", using an address from the new Electrum wallet instead of the Coinbase address, to send all bitcoin from the old Electrum wallet to the new Electrum wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows your original black Ledger and processor 1's original orange Ledger to be used together to send bitcoin
330. Repeat these steps for every Electrum wallet created with the old blue Ledger
331. After all Electrum wallets are recreated, processor destroys all "My 24-word recovery phrase" cards for old blue Ledger
    a. Hint: this is an extra safety precaution

Recovery – You lose black Ledger and Processor 1 loses orange Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to both the black Ledger and the orange Ledger
Warning: assume this evil person also has the PIN codes to both the black Ledger and the orange Ledger
Hint: Bitcoin is still safe since evil person does not have access to Electrum
Warning: if evil person were to gain access to Electrum, bitcoin could be stolen so speed is essential

332. Processor 1 purchases orange Ledger and you purchase black Ledger
333. Processor 1 receives new orange Ledger and you receive new black Ledger
334. You follow the steps in "Set Up Ledger Nano S Plus devices" for the new black Ledger
335. Processor 1 recreates old orange Ledger with new orange Ledger by following the "Recreate old (lost) Ledger" steps
336. Create a new Electrum wallet following the steps in "Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate"
    a. Hint: use your new black Ledger, processor 1's recreated orange Ledger, and processor 2's original blue Ledger to create a new 2 of 3 multisig wallet in Electrum
337. Follow the steps in "Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum", using an address from the new Electrum wallet instead of the Coinbase address, to send all bitcoin from the old Electrum wallet to the new Electrum wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows processor 1's recreated original orange Ledger and processor's original blue Ledger to be used together to send bitcoin
338. You destroy all "My 24-word recovery phrase" cards for old black Ledger
    a. Hint: this is an extra safety precaution

Recovery – You lose black Ledger and Processor 2 loses blue Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to both the black Ledger and the blue Ledger
Warning: assume this evil person also has the PIN codes to both the black Ledger and the blue Ledger
Hint: Bitcoin is still safe since evil person does not have access to Electrum
Warning: if evil person were to gain access to Electrum, bitcoin could be stolen so speed is essential

339. Processor 2 purchases two blue Ledgers and you purchase one black Ledger
340. Processor 2 receives two new blue Ledgers and you receive one new black Ledger
341. You follow the steps in "Set Up Ledger Nano S Plus devices" for the new black Ledger
342. Processor 2 recreates old blue Ledger with new blue Ledger by following the "Recreate old (lost) Ledger" steps
343. Processor 2 follows the steps in "Set Up Ledger Nano S Plus devices" for the second new blue Ledger
    a. Hint: will use recreated blue Ledger to access old 2 of 3 multisig wallets and new blue Ledger to create new 2 of 3 multisig wallets

Warning: processor 2's original blue Ledger was used to create every Electrum wallet, so the following steps must be taken for every Electrum wallet managed by processor 2.

344. Create a new 2 of 3 multisig wallet in Electrum following the steps in "Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate"
    a. Hint: use your new black Ledger, processor 1's original orange Ledger, and processor 2's new blue Ledger to create a new 2 of 3 multisig wallet in Electrum
345. Follow the steps in "Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum", using an address from the new 2 of 3 multisig

wallet instead of the Coinbase address, to send all bitcoin from the old 2 of 3 multisig wallet to the new 2 of 3 multisig wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows processor 1's original orange Ledger and processor 2's recreated blue Ledger to be used together to send bitcoin

346. You destroy all "My 24-word recovery phrase" cards for old black Ledger
    a. Hint: this is an extra safety precaution

Recovery – Processor 1 loses orange Ledger and Processor 2 loses blue Ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to both the blue Ledger and the orange Ledger
Warning: assume this evil person also has the PIN codes to both the blue Ledger and the orange Ledger
Hint: Bitcoin is still safe since evil person does not have access to Electrum
Warning: if evil person were to gain access to Electrum, bitcoin could be stolen so speed is essential

347. Processor 2 purchases two blue Ledgers and processor 1 purchases one orange Ledger
348. Processor 2 receives two new blue Ledgers and processor 1 receives one new orange Ledger
349. Processor 1 follows the steps in "Set Up Ledger Nano S Plus devices" for the new orange Ledger
350. Processor 2 recreates old blue Ledger with new blue Ledger by following the "Recreate old (lost) Ledger" steps
351. Processor 2 follows the steps in "Set Up Ledger Nano S Plus devices" for the second new blue Ledger
    a. Hint: will use recreated blue Ledger to access old 2 of 3 multisig wallets and new blue Ledger to create new 2 of 3 multisig wallets

Warning: Processor 2's original blue Ledger was used to create every 2 of 3 multisig wallet in Electrum, so the following steps must be taken for every 2 of 3 multisig wallet managed by processor 2.

352. You, processor 1, and processor 2 meet with Ledgers
    a. Hint: processor 2 has recreated old blue Ledger
    b. Hint: processor 2 has new blue Ledger
    c. Hint: processor 1 has new orange Ledger
    d. Hint: you have original black Ledger
353. Create a new Electrum wallet following the steps in "Create a Multisignature ("Multisig") 2 of 3 Wallet with Electrum – Ledgers separate"
    a. Hint: use your original black Ledger, processor 1's recreated orange Ledger, and processor 2's new blue Ledger to create a new 2 of 3 multisig Electrum wallet
354. Follow the steps in "Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum", using an address from the new Electrum wallet instead of the Coinbase address, to send all bitcoin from the old Electrum wallet to the new Electrum wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows your original black Ledger and processor 2's recreated blue Ledger to be used together to send bitcoin
355. Processor 1 destroys all "My 24-word recovery phrase" cards for old orange Ledger
    a. Hint: this is an extra safety precaution

Recovery – Processor 1 loses orange Ledger, Processor 2 loses blue Ledger, and you lose black ledger

Your Ledger = black
Your Ledger = orange on loan to processor 1
Processor 2 Ledger = blue owned by processor 2

Warning: assume an evil person has access to all Ledgers
Warning: assume this evil person also has the PIN codes to all ledgers
Warning: Bitcoin is not safe, speed is essential

356. Processor 1 purchases one orange Ledger, processor 2 purchases two blue Ledgers, and you purchase one black Ledger
357. Processor 1 receives one new orange Ledgers, processor 2 receives two new orange Ledgers, and you receive one new black Ledger

358. You follow the steps in “Set Up Ledger Nano S Plus devices” for the new black Ledger
359. Processor 2 recreates original blue Ledger with new blue Ledger by following the “Recreate old (lost) Ledger” steps
360. Processor 1 recreates original orange Ledger with new orange Ledger by following the “Recreate old (lost) Ledger” steps
361. Processor 2 follows the steps in “Set Up Ledger Nano S Plus devices” for the second new blue Ledger
    a. Hint: will use recreated blue Ledger to access old Electrum wallets and new blue Ledger to create new Electrum wallets

Warning: the processor 2’s old blue Ledger was used to create every Electrum wallet, so the following steps must be taken for every Electrum wallet managed by processor 1.

362. Create a new Electrum wallet following the steps in “Create a Multisignature (“Multisig”) Wallet with Electrum”
    a. Hint: use your new black Ledger, processor 1’s recreated orange Ledger, and processor 2’s new blue Ledger to create a new 2 of 3 multisig wallet in Electrum
363. Follow the steps in “Send Bitcoin from Your Multisig Wallet to Coinbase through Electrum”, using an address from the new Electrum wallet instead of the Coinbase address, to send all bitcoin from the old Electrum wallet to the new Electrum wallet
    a. Hint: 2 of 3 multisig wallet in Electrum allows processor 1’s recreated orange Ledger and processor 2’s recreated blue Ledger to be used together to send bitcoin

Recreate old (lost) Ledger

Hint: requires the “My 24-word recovery phrase” card from the original Ledger
Hint: following these steps on a new Ledger will recover the private key associated

364. Remove Ledger Nano S Plus device from package
365. Remove the envelope labeled “Hello” from the package
366. Open the envelope and set all three “Confidential My 24-word recovery phase” cards to the side
367. Remove the USB cable from the package
368. Flip open the Ledger Nano S Plus to expose the USB port and connect the USB cable
369. Connect the other end of the USB cable to your computer
    a. Hint: the screen on the Ledger Nano S Plus will light up when connected
370. Press the right button 5 times until “Restore from recovery phrase” is on the screen
371. Push both buttons at the same time
372. The screen will now say “Choose PIN”
373. Push both button at the same time again
374. You will now enter a PIN of your choosing
    a. Hint: this PIN must be between 4 and 8 digits long
    b. Hint: do not use an obvious combination that an attacker could find like your birthday or the last four digits of your phone number
375. Use the right button to increment the number and the left button to decrement the
376. When you have incremented / decremented to the first number you want for your PIN, push both buttons to move on to the second number
    a. Repeat until you have entered at least four numbers
377. Once you have at least four numbers, a check mark will appear in the number space, if you are finished with your PIN push both buttons with the check mark to signal that you have completed entering your PIN or keep incrementing / decrementing until you reach 8 digits
378. Re-enter the PIN to confirm
379. Push both buttons at the same time on the screen that says “Enter your recovery phrase”
380. Push both buttons at the same time on “24 words”
381. Use the left – right buttons to enter in the first word letter-by-letter, pushing both buttons at the same time to confirm a letter and move on to the next
    a. Hint: Ledger screen will eventually suggest a word, if the suggested word matches your word then press both buttons to select it
382. Push both buttons to confirm the word
383. Repeat for the next 23 words

384. Once the final word is entered, screen will read "Your device is ready"
385. The private key of the old Ledger has been restored and this Ledger can now be used to access your Electrum wallet