Lab 05:
Building a Multisignature Wallet

Nataliya Urakhchina

BLOCKCHAIN
AT BERKELEY

LAB OUTLINE

1 ▶ TYPES OF CONTRACT WALLETS

2 ▶ MULTISIG WALLET

3 ▶ ASSIGNMENT

BASIC: WHAT IS A WALLET?

- At a high level:
  - An application that serves as the primary user interface.
  - Controls access to a user’s money, managing keys and addresses, tracking the balance, and creating and signing transactions.
- At a low level:
  - Refers to the data structure used to store and manage a user’s keys.

BASIC: WHAT IS A WALLET?

- Bitcoin wallet: ECDSA public/private keypair, usually 256 bit.
- Private key allows **sending** money out of the wallet.
- Public key allows **receiving** money to the wallet, also considered as the “wallet address”.
- Transactions can be viewed on the blockchain using the public key.

1

TYPES OF WALLETS

TWO PRIMARY TYPES

SEEN IN BITCOIN

- Nondeterministic wallets
  - Each key is independently generated from a random number.
  - The keys are not related to each other.

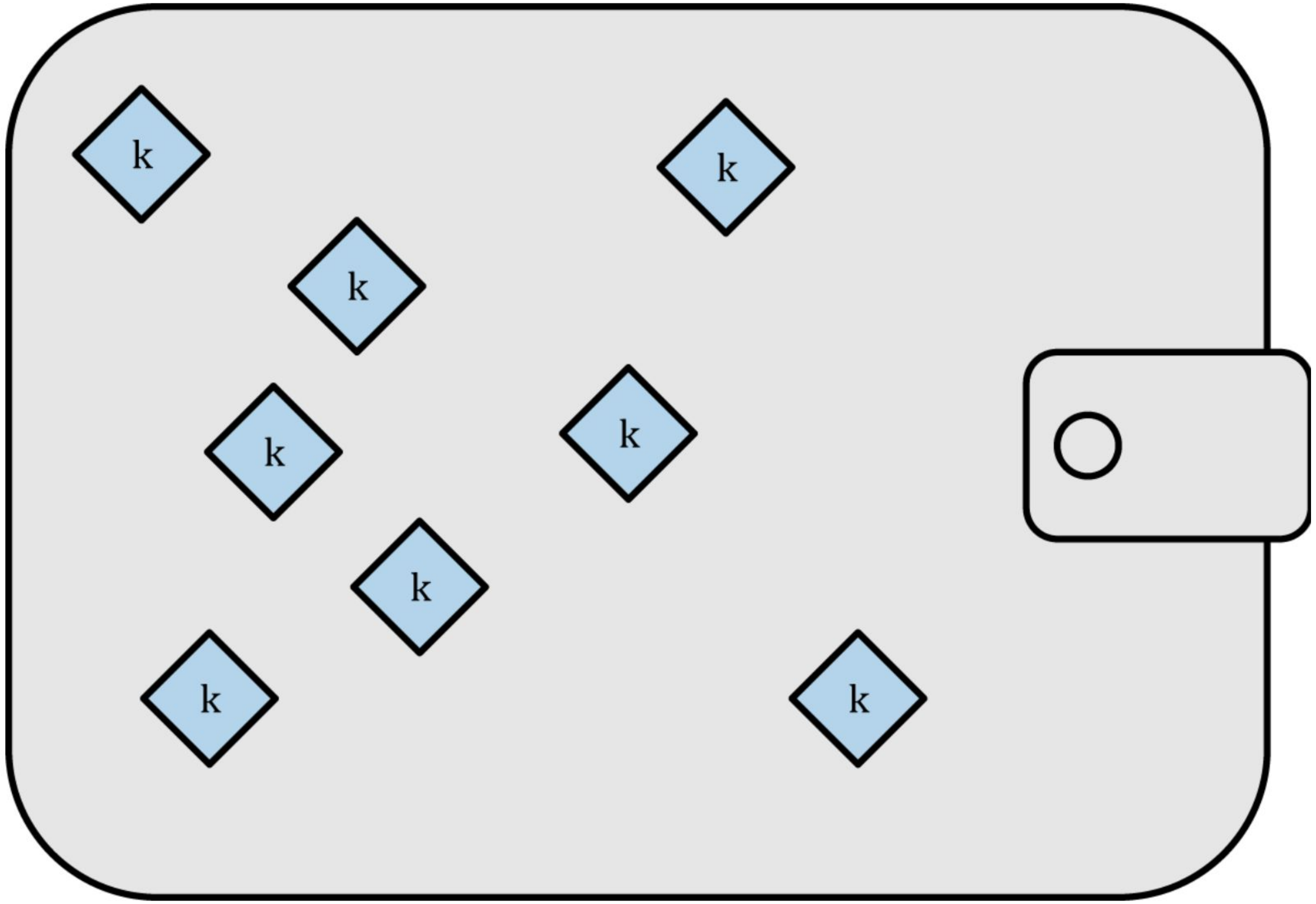
- Deterministic wallets
  - Where all the keys are derived from a single master key.
  - All the keys in this type of wallet are related to each other and can be generated again if one has the original seed.

AUTHOR: NATALIYA URAKHCHINA

NONDETERMINISTIC (RANDOM) WALLETS

- In the first Bitcoin wallet, wallets were a collection of randomly generated private keys.
- Stores private keys but also generates these private keys.
- For example, the original Bitcoin Core client pregenerates 100 random private keys when first started and generates more keys as needed, using each key only once.
- Example of what a nondeterminisitc wallet does:
  - generates **privateKey1**, as well as a corresponding **publicAddress1**
  - generates **privateKey2**, as well as a corresponding **publicAddress2**
- Disadvantage of random keys:
  - Must keep a copy of each key.
  - Each key must be backed up, or the funds it controls are irrevocably lost if the wallet becomes inaccessible.

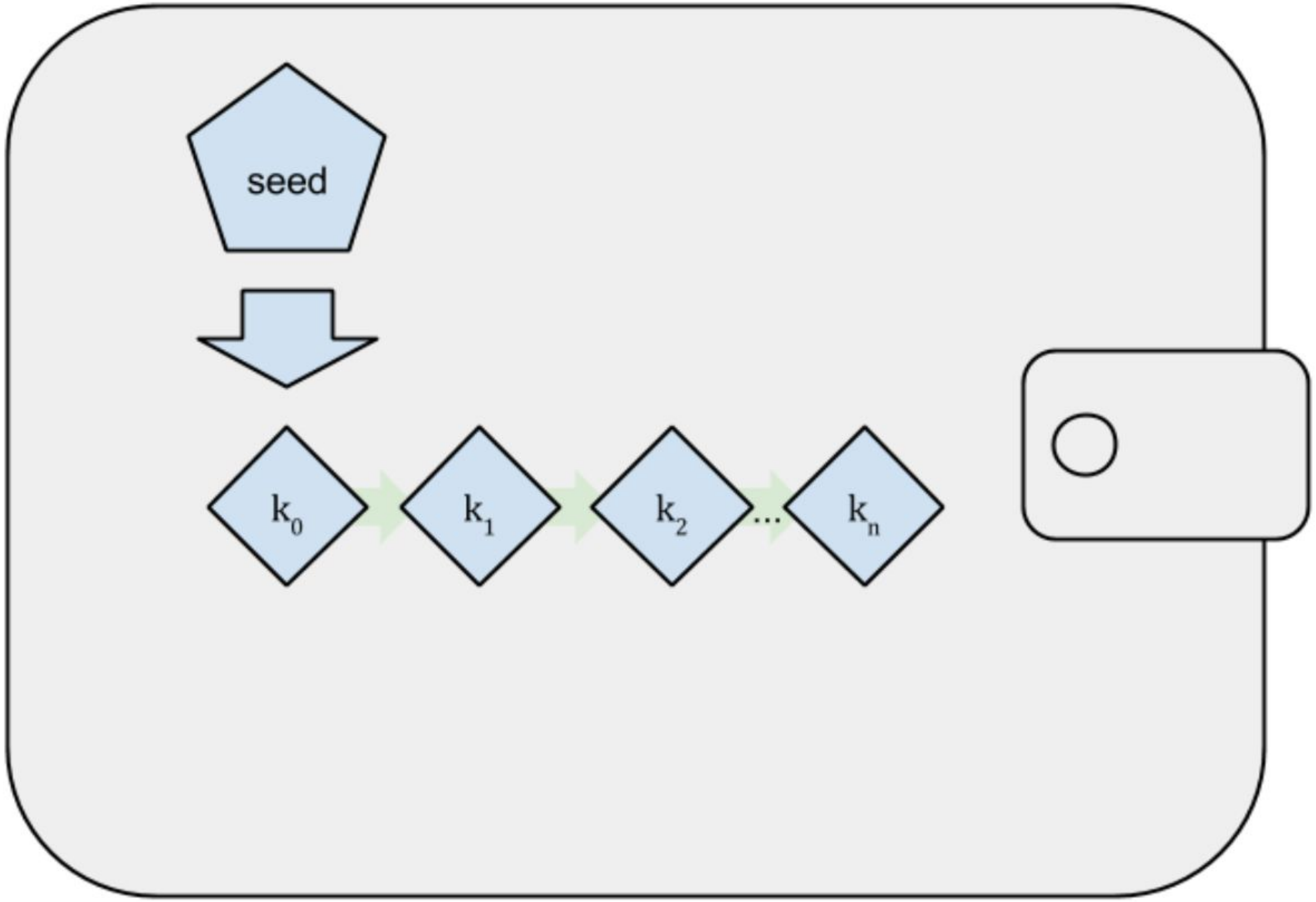
NONDETERMINISTIC (RANDOM) WALLETS



Source

Type-0 nondeterministic (random) wallet: a collection of randomly generated keys

DETERMINISTIC WALLETS

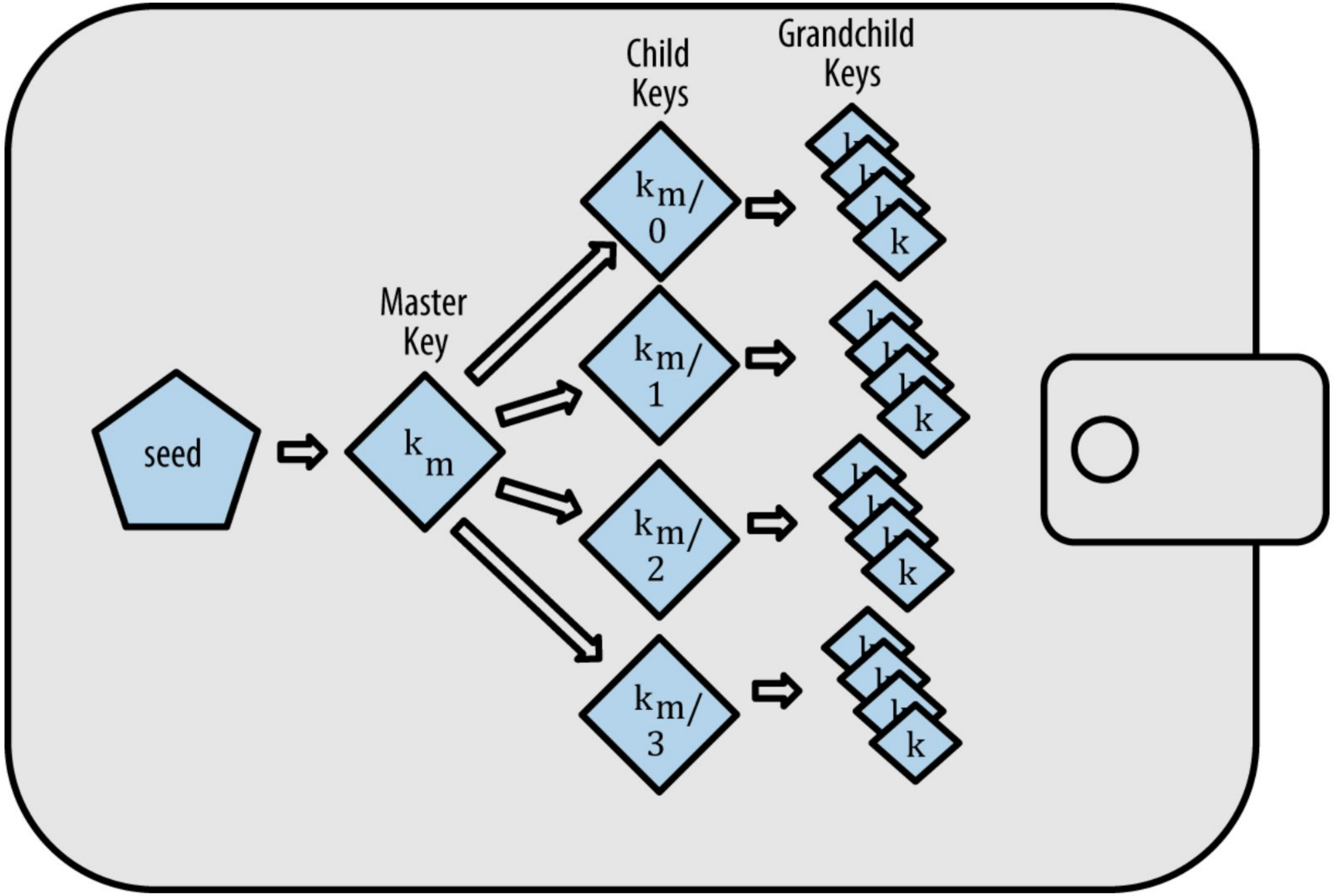


Source

Type-1 deterministic (seeded) wallet: a deterministic sequence of keys derived from a seed

AUTHOR: NATALIYA URAKHCHINA

HD WALLETS



Source

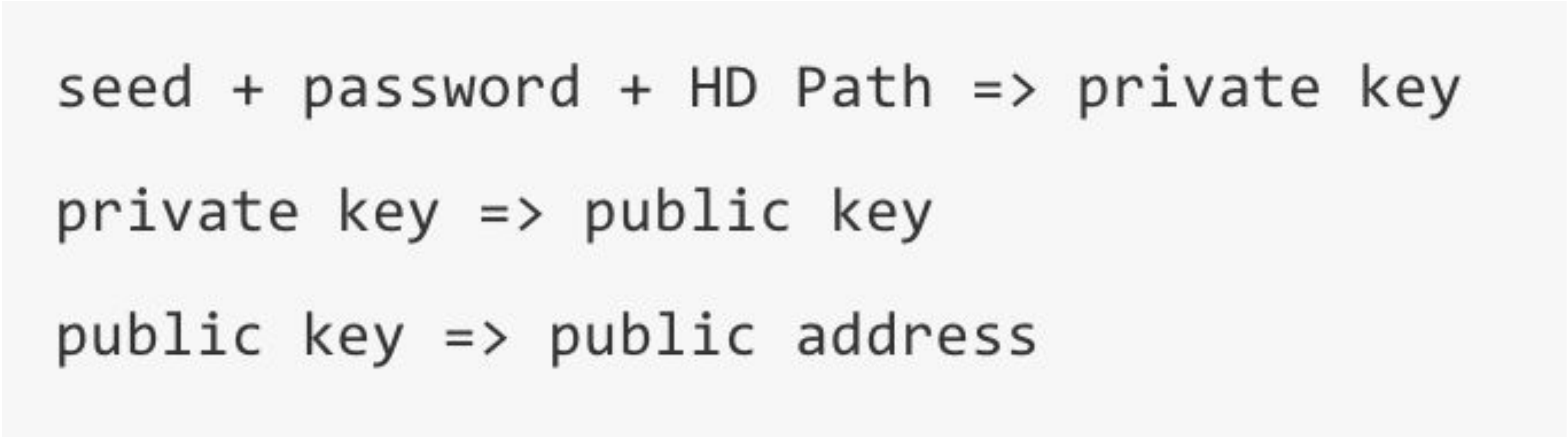
Type-2 HD wallet: a tree of keys generated from a single seed

SEEDS AND MNEMONICS

BIP39 SEEDS

- Special kinds of phrases that can generate private keys.
- Bip39 seed phrases are a standard in the cryptocurrency community.
- Mnemonic code words are word sequences that represent (encode) a random number used as a seed to derive a deterministic wallet

Bip39 Seed Phrase



```
seed + password + HD Path => private key

private key => public key

public key => public address
```

- In order to steal the funds out of a wallet, someone needs to know the Bip39 seed phrase, and the password.
- Then they can just guess all the various HD paths until they get the private key.

2

MULTI-SIG WALLET

MOTIVATION

- Contract Wallets can be setup as Multisig Wallets.
- Simple Wallets and Multisig Wallets are both examples of Contract Wallets.
- A Simple Wallet:
  - only one Account both creates and owns the wallet
- Multisig Wallet:
  - has several owner Accounts one of which will also be the creator Account.
  - M-of-N type wallets

MULTI-SIG WALLET USE CASES

- **Use case one:** You own some ether and want to store it securely but are concerned that just relying on a single private key may not be safe. So you create a Multisig Wallet, a 2-of-3 wallet, but all the owner Accounts are under your control, that is, you control all the private keys.

- **Use case two:** You set up a Multisig Account jointly owned by say two people, you and Alice. So you have one private key and Alice the other.

THE BASICS

WHAT A MULTI-SIGNATURE WALLET NEEDS

- A list of people who are allowed to do things
- Rules on how many of those people have to agree before it happens
- A way to receive ether
- A way to submit a request
- A way to agree to a request (and submit it if you are last)
- A way to resubmit the request if it fails

3

ASSIGNMENT

THE ASSIGNMENT

ETHEREUM MULTI SIG WALLET + BASIC WEB3 INTEGRATION AND EVENTS

- https://github.com/Blockchain-for-Developers/sp18-midterm-pt2

SEE YOU NEXT TIME