FAQ: Substrate Hardware Wallet Support

With the widespread misinformation about generic app support and the inherent risks, it's vital to have an informed discussion about the challenges of forking our Zondax app in developer mode to allow blind signing of Substrate messages.

We would like to start the discussion with a FAQ that aims to clarify these concerns and instigate an objective conversation on the topic.

In the following days, we will move over to discuss a design for our next generation app.

Please, find the FAQ here and feel free to ask as many questions as you want.

1. Aren't hardware wallets designed to keep private keys safe?

Hardware wallets do secure your private keys, but without understanding how your private key is used, you remain vulnerable. If you're unable to independently confirm transactions, you risk blind signing. This is why we advise against using devices like Yubikey as hardware wallets.

2. What makes a well-designed Ledger app (hardware wallet) secure?

A well-designed Ledger app operates under the assumption that the browser or client app is fully compromised.

While the user might see "Alice sends Bob 100 DOTs" on their computer screen, a completely different set of bytes could be communicated to the hardware through the USB cable, such as "Sign Alice send Hacker 999 DOTs".

A secure Ledger app would display the actual transaction about to be signed on the device screen, not merely echoing what the browser or mobile phone indicates.

Thus, when the user sees "Alice send Hacker 999 DOTs", they will reject the transaction and avoid exploitation.

3. What happens when only a hash is shown?

Presenting only a hash is barely secure. Even if users see the hash of "Alice sends Bob 100 DOTs", they might end up signing a transaction that represents "Alice send Hacker 999 DOTs". While some argue that users can independently calculate the hash, this is generally impractical and poses a significant risk of compromise.

Let’s assume:

- “Alice sends Bob 100 DOTs” has a hash 77719827b3918273777
- “Alice send Hacker 999 DOTs” has hash 66634987a989172666

- User is using a low quality app.
- User is shown “Alice sends Bob 100 DOTs”, 66634987a989172666 (the bad one!)
- The user will see it on their device. Sign hash 66634987a989172666?
- The hash matches.. Sign, user exploited

People may claim that they can calculate the hash independently, pen and paper, etc.. but the general user will never do that.. And many users will be compromised.

4. Why have Zondax’s Polkadot Ledger apps been safe?

Zondax’s Polkadot Ledger apps prioritize the prevention of blind signing, ensuring the user is always aware of the exact transaction they are signing.

5. What challenges does the Substrate ecosystem present?

The Substrate ecosystem is complex, with standard pallets being composed in various ways by different parachains. When a parachain runtime is compiled, sequential numbers are assigned to each pallet and method, generating a metadata file. However, this doesn't indicate the exact version and fork used, creating complexities and potential risks during transaction signing.

6. How about on-chain upgrades? Why are they conflictive?

Great question!!! We will explain this in detail soon!

7. What is provided today (current app built by Zondax) ?

- Clear signing for most pallets and methods
    - https://github.com/Zondax/ledger-polkadot/blob/main/README.md
    - https://github.com/Zondax/ledger-kusama/blob/main/README.md
- Very extensive testing (more than 3000 tests per app)
- Emulation testing
- Fuzzing
- A large amount of approved security audits
- Support for Ledger Nano S, X, S+ and Stax

8. Why do we dislike Equilibrium's proposal?

Equilibrium is proposing to use an existing Zondax app that directly signs Polkadot/Kusama pallets, removing security checks and allowing blind signing where the original app would have intentionally denied it.

In our opinion, this compromises security and fosters a false sense of safety, which is a regressive move for the ecosystem.

Moreover, we cannot avoid stating that we are shocked that the development plan seems to bluntly claim features and activities that already exist and have been available for a long time.

9. Why did Zondax not build or propose this?

Though very minimal effort is required, we always believed this approach would render the ecosystem insecure. We discourage this practice, particularly for smaller parachains, due to the heightened risks to users.