Multi-Sig accounts

Multi-signature (multi-sig) accounts provide an enhanced security mechanism by requiring multiple approvals (signatures) for transactions. This guide will walk you through setting up a multi-sig account, signing and broadcasting transactions using seid.

Creating a multi-sig account

1. Adding Accounts to Your Local Keychain

First, add two accounts to your local keychain:

seid keys add ms1 seid keys add ms2 These commands create two key pairs named ms1 and ms2.

1. Creating a Multi-Sig Account

Next, create a multi-sig account that requires signatures from both ms1 and ms2:

seid keys add ms1ms2 --multisig-threshold=2 --multisig=ms1,ms2 This command sets up a multi-sig account named ms1ms2 with a threshold of 2, meaning it requires signatures from both ms1 and ms2 to authorize transactions.

Signing and Broadcasting a Transaction

Here are the steps to sign and broadcast a transaction from a multi-sig account.

1. Define an Unsigned Transaction

Create an unsigned-tx.json file with your unsigned transaction. Below is an example of a JSON structure for sending tokens using a bank send message:

{ "body": { "messages": [{ "@type": "/cosmos.bank.v1beta1.MsgSend", "from_address": "MULTI_SIG_ACCOUNT", "to_address": "DESIRED_DESTINATION_ADDRESS", "amount": [{ "denom": "usei", "amount": "10" }] }], "memo": "", "timeout_height": "0", "extension_options": [], "non_critical_extension_options": [] }, "auth_info": { "signer_infos": [], "fee": { "amount": [{ "denom": "usei", "amount": "100000" }], "gas_limit": "200000", "payer": "", "granter": "" } }, "signatures": [] } Replace MULTI_SIG_ACCOUNT with your multi-sig account address and DESIRED_DESTINATION_ADDRESS with the recipient's address.

1. Sign the Unsigned Transaction

Sign the unsigned transaction from both ms1 and ms2:

seid tx sign unsigned-tx.json --multisig=multisigAccountName --from=ms1 --output-document=signer1_signedTx.json --node YOUR_RPC_URL

seid tx sign unsigned-tx.json --multisig=multisigAccountName --from=ms2 --output-document=signer2_signedTx.json --node YOUR_RPC_URL These commands create signer1_signedTx.json and signer2_signedTx.json, which contain the signatures from ms1 and ms2, respectively.

1. Combine Signatures

Combine the signatures into a single transaction file:

seid tx multisign unsigned-tx.json ms1ms2 signer1_signedTx.json signer2_signedTx.json > signedTx.json This command merges the individual signatures into a single transaction file named signedTx.json.

1. Broadcast the Multi-Sig Transaction

Finally, broadcast the signed multi-sig transaction to the network:

seid tx broadcast signedTx.json This command sends the combined, signed transaction to the Sei blockchain for processing.

Summary

By following these steps, you can set up and use multi-sig accounts on the Sei blockchain. This process enhances security by requiring multiple signatures for transaction approval, reducing the risk of unauthorized transactions. Multi-sig accounts are particularly useful for managing shared assets and ensuring that multiple parties must agree before any significant action is taken.

Last updated onMay 23, 2024 Pointer Contracts IBC Protocol