# #

Key

#

A note on HD wallet

HD Wallets, originally specified in Bitcoin's BIP32open in new window , are a special kind of wallet that let users derive any number of accounts from a single seed. To understand what that means, let us first define some terminology:

- Wallet
- : Set of accounts obtained from a given seed.
- Account
- : A pair of public key/private key.
- Private Key
- : A private key is a secret piece of information used to sign messages. In the blockchain context, a private key identifies the owner of an account. The private key of a user should never be revealed to others.
- Public Key
- : A public key is a piece of information obtained by applying a one-way mathematical function on a private key. From it, an address can be derived. A private key cannot be found from a public key.
- Address
- : An address is a public string with a human-readable prefix that identifies an account. It is obtained by applying mathematical transformations to a public key.
- Digital Signature
- : A digital signature is a piece of cryptographic information that proves the owner of a given private key approved of a given message without revealing the private key.
- Seed
- : Same as Mnemonic.
- Mnemonic
- : A mnemonic is a sequence of words that is used as seed to derive private keys. The mnemonic is at the core of each wallet. NEVER LOSE YOUR MNEMONIC. WRITE IT DOWN ON A PIECE OF PAPER AND STORE IT SOMEWHERE SAFE. IF YOU LOSE IT, THERE IS NO WAY TO RETRIEVE IT. IF SOMEONE GAINS ACCESS TO IT, THEY GAIN ACCESS TO ALL THE ASSOCIATED ACCOUNTS.

At the core of a HD wallet, there is a seed. From this seed, users can deterministically generate accounts. To generate an account from a seed, one-way mathematical transformations are applied. To decide which account to generate, the user specifies apath , generally aninteger (0 ,1 ,2 , ...).

By specifyingpath to be0 for example, the Wallet will generatePrivate Key 0 from the seed. Then,Public Key 0 can be generated fromPrivate Key 0 . Finally,Address 0 can be generated fromPublic Key 0 . All these steps are one way only, meaning thePublic Key cannot be found from theAddress , thePrivate Key cannot be found from thePublic Key , ...

Account0 Account1 Account2 +------------------+ +------------------+ +------------------+| | | | | | | Address0 | | Address1 | | Address2 | | ^| | ^| | ^| | | | | | | | | | | | | | | | | | | | | | | | | | | | | +| | +| | +| | Public key0 | | Public key1 | | Public key2 | | ^| | ^| | ^| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | +| | +| | +| | Private key0 | | Private key1 | | Private key2 | | ^| | ^| | ^| +------------------+ +------------------+ +------------------+| | | | | | | | | +--+| | +---------+---------+| | | Mnemonic(Seed) | | | +---------------+ The process of derivating accounts from the seed is deterministic. This means that given the same path, the derived private key will always be the same.

The funds stored in an account are controlled by the private key. This private key is generated using a one-way function from the mnemonic. If you lose the private key, you can retrieve it using the mnemonic. However, if you lose the mnemonic, you will lose access to all the derived private keys. Likewise, if someone gains access to your mnemonic, they gain access to all the associated accounts.

#

IRIShub Key

The IRIShub Wallet is a HD Wallet base on BIP44open in new window . BIP44 defines a logical hierarchy for deterministic wallets based on an algorithm described in BIP32open in new window , which allows the handling of multiple coins, multiple accounts, external and internal chains per account and millions of addresses per chain, such as BTC and ETH.

BIP44 defines the following 5 levels in BIP32 path:

m / purpose' / coin_type' / account' / change / address_index The IRIShub coin_type is same as cosmos stake tokenATOM 118 registered in SLIP44open in new window .

So the prefix of IRIShub key BIP44 path is44'/118'/ , and its default path is44'/118'/0'/0/0 .