CS 6750 Fall 2022 M3

Henry Duong
hduong8 @gatech.edu

***Abstract*—This project will investigate the software-hardware hybrid interface involved in authorizing a transaction using a hardware cryptocurrency wallet, such as the Ledger Nano S.

Authorizing a transaction is one of the fundamental actions that users utilize a hardware cryptocurrency wallet to perform. The specifics of the transaction can be abstracted, as the basic steps that the user needs to undertake are exactly the same. There are unique security concerns to consider for performing this action, as it can potentially involve a transfer of value.

This project is interested in applying the principles of human centered design under these unique constraints, and to investigate the possibility of improving upon the current predominant hardware wallet design without sacrificing security and other domain specific considerations.

1 BRAINSTORMING

1.1 Plan

Brainstorming for redesigns will be done by me on a laptop and a notebook while sitting at a chair. The brainstorming session will last about one hour. The goal is to generate 5 to 6 design alternatives for the Ledger wallet, and select the best 3 for the next step.

The other terminating condition for the brainstorm session is if a maximum time of one hour has been reached.

1.2 Execution

***Brainstorming Notes*—Some of the main pain points that the redesigns need to solve are:

1. Difficult unlocking process
2. Hard to connect to laptop or smart phone via wired connection
3. Hard to read detailed transaction information on a small LCD screen

We make the observation that design alternatives can potentially take two broad approaches:

1. Buttonless design based on a touchscreen interface
2. A screenless design that does not try to display transaction details, but only provides a proof (in the form of a hash or hexstring) to be checked for security.

There are two sub-designs based on the *buttonless touchscreen approach*:

1. USB drive sized thin touchscreen slab design, with hard carrying case to provide protection from accidental damage. This design would be the minimum amount of screen space required for the controls to be relatively easy to use and see the transaction information well.
2. A credit card sized ultra thin touchscreen slab design, with a soft or semi-hard sleeve to provide protection . This design would have a lot more screen space and be able to create bigger GUI control elements as well as display transaction information more clearly. The form factor is meant to be easy to carry inside a wallet.

The screen less approach produces the following design alternatives:

1. Small round form factor that does not have a screen at all and just has a button with fingerprint sensor, and a small built-in speaker and microphone that can read out loud the digest of the transaction parameters, and accept voice inputs for commands
2. Design with a very small LCD screen to display the cryptographic digest and a keypad for input and authentication
3. Design with a very small LCD screen to display the cryptographic digest and a trackpad for gesture based input and authentication

***Brainstorming Notes Scans*—See the scans of the brainstorming notes here.**

1.3 Selection Criteria

The selection criteria for prototyping is on the principle of improving usability and functionality without sacrificing the core reason of why people use hardware crypto wallets in the first place, which is security.

A significant area of usability to improve is the ability for the user to check that the transaction parameters being signed are the correct ones. This is also a core security requirement. I will evaluate this and assigned a score of 1 to 5 to the

alternate design. Another major area to judge on is how easy the unlock process is, without compromising security. These two criteria should be sufficient to pick out three design alternatives to move forward to the next stage. I will estimate the time to unlock based on the alternative design and assign it a score from 1 to 5. A third area to evaluate on is portability and resilience to physical damage. Th ideal hardware wallet should be highly portable and hard to damage. This will also receive a score from 1 to 5.

The sum of these three scores will be added together, and the designs with the top three scores will move to the next stage.

Table 1—Design Alternative Score Table

Design Name **Design Name**	**Transaction Details**	**Unlocking**	**Portability and Resilience**	**Sum**
1. USB form touchscreen	4	4	4	12
2. Credit card form touchscreen	5	5	4	14
3. Speaker and voice input based	3	4	5	12
4. Small LCD with keypad	3	5	4	12
5. Small LCD with trackpad	3	4	4	11

Design 2 has a lead over the rest so will automatically advance. Design 1, 3, 4 have a three way tie. Design 1 is fairly similar to design 2 (only screen size is different), so I will prototype design 3 and design 4.

2 PROTOTYPE 1 - TEXTUAL

Selection—This prototype will be a textual prototype and on the credit card sized ultra thin touchscreen slab design.

Design—As the name indicates, the **form factor** would roughly resemble that of a credit card, where the bulk of the real estate is a touchscreen. The touchscreen would serve the dual purpose of input and output device for this fairly minimalist

design. It would display all the transaction details and also create GUI control elements that users can touch and interact with. The device would be charged wirelessly through a wireless charging protocols such as Qi. The device would have a Bluetooth wireless adapter embedded and rely on that for short range communication with a second device, such as a laptop and a smart phone for signing transactions. The device would not have any ports for wired connections.

For unlocking, the user can also use the touchscreen itself to input a passcode, or use a combination of both the passcode and fingerprint for unlocking the device.

For signing a transaction, key information would be displayed on the touchscreen itself, and the user can interact with the GUI to confirm or reject a transaction. After the transaction is sent, the transaction confirmation information will be displayed on the device touchscreen directly. These functionalities would work in a similar way to existing smartphone touchscreen interfaces.

Evaluation—

1. Functionality
   - Users can authorize transactions on the Ledger wallet while using it with Ledger Live or a third party wallet: **Met**
   - Users can authorize basic balance transfers and smart contract interactions such as staking or DeFi: **Met**
2. Usability
   - Users can unlock the device easily: **Met**
   - Users can authorize transactions while being able to see the transaction information: **Met: good sized touchscreen for displaying information**
   - Users can receive some form of confirmation that the transaction has been sent: **Met**
3. Security
   - The unlock process should be highly secure and prevent unauthorized unlocks as much as possible: **Met: fingerprint and passcode**

Overall, this design meets the listed requirements from M2 extremely well, and offers a very elegant solution to most of the pain points. The only concern is how resilient the form factor is to physical damage. This can be partially mitigated by selling the wallet with a hard or soft sleeve for extra protection against accidental drops or damage during transportation.

3 PROTOTYPE 2 - VERBAL

Selection—This prototype will be a verbal prototype of the speaker and voice input based screenless design.

Design—*Q: Why does the hardware wallet need to display information at all? Why can't it just store the private key and show the information either on the smartphone or laptop screen that it's connected to?*

A: The primary reason for this is to prevent man-in-the-middle attacks. The Ledger wallet's Secure Element accepts in transaction parameters and outputs the encrypted signed bytes. But how do we know the transaction that's shown on the user's laptop or smartphone is the same as the one that's being sent into the Ledger to be signed? If the Ledger application on the laptop or smart phone is compromised, it's very possible for it to display transaction information to the user that does not match what it's actually sending into the Ledger to be signed.

This is why the existing Ledger designs all have an LCD screen that display the transaction parameters, so the user can see what they are actually signing on the Ledger itself, and circumvent man-in-the-middle attacks.

Q: Is there a way to reduce the amount of information to display or convey through the hardware wallet while still verifying the parameters passed in are truthful?

A way to do this is through using common cryptographic primitives, such as a hash function. We can hash the function parameters and generate a hexstring digest so that if any of the parameters is altered, this digest will also change. In this case, then the hardware wallet only needs to display the hexstring digest, which is much shorter than all the transaction parameters potentially are. Then the user can compare this digest to the information on the laptop or smartphone (which should also display the digest) to check.

Q: What would a possible screenless design look like and how would it accept inputs and give outputs?

It would take the form factor of a small round token or button, similar to an Apple Airtag but thicker to store the speaker and microphone. It should be portable enough to put this on a keychain easily. The front side of the device would be a fingerprint sensor that doubles as a button, similar to the "On" button on newer Macbooks.

The device would be charged wirelessly through a wireless charging protocols such as Qi. The device would have a Bluetooth wireless adapter embedded and rely on that for short range communication with a second device, such as a laptop and a smart phone for signing transactions. The device would not have any ports for wired connections. The device will have a built-in speaker that can produce sounds, including reading of a hexstring proof, and it will have a microphone to accept voice inputs.

Q: How would a user check if the transaction parameters passed into the device for signing are truthful?

The device would heavily rely on the smart phone or laptop its connected to while signing transactions to display all the relevant information. The device itself needs to be able to read aloud a hexstring proof that can be checked against what's being displayed on the smart phone or laptop screen. If the two hexstrings match, one that's read aloud by the device and one displayed on the laptop or smartphone screen, then the transactions parameters can be assured to be truthful.

Q: How does a user unlock the device?

Fingerprint and voiceprint.

Q: How does a user sign or cancel a transaction? How is transaction confirmation displayed after being sent?

Through voice commands: confirm or cancel. Or by pressing on the fingerprint sensor: 2 seconds then lift is cancel (short press), 5 seconds then lift is confirm (long press). The transaction confirmation will mainly be displayed on the laptop or smart phone screen, but the device can make a sound as well.

Evaluation—

1. Functionality
   - Users can authorize transactions on the Ledger wallet while using it with Ledger Live or a third party wallet: **Met**
   - Users can authorize basic balance transfers and smart contract interactions such as staking or DeFi: **Met**
2. Usability
   - Users can unlock the device easily: **Met**

- Users can authorize transactions while being able to see the transaction information: **Partially met: user must listen to the hexstring read aloud and compare**
- Users can receive some form of confirmation that the transaction has been sent: **Met**

3. Security
   - The unlock process should be highly secure and prevent unauthorized unlocks as much as possible: **Partially met: fingerprint and voiceprint, which are less secure than some of the other options**

Overall, this design meets the functionality requirements through some clever use of cryptography and engineering, but there are concerns with how well the user can hear the hexstring proof in some environments and the user experience of comparing that to one displayed on screen. But the ultra compact design should be really good for portability and device resilience.

4 PROTOTYPE 3 - WIREFRAME

Selection—This prototype will be a wireframe prototype of the small LCD with keypad design.

Design—The device consists of a small LCD screen on top for output and a keypad at the bottom for input. The device would be charged wirelessly through a wireless charging protocols such as Qi. The device would have a Bluetooth wireless adapter embedded and rely on that for short range communication with a second device, such as a laptop and a smart phone for signing transactions. The device would not have any ports for wired connections.

Unlocking the device:

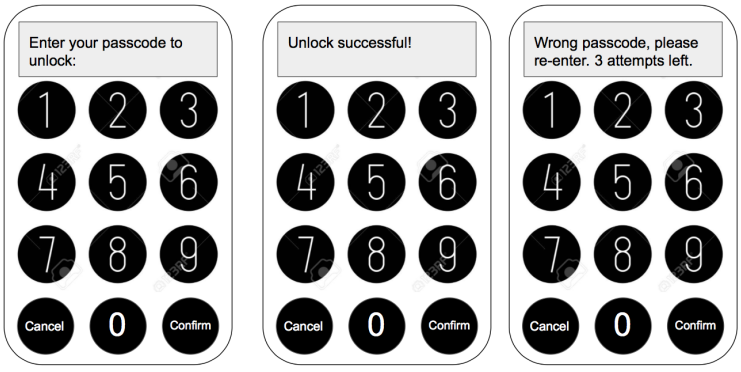

Figure 1—Wireframe for unlocking the device.

Sending a transaction:

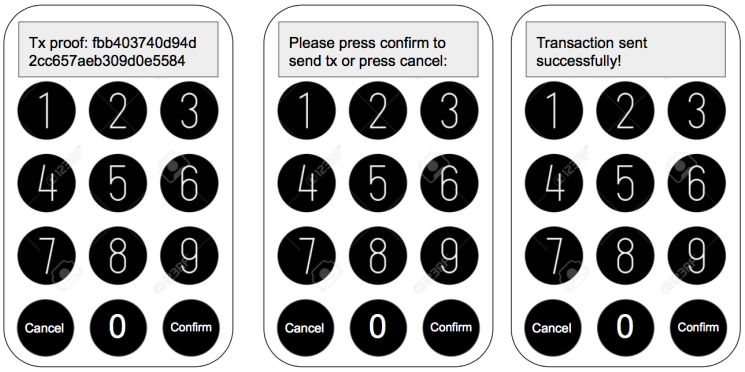

Figure 2—Wireframe for sending a transaction.

Evaluation—

1. Functionality
   - Users can authorize transactions on the Ledger wallet while using it with Ledger Live or a third party wallet: **Met**
   - Users can authorize basic balance transfers and smart contract interactions such as staking or DeFi: **Met**
2. Usability
   - Users can unlock the device easily: **Met: passcode with keypad**
   - Users can authorize transactions while being able to see the transaction information: **Partially met: user read the hexstring and compare**
   - Users can receive some form of confirmation that the transaction has been sent: **Met**
3. Security
   - The unlock process should be highly secure and prevent unauthorized unlocks as much as possible: **Partially met: passcode only, could be brute-forced**

Overall, this design meets the requirements, but is albeit a little more boring. There could be more features incorporated that allow users to input some parameters such as the transfer amount using the keypad instead of inputting on the connected smartphone or laptop only to utilize the keypad more fully.