Shielded Transfers

In Namada, shielded transfers are enabled by the Multi-Asset Shielded Pool (opens in a new tab) (MASP). The MASP is a zero-knowledge circuit (zk-SNARK (opens in a new tab)) that extends the Zcash Sapling circuit (opens in a new tab) to add support for sending arbitrary assets. All assets in the pool share the same anonymity set, this means that the more transactions are issued to MASP, the stronger are the data protection guarantees.

Using MASP

If you are familiar with Zcash, the set of interactions you can execute with the MASP are similar:

- Shielding transfers: transparent to shielded addresses
- Shielded transfers: shielded to shielded addresses
- Unshielding transfers: shielded to transparent addresses

We distinguish two kinds of keys:

- ASpending Key
- is a type of private key that allows any user in possession of it to spend the balance of the associated address. For shielded addresses, possessing the Spending Key also allows the user to view the addressâ balance and transaction data.
- AViewing Key
- allows any user in possession of it to view and disclose transaction details. It is derived from the Spending Key and hold the same alias.

Shielding transfers

To conduct a shielding transfer, the user must first be in possession of a transparent account with some token balance.

Generate your Spending Key

One can randomly generate a new spending key with:

namadaw

gen

--shielded

--alias

< your-spending-key-alia s

> ð¡ This command will also generate a corresponding Viewing Key sharing the same alias.

Create a new payment address

To create a payment address from one's spending key, one can run:

namadaw

gen-payment-addr \ --key

< your-spending-key-alia s

\ --alias

< your-payment-address-alia s

> ð¡ This command will generate a different payment address each time the user runs the command. Payment addresses can be reused or discarded as the user likes, and any relationship between addresses cannot be deciphered by any other user without the spending key.

Send your shielding transfer

Once one has a payment address, one can transfer a balance from their transparent account to their shielded account with:

namadac

transfer \ --source

< your-established-account-alia s

\ --target

< your-payment-address-alia s

\ --token

btc \ --amount

< amount-to-shiel d

View one's balance

Once this transfer has been broadcasted, validated, and executed on the blockchain, one can view their spending key's balance:

namadac

balance

--owner

< your-spending-key-alia s

Shielded transfers

Once the user has a shielded balance, it can be transferred to a another shielded address:

namadac

transfer \ --source

< your-spending-key-alia s

\ --target

< destination-payment-addres s

\ --token

btc \ --amount

< amount-to-transfe r

\ --signing-keys

< your-implicit-account-alia s

Unshielding transfers

It is also possible to transfer the balance to a transparent account:

namadac

transfer \ --source

< your-spending-key-alia s

\ --target

< some-transparent-address-alia s

\ --token

btc \ --amount

< amount-to-unshiel d

\ --signing-keys

< your-implicit-account-alia s

Shielded Address/Key Generation

Spending Key Generation

When the client generates a spending key, it automatically derives a viewing key for it. The spending key acts as the "source" of any transfer from any shielded address derived from it. The viewing key is able to determine the total unspent notes that the spending key is authorized to spend.

Payment Address Generation

Payment addresses can be derived from both spending keys as well as viewing keys. The payment address acts as a destination address in which any tokens received by this address is spendable by the corresponding spending key. Only the payment address' spending key and viewing key are able to spend and view the payment address's balance, respectively. Below are examples of how payment addresses can be generated:

namadaw gen-payment-addr --alias my-pa1 --key my-sk namadaw gen-payment-addr --alias my-pa2 --key my-vk

Manual Key/Address Addition

It is also possible to manually add spending keys, viewining keys, and payment addresses in their raw form. This is demonstrated by the commands below.

namadaw add --alias my-sk --value
xsktest1qqqqqqqqqqqqqq9v0sls5r5de7njx8ehu49pqgmqr9ygelg87l5x8y4s9r0pjlvu69au6gn3su5ewneas486hdccyayx32hxvt64p3d0hfuprpgcgv2q9gdx3jvxrn02f0nnp3jtdd6f5vwscfuyum083cvfv4jun75ak5
namadaw add --alias my-vk --value
xfvktest1qqqqqqqqqqqqqqpagte43rsza46v55dlz8cffahv0fnr6eqacvnrkyuf9lmndgal7erg38awgq60r259csg3lxeeyy5355f5nj3ywpeqgd2guqd73uxz46645d0ayt9em88wflka0vsrq29u47x55psw93ly80lvftzdr5
namadaw add --alias my-pa --value patest10qy6fuwef9leccl6dfm7wwlyd336x4y32hz62cnrvlrl6r5yk0jnw80kus33x34a5peg2xc4csn

Making Shielded Transactions

Shielding Transactions

In order to shield tokens from a transparent address, the user must first generate a shielded payment address in which the user holds the spending key for. It is then possible to make a transfer from the transparent address to the newly created shielded payment address. Once this process is completed, the new tokens are now considered "shielded". The gas fee is charged to the source address that makes the transfer to the shielded payment address. Shielding tokens can be done as following:

namadac transfer --source Bertha --amount 50 --token BTC --target my-pa

Unshielding Transactions

"Unshielding" is the process of transferring token balances from the shielded set to the transparent one. When the user makes a transfer from a shielded account (using the corresponding spending key) to a transparent account, the newly transferred funds are considered "unshielded". The gas fee is charged to the signer's address (which should default to the target address). Once the transaction is complete, the spending key will no longer be able to spend the transferred amount. Below is an example of how an unshielding transaction is performed:

namadac transfer --target Bertha --amount 45 --token BTC --source my-sk

Shielded Transactions

Shielded transfers are made from one shielded account to another. From a user perspective, this is almost equivalent to a transparent-transparent token transfer, except the gas fee is paid by the signer of the transaction. The command for performing a shielded transfer is given below:

namadac transfer --source my-sk --amount 5 --token BTC --target your-pa

Viewing Shielded Balances

The viewing key that is derived from a spending key allows any user holding that key to view the balances attached to corresponding spending key. It is possible to use this viewing key to either decipher the full balance of the corresponding viewing key or query a subset of them.

namadac balance namadac balance --owner namadac balance --owner --token BTC namadac balance --token BTC

Listing Shielded Keys/Addresses

The wallet is able to list all the spending keys, viewing keys, and payment addresses that it stores. Below are examples of how the wallet's storage can be queried:

namadaw list --keys namadaw list --keys --unsafe-show-secret namadaw list --keys --unsafe-show-secret --decrypt namadaw list --addr

Finding Shielded Keys/Addresses

The wallet is able to find any spending key, viewing key or payment address when given its alias. Below are examples of how the wallet's storage can be queried:

namadaw find --alias my-alias namadaw find --alias my-alias --unsafe-show-secret

Shielded Rewards Fees on Namada