HD Paths and Coin Types

When deriving a private key from a mnemonic phrase, the hierarchical deterministic (HD) path involves multiple parameters, including the coin type. The coin type determines the blockchain ecosystem for which the key is derived, making it crucial when dealing with different wallets and blockchains.

Coin Type Parameter

The second parameter in the HD path specifies the coin type, which is defined by the BIP-44 standard. This parameter identifies the blockchain ecosystem associated with the derived keys.

•Ethereum (Coin Type 60) : Wallets like MetaMask use coin type 60. The HD path for Ethereum typically looks like this: m/44'/60'/0'/0/0.

•Cosmos (Coin Type 118) : Wallets for Cosmos-based chains, such as Compass, use coin type 118. The HD path for Cosmos typically looks like this: m/44'/118'/0'/0/0.

Implications

Due to the different coin types, a mnemonic phrase used to derive keys for Ethereum (coin type 60) cannot be directly used in a Cosmos wallet (coin type 118) to access the same accounts. This is because the HD path determines a different set of keys for each coin type, meaning the derived addresses will differ.

Private Key Export

Users can export their private key from MetaMask (derived using coin type 60) and import it into any Cosmos wallet. This works because the private key, once derived, can be used across different blockchain ecosystems, provided the receiving wallet supports the import function. This allows users to manage their assets across various blockchains using the same underlying cryptographic key.

Example HD Paths

•Traditional Cosmos Path : m/44'/118'/0'/0/0

•Traditional EVM Path : m/44'/60'/0'/0/0

Last updated onMay 23, 2024 Execute Multiple Transactions Proposals