

VAULT12

OVERVIEW

Vault Platform Integration

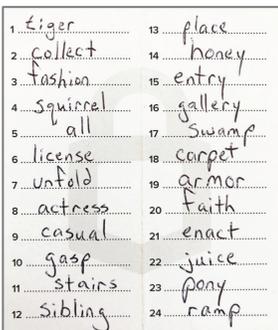
Integration Summary

In this document, we describe how companies can integrate with the new Vault12 distributed storage platform for storing current and future, high-value cryptographic assets.

1. Introduction

Cryptocurrencies today are just at the beginning of a new shift towards empowering individual ownership secured by fundamental cryptography. In looking at how crypto assets are protected in everyday scenarios, it turns out that everyone relies on paper to back up their digital crypto assets.

The standard, de facto backup mechanism for digital crypto assets is and has always been, paper. In a survey of the 20 top wallets, 18 had only one mechanism to back up the all-important seed-phrase or private key – this was to write down the seed phrase onto a piece of paper and store it securely. The other 2 wallets also provided a paper backup option but added the ability to store an encrypted digital version, presumably on a USB device, or more likely, on a local laptop or in the cloud.



1.1 The weakest link in crypto

Storing your valuable backup on a piece of paper obviously has numerous drawbacks for the casual crypto owner, including



Paper backups and wallets are often kept in the same location and are therefore subject to the same risks as the owner's main wallet: fire, natural disasters, burglary, etc.



Casual owners are likely to forget the "secret storage location" of their piece of paper after a few years.



By nature, paper is not a long-term storage medium, and can easily become unreadable after years through natural wear and tear.



By nature, paper is not a long-term storage medium, and can easily become unreadable after years through natural wear and tear.



Casual users are confused about the role and function of paper backups and usually blame the wallet vendor for any incidents regarding wallet backup and recovery. That creates a significant load of unresolvable cases for customer service and increases customer dissatisfaction with the wallet brand.



In financially unstable countries where cryptocurrency ownership is crucial, access to bank safe deposit boxes (the usual storage location of paper backups) is usually restricted during any bank crisis, exactly when users might need immediate access to their crypto-asset

VECTOR KOD

This list can go on and on. Essentially, while designed with good intentions to protect crypto owner’s assets from criminals and hackers, over time, paper backups have become the actual leading cause of people losing access to their crypto assets. It creates a false sense of security because any random event can destroy the user’s main wallet, which is when they realize they actually do not remember or cannot access the paper backup they thought they had. As the number of cryptocurrency owners grows, the problem, losses and resulting customer dissatisfaction with securing cryptocurrency assets will only grow – with users often directing blame at the wallet vendors for their loss.

Moving from paper backups to Vault12 distributed storage solves all these legacy storage issues and empowers user to backup any number of high value digital assets in a highly secure way.

1.2 Inheritance

One of the reasons why a seed phrase back up may be needed is in the event of crypto assets being inherited. There have been documented cases of the inheritor not being able to access assets after the owner has passed away. The Vault12 solution was designed to cater to this eventuality and to provide a path for the executor of an estate to recover seed phrases at an appropriate time in the future.

1.3 Additional Risks

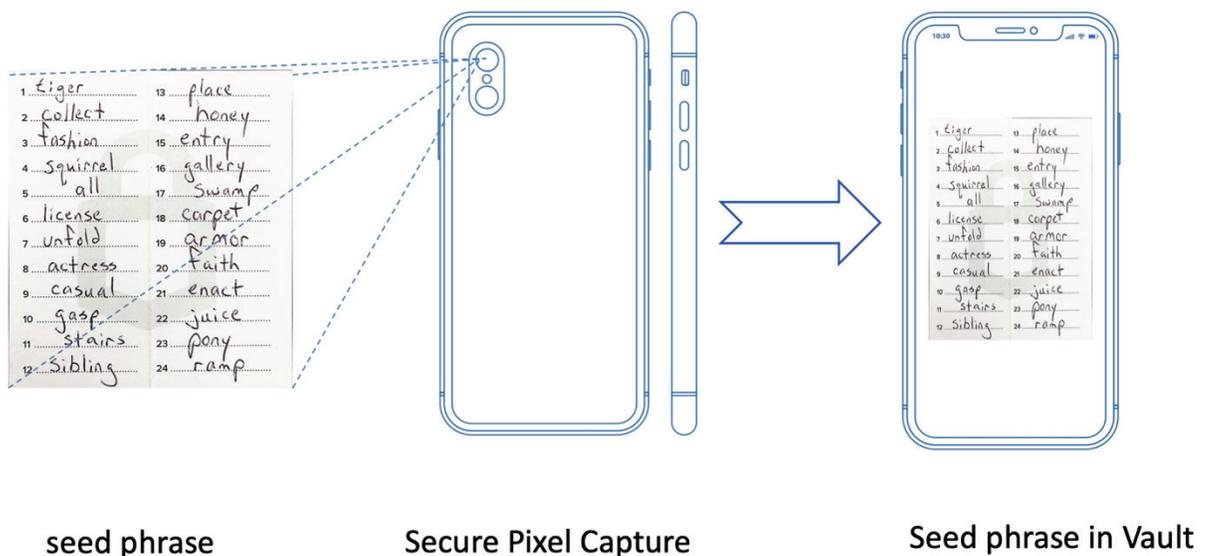
Risk	Traditional	Vault12
Local Device storage	Devices can be lost or stolen	Even when devices are lost, the backup can be recovered
Screenshot	Screenshots can be obtained by direct access	No screenshots are ever stored in cloud or on device
Cloud Backup	Cloud backups are susceptible to hacking	Nothing is backed up to servers or cloud – or indeed locally.
Exchange	Exchanges have been repeatedly hacked and continue to be targets	There is no central location where seed phrases are stored
Dropbox	Storage in folder sharing apps still creates the possibility that access to seed phrases may be granted accidentally or passwords hacked	There is no central location where seed phrases are stored
Customer Service Load	Most consumers are very used to being able to recover their bank account passwords, so losing a seed phrase will result in inquiries directly to support. Unlikely that new consumers will understand why seed phrases are non-recoverable by Support.	Seed phrases are easily recovered if stored via Vault12. Vendors who wish to be part of the recovery solution can make sure that they Guard their customer Vaults (for a small fee).

2. Integration with Vault12

2.1 Legacy Integrations

Millions of people have legacy paper backups that are a constant source of risk, both of disclosure but also of loss. We offer two scenarios how to transfer legacy paper backups into Vault12.

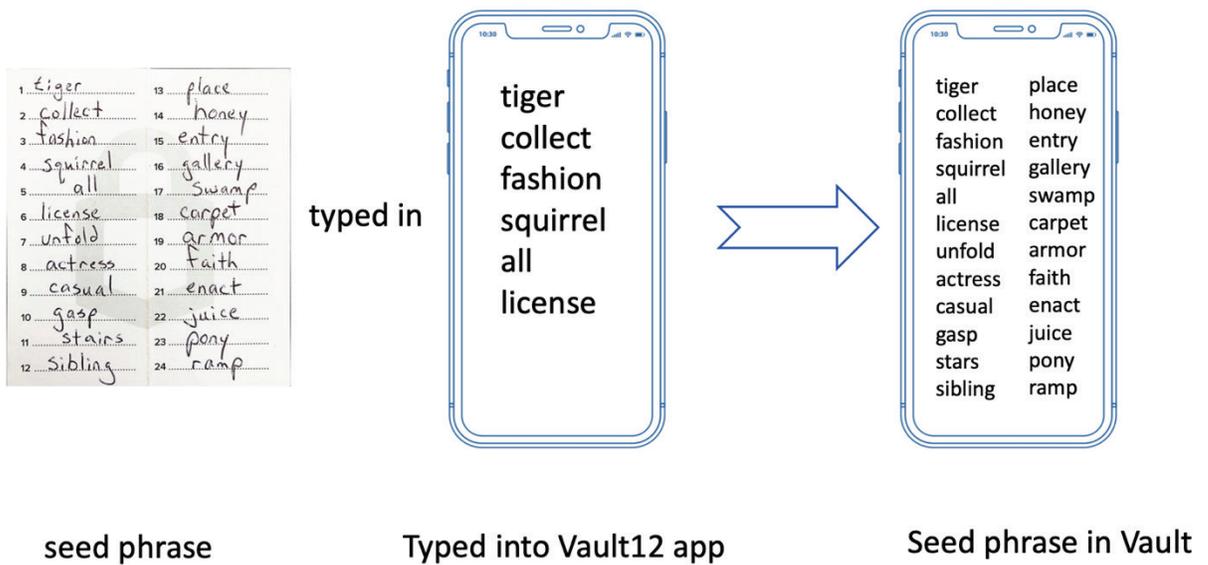
2.1.1 Pixel capture



The Vault12 camera mode uses direct connection to the phone camera to capture hardware pixel data into its memory buffer. That buffer is immediately encrypted and sharded for p2p transmission to the Guardian devices. We use native hardware directly, and completely bypass any local “Camera” or “Photo” APIs that might create a file from user picture.

This approach allows millions of existing wallet customers to upgrade their paper backup quickly and securely into a fully digital form and get rid of constant risk factor exposed by the paper copy.

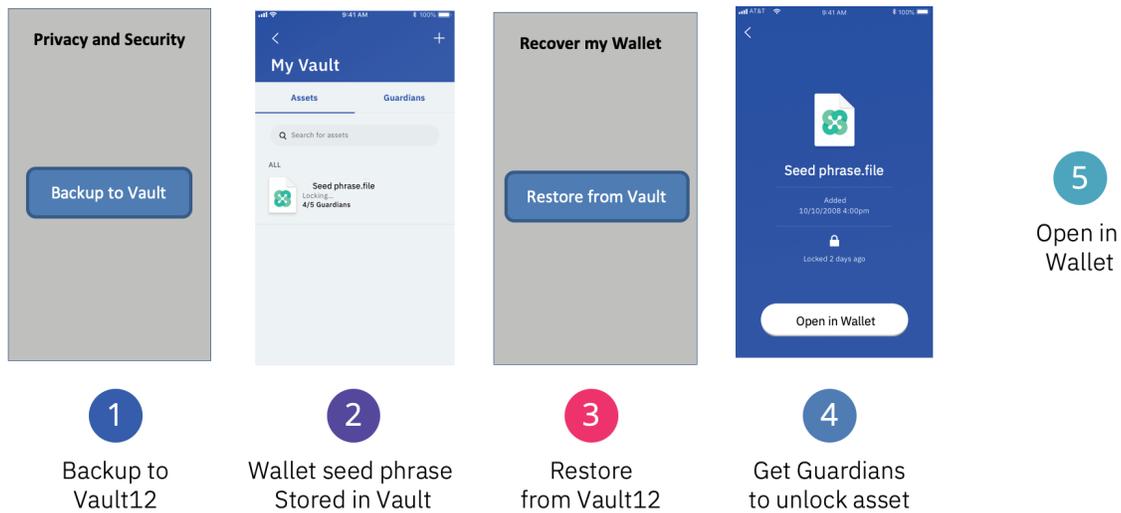
2.1.2 Secure Note



For those users who prefer not to use the camera for paper backup, the same functionality is offered via a "Secure Note" function. The user enters their seed phrase manually, which is connected to the memory-only buffer.

After the note is complete, the buffer is encrypted, and sharded to disk and the buffer is zero-ed out.

2.2 Mobile integrations

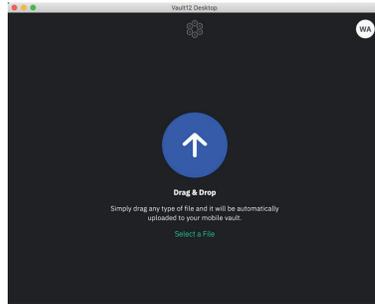
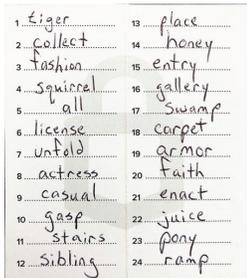


If a user wallet is already set up and allows for export of a seed phrase or similar root key, Vault12 can support a secure app-to-app communication mode to establish a secure channel between wallet app and Vault12 in a potentially insecure OS shared environment.

During backup flow, Wallet app initiates the backup process, and Vault12 places all user assets received from the Wallet app into the Vault.

During restoration flow, Vault12 initiates the restore, and sends recovery assets to be processed by the Wallet app.

2.4 Desktop integrations



1. Drag file from desktop
2. Desktop Utility syncs with mobile Vault
3. File can be recovered via Guardians

2.4.1 Native integration

For wallets that include desktop frontends, instead of app-to-app integration, Wallet vendors can opt to compile the “Vault12 desktop” core library into their frontend client. This removes additional steps of the app-2-app communication setup, and the Vault12 mobile client can communicate directly with desktop app using our existing desktop utility protocols.

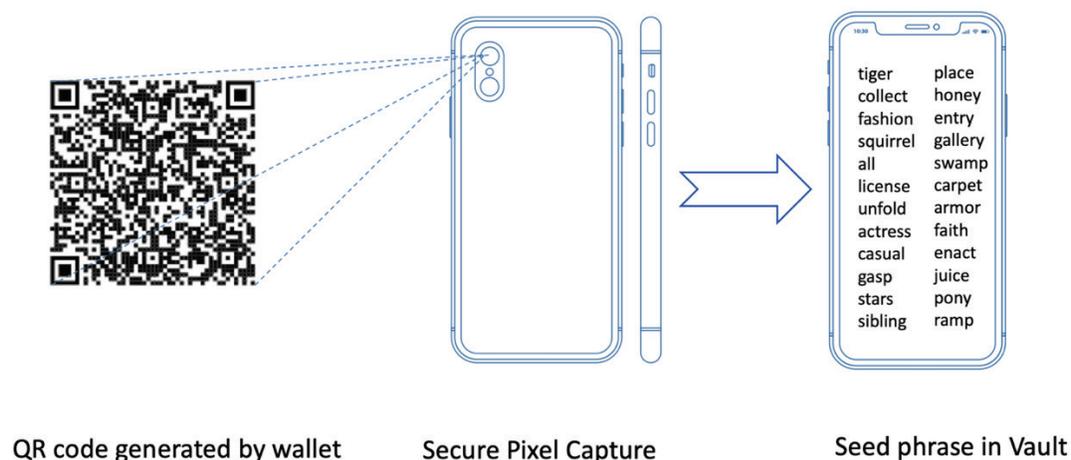
Wallet desktop application will be using internal API following the same workflow concepts: putting assets into Vault or restoring wallet state from assets received from the Vault. Asset form can be any file format selected by Wallet vendor.

2.4.2 Application integrations

Wallet vendors who prefer not to link with Vault12 libraries, can choose a number of other options to integrate with Vault12 Desktop Utility (VDU).

- Communicate via shared encrypted shared folder messaging protocol similar to [3.2](#). That option requires the least amount of involvement from the end user.
- For power users who prefer more direct control, we can encrypt the backup payload using any standard crypto libraries (AES, NaCl, etc) and export backup data as binary file with custom vendor extension. User manually drags and drops export file into VDU, which recognizes vendor metadata for custom processing. Backup encryption key can be derived from user password (making knowledge of the password a requirement for restoration) or passed along to VDU for sharding as part of backup metadata (allowing for 0-dependency restore).

2.5 QR Code Integration



If a wallet is physically separate from the phone (hardware wallet or desktop app), high security integration can be established using QR codes as a communication channel. In this case communicating app displays series of QR codes to the camera of the receiving app. The protocol follows same approach as “App to App” integration without the unnecessary key fingerprint verification step. Sending application breaks communication traffic into 1-2kb messages each generating one QR code.

3. Summary

The next generation of crypto owners will not understand why they have to use paper and lose the convenience of what they have come to know as standard financial services practice – e.g. bank account passwords, which are recoverable. In the near future, the security levels we expect for today’s cryptocurrency storage will apply to fully digital house keys, car keys, real estate titles and a variety of personal property and documents that are currently secured by cryptographic keys. A better solution is needed to bring security and backup to consumers at the forefront of this digital economy.

The Vault12 platform has been designed with integration in mind to make it as easy as possible for consumers to safely backup their crypto assets, as well as giving wallet providers multiple options to integrate depending on where they are in the product cycle. We believe a simple path to making crypto safe will help expand the crypto economy and foster trust of this new approach.

About Vault12

Vault12 enables you to safeguard your cryptocurrencies, using a cryptographically secure network made up of trusted people and devices. The company has introduced a fully-private, self-managed and highly-reliable cryptostorage system that uses an approach invented by Adi Shamir, one of the world's foremost cryptographers and co-inventor of the RSA algorithm. The cryptographic algorithm of Hierarchical Threshold Shamir's Secret Sharing (HTS3) combines the personal control and complete privacy of self-managed cryptostorage with the reliability, high redundancy and elimination of a single point of failure associated with delegated storage.

For more information, visit vault12.com