Wallets

Objectives

Objective

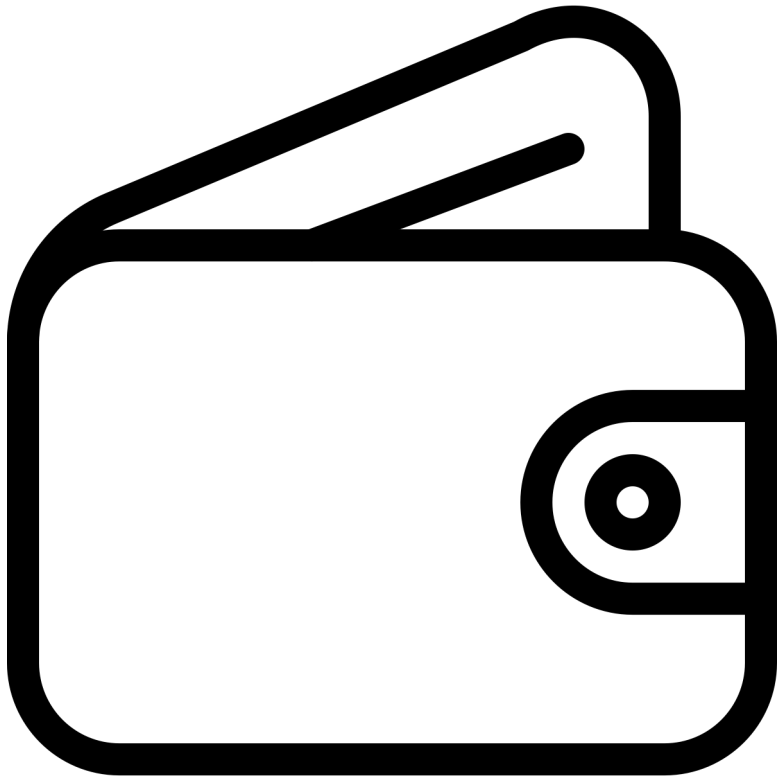
Explain key features of the three classes of wallets

Objective

Describe how wallets are programmed to interact with a blockchain and help end users

What is a Wallet?

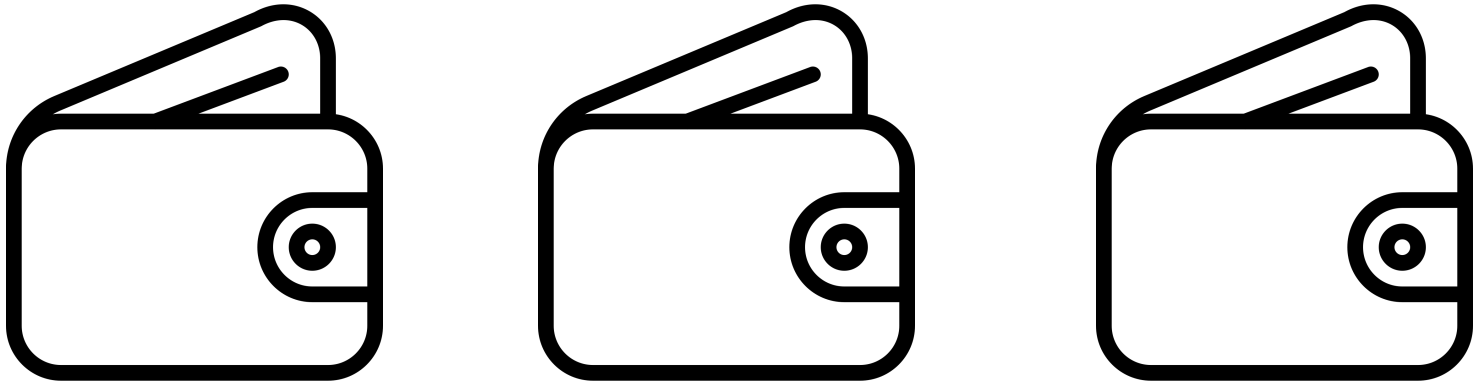
- An application that stores and manages keys
- Possibly the most important application that interacts with a blockchain
- Secure storage and access to private and public keys crucial for signing messages/transactions



Classes of Wallets

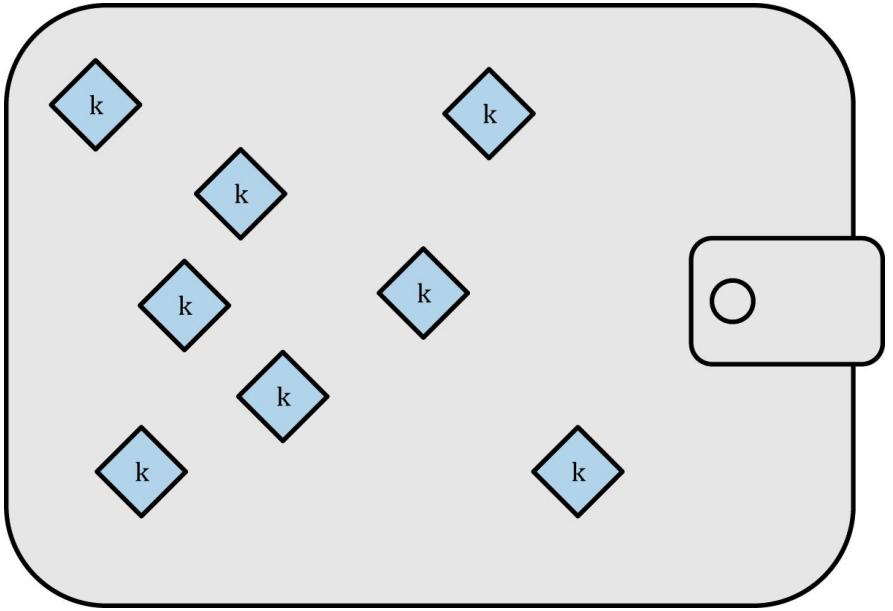
Three main classes of wallets

- Nondeterministic
- Deterministic
- Hierarchical



Nondeterministic Wallets

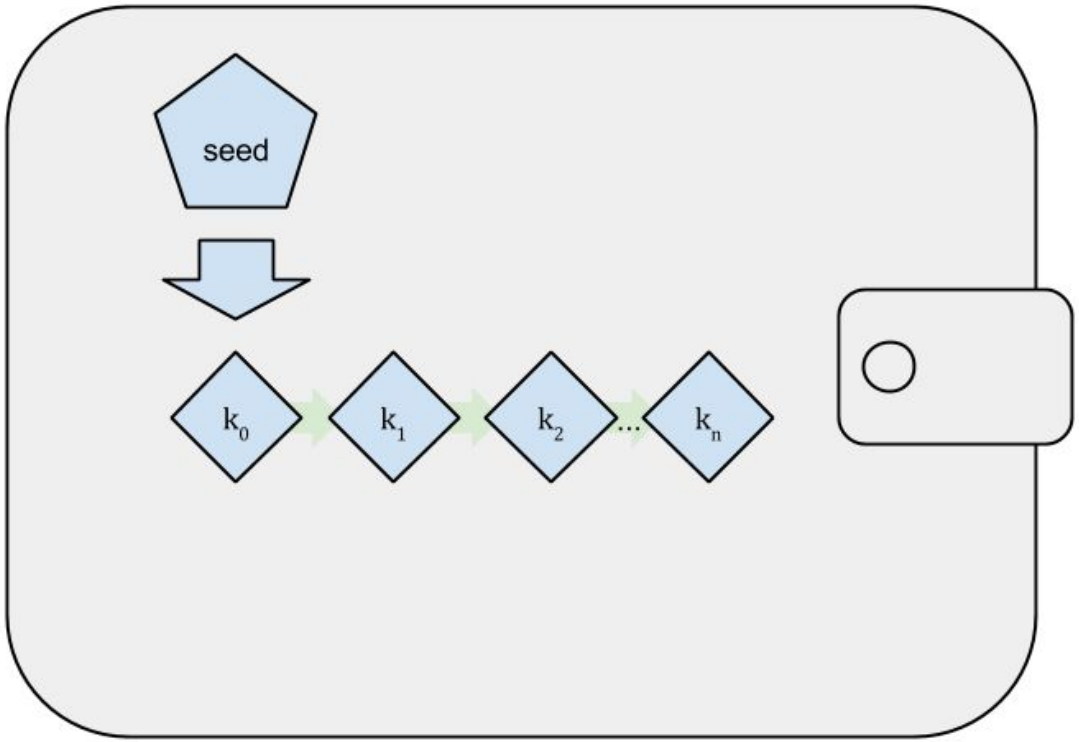
- Contain private keys (source of public keys)
- Independently generated at random
- Require frequent backups for every key generated
- Value associated with the keys may become inaccessible



Deterministic Wallets

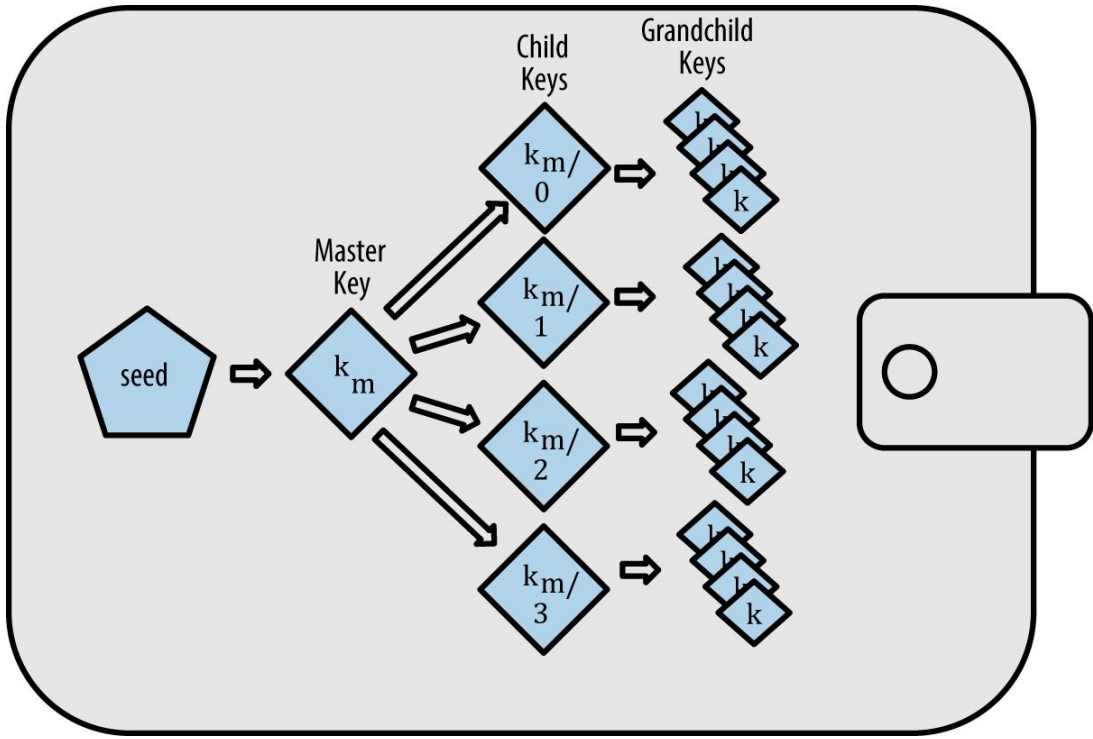
- Contain private keys collectively derived from an initial seed
- Can be derived by a simple algorithm such as
- Allow for easy backup and storage of keys
- Industry standard for most end users

the n^{th} private key = SHA256(seed + n)



Hierarchical Deterministic (HD) Wallets

- A subset of deterministic wallets
- Keys are derived from a single seed in a tree structure
- Keys may be derived from parent keys, which can derive their own child keys, which can derive grandchildren keys…
- Allows for more structure and varied uses within a single wallet application
- Allows public keys to be generated without the associated private keys



Mnemonic Codes/Seeds

- A standard created in BIP 0039
  - For initial seed generation
  - For human-readable representation of a seed
- Easy-to-remember words that represent a seed
- For seeds used in deterministic wallets
- Mnemonic code length can range from 12 to 24 words (depends on required entropy level)