lokblok

toughbox

Toughbox secure backup and recovery for digital secrets

WHAT IS IT?

Introducing Toughbox, a revolutionary cloud API service designed to provide unrivalled security and peace of mind for the safe backup and recovery of BIP39 seed phrases and cryptocurrency private keys.

HOW DOES IT WORK?

Toughbox achieves exceptional security by enrolling your secrets for recovery through a set of trusted guardians, designated by you. These Guardians neither store nor have access to your backup, ensuring that your secrets remain confidential at all times. When needed and authorized, your secret splits are recovered and reconstructed on your system.

The SDK includes client and guardian libraries for seamless integration into your applications. Compatible with Windows, MacOS, Linux, Android, and iOS, Toughbox provides a simple REST API implementing remote procedures for enrolling and recovering secrets.

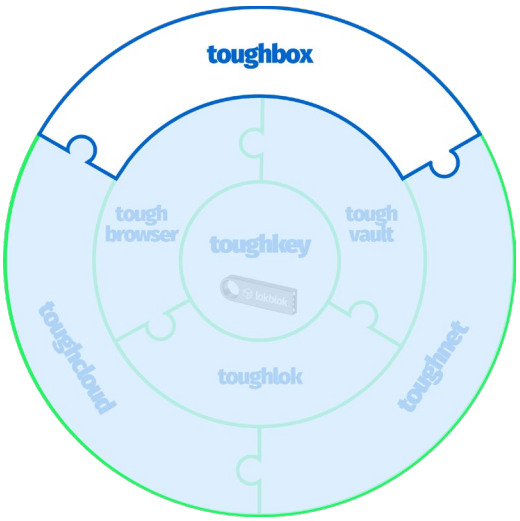
WHY USE IT?

As cryptocurrencies become increasingly valuable and widely adopted, the need for secure backup and recovery solutions for private keys has become more critical than ever. Private keys are what allows users to access, manage, and transact with their digital assets. Losing access to a private key can result in the permanent loss of the associated cryptocurrency holdings.

Despite many people being aware of the criticality of keeping private keys safe, many have not considered what would happen if they did lose their key or backup seed phrase.

Whether they're using a hardware or a software wallet, various scenarios can arise where users may need to recover their private keys. One common situation is hardware failure or loss, such as a damaged computer or a misplaced mobile device. In these cases, users who have not securely backed up their private keys risk losing access to their cryptocurrency holdings, as the keys may be unrecoverable from the damaged or lost device. Another scenario is forgetting the password or seed phrase associated with a software wallet. Without a proper recovery mechanism in place, users could find themselves locked out of their digital assets.

Moreover, security threats like hacking, malware, phishing attacks or even confiscation by authorities can compromise the safety of users' private keys. In these instances, having a reliable backup solution is essential to protect and recover the keys, minimizing the potential loss of valuable digital assets. In time, hardware becomes outdated, and individuals



Lokblok Zero Trust Ecosystem

upgrade their laptops or phones. Users who wish to transfer their cryptocurrency wallets or applications to new devices or systems also need a secure and seamless method for recovering their private keys.

SO, WHAT ARE THE OPTIONS FOR BACKING UP YOUR PRIVATE KEY?

Writing down a seed phrase on paper or engraving it into metal and storing it in a secure location may seem like a simple solution to the problem of backing up and recovering private keys, but these methods come with their own limitations and risks that make them less than ideal.

Paper is vulnerable to fire, water, and environmental factors like humidity and temperature fluctuations. In the event of a natural disaster or an accident, a paper backup may be destroyed, leaving users without access to their digital assets.

Similarly, engraving the seed phrase into metal provides a more durable solution, but it's not without drawbacks too. Metal backups are still prone to theft, loss, or damage if stored in an insecure location. Both paper and metal backups require users to be vigilant about the physical security of their seed phrases, which adds an unneeded extra layer of stress and complexity to the management of digital assets. Both act as a single point of failure for backups.

A digital solution like Toughbox, on the other hand, offers several advantages over traditional physical backups. With seed phrases and keys distributed over a user defined number of guardians, there is no longer a single point of failure for the backup. Users can access their seed phrases remotely, recover them in case of device loss or failure, and easily update or manage them as needed. Furthermore, there is no need to trust one person / location / entity with your keys, further building on the idea of 'trustlessness' and the mantra of 'Your keys, your crypto'.

TOUGHBOX OFFERS:

Uncompromising security: Your secrets are never stored on any system, eliminating the risk of exposure or theft.

Flexible recovery options: Designate guardians to assist in recovering your secrets when needed without granting them access to your backups.

Versatile compatibility: Works with various operating systems and mobile platforms, making it an ideal solution for developers.

Seamless integration: The SDK allows for effortless integration into your applications, streamlining the enrolment and recovery process.

TECHNICAL SPECIFICATION

Rest API
Patented Secret Sharing
Hardware, Software & Hybrid Keys
Library that supports multiple languages

SUMMARY

Toughbox is the easy choice for developers looking to include a secure method for back-up and recovery of BIP39 seed phrases and cryptocurrency private keys in their applications. However, it's not just for cryptocurrency – it can be used for recovery of any secrets. By ensuring secrets are never stored on any system, Toughbox provides unrivalled security and peace of mind. With its versatile cross-platform compatibility and seamless integration capabilities, Toughbox is the ideal choice for backup and recovery of secrets.