

# A Salesforce Administrator Guide to Web3 Wallets

Web3 Enabler



## Table of Contents

[Overview](#)

[Best Practices for Key Management](#)

[Create Policies Around Wallet Access](#)

[Key Web3 Wallet Terms](#)

[Types of Web3 Wallets](#)

## Overview


Below are several icons you may see throughout this document.



Ideas: This icon identifies material that may be good to remember or helpful hints.




Notes: This icon tells you there is additional module context or information.

 Warnings: This icon notes activities that done or not done, may have negative outcomes.

## Best Practices for Key Management

A user's Web3 wallet address is a public key belonging to that user. Other individuals and businesses need that public key to send funds to the user. Those wallet addresses, as well as their associated transactions, are also visible on Block Explorers, such as [Etherscan](#) for Ethereum or [Blockcypher](#) for Bitcoin.

A user's wallet also has a private key, which must only be known to that user. If a malicious actor discovers a user's private key, that bad actor can steal that users' funds!

 Notes: Web3 Enabler only stores public keys. For EVM networks, this is the public key to the "Account" you are using with Web3 Enabler.

For UTXO networks, this is the "extended public key" that creates transactional addresses. In all circumstances, Web3 Enabler relies upon publicly available information to report transactions. Only the "wallet holder" with the private keys can "spend those coins" – including transferring them to a fiat off-ramp.

## Create Policies Around Wallet Access

Whoever controls the private keys controls the cryptocurrencies. You should generally have at least two people with access to the wallet to avoid losing your coins. You should decide how much crypto exposure you want to have, and convert to fiat when your coins on hand exceed it. One of Web3 Enabler's wallet management best practices is that it uses your public key only, and does not have access to your coins.

## Key Web3 Wallet Terms

**Seed Phrase** - A seed phrase (sometimes called a recovery phrase) is a randomly generated set of words that a crypto wallet user uses as a proof of ownership.

⚠️ Warnings: If a user loses his/her/their seed phrase, that user could lose access to the funds contained in that wallet. Also, if a seed phrase is stolen, a bad actor may be able to steal the wallet owner's funds.

💡 Ideas: Therefore, it is recommended, as a best practice, get a wallet owner to securely store a seed phrase as soon as it is generated.

**Custody** - The term, custody, when applied to web3 wallets, describes who holds a wallet user's private keys and is therefore responsible for users' funds.

A custodial wallet, such as the wallets offered by [Coinbase](#) or [Kraken](#), holds a user's private keys.

💡 Ideas: Custodial wallets are good for non-technical users who do not want to manage private keys.


With a non-custodial wallet (also known as a self-custody wallet), such as [Uniswap](#), [Trust Wallet](#) and [MetaMask](#), users hold and are responsible for managing their own private keys.

## Types of Web3 Wallets

**Software Wallet** - Software wallets, such as [MetaMask](#), [Exodus](#) and [Coinbase Wallet](#), allow users to access their digital assets from applications (web, desktop or mobile) or browser extensions.

⚠️ Warnings: Since software wallets are, by definition, online, wallet activity is easily traceable, which is good for transparency but suboptimal for potential security risks to those wallets.

**Hardware Wallet** - Hardware wallets, such as [Ledger](#) and [Trezor](#), are devices that can be purchased and used for offline storage of digital assets.

 Warnings: Since hardware wallets are, by definition, offline, wallet activity is less easily traceable than it is on software wallets but offer enhanced security and privacy for users' assets.

**Multi-Signature Wallet** - Multi-Signature wallets (also called “multi-sigs”) are web3 wallets that have enhanced security settings that typically require two or more people to authorize an outbound transactions.