Radix Ledger Hardware Wallet Support Update

9 July 2021

As we move into the final weeks before the Radix Olympia mainnet launch, we want to give you all an update on support for Radix and the XRD token in the Ledger Nano S hardware wallet. We know many of you plan to use a Ledger device at mainnet launch to hold and stake your XRD tokens, and so we want to explain how that's going to work – as well as provide a little more background on why Ledger support was listed as one of our reasons for our slight mainnet launch delay.

Radix is working on Ledger Nano S

First, Radix and XRD support is working well on Ledger Nano S and we are confident that it will be ready for use at mainnet launch.

The Radix Desktop Wallet (for MacOS, Windows, and Linux) will include the ability to connect a Ledger device and use it with the full functionality provided by the Desktop Wallet – including sending and receiving transactions, as well as staking to and unstaking from Radix validator nodes. We think it will be a great option for members of the community that want the extra peace of mind of using a hardware wallet to protect their private key.

Also, we're happy to be able to say that it is very likely that Ledger Nano X support will be possible. Recent updates from Ledger HQ (more on this below) have made it much more streamlined to support both the Nano S and X devices and so our Ledger app *may* work on both at launch. However, for the time being Ledger Nano S is still where we are doing our testing and so we continue to strongly recommend Nano S for those who want to use a Ledger with high confidence right away.

How loading Radix Ledger support will work

The Ledger hardware devices work by running individual "apps" for each network/token. Each of these apps contain all of the logic needed to derive accounts (from its internal protected seed) and read, display, and sign transactions for the network.

To add support for Radix, you will need to load a Radix Ledger app onto your Ledger device before you can use it with the Radix Desktop Wallet. There are two ways that this can happen:

Sideloading the Radix Ledger app

You can directly download the Radix Ledger app to your computer and from there load it onto your Ledger device; this is called "sideloading". Because this requires no support from Ledger HQ (the company that builds the Ledger device) sideloading is the typical approach for new integrations on Ledger – especially in the case of ensuring support for an unreleased network before its launch – and **this is the approach that Radix is certain to have ready on July 28**.

Sadly, the sideloading process is unavoidably less user-friendly. While those who have experience with a command line and developer tools should be able to work from instructions we will provide on GitHub, this will pose a challenge for many users. So we are currently working on bundling up the sideloading process into more accessible options for each of the supported OSes (MacOS, Windows, and Linux). We will have these options available at least a couple of days before mainnet launch so you can try out the process yourself.

(As an alternative, for those who are simply looking for a good secure method to initially receive XRD tokens and stake them, we will also be publishing a guide of best practices to use the Radix Desktop Wallet without a hardware wallet.)

Loading the Radix Ledger app with the Ledger Live Manager

Ledger HQ provides its own desktop application called Ledger Live that includes a curated Manager area, where you can load new Ledger apps directly onto your device. Radix is committed to being listed in the Ledger Live Manager as soon as possible.

While convenient for users, being listed in the Manager requires an in-depth review process, including submission of test software, documentation, design files, and more to Ledger HQ. Ledger accepts submissions from any project, but typically this submission is done well after a network's launch when evaluation can happen directly using mainnet and when Ledger HQ can see some proof that the network has reached a level of adoption to warrant their priority.

Nonetheless, we provided Ledger HQ with a preliminary submission on July 9th that they may evaluate against a test network. We will be urgently following up with Ledger HQ and are doing everything we can to ensure Radix is squarely on their radar screen (including but not limited to shipments of cupcakes and sweet Radix swag). But be aware that this process is ultimately out of our hands, and approvals can sometimes take months even for high-profile projects.

A little more history on Radix Ledger integration

Ledger integration has been a long road for us, with work starting more than a year ago. While the sections above explain everything you really need to know, we also wanted to give you a little more complete view on how we got here.

Ledger hardware wallets, and other similar products like Trezor, are interesting little devices. Their essential function is to hold a unique unguessable "seed" that is burned into it at the factory, and use that seed to generate addresses on different blockchains and sign transactions for each of those blockchains using it. Simple, right? Well, what you're talking about here is a *tiny computer* that can load and run apps for each blockchain.

Few users want to spend $1000 on this tiny computer, though, and so these companies have done an admirable job of making this possible on a very simple (but secure) piece of hardware. What this means for us, however, is that creating a Radix Ledger app isn't just a matter of porting over some existing Java code – it requires totally re-implementing Radix-specific logic in a highly specialized development environment using a form of C, and some very careful management of a small amount of memory. And this in turn means that we need to carefully design some very specific communication between the Ledger and the "client app" (Radix Desktop Wallet in our case) that it will connect to.

Nonetheless, our hero Alex Cyon surmounted these challenges and completed a functional integration some time ago, we were pleased, and we put this work on the shelf for a time closer to mainnet launch.

Then the realities of software development happened. Our decision to move to a much more streamlined and accessible JSON-RPC connection to nodes to create transactions meant a refactor of the Desktop Wallet. And working through the final details of things like emissions, network fees, validator registration, etc. – including some great feedback during Betanet – meant some relatively minor refactoring of our "transaction model", basically how the contents of transactions are put together.

These changes – otherwise manageable and typical for a complex software development – had an outsize effect on the Ledger integration. Previous assumptions that had to be frozen into exquisitely optimized C code shifted, each time requiring substantial rework and retesting, involving many members of the development team.

Around the same time, we became aware of a substantial update from Ledger HQ to the reference code that they provide as the basis of Ledger apps. Wonderfully, this new reference code made universal apps for Nano S and X possible – as well as offering a number of important general improvements. Reimplementing with our new API/wallet/TX model as well as the new reference code became the new mission for our hero, and he has delivered.

And this brings us to the present. We're very pleased to get a Radix Ledger app submitted to Ledger HQ ahead of mainnet launch, and hope that this will help us put us in the best possible position to be listed on the Ledger Live Manager as soon as possible while providing a sideloading solution for our earliest Radix users, supporters, and token holders.