

# Bitcoin Wallet Architecture

*Hierarchical Deterministic (HD) Wallet Components*

## Seed Phrase (Mnemonic)

12 or 24 words - Master backup for entire wallet

e.g., "witch collapse practice feed shame open despair creek road again ice least" BIP39/BIP32

### Master Private Key

☐ Never exposed

### Derivation Path

m/44'/0'/0'/0/0

#### Account 0

##### Private Key

☐

##### Public Key

✓

##### Address

1A1zP1...

#### Account 1

##### Private Key

☐

##### Public Key

✓

##### Address

3J98t1...

...

Multiple Accounts

### Blockchain Interaction

- Balance Calculation:
- Query blockchain for UTXOs
  - Sum unspent outputs
  - Display to user

### Wallet Functions

- ☐ Send: Sign tx with private key
- ☐ Receive: Generate new address
- ☐ Balance: Query blockchain
- ☐ History: Fetch transactions
- ☐ Backup: Export seed phrase

⚠ Security: Never share seed phrase or private keys!  
Whoever has the seed can control ALL funds in the wallet.