Wallet Module

This module provides the functionality to control the account.

Private Key

Class for wrappingSigningKey that is used for signature creation and public key derivation.

generate(path)

This function generates new private key with random mnemonic phrase.

info If path is not given, default to Band's HD prefix 494 and all other indexes being zeroes. Parameter

- path
-
- optional: HD path that follows the BIP32 standard.

Return

- Tuple[str,]
- : Tuple of mnemonic phrase andPrivateKey
- instance.

Example

from pyband . wallet import PrivateKey

mnemonic , priv = PrivateKey . generate (path = "m/44'/494'/0'/0/3")

from_mnemonic(word, path)

This function creates aPrivateKey instance from a given mnemonic phrase and a HD derivation path.

info If path is not given, default to Band's HD prefix 494 and all other indexes being zeroes. Parameter

- words
-
- : Mnemonic phrase for recovers a private key.
- path
-
- (optional): HD path that follows the BIP32 standard.

Return

-
- :PrivateKey
- object.

Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_mnemonic ("test mnemonic")

from_hex(priv)

This function creates aPrivateKey instance from a given hex that represents a signing key.

Parameter

- priv
-
- : Hex representation of signing key.

Return

-
- :PrivateKey
- object.

Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_hex ("2442b724db7189468f16accc0fc505f0609817eb129e13702e696d8b84609ea9")

to_hex

This function returns a hex representation of a signing key.

Return

-
- : A hex representation of signing key.

Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_mnemonic ("test mnemonic") print (priv . to_hex ( )) Result

2cb2e2d3582cebf0664d9cda0b89c5d478ae12fac19a6f4ed9c10a7406a19615

to_public_key

This function returns aPublicKey that is associated with this private key.

Return

-
- : APublicKey
- that can be used to verify the signatures made with thisPrivateKey
- .

Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_mnemonic ("test mnemonic") print (priv . to_public_key ( ) . to_hex ( )) Result

02b2b0d35cb1c6d3923813c64e46a82d29e12d03288f438b9d3cf232d9a22bcb83

sign(msg)

This function returns a signature of the associated private key. The message is signed by using the edcsa sign_deterministic function.

Parameter

- msg
-
- : Message that will be hashed and signed.

Return

-
- : A signature of this private key over the given message.

Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_mnemonic ("test mnemonic") print (priv . sign (b"test message") . hex ( )) Result

4bbc9a7ea54b47b11c67a4074e8d9bca068cb64c788f67342c4033b1b6f0553e1bc63cdf9bc2fb6e89c1e965c1e0f0712a51c250627282309cd2fccf1470f4f6

Public Key

Class for wrappingVerifyKey that is used for signature verification.

from_acc_bech32(bech)

This function creates aPublicKey instance from bech32-encoded with account public key prefixbandpub .

Parameter

- bech
-
- : A bech32-encoded with account public key prefix.

Return

- PublicKey
- : APublicKey
- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v")

from_val_bech32(bech)

This function creates aPublicKey instance from bech32-encoded with validator public key prefixbandvaloperpub .

Parameter

- bech
-
- : A bech32-encoded with validator public key prefix.

Return

- PublicKey
- : APublicKey
- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_val_bech32 ("bandvaloperpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q69gsm29")

from_cons_bech32(bech)

This function creates aPublicKey instance from a bech32-encoded with validator consensus public key prefixbandvalconspub .

Parameter

- bech
-
- : A bech32-encoded with validator consensus public key prefix.

Return

- PublicKey
- : APublicKey
- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_cons_bech32 ("bandvalconspub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6r8ytws")

to_hex

This function returns a hex representation of the verified key.

Return

-
- : A hex representationof the verified key.

Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v") print (public_key . to_hex ( )) Result

0351e98e1be097250f2ff4188c0aace0a716e69a992cd77f9dfe436b3e8b34280d

to_public_key_proto()

This function returns a public key in type protobuf.

Return

-
- : A public key of type protobuf (SECP256k1).

to_acc_bech32

This function returns bech32-encoded with account public key prefixbandpub .

Return

-
- : A bech32-encoded with account public key prefix.

Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v") print (public_key . to_acc_bech32 ( )) Result

bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v

to_val_bech32

This function returns a bech32-encoded with validator public key prefixbandvaloperpub .

Return

-
- : A bech32-encoded with validator public key prefix.

Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v") print (public_key . to_val_bech32 ( )) Result

bandvaloperpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q69gsm29

to_cons_bech32

This function returns a bech32-encoded with validator consensus public key prefixbandvalconspub .

Return

-
- : A bech32-encoded with validator consensus public key prefix.

Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v") print (public_key . to_cons_bech32 ( )) Result

bandvalconspub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6r8ytws

to_address

This function returns anAddress instance from this public key.

Return

-
- : AnAddress
- instance

Example

from pyband . wallet import PublicKey

public_key

PublicKey . from_acc_bech32 ("bandpub1addwnpepqdg7nrsmuztj2re07svgcz4vuzn3de56nykdwlualepkk05txs5q6mw8s9v") print (public_key . to_address ( ) . to_hex ( )) Result

8bb66ae5bb7e5ce1035557cf1c77430b987683d2

verify(msg, sig)

This function is used to verify a signature made from the given message.

Parameter

- msg
-
- : A data signed by the signature, will be hashed using sha256 function.
- sig
- <bytes
- : An encoded signature

Return

-
- : True, if the verification success.

Exception

Type Description BadSignatureError If the signature is invalid or malformed Example

from pyband . wallet import PrivateKey

priv

PrivateKey . from_mnemonic ("test mnemonic") public_key = priv . to_public_key ( ) msg =

b"test message" sig = priv . sign (msg) print (public_key . verify (msg , sig)) Result

True

Address

Class for wrappingAddress .

from_acc_bech32(bech)

This function creates anAddress instance from the given bech32-encoded with account prefixband .

Parameter

- bech
-
- : A bech32-encoded with account prefix.

Return

-
- : AnAddress
- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import Address

address

Address . from_acc_bech32 ("band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c")

from_val_bech32(bech)

This function creates an Address instance from the given bech32-encoded with validator prefixbandvaloper .

Parameter

- bech
-
- : A bech32-encoded with validator prefix.

Return

-
- : AnAddress

- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import Address

address

Address . from_val_bech32 ("bandvaloper13eznuehmqzd3r84fkxu8wklxl22r2qfm8f05zn")

from_cons_bech32(bech)

This function creates an Address instance from the given bech32-encoded with validator consensus prefixbandvalcons .

Parameter

- bech
-
- : A bech32-encoded with validator consensus prefix.

Return

-
- : AnAddress
- instance

Exception

Type Description ValueError Invalid bech32 prefix Example

from pyband . wallet import Address

address

Address . from_cons_bech32 ("bandvalcons13eznuehmqzd3r84fkxu8wklxl22r2qfmn6ugwj")

to_hex

This function returns a hex representation ofAddress .

Return

-
- : A hex representation ofAddress
- .

Example

from pyband . wallet import Address

address

Address . from_acc_bech32 ("band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c") print (address . to_hex ( )) Result

8e453e66fb009b119ea9b1b8775be6fa9435013b

to_acc_bech32

This function returns a bech32-encoded with account prefix bandband .

Return

-
- : A bech32-encoded with account prefix.

Example

from pyband . wallet import Address

address

Address . from_acc_bech32 ("band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c") print (address . to_acc_bech32 ( )) Result

band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c

to_val_bech32

This function returns a bech32-encoded with validator prefixbandvaloper .

Return

-
- : A bech32-encoded with account prefix.

Example

from pyband . wallet import Address

address

Address . from_acc_bech32 ("band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c") print (address . to_val_bech32 ( )) bandvaloper13eznuehmqzd3r84fkxu8wklxl22r2qfm8f05zn

to_cons_bech32

This function returns a bech32-encoded with validator consensus prefixbandvalcons .

Return

-
- : A bech32-encoded with account prefix.

Example

from pyband . wallet import Address

address

Address . from_acc_bech32 ("band13eznuehmqzd3r84fkxu8wklxl22r2qfmtlth8c") print (address . to_cons_bech32 ( )) Result

bandvalcons13eznuehmqzd3r84fkxu8wklxl22r2qfmn6ugwj Previous Transaction Module Next Getting Started