Hierarchical Deterministic (HD) Wallet Version 3.0.0 (v3) Alpha-1

Prepared by Meheret Tesfaye Batu

Open-Source, GitHub Link - https://github.com/meherett/python-hdwallet

Introduction

In the dynamic landscape of cryptocurrencies, managing multiple digital assets securely and efficiently has become increasingly challenging. This whitepaper introduces a comprehensive solution: the Hierarchical Deterministic (HD) Wallet Generator, which supports over 200 cryptocurrencies. This tool is designed to streamline wallet management while upholding the highest standards of security and usability.

Motivation

The Hierarchical Deterministic Wallet (HDWallet) offers enhanced security, convenience, and control over digital assets. By utilizing a single seed phrase, users can generate an entire tree of private and public keys, simplifying key management and ensuring robust protection against loss or theft. This structure not only facilitates the creation and management of multiple cryptocurrency accounts but also enhances privacy by generating a unique address for each transaction.

The motivation for developing this HD Wallet Generator stems from the growing need for a unified, secure, and user-friendly solution to manage diverse cryptocurrency holdings. As the number of supported cryptocurrencies continues to expand, users face the complexity of handling multiple wallets and keys. Our solution addresses these challenges by providing a single platform that supports a wide array of digital assets, significantly improving the cryptocurrency experience by simplifying investment management, enhancing security, and maintaining privacy.

Background

The concept of Hierarchical Deterministic (HD) Wallet emerged as a response to the growing need for secure and manageable cryptocurrency key generation. HDWallet was first proposed in Bitcoin Improvement Proposal 0032 (BIP32) by Pieter Wuille in 2012. This innovation aimed to simplify key management by allowing users to generate an entire tree of keys from a single seed phrase. This structure provided enhanced security, convenience, and control, enabling users to derive multiple private and public keys without the need to store each one separately. HDWallets significantly improved the process of creating and managing multiple cryptocurrency accounts, providing robust protection against loss or theft and ensuring privacy by generating unique addresses for each transaction.

Why HDWallet?

Enhanced Security: HDWallet generates all keys from a single master seed, simplifying the backup and restoration process. This reduces the risk associated with losing individual private keys and offers a secure means of recovery in case of device loss or theft.

Simplified Management: Users can manage multiple cryptocurrencies and accounts within a single wallet, reducing complexity. This all-in-one approach eliminates the need for multiple wallets and disparate key management systems, providing a more streamlined and user-friendly experience.

Interoperability: HDWallet adheres to standardized protocols (e.g., BIP32, BIP39, BIP44, BIP84, BIP86, BIP141, CIP1852), ensuring compatibility across various platforms and services. This standardization allows for seamless integration with different cryptocurrency ecosystems and enhances the usability of the wallet across different applications and services.

Privacy: HDWallets enhance user privacy by generating a unique address for each transaction. This prevents the reuse of addresses, making it more difficult for third parties to trace transactions back to the user, thereby protecting the user's financial privacy.

Flexibility: The HDWallet supports over 200 cryptocurrencies, providing users with the flexibility to manage a diverse portfolio of digital assets within a single platform. This extensive support ensures that users can easily handle a wide range of cryptocurrencies without needing to switch between multiple wallets or services.

User Experience: The HDWallet Generator is designed with a focus on user experience, offering a simple and intuitive interface that makes it easy for both novice and experienced users to manage their digital assets. The user-friendly design ensures that users can quickly and efficiently access the features they need.

Future-Proofing: As the cryptocurrency landscape continues to evolve, the HDWallet is built to accommodate new standards and protocols, ensuring that it remains a relevant and valuable

tool for users. This adaptability allows the wallet to support future developments in the cryptocurrency space, providing long-term value to its users.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a form of public key cryptography that leverages the mathematical properties of elliptic curves to provide high levels of security with relatively small key sizes. ECC is widely used in various applications, including secure communications, digital signatures, and cryptocurrency systems, due to its efficiency and strong security characteristics. The HDWallet library supports multiple ECC types to cater to different use cases and preferences in the cryptocurrency ecosystem.

Above version-3 of HDWallet supported ECC types:

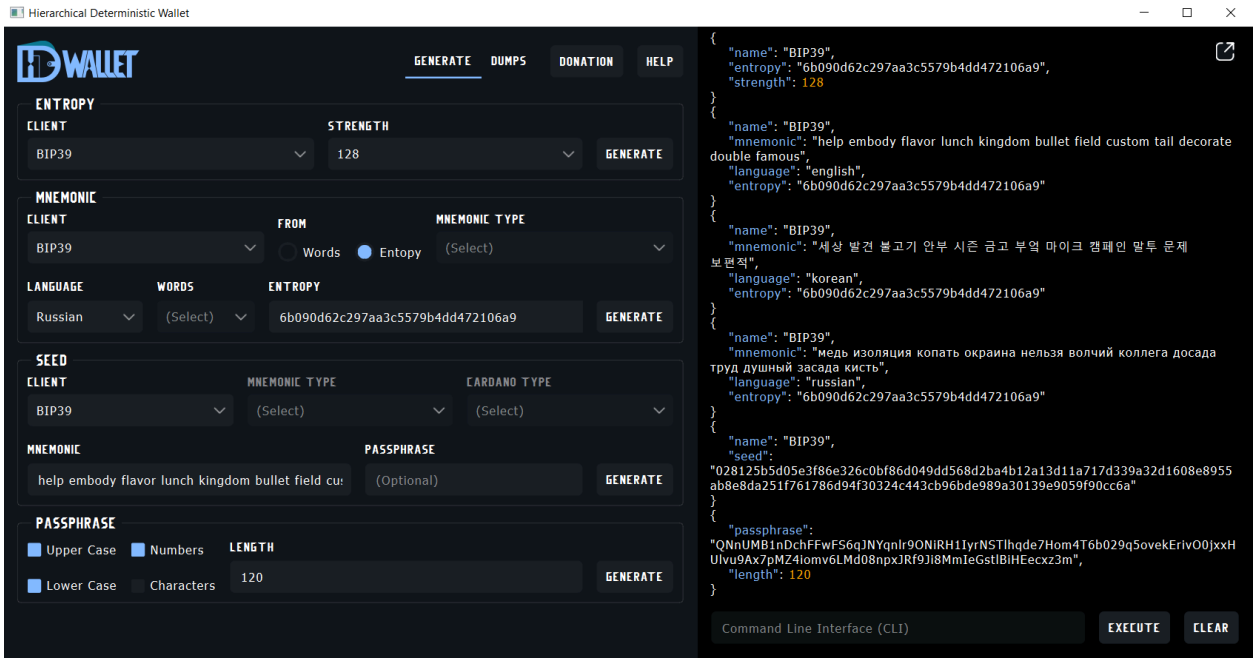
- ☑ **Kholaw-Ed25519**: A tailored implementation of Ed25519 for deterministic key generation, ensuring compatibility with both BIP32 and Ed25519 standards. For more: https://github.com/LedgerHQ/orakolo/blob/master/papers/Ed25519_BIP%20Final.pdf
- ☑ **SLIP10-Ed25519**: A standardized approach for hierarchical deterministic key derivation using the Ed25519 curve within the SLIP-0010 framework.
- ☑ **SLIP10-Ed25519-Blake2b**: Combines Ed25519 with the Blake2b hashing function for enhanced security and performance in key derivation.
- ☑ **SLIP10-Ed25519-Monero**: Adapts Ed25519 for use with Monero, leveraging its privacy features like ring signatures and stealth addresses.
- ☑ **SLIP10-Nist256p1**: Based on the NIST P-256 curve, providing a balance of security and performance within the SLIP-0010 standard.
- ☑ **SLIP10-Secp256k1**: Utilizes the secp256k1 curve, widely used in Bitcoin and other cryptocurrencies, for efficient and secure key management within the SLIP-0010 framework.

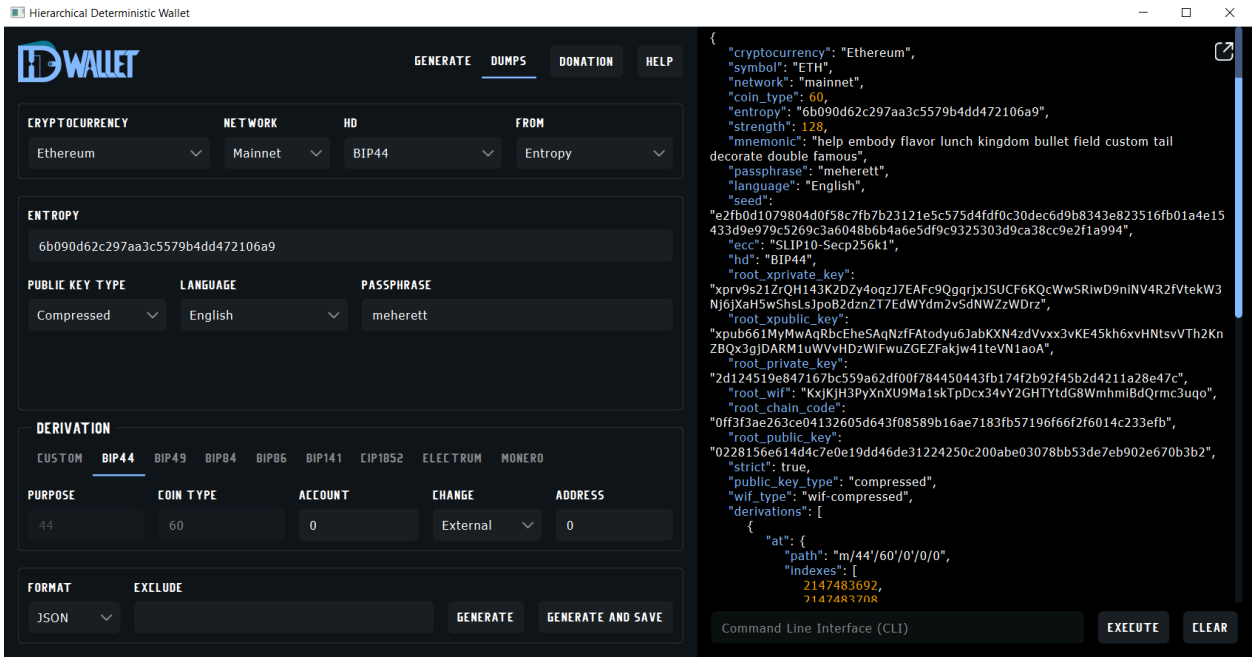
Below HDWallet version-3, only supports **SLIP10-Secp256k1** ECC type.

V3 - Desktop Application

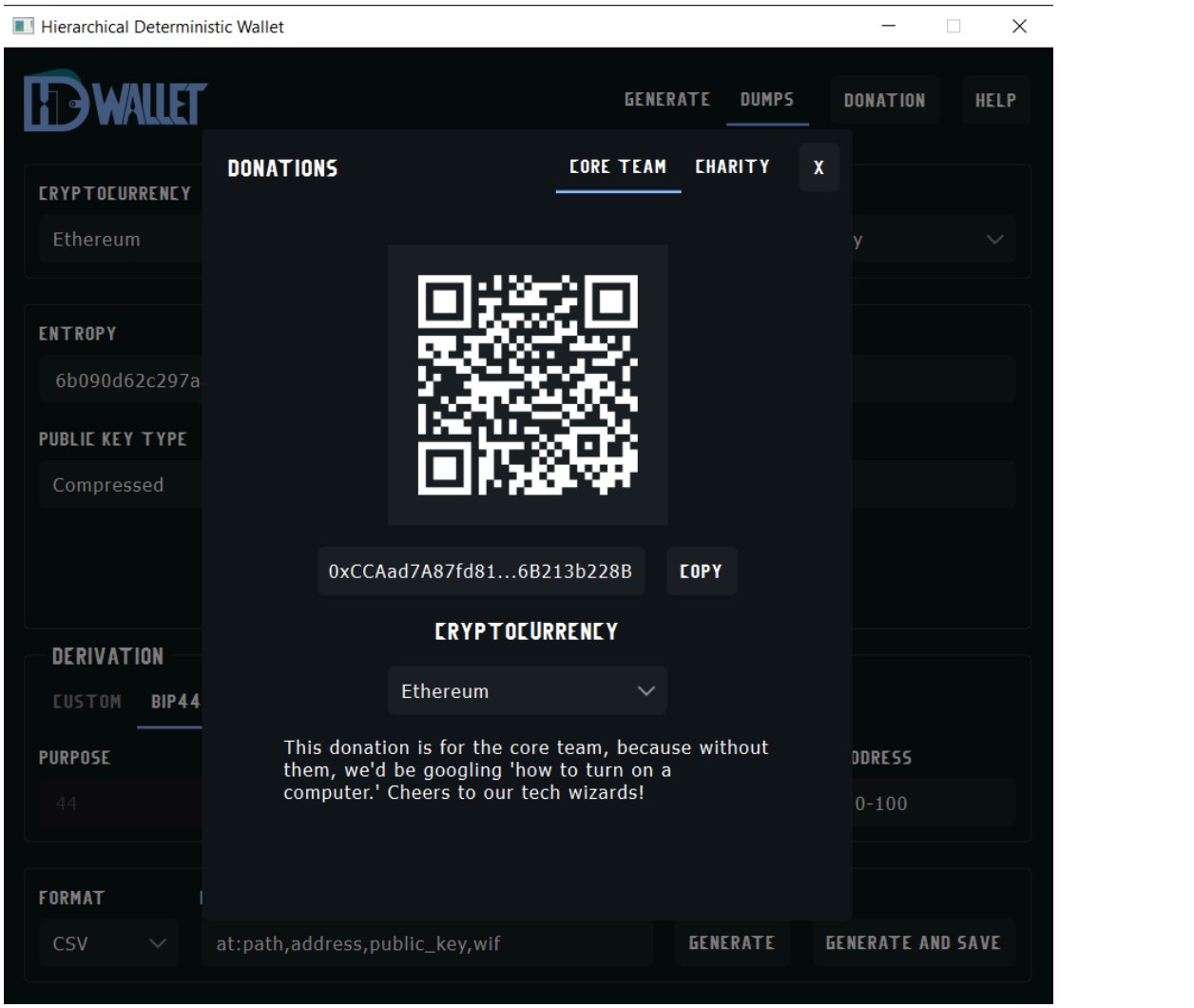
HDWallet version-3 includes a desktop application with a user interface (UI) to simplify wallet management further. The desktop application provides:

- A visual interface for creating and managing wallets.
- Support for generating and viewing addresses.
- Enhanced user experience with an intuitive design.


Hierarchical Deterministic Wallet
HD WALLET
GENERATE
DUMPS
DONATION
HELP
ENTROPY
CLIENT
BIP39
STRENGTH
128
GENERATE
MNEMONIC
CLIENT
BIP39
FROM
Words
Entopy
MNEMONIC TYPE
(Select)
LANGUAGE
Russian
WORDS
(Select)
ENTROPY
6b090d62c297aa3c5579b4dd472106a9
GENERATE
SEED
CLIENT
BIP39
MNEMONIC TYPE
(Select)
CARDANO TYPE
(Select)
MNEMONIC
help embody flavor lunch kingdom bullet field cus
PASSPHRASE
(Optional)
GENERATE
PASSPHRASE
Upper Case
Numbers
Lower Case
Characters
LENGTH
120
GENERATE
{
"name": "BIP39",
"entropy": "6b090d62c297aa3c5579b4dd472106a9",
"strength": 128
}
{
"name": "BIP39",
"mnemonic": "help embody flavor lunch kingdom bullet field custom tail decorate double famous",
"language": "english",
"entropy": "6b090d62c297aa3c5579b4dd472106a9"
}
{
"name": "BIP39",
"mnemonic": "세상 발견 볼고기 안부 시즌 금고 부엌 마이크 캠페인 맏투 문제 보편적",
"language": "korean",
"entropy": "6b090d62c297aa3c5579b4dd472106a9"
}
{
"name": "BIP39",
"mnemonic": "медь изоляция копать окраина нельзя волчий коллега досада труд душный засада кисть",
"language": "russian",
"entropy": "6b090d62c297aa3c5579b4dd472106a9"
}
{
"name": "BIP39",
"seed": "028125b5d05e3f86e326c0bf86d049dd568d2ba4b12a13d11a717d339a32d1608e8955ab8e8da251f761786d94f30324c443cb96bde989a30139e9059f90cc6a"
}
{
"passphrase": "QNnUMB1nDchFFwFS6qJNYqnlr9ONiRH1IyrNSTlhqde7Hom4T6b029q5ovekErivO0jxxHUlvu9Ax7pMZ4iomv6LMd08npxJRf9Jl8MmIeGstlBiHEecxz3m",
"length": 120
}
Command Line Interface (CLI)
EXECUTE
CLEAR


Hierarchical Deterministic Wallet
HD WALLET
GENERATE
DUMPS
DONATION
HELP
CRYPTOCURRENCY
Ethereum
NETWORK
Mainnet
HD
BIP44
FROM
Entropy
ENTROPY
6b090d62c297aa3c5579b4dd472106a9
PUBLIC KEY TYPE
Compressed
LANGUAGE
English
PASSPHRASE
meherett
DERIVATION
CUSTOM
BIP44
BIP49
BIP84
BIP86
BIP141
CIP1852
ELECTRUM
MONERO
PURPOSE
44
COIN TYPE
60
ACCOUNT
0
CHANGE
External
ADDRESS
0
FORMAT
JSON
EXCLUDE
GENERATE
GENERATE AND SAVE
{
"cryptocurrency": "Ethereum",
"symbol": "ETH",
"network": "mainnet",
"coin_type": 60,
"entropy": "6b090d62c297aa3c5579b4dd472106a9",
"strength": 128,
"mnemonic": "help embody flavor lunch kingdom bullet field custom tail decorate double famous",
"passphrase": "meherett",
"language": "English",
"seed": "e2fb0d1079804d0f58c7fb7b23121e5c575d4fdf0c30dec6d9b8343e823516fb01a4e15433d9e979c5269c3a6048b6b4a6e5df9c9325303d9ca38cc9e2f1a994",
"ecc": "SLIP10-Secp256k1",
"hd": "BIP44",
"root_xprivate_key": "xprv9s21ZrQH143K2DZy4oqzJ7EAFc9QgqrjxJSUCF6KQcWwSRiwD9niNV4R2fVtekW3Nj6jXaH5wShsLsJpoB2dznZT7EdWYdm2vSdNWZzWDrz",
"root_xpublic_key": "xpub661MyMwAqRbcEheSAqNzfFAtodyu6JabKXN4zdVvxx3vKE45kh6xvHNtsvVTh2KnZBQx3gjDARM1uWVVvHDzWiFwuZGEZFakjw41teVN1aoA",
"root_private_key": "2d124519e847167bc559a62df00f784450443fb174f2b92f45b2d4211a28e47c",
"root_wif": "KxjKjH3PyXnXU9Ma1skTpDcx34vY2GHTYtdG8WmhmiBdQrmc3uqo",
"root_chain_code": "0ff3f3ae263ce04132605d643f08589b16ae7183fb57196f66f2f6014c233efb",
"root_public_key": "0228156e614d4c7e0e19dd46de31224250c200abe03078bb53de7eb902e670b3b2",
"strict": true,
"public_key_type": "compressed",
"wif_type": "wif-compressed",
"derivations": [
{
"at": {
"path": "m/44'/60'/0'/0/0",
"indexes": [
2147483692,
Command Line Interface (CLI)
EXECUTE
CLEAR


Terminal
m/44'/60'/0'/0/63, 0x97f26116c2e185bfd598eeeb3a01fc739cf8DFaf, 0224875c5798de7cb1afe16e294f7f3afe778de2f3a99711c850cd6ffebca4e151, L3ot2q4vjP1aGnhPaNr3wY6RdFKqKbzDnDEfiesB3qmtrktKZ1Ep
m/44'/60'/0'/0/64, 0x14F1F297EE5B5aD97AaC5d6472296E3dDE50A735, 03922cbd6a7e31421d5aae217fa0a2d572a6195818cabdabf6d6b1346a15168661, L1WWU6ktrqBYZPdGWEmLstjXWtBttpUeNfaojeY8ocgrSdeqRHi
m/44'/60'/0'/0/65, 0x84BD5bA2E92Df7ffDc7476943c0f44440cd5599F, 03e1a6381875756l625e282e24a516543f5d9bf8ac7d3d0f30946682baf29627c, L2zBARcZWF7sVKyGsGR62unjSG78T34ewV3jt7Ciszgg1c9vdX1x
m/44'/60'/0'/0/66, 0xe9F8765F140c9300639a47ff8c342Fcc0134d9b9, 0378e904e3bd25b8cc0128420b336cc12c7fdf359d62e4f835fafb3b7b64e2ddbc, L5nqJ4Npgmv616HPUwMERTBjEVnpMmFsYNhJPKwbfM5nX6F2vjiA
m/44'/60'/0'/0/67, 0xf4a3D2D57c08530F5D450646B6A9E436d087D046, 031a5d8e15e02d84e1fc36554f6792ef14c16e0bd88e286dee1bb64a243ac69330, L3p6kd4kLutgrzrq2MWBc83J9kikNPwXG7ynbGZTGzqcUBB4kGxz
m/44'/60'/0'/0/68, 0x2a97a15C6dCB04129F573D5Cc66F92988512f19E, 02cfd6b1371a82f8a7d5753aabc5e7e6b831491b4c0e4bf9547ca68840ee5a343c, KwP7inv1JEhvLuBbvEeaBg6grByZ1H5Qqn6hbg9sri4p95HXG3JA
m/44'/60'/0'/0/69, 0x924B44DcFCC875fE6BD521EbCbE5D8775140I341, 02bd02b9b4d6bd5c777abb9ac68104a618bdd03fb9aee43ba79c61cc6a6a79f42d, K2soSw4pUtn7bK7T8FzZXHFUFrBqGqMz1Jp1R6LzNeTAmNB9C36
m/44'/60'/0'/0/70, 0x478E9772Db81C360e3347Af70d79299aB6a0117F, 02e07759lb9034ba93a072cac5aa49b9cfc361094ff09d53db288beec69c5331fa, L3dmZqMLrJcyqWpWP1deM3CTCodmi98VU6zMbTHV2LinKxDiWUFJ
m/44'/60'/0'/0/71, 0xe8D104ace1C0A02A3e82414dBDb1a325f7b26d2d, 0321c9b0df0a6268c855d1c87c756ea088a16082db054ffee834ee0b7439405f95, L5KGyd5Fw1xrkgVgxqSKFr9wzDq2sBzFoTV8YQbEfHW4SQMxR3t
m/44'/60'/0'/0/72, 0x3fc264b045b48Fc920BF4A230A982723cA1C236f, 02b04cfa74df793f7a3d9f3ce65e44e6d81c2b370f9349567b3625058654f24fe8, L2vvjkfuy4CWhpn1FYneQAMqnGo13DJtdao9o9hz9uHs4r3bh1VV
m/44'/60'/0'/0/73, 0x0bA0aBd3BE598d5aB672c691962D833fF5f15Df8, 025089ea5f60f99df2a4063ac57b0e088b97fe77c3369e1b9025d790cf061644f2, L4LF5EtFjYk2No4CW8g79P695ymb6k1QE9h31mMFcWzUh26d7Yq2
m/44'/60'/0'/0/74, 0x3b1f390Ae94A7cf49014c09Fe047ADd990B948C6, 02c78a3c14611bc501cb8554bf20ef6f288f565a3c92239c99f9092702dfd43e22, Kym4qFnCVKDFb6nPfqCv4DsB2Jov5Ef2uxxA9ZFEUBERJrGyqw9j
m/44'/60'/0'/0/75, 0xb8FFA5F251690886D961047A68441C23DDF10DfD, 02c5271e194642136e813efb17f02a55ef479dca8723ec71abaea80fa175c04769, Kyoo7ynBTanCqpB4TT2jwtTLnyaG1v36S7v8LobrL6vRRnDnmzmk
m/44'/60'/0'/0/76, 0x084e5585A7972bb4C701dB00F9ac0f88d22Bdaf5, 03672f0dc862ebb66ea4c84aa9c13a526c2c3d39cea9f5f4062c4d35b4b2576fa3, L2F4rvtbVgMQjJdks9iSUDp51N2QWEDMjvoqdexCm41pmAMjhjq8
m/44'/60'/0'/0/77, 0x7A4cF69c35b5B90F023022CCdDB6a8121B27F31a, 025042600e6ff143f1c799976a51682f547b29071a0f485950c5a3bb2e02a6d3b5, L4A7oofqPNfbLAwB5nrvZ5ZTNDQC8vUg8wCCKZwLqZReRmuo5mCU
m/44'/60'/0'/0/78, 0x90549087e69519842ADD0Fe32b97Ccd601c83390, 02a29a54ed546af9adefecf39bbf9eed817a88bb26976521f9036c45262a30bec2, L4KoFR9SuK4zzG5vLecaxvJ63kpNNHs9YGtvH85fkXWBGkRP6EDT
m/44'/60'/0'/0/79, 0x101F0D72453892A2344DCf93Ca4FC7A2e7A4B017, 03df04fb87b31ae168a607a99c10ad36f0b2d32f23ff177998d6ff3e12f1fc1991, KwJEsaBJnKLfwN1aLuvjmUone48KFDmnPRkZLmYigewP6F9sQMbA
m/44'/60'/0'/0/80, 0xca1fB24f6dc0E0B03BC264512606d7F70054E43c, 02d2f485cd522a68fe96c41775139391c4c2052af6596d643da0f339054b5eb6ca, L5YWkSWhWs6W382YN3zerqUHsAQYfd5Y9EfdJM1fEGLG1BpCpE7D
m/44'/60'/0'/0/81, 0xc276323B8463E04BE677E1a154eF19E841367B1e, 0354aa681e1ed03a4ce09c58f90c0978ba17b4d1fb52f9b51598451580491455596, KzfUoLux2Si322jGqfr9xpPTKieNcPbgaA86ekuhdd4nFxhgCRow
m/44'/60'/0'/0/82, 0xbb15589F5eff45c9CBC544f7C092d569EeC2A142, 02d5d536edb96c80499355467813496336e6b355f6ea0e4aceb1e8345fc531fe864, KyHKcgvTjG81JhEm1dhrtD9BQMbWo3MhLSgmQ2a9FquJpg5GcFrG
m/44'/60'/0'/0/83, 0x092132BAaE8B72128fa6627D1C6734Fd7a4203C1, 023817c7d70264c9967c949e50f0d35b826a63efaba50154da0b5eecaed13f97bc, KzT1y57P5qZ3uwov6ykJLdRmYicFAW8Fhpzd1u39DNJYVrm28Dqn
m/44'/60'/0'/0/84, 0x113583553Da2C72Ab1a55b67054aFAB9F3b75BB9, 02cc2b09bad8dd431bd40dce81ce7dd7b275973Db8f421453a2b71958d80022282, L1fB3CKvr99Sxentq2bmaXxR7gBosuyuRtnTq3vuTQiv1xk4VrM
m/44'/60'/0'/0/85, 0xA3f971C046eded3e43aF5b3949Beb7753DD52fdc, 035ee7651cdb23040be344efa993b2dc35e060ccc4089bf395ef8e34843301895 3, L4vrvcuGyrUnD6uGqY8yABC74V6kfFk7QGUfHpfiV5YJp7cb12tQ
m/44'/60'/0'/0/86, 0xe6bD57020A8928b0D6928A2456251d711661DD0c, 02f2228dc32749552dd38e405727d17f01d886cbce57a688b2b7818186ccc100d7, KwF3T5TWmUV9RYK55qwAkse8JBik9RPJd4Z9N3fX5jMyCBV5aSrc
m/44'/60'/0'/0/87, 0xf59cCFa2661B4EE0212Db03751b8f58735bF92f8, 02d76f44e5b1903e12a18104f6b95aa8fd8e5bf5598b1a0dbaa65cfe457342b4bc, KwJRcettj4Smpnfo9tHeN97yp9LeZbNTUsNngZr7K2TSjhvNcRYo
m/44'/60'/0'/0/88, 0x565f094A022E7dDbe28EED0308bfF5AFA4E481B8, 03c5c20a8c8ad78a2188cf6deef10377f8ae6676cf5d7a61fb0aa8df07e47459f3, Kz9bsGXexHmA498oYtMUy5hLYiRvusGrQ51h6uwgdsKTWEHbPthr
m/44'/60'/0'/0/89, 0xe0a28581140e5713Ad7eB726Ab9749E7bd7e2A9a, 030a1b5aa323720f13fbdcb63db0a8953330dc109081c4c3bf3391df7912f72668, L5mSfGxa8gQM2ou8PsRT5pLCJRTkjqQHcTqAgodvZWwzCCrnvMGM
m/44'/60'/0'/0/90, 0x979ce65b4410aecC236bCE0a73a18CD6b46cFc1A, 0348f42c36d814f053ef2e894c05c58e706a9d8da9f0844d08eb53e662b1cfb1b2, L2CktBNPqMLyzcyXdR1RyUQdzHowfbDVy6V8h3JD8U5BH2HcHK6F
m/44'/60'/0'/0/91, 0x9e154FB6a371Bd38805421bDa0eaf8F5E7192bE0, 03098f6e64e5e8ceccf09d3b7a9a4ab2fe2a3497ce9ea560e7fc89e9805aab75d4, L3kEV8ZA5y7vDGc3BbZcpuKJfYUofiA1YXwU3M2yhCZAYVofS4db
m/44'/60'/0'/0/92, 0x9DfCc0422ddF3073d63d6eBD71E3f10fBB24be46, 038284ebd1abeeddd8bc9d14e743edd9516e261fbe49b2c1320eab8f8774ac5614, L4Tz3iQ8bTPPpYUrPHeYUNk8DXqVnsuQEfpxtoQM6WUi6xjSDAWQ
m/44'/60'/0'/0/93, 0x2D203EF465a8ce35Ba9e1C8153035687EB934BA9, 025992bdb7dfa1763c58a651d0a7816a5429a8f5f8c145a3282d17c00ecef0f63a, L3fVBrkgZs6kpHTQE1ftmkocj12qPuviRnoTcdutw5Jb1zn8Rwb3
m/44'/60'/0'/0/94, 0xE451dBDD5130B6b29A3E938999c60B76Cd2d75cB, 022af8d03f7c3cf0f7ecc3755d44a3fbde6f714b9f0dc807ab75d1f0143089fb39, Kxjm6NUduqNtQzp6NdWZpDK5SAWDyRmZ65wJgmkrjFyqXgmr9GKk
m/44'/60'/0'/0/95, 0xA56ccfA9380FbF2043233acc4eF1BDE96Ab41a42, 039806c7e51b85d3053db1c0caa4a5d722b7315fdd772d2b0317d9dc96c424732, KxqCqBFcrC44jeujmeoem3rDpUsmRbVVK1FQNoYgQmX5BQMgSKea
m/44'/60'/0'/0/96, 0x9F6FF2d2156deb0871483ce6507b0880B3c9F, 031e34b4c9230def93498b470f1525d97828b38797d08f5d112d009658e47bc73a, L5CdYWq73yuUksL7QF3BCh7XiV7aPpd9V6e4BoLuFX3BKpJ9h
m/44'/60'/0'/0/97, 0xA24f23a0502adF65bd1892254BF011482bAF25Ce, 03dd96888d95b3a785de342987a3aaffb055ebb552303389de4935262f44cdfc55, L3yyrk6m1ZiyNBp9CAnqZQKPad889GLg5mVNaUBReX8vAcTpK83Z
m/44'/60'/0'/0/98, 0xD6b4bc902dDF4886153cfC64698fC55191FAcB42, 03082cb8ae4c10279837fc09114e742d65091f9e43728201f84764345290df8eaea, L3wsDx8jV7LFR6RpbRMw57gWv8sHq2vWQB13Y8xUH3wZ2jV1XtQ
m/44'/60'/0'/0/99, 0x3560455e7C230971c18AE58b7Dd92aaABFC075Fc, 03b8f0d9ebbf28f9c19ca01c74e0daeac9b5354c3c5a5e65cc51b89926cc7cd9e7, L1UeU3aUpsydkpkGYqG1Qe8r8zhoupWh9ixHPdo2ScU1cFwkegp
m/44'/60'/0'/0/100, 0x4A3938850291d981CD81Fbd7452c0168acCfe454, 02564b0d72e37816456af2dafa1c8985e45e13e37ca1aa3817c9e95f08cf85c242, L2SxwWMokuw9n6Vo72vedXAzNqUdTLFVpDN5Aeqq9Qecq6Xq4wNa
Command Line Interface (CLI)
EXECUTE
CLEAR


Hierarchical Deterministic Wallet
WALLET
GENERATE
DUMPS
DONATION
HELP
DONATIONS
CORE TEAM
CHARITY
X
CRYPTOCURRENCY
Ethereum
ENTROPY
6b090d62c297a
PUBLIC KEY TYPE
Compressed
0xCCAad7A87fd81...6B213b228B
COPY
CRYPTOCURRENCY
Ethereum
This donation is for the core team, because without them, we'd be googling 'how to turn on a computer.' Cheers to our tech wizards!
DERIVATION
CUSTOM
BIP44
PURPOSE
44
0-100
FORMAT
CSV
at:path,address,public_key,wif
GENERATE
GENERATE AND SAVE

Supported Standards

- BIP32: Hierarchical Deterministic Wallets
- BIP38: Passphrase-protected private key
- BIP39: Mnemonic Code for Generating Deterministic Keys
- BIP44: Multi-Account Hierarchy for Deterministic Wallets
- BIP49: Derivation scheme for P2WPKH-nested-in-P2SH based accounts
- BIP84: Derivation scheme for P2WPKH based accounts
- BIP86: Key Derivation for Single Key P2TR Outputs
- BIP141: Segregated Witness (Consensus layer)
- CIP1852: HD (Hierarchy for Deterministic) Wallets for Cardano
- Algorand: Entropy, Mnemonic and Seed standards
- Electrum-V1: Entropy, Mnemonic and Seed standards
- Electrum-V2: Entropy, Mnemonic and Seed standards
- Cardano: Seed standards
- Monero: Entropy, Mnemonic and Seed standards

Available Cryptocurrencies

This library simplifies the process of creating a new hierarchical deterministic wallets for:

	Cryptocurrency	Symbol	Networks	Coin Type
1.	Adcoin	ACC	mainnet	161
2.	Akash-Network	AKT	mainnet	118
3.	Algorand	ALGO	mainnet	283
4.	Anon	ANON	mainnet	220
5.	Aptos	APT	mainnet	637
6.	Arbitrum	ARB	mainnet	60
7.	Argoneum	AGM	mainnet	421
8.	Artax	XAX	mainnet	219
9.	Aryacoin	AYA	mainnet	357
10.	Asiacoin	AC	mainnet	51
11.	Auroracoin	AUR	mainnet	85
12.	Avalanche	AVAX	mainnet	9000
13.	Avian	AVN	mainnet	921
14.	Axe	AXE	mainnet	4242
15.	Axelar	AXL	mainnet	118
16.	Band-Protocol	BAND	mainnet	494
17.	Bata	BTA	mainnet	89
18.	Beetle-Coin	BEET	mainnet	800
19.	Bela-Coin	BELA	mainnet	73
20.	Binance	BNB	mainnet	714
21.	Bit-Cloud	BTDX	mainnet	218

22. Bitcoin	BTC	mainnet, testnet, regtest	0
23. Bitcoin-Atom	BCA	mainnet	185
24. Bitcoin-Cash	BCH	mainnet, testnet, regtest	145
25. Bitcoin-Cash-SLP	SLP	mainnet, testnet	145
26. Bitcoin-Gold	BTG	mainnet	156
27. Bitcoin-Green	BITG	mainnet	222
28. Bitcoin-Plus	XBC	mainnet	65
29. Bitcoin-Private	BTCP	mainnet, testnet	183
30. Bitcoin-SV	BSV	mainnet	236
31. BitcoinZ	BTCZ	mainnet	177
32. Bitcore	BTX	mainnet	160
33. Bit-Send	BSD	mainnet	91
34. Blackcoin	BLK	mainnet	10
35. Blocknode	BND	mainnet, testnet	2941
36. Block-Stamp	BST	mainnet	254
37. Bolivarcoin	BOLI	mainnet	278
38. Brit-Coin	BRIT	mainnet	70
39. Canada-eCoin	CDN	mainnet	34
40. Cannacoin	CCN	mainnet	19
41. Cardano	ADA	mainnet, testnet	1815
42. Celo	CELO	mainnet	52752
43. Chihuahua	HUA	mainnet	118
44. Clams	CLAM	mainnet	23
45. Club-Coin	CLUB	mainnet	79
46. Compcoin	CMP	mainnet	71
47. Cosmos	ATOM	mainnet	118
48. CPU-Chain	CPU	mainnet	363
49. Crane-Pay	CRP	mainnet	2304
50. Crave	CRAVE	mainnet	186
51. Dash	DASH	mainnet, testnet	5
52. DeepOnion	ONION	mainnet	305
53. Defcoin	DFC	mainnet	1337
54. Denarius	DNR	mainnet	116
55. Diamond	DMD	mainnet	152
56. Digi-Byte	DGB	mainnet	20
57. Digitalcoin	DGC	mainnet	18
58. Divi	DIVI	mainnet, testnet	301
59. Dogecoin	DOGE	mainnet, testnet	3
60. eCash	XEC	mainnet, testnet	145
61. E-coin	ECN	mainnet	115
62. EDR-Coin	EDRC	mainnet	56
63. e-Gulden	EFL	mainnet	78
64. Einsteinium	EMC2	mainnet	41
65. Elastos	ELA	mainnet	2305

66. Energi	NRG	mainnet	9797
67. EOS	EOS	mainnet	194
68. Ergo	ERG	mainnet, testnet	429
69. Ethereum	ETH	mainnet	60
70. Europe-Coin	ERC	mainnet	151
71. Evrmore	EVR	mainnet, testnet	175
72. Exclusive-Coin	EXCL	mainnet	190
73. Fantom	FTM	mainnet	60
74. Feathercoin	FTC	mainnet	8
75. Fetch.ai	FET	mainnet	118
76. Filecoin	FIL	mainnet	461
77. Firo	FIRO	mainnet	136
78. Firstcoin	FRST	mainnet	167
79. FIX	FIX	mainnet, testnet	336
80. Flashcoin	FLASH	mainnet	120
81. Flux	FLUX	mainnet	19167
82. Foxdcoin	FOXD	mainnet, testnet	175
83. Fuji-Coin	FJC	mainnet	75
84. Game-Credits	GAME	mainnet	101
85. GCR-Coin	GCR	mainnet	49
86. Go-Byte	GBX	mainnet	176
87. Gridcoin	GRC	mainnet	84
88. Groestl-Coin	GRS	mainnet, testnet	17
89. Gulden	NLG	mainnet	87
90. Harmony	ONE	mainnet	1023
91. Helleniccoin	HNC	mainnet	168
92. Hempcoin	THC	mainnet	113
93. Horizen	ZEN	mainnet	121
94. Huobi-Token	HT	mainnet	553
95. Hush	HUSH	mainnet	197
96. Icon	ICX	mainnet	74
97. Injective	INJ	mainnet	60
98. InsaneCoin	INSN	mainnet	68
99. Internet-Of-People	IOP	mainnet	66
100. IRISnet	IRIS	mainnet	566
101. IX-Coin	IXC	mainnet	86
102. Jumbucks	JBS	mainnet	26
103. Kava	KAVA	mainnet	459
104. Kobocoin	KOBO	mainnet	196
105. Komodo	KMD	mainnet	141
106. Landcoin	LDCN	mainnet	63
107. LBRY-Credits	LBC	mainnet	140
108. Linx	LINX	mainnet	114
109. Litecoin	LTC	mainnet, testnet	2

110.	Litecoin-Cash	LCC	mainnet	192
111.	LitecoinZ	LTZ	mainnet	221
112.	Lkrcoin	LKR	mainnet	557
113.	Lynx	LYNX	mainnet	191
114.	Mazacoin	MZC	mainnet	13
115.	Megacoin	MEC	mainnet	217
116.	Metis	METIS	mainnet	60
117.	Minexcoin	MNX	mainnet	182
118.	Monacoin	MONA	mainnet	22
119.	Monero	XMR	mainnet, stagenet, testnet	128
120.	Monk	MONK	mainnet	214
121.	MultiversX	EGLD	mainnet	508
122.	Myriadcoin	XMY	mainnet	90
123.	Namecoin	NMC	mainnet	7
124.	Nano	XNO	mainnet	165
125.	Navcoin	NAV	mainnet	130
126.	Near	NEAR	mainnet	397
127.	Neblio	NEBL	mainnet	146
128.	Neo	NEO	mainnet	888
129.	Neoscoin	NEOS	mainnet	25
130.	Neurocoin	NRO	mainnet	110
131.	New-York-Coin	NYC	mainnet	179
132.	Nine-Chronicles	NCG	mainnet	567
133.	NIX	NIX	mainnet	400
134.	Novacoin	NVC	mainnet	50
135.	NuBits	NBT	mainnet	12
136.	NuShares	NSR	mainnet	11
137.	OK-Cash	OK	mainnet	69
138.	OKT-Chain	OKT	mainnet	996
139.	Omni	OMNI	mainnet, testnet	200
140.	Onix	ONX	mainnet	174
141.	Ontology	ONT	mainnet	1024
142.	Optimism	OP	mainnet	60
143.	Osmosis	OSMO	mainnet	118
144.	Particl	PART	mainnet	44
145.	Peercoin	PPC	mainnet	6
146.	Pesobit	PSB	mainnet	62
147.	Phore	PHR	mainnet	444
148.	Pi-Network	PI	mainnet	314159
149.	Pinkcoin	PINK	mainnet	117
150.	Pivx	PIVX	mainnet, testnet	119
151.	Polygon	MATIC	mainnet	60
152.	PoSW-Coin	POSW	mainnet	47
153.	Potcoin	POT	mainnet	81

154.	Project-Coin	PRJ	mainnet	533
155.	Putincoin	PUT	mainnet	122
156.	Qtum	QTUM	mainnet, testnet	2301
157.	Rapids	RPD	mainnet	320
158.	Ravencoin	RVN	mainnet, testnet	175
159.	Reddcoin	RDD	mainnet	4
160.	Ripple	XRP	mainnet	144
161.	Ritocoin	RITO	mainnet	19169
162.	RSK	RBTC	mainnet, testnet	137
163.	Rubycoin	RBY	mainnet	16
164.	Safecoin	SAFE	mainnet	19165
165.	Saluscoin	SLS	mainnet	572
166.	Scribe	SCRIBE	mainnet	545
167.	Secret	SCRT	mainnet	529
168.	Shadow-Cash	SDC	mainnet, testnet	35
169.	Shentu	CTK	mainnet	118
170.	Slimcoin	SLM	mainnet, testnet	63
171.	Smileycoin	SMLY	mainnet	59
172.	Solana	SOL	mainnet	501
173.	Solarcoin	SLR	mainnet	58
174.	Stafi	FIS	mainnet	907
175.	Stash	STASH	mainnet, testnet	49344
176.	Stellar	XLM	mainnet	148
177.	Stratis	STRAT	mainnet, testnet	105
178.	Sugarchain	SUGAR	mainnet, testnet	408
179.	Sui	SUI	mainnet	784
180.	Syscoin	SYS	mainnet	57
181.	Terra	LUNA	mainnet	330
182.	Tezos	XTZ	mainnet	1729
183.	Theta	THETA	mainnet	500
184.	Thought-AI	THT	mainnet	502
185.	TOA-Coin	TOA	mainnet	159
186.	Tron	TRX	mainnet	195
187.	TWINS	TWINS	mainnet, testnet	970
188.	Ultimate-Secure-Cash	USC	mainnet	112
189.	Unobtanium	UNO	mainnet	92
190.	Vcash	VC	mainnet	127
191.	VeChain	VET	mainnet	818
192.	Verge	XVG	mainnet	77
193.	Vertcoin	VTC	mainnet	28
194.	Viacoin	VIA	mainnet, testnet	14
195.	Vivo	VIVO	mainnet	166
196.	Voxels	VOX	mainnet	129
197.	Virtual-Cash	VASH	mainnet	33

198.	Wagerr	WGR	mainnet	0
199.	Whitecoin	XWC	mainnet	559
200.	Wincoin	WC	mainnet	181
201.	XinFin	XDC	mainnet	550
202.	XUEZ	XUEZ	mainnet	225
203.	Ycash	YEC	mainnet	347
204.	Zcash	ZEC	mainnet, testnet	133
205.	ZClassic	ZCL	mainnet	147
206.	Zetacoin	ZET	mainnet	719
207.	Zilliqa	ZIL	mainnet	313
208.	ZooBC	ZBC	mainnet	883

Team Members

- **Meheret Tesfaye Batu**

  Pythonista, Cryptographer & Blockchain Engineer at Qtum blockchain

  Role: Creator and Main-maintainer behind this HDWallet project

- **Eyoel TadesseYaea**

  Desktop App Engineer

  Role: Maintainer desktop application

- **Abenezer Lulseged Wube**

  Desktop UI Designer

  Role: Design desktop UI

- **Betselot Kidane Tesema**

  UX/UI Designer

  Role: Logo, Fonts and other art design

Thank you!