

# 한 번에 끝내는 블록체인 개발 A to Z

---

## Chapter 2

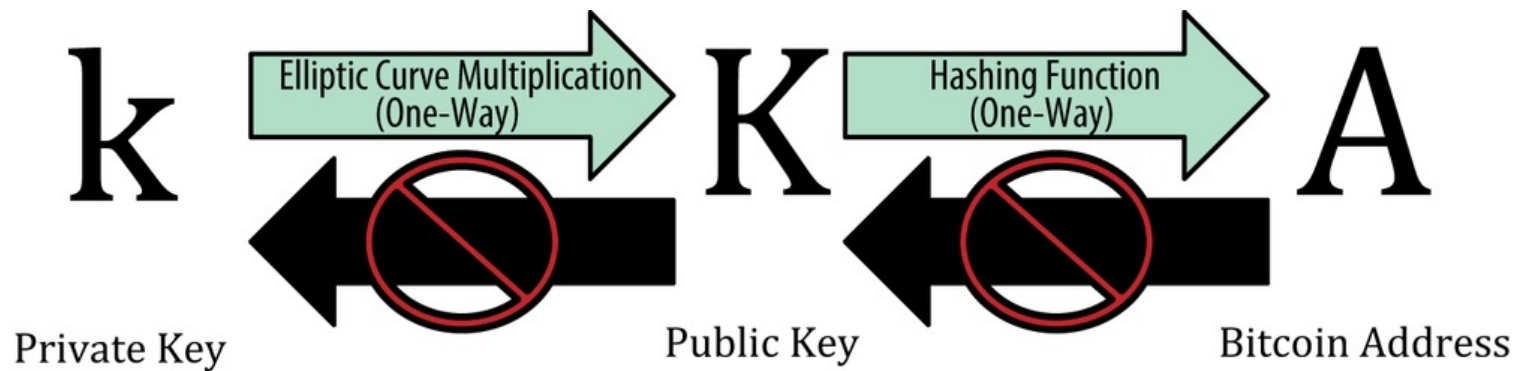
### 블록체인 Wallet 개발하기

Chapter 2

블록체인 Wallet 개발하기

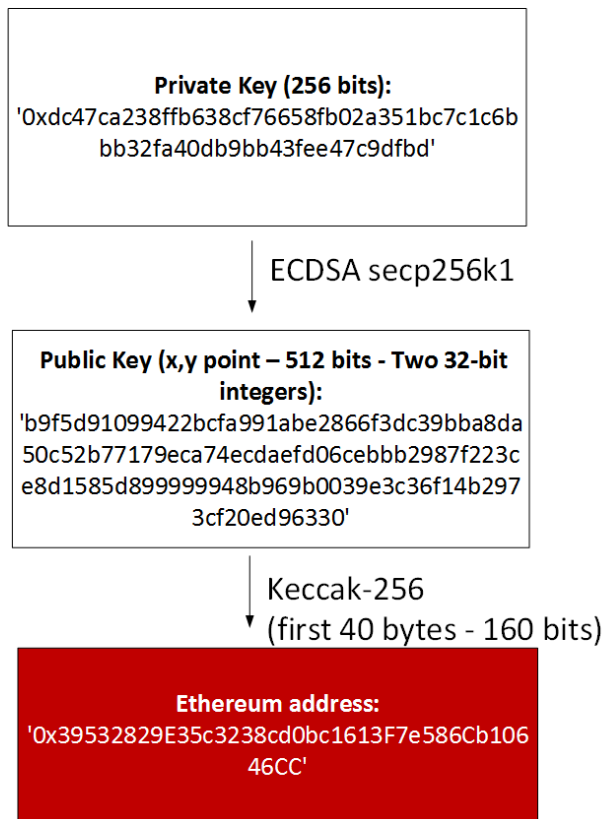
# Wallet 구조

# 지갑 주소 생성하기



# 지갑 주소 생성하기

- ECDSA : 타원곡선 알고리즘
- secp256k1: 타원곡선을 만들기 위한 상수 표준
- Keccak-256: 해시함수



# 니모닉 코드

- 지갑을 쉽게 복구하기 위한 단어
- 니모닉 != 프라이빗 키
- 시드 만들기가 중요한 것



METAMASK

< 뒤로

## 비밀 백업 구문 확인

각 구문을 선택하여 구문이 올바른지 확인하세요.

boil

brass

chicken

during

magic

now

random

ready

shift

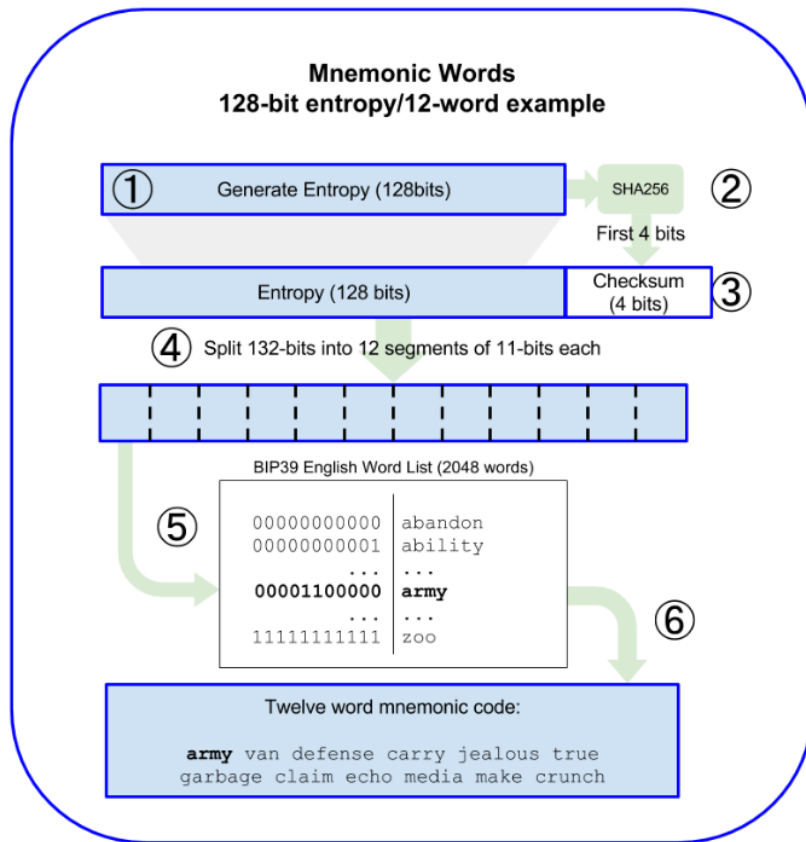
shine

tiny

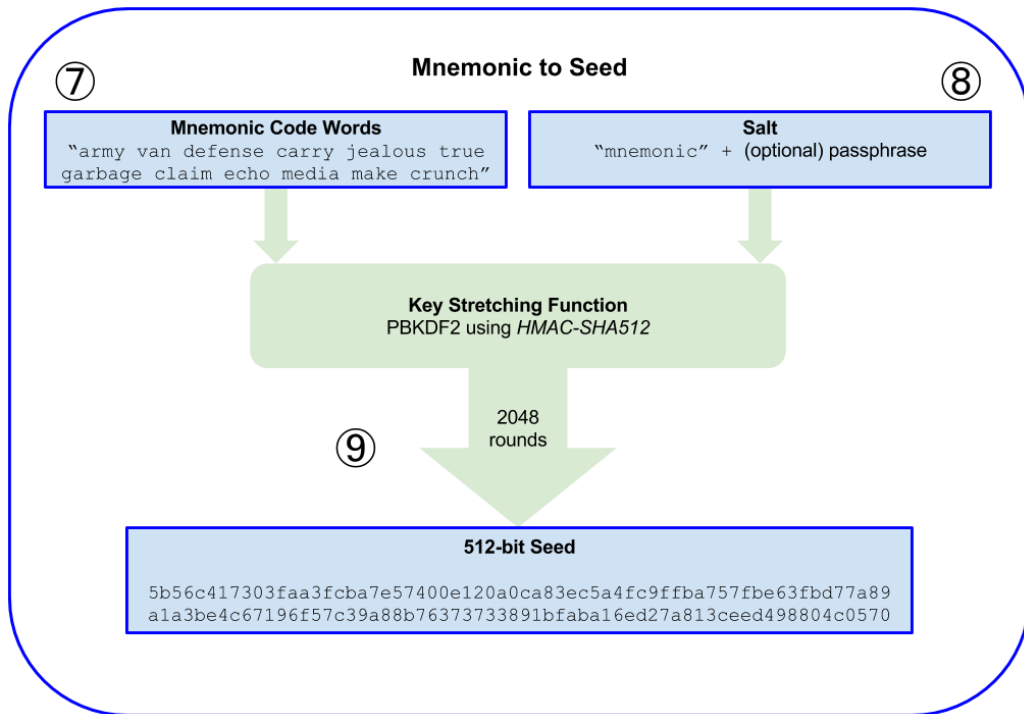
upon

확인

# 엔트로피에서 니모닉코드까지

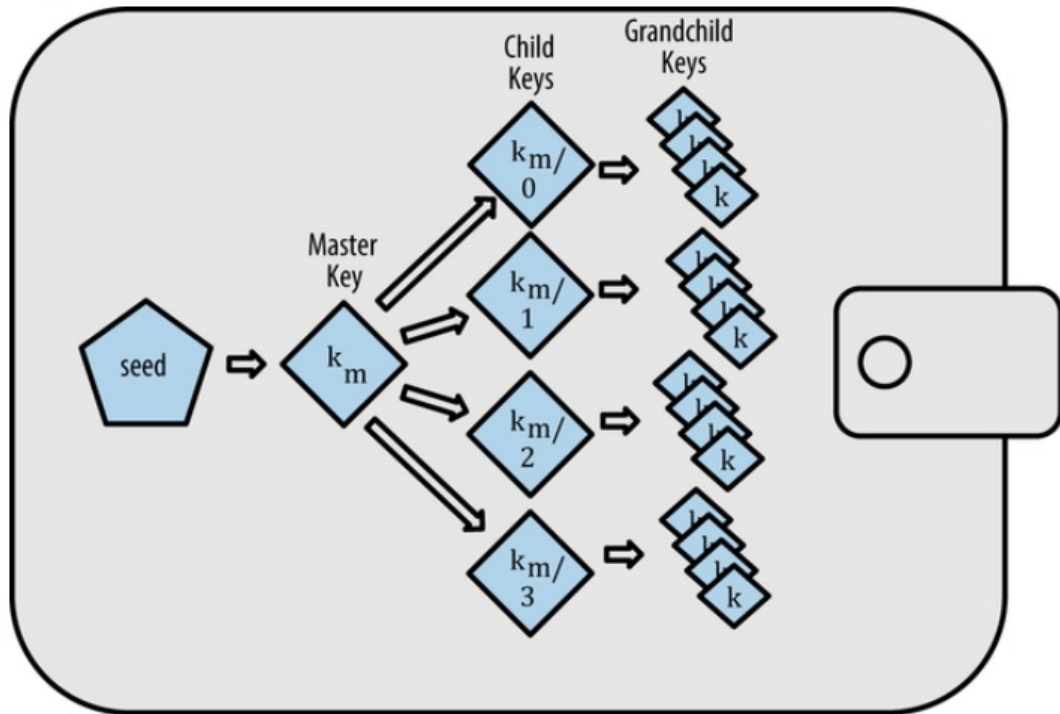


# 니모닉에서 시드까지



# HD 지갑

- 계층 결정적 지갑





# HD 지갑

## Mnemonic Code Converter

### Mnemonic

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect, since the words require a particular structure (the last word contains a checksum).

For more info see the [BIP39 spec](#).

Generate a random mnemonic: **GENERATE** 15 words, or enter your own below.

☐ Show entropy details

☐ Hide all private info

☒ Auto compute

Mnemonic Language English 日本語 Español 中文(简体) 中文(繁體) Français Italiano 한국어 Čeština Português

BIP39 Mnemonic forget inherit click report spread south august connect excuse energy rally belt canvas fix aisle

☐ Show split mnemonic cards

BIP39 Passphrase  
(optional)

BIP39 Seed

c56c761a70521dae2a9d3cf58882bf9b35f96ca08a8d9eea762c04f51f67e38ce9acbd50b7cfc691d80896e82bff165631b14e141ec9c327406ebe835ba8bb7

Coin

BTC - Bitcoin

<https://iancoleman.io/bip39>