Offline Transaction Signing with the Solana CLI

Some security models require keeping signing keys, and thus the signing process, separated from transaction creation and network broadcast. Examples include:

- Collecting signatures from geographically disparate signers in a[multi-signature scheme](#)
- Signing transactions using an[air-gapped](#)
- signing device

This document describes using Solana's CLI to separately sign and submit a transaction.

Commands Supporting Offline Signing

At present, the following commands support offline signing:

- [create-stake-account](#)
- [create-stake-account-checked](#)
- [deactivate-stake](#)
- [delegate-stake](#)
- [split-stake](#)
- [stake-authorize](#)
- [stake-authorize-checked](#)
- [stake-set-lockup](#)
- [stake-set-lockup-checked](#)
- [transfer](#)
- [withdraw-stake](#)
- [create-vote-account](#)
- [vote-authorize-voter](#)
- [vote-authorize-voter-checked](#)
- [vote-authorize-withdrawer](#)
- [vote-authorize-withdrawer-checked](#)
- [vote-update-commission](#)
- [vote-update-validator](#)
- [withdraw-from-vote-account](#)

Signing Transactions Offline

To sign a transaction offline, pass the following arguments on the command line

1. --sign-only
2. , prevents the client from submitting the signed transaction
3. to the network. Instead, the pubkey/signature pairs are printed to stdout.
4. --blockhash BASE58_HASH
5. , allows the caller to specify the value used to
6. fill the transaction'srecent_blockhash
7. field. This serves a number of
8. purposes, namely:Eliminates the need to connect to the network and query a recent blockhash
9. via RPC
10. Enables the signers to coordinate the blockhash in a multiple-signature
11. scheme

Example: Offline Signing a Payment

Command

solana@offline solana transfer --sign-only --blockhash 5Tx8F3jgSHx21CbtjwmdaKPLM5tWmreWAnPrbqHomSJF \ recipient-keypair.json 1 Output

Blockhash: 5Tx8F3jgSHx21CbtjwmdaKPLM5tWmreWAnPrbqHomSJF Signers (Pubkey=Signature):
FhtzLVsmcV7S5XqGD79ErgoseCLhZYmEZnz9kQg1Rp7j=4vC38p4bz7XyiXrk6HtaooUqwxTWKocf45cstASGtmrD398biNJnmTcUCVEojE7wVQvgdYbjHJqRFZPpzfCQpmUN

{"blockhash":"5Tx8F3jgSHx21CbtjwmdaKPLM5tWmreWAnPrbqHomSJF","signers":
["FhtzLVsmcV7S5XqGD79ErgoseCLhZYmEZnz9kQg1Rp7j=4vC38p4bz7XyiXrk6HtaooUqwxTWKocf45cstASGtmrD398biNJnmTcUCVEojE7wVQvgdYbjHJqRFZPpzfCQpmUN"]}'

Submitting Offline Signed Transactions to the Network

To submit a transaction that has been signed offline to the network, pass the following arguments on the command line

1. --blockhash BASE58_HASH
2. , must be the same blockhash as was used to sign
3. --signer BASE58_PUBKEY=BASE58_SIGNATURE
4. , one for each offline signer. This
5. includes the pubkey/signature pairs directly in the transaction rather than
6. signing it with any local keypair(s)

Example: Submitting an Offline Signed Payment

Command

solana@online solana transfer --blockhash 5Tx8F3jgSHx21CbtjwmdaKPLM5tWmreWAnPrbqHomSJF \ --signer FhtzLVsmcV7S5XqGD79ErgoseCLhZYmEZnz9kQg1Rp7j = 4vC38p4bz7XyiXrk6HtaooUqwxTWKocf45cstASGtmrD398biNJnmTcUCVEojE7wVQvgdYbjHJqRFZPpzfCQpmUN recipient-keypair.json 1 Output

4vC38p4bz7XyiXrk6HtaooUqwxTWKocf45cstASGtmrD398biNJnmTcUCVEojE7wVQvgdYbjHJqRFZPpzfCQpmUN

Offline Signing Over Multiple Sessions

Offline signing can also take place over multiple sessions. In this scenario, pass the absent signer's public key for each role. All pubkeys that were specified, but no signature was generated for will be listed as absent in the offline signing output

Example: Transfer with Two Offline Signing Sessions

Command (Offline Session #1)

solana@offline1 solana transfer Fdri24WUGtrCXZ55nXiewAj6RM18hRHPGAjZk3o6vBut 10 \ --blockhash 7ALDjLv56a8f6sH6upAZALQKkXyjAwwENH9GomyM8Dbc \ --sign-only \ --keypair fee_payer.json \ --from 674RgFMgdqdRoVtMqSBg7mHFbrrNm1h1r721H1ZMquHL Output (Offline Session #1)

Blockhash: 7ALDjLv56a8f6sH6upAZALQKkXyjAwwENH9GomyM8Dbc Signers (Pubkey=Signature):
3bo5YiRagwmRikuH6H1d2gkKef5nFZXE3gJeoHxJbPjy=ohGKvpRC46jAduwU9NW8tP91JkCT5r8Mo67Ysnid4zc76tiiV1Ho6jv3BKFSbBcr2NcPPCarmfTLSkTHsJCtdYi Absent

Signers (Pubkey): 674RgFMgdqdRoVtMqSBg7mHFbrrNm1h1r721H1ZMquHL Command (Offline Session #2)

solana@offline2 solana transfer Fdri24WUGtrCXZ55nXiewAj6RM18hRHPGAjZk3o6vBut 10 \ --blockhash 7ALDjLv56a8f6sH6upAZALQKkXyjAwwENH9GomyM8Dbc \ --sign-only \ --keypair from.json \ --fee-payer 3bo5YiRagwmRikuH6H1d2gkKef5nFZXE3gJeoHxJbPjy Output (Offline Session #2)

Blockhash: 7ALDjLv56a8f6sH6upAZALQKkXyjAwwENH9GomyM8Dbc Signers (Pubkey=Signature): 674RgFMgdqdRoVtMqSBg7mHFbrrNm1h1r721H1ZMquHL=3vJtnba4dKQmEAieAekC1rJnPUndBcpvqRPRMoPWqhLEMCty2SdUxt2yvC1wQW6wVUa5putZMt6kdwCaTv8gk7sQ Absent Signers (Pubkey): 3bo5YiRagwmRikuH6H1d2gkKef5nFZXE3gJeoHxJbPjy Command (Online Submission)

solana@online solana transfer Fdri24WUGtrCXZ55nXiewAj6RM18hRHPGAjZk3o6vBut 10 \ --blockhash 7ALDjLv56a8f6sH6upAZALQKkXyjAwwENH9GomyM8Dbc \ --from 674RgFMgdqdRoVtMqSBg7mHFbrrNm1h1r721H1ZMquHL \ --signer 674RgFMgdqdRoVtMqSBg7mHFbrrNm1h1r721H1ZMquHL=3vJtnba4dKQmEAieAekC1rJnPUndBcpvqRPRMoPWqhLEMCty2SdUxt2yvC1wQW6wVUa5putZMt6kdwCaTv8gk7sQ \ --fee-payer 3bo5YiRagwmRikuH6H1d2gkKef5nFZXE3gJeoHxJbPjy \ --signer 3bo5YiRagwmRikuH6H1d2gkKef5nFZXE3gJeoHxJbPjy=ohGKvpRC46jAduwU9NW8tP91JkCT5r8Mo67Ysnid4zc76tiiV1Ho6jv3BKFSbBcr2NcPPCarmfTLSkTHsJCtdYi Output (Online Submission)

ohGKvpRC46jAduwU9NW8tP91JkCT5r8Mo67Ysnid4zc76tiiV1Ho6jv3BKFSbBcr2NcPPCarmfTLSkTHsJCtdYi

Buying More Time to Sign

Typically a Solana transaction must be signed and accepted by the network within a number of slots from the blockhash in itsrecent_blockhash field (~1min at the time of this writing). If your signing procedure takes longer than this, aDurable Transaction Nonce can give you the extra time you need.Previous Solana CLI: Durable Transaction Nonces
Next Solana CLI: Off-Chain Message Signing