Paper Wallets using the Solana CLI

This document describes how to create and use a paper wallet with the Solana CLI tools.

We do not intend to advise on how tosecurely create or manage paper wallets. Please research the security concerns carefully.

Overview

Solana provides a key generation tool to derive keys fromBIP39 -compliant seed phrases. Solana CLI commands for running a validator and staking tokens all support keypair input via seed phrases.

Paper Wallet Usage

Solana commands can be run without ever saving a keypair to disk on a machine. If avoiding writing a private key to disk is a security concern of yours, you've come to the right place.

Even using this secure input method, it's still possible that a private key gets written to disk by unencrypted memory swaps. It is the user's responsibility to protect against this scenario.

Before You Begin

- Install the Solana command-line tools

Check your installation

Check thatsolana-keygen is installed correctly by running:

solana-keygen --version

Creating a Paper Wallet

Using thesolana-keygen tool, it is possible to generate new seed phrases as well as derive a keypair from an existing seed phrase and (optional) passphrase. The seed phrase and passphrase can be used together as a paper wallet. As long as you keep your seed phrase and passphrase stored safely, you can use them to access your account.

For more information about how seed phrases work, review thisBitcoin Wiki page .

Seed Phrase Generation

Generating a new keypair can be done using thesolana-keygen new command. The command will generate a random seed phrase, ask you to enter an optional passphrase, and then will display the derived public key and the generated seed phrase for your paper wallet.

After copying down your seed phrase, you can use thepublic key derivation instructions to verify that you have not made any errors.

solana-keygen new --no-outfile If the--no-outfile flag isomitted , the default behavior is to write the keypair to~/.config/solana/id.json , resulting in afile system wallet . The output of this command will display a line like this:

pubkey: 9ZNTfG4NyQgxy2SWjSiQoUyBPEvXT2xo7fKc5hPYYJ7b The value shown afterpubkey: is yourwallet address .

Note: In working with paper wallets and file system wallets, the terms "pubkey" and "wallet address" are sometimes used interchangeably.

For added security, increase the seed phrase word count using the--word-count argument For full usage details, run:

solana-keygen new --help

Public Key Derivation

Public keys can be derived from a seed phrase and a passphrase if you choose to use one. This is useful for using an offline-generated seed phrase to derive a valid public key. Thesolana-keygen pubkey command will walk you through how to use your seed phrase (and a passphrase if you chose to use one) as a signer with the solana command-line tools using theprompt URI scheme.

solana-keygen pubkey prompt:// Note that you could potentially use different passphrases for the same seed phrase. Each

unique passphrase will yield a different keypair. Thesolana-keygen tool uses the same BIP39 standard English word list as it does to generate seed phrases. If your seed phrase was generated with another tool that uses a different word list, you can still usesolana-keygen , but will need to pass the--skip-seed-phrase-validation argument and forego this validation.

solana-keygen pubkey prompt:// --skip-seed-phrase-validation After entering your seed phrase withsolana-keygen pubkey prompt:// the console will display a string of base-58 characters. This is thederived solana BIP44wallet address associated with your seed phrase.

Copy the derived address to a USB stick for easy usage on networked computers If needed, you can access the legacy, raw keypair's pubkey by instead passing theASK keyword:

solana-keygen pubkey ASK A common next step is tocheck the balance of the account associated with a public key For full usage details, run:

solana-keygen pubkey --help

Hierarchical Derivation

The solana-cli supportsBIP32 andBIP44 hierarchical derivation of private keys from your seed phrase and passphrase by adding either the?key= query string or the?full-path= query string.

By default,prompt: will derive solana's base derivation pathm/44'/501' . To derive a child key, supply the?key≠ query string.

solana-keygen pubkey prompt://?key

0 /1 To use a derivation path other than solana's standard BIP44, you can supply?full-path=m/// .

solana-keygen pubkey prompt://?full-path

m/44/2017/0/1 Because Solana uses Ed25519 keypairs, as perSLIP-0010 all derivation-path indexes will be promoted to hardened indexes -- eg.?key=0'/0' ,?full-path=m/44'/2017'/0'/1' -- regardless of whether ticks are included in the query-string input.

Verifying the Keypair

To verify you control the private key of a paper wallet address, usesolana-keygen verify :

solana-keygen verify < PUBKEY

> prompt:// where is replaced with the wallet address and the keywordprompt:// tells the command to prompt you for the keypair's seed phrase;key andfull-path query-strings accepted. Note that for security reasons, your seed phrase will not be displayed as you type. After entering your seed phrase, the command will output "Success" if the given public key matches the keypair generated from your seed phrase, and "Failed" otherwise.

Checking Account Balance

All that is needed to check an account balance is the public key of an account. To retrieve public keys securely from a paper wallet, follow thePublic Key Derivation instructions on anair gapped computer . Public keys can then be typed manually or transferred via a USB stick to a networked machine.

Next, configure thesolana CLI tool toconnect to a particular cluster :

solana config set --url < CLUSTER URL

(i.e. https://api.mainnet-beta.solana.com)

Finally, to check the balance, run the following command:

solana balance < PUBKEY

Creating Multiple Paper Wallet Addresses

You can create as many wallet addresses as you like. Simply re-run the steps inSeed Phrase Generation orPublic Key Derivation to create a new address. Multiple wallet addresses can be useful if you want to transfer tokens between your own accounts for different purposes.

Support

You can find additional support and get help on the Solana StackExchange . Previous Command Line Wallets Next File System Wallets using the CLI