
# The GridPlus Lattice1 Hardware Wallet

## Overview

The GridPlus Lattice1 and SafeCards comprise the only cryptocurrency hardware solution providing active signing security for an unlimited number of wallets. This flexibility combined with enterprise-grade protection against physical and digital attack vectors makes GridPlus the right choice for anyone doing more than simply holding crypto.

This guide is intended to explain the GridPlus Lattice1 and SafCards for reviewers, media, affiliate sales partners, and anyone else looking to learn more.

## Introduction

The Lattice1 is the hardware wallet for every web3 user who actively signs transactions. Today's crypto users sign every day to curate their NFT collections, log into sites,

interact with DeFi protocols, and more. Legacy hardware wallets put these users at risk because they do not provide signing security for more than simple value transfers.

Why is this a problem? When users can't see precisely what they're signing on a separate secure device, they're likely to approve malicious transactions themselves. Since most hardware wallets don't provide signing security, users simply click to approve all signing requests without review - it's called blind signing.

When your computer or phone is compromised it can display a signing request that is different than what you're actually approving. The *only* way to prevent this is with a separate device that clearly displays the transaction details.

Early hardware wallets were designed before most signing took place on smart contract chains, so they were designed with firmware and screens meant only to confirm the recipient address when you sent Bitcoin. Most hardware wallet companies still sell products built on this foundation which puts their customers at risk.

Blockchain technology is constantly evolving and more complex transactions and use cases demand a different and more flexible approach to keep users safe from new risks as they arise.

## Why do all cryptocurrency users need hardware wallets?

Hardware wallets accomplish two goals:

1) Securely store your keys.
2) Provide a secure screen to verify what you're signing.

Secure key storage protects against attack vectors including direct theft of private keys and malware designed to automatically sign transactions.

A secure screen with readable transactions prevents against social engineering attacks designed to get a user to sign a malicious transaction, misleading websites, web3 site hacks misdirecting a user, and more.

Many kinds of consumer electronics feature secure chipsets which could store a private key, but without secure signing this is of limited use. Computers and phones use generalized operating systems that don't limit what is displayed on your screen and therefore can never be used for secure signing.

# What unique features make the Lattice1 the best hardware wallet on the market?

**Infinite Secure Wallets:** Managing more than one wallet is cumbersome; the Lattice1 and SafeCards let you manage every wallet you've created from a single device and pair addresses from each with your favorite software.

**Cost-Effective:** Most crypto users use more than one wallet. With the Lattice1 you don't need to buy a new hardware device for each seed phrase, making it more cost-effective than alternatives.

**Enterprise-Grade Hardware Security:** The Lattice1 is designed to be secure even when a sophisticated hardware hacker has their hands on your device. An anti-tamper mesh acts as a tripwire which will erase your secrets instead of letting your private keys be exported to a computer so that your PIN can be brute-forced.

**Easy Secure Backups:** Using plaintext mnemonics seed phrases as backups on paper, metal, or in the cloud means anyone who can see these words has unlimited access to your crypto. GridPlus SafeCards make backing up and restoring your accounts fast, simple, and reliable all while keeping your secrets safe from prying eyes.

**See What You're Signing:** Hardware wallets empower users to keep themselves safe by checking the signing request they see on their computer or phone against a secure screen to ensure they're not the victim of an attack. The Lattice1 parses transaction data to clearly show users the most important information so that they can make safe decisions at a glance.

Go to the Lattice1 product page to learn more about these features.

# Frequently Asked Questions

### Where is the Lattice1 manufactured?

All Lattice1 devices are manufactured in Austin, Texas in an ITAR compliant facility used by defense contractors.

### Will this work with my operating system?

You can pair any device that can connect to a web browser on the same WiFi network as your Lattice1.

**Why does the Lattiice1 connect with WiFi instead of USB – isn't that dangerous?**

The Lattice1 has a smaller attack surface than USB hardware wallets. This is made possible by two completely separate hardware environments inside the case, ensuring your private keys are never exposed to the outside world.

The General Compute Environment runs Linux and provides connectivity. The Hardware Security Module generates signatures and is completely cut off from the outside world.

Requests and signatures pass through a size-limited mailbox that only one side connects to at a time.

Separating the GCE from the HSM yields many security benefits over legacy wallets:

- The HSM is isolated from the outside world.
- No accessible factory or engineering debug features.
- Fixed mailbox size eliminates overflow attacks.
- Risk of supply chain attacks greatly diminished.

The secure mailbox protects your assets from remote attacks and the anti-tamper mesh protects them from physical attacks.

**Are my private keys stored on the Lattice1 or the SafeCards?**

The Lattice1 hardware wallet stores a single seed phrase which lets you use an unlimited number of addresses. You don't need SafeCards to use the Lattice1.

SafeCards extend the functionality of the Lattice1: each card can hold a separate seed phrase. Simply insert a SafeCard, enter your six-digit PIN, and then you can sign for any of the addresses on that card. Tools such as MetaMask let you simultaneously pair as many addresses from your Lattice1 and different SafeCards as you would like so you can enjoy hardware security for all of your wallets with one device.

SafeCards are also a secure way to backup your accounts so you don't have to rely on risky written seed phrases. Users can easily make copies of backups and restore accounts to their Lattice1 without entering their seed phrase.

**How many SafeCards come bundled with the Lattice1?**

The Lattice1 includes one SafeCard and additional packs of two are available at https://gridplus.io/products/safe-cards.

**Can I still recover my SafeCard backups if I don't have a Lattice1 anymore?**

We believe when you buy a hardware product you should have complete control and ownership of it so we have provided open-source software to use a third-party card reader to manage your SafeCards and recover your private keys and seed phrase.

**How do I know the seed phrase I generate is truly random?**

The Lattice1 follows NIST standard SP800-90 for generation of random numbers using multiple sources of entropy. The Lattice1 HSM's random noise signal comes from a ring oscillator that takes into account temperature and voltage variations within the secure enclave, a unique hardware fingerprint of each device's PUF chip (physically uncloneable function; each Lattice chip is unique like a snowflake), as well as additional sources of noise. Strict adherence to this standard and using physical sources of entropy rather than relying on software puts the Lattice1's entropy a class ahead of other commercially available cryptocurrency wallets.

For an additional layer of assurance, users can always securely generate a seed phrase with the method of their choosing and import it into their Lattice1.

**How can I ensure that my GridPlus hardware and firmware is authentic and has not been tampered with in any way?**

The Lattice1 includes a tool that lets any user quickly and easily verify the integrity of their GridPlus devices and firmware.

Every Lattice1 has a unique ID key pair saved on it when it is created at the factory. The public key from this pair is signed by our issuer multisig and the resulting signature is saved in the device – we call this signature "the certificate."

When you use the security verification feature, your Lattice's ID key signs a user created message and exports the result along with the certificate. The data is displayed as a QR code and can be scanned, bringing the user to a gridplus.io subdomain page which informs them whether both the Lattice1's ID key signed the provided message (what the user just typed in should be on the page as the message) and if the card's ID key was itself signed by GridPlus.

If everything is correct a user is shown a clear message showing that their Lattice1 is secure and has not been tampered with in any way.

# Additional Resources

Media Kit: Logos, product shots, our branding guide, and other assets.

Knowledge Base: More in-depth information on the Lattice1 and SafeCards.

YouTube: Tutorial videos and more.

# Affiliate Sales

You can sign up for our affiliate sales program and create a referral link to receive a commission on Lattice1 sales at affiliate.gridplus.io.

Need anything else? Email us at affiliates@gridplus.io.