한 번에 끝내는
블록체인 개발 A to Z

Chapter 2

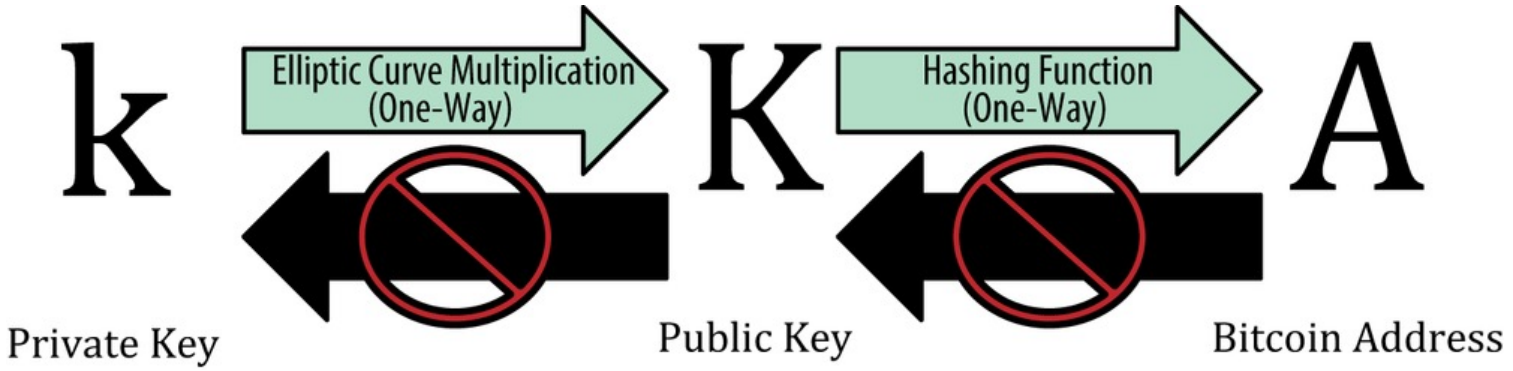
블록체인 Wallet 개발하기

Chapter 2

블록체인 Wallet 개발하기

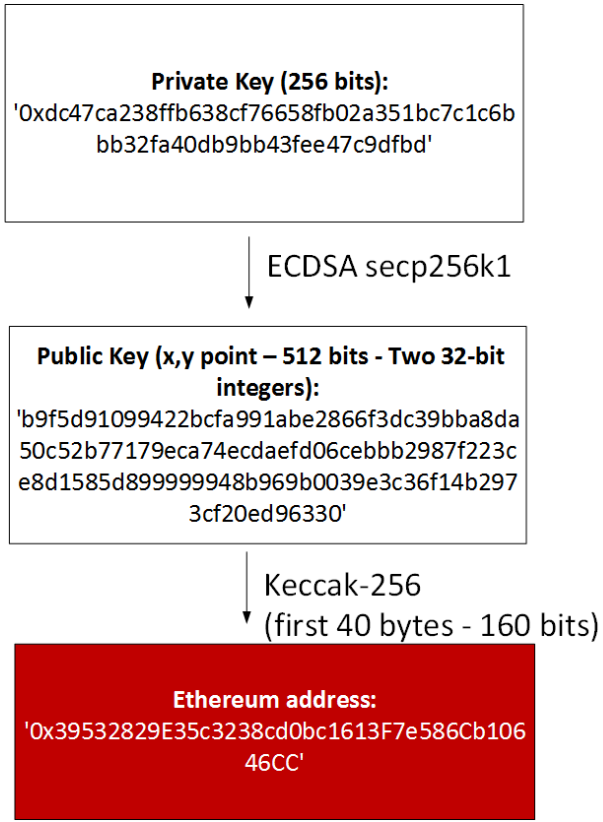
Wallet 구조

지갑 주소 생성하기


k
Elliptic Curve Multiplication
(One-Way)
K
Hashing Function
(One-Way)
A
Private Key
Public Key
Bitcoin Address

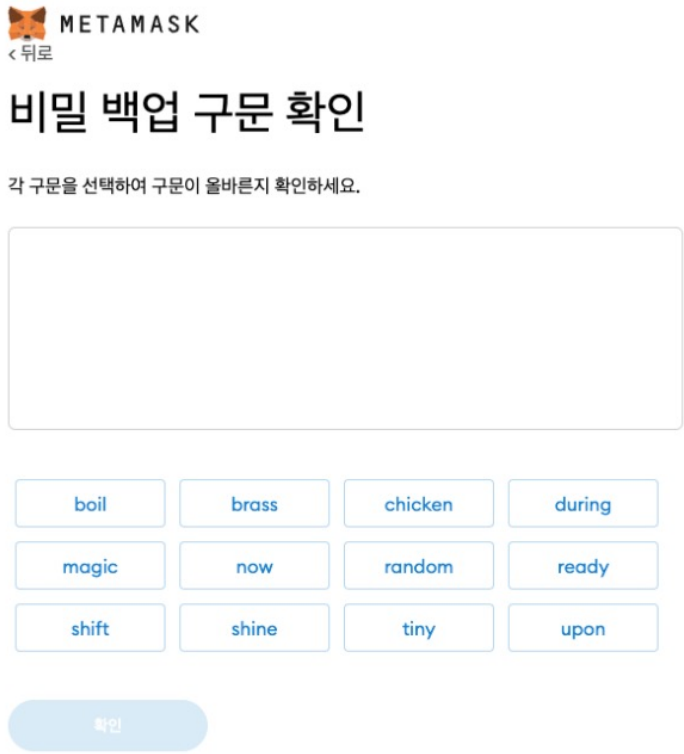
지갑 주소 생성하기

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

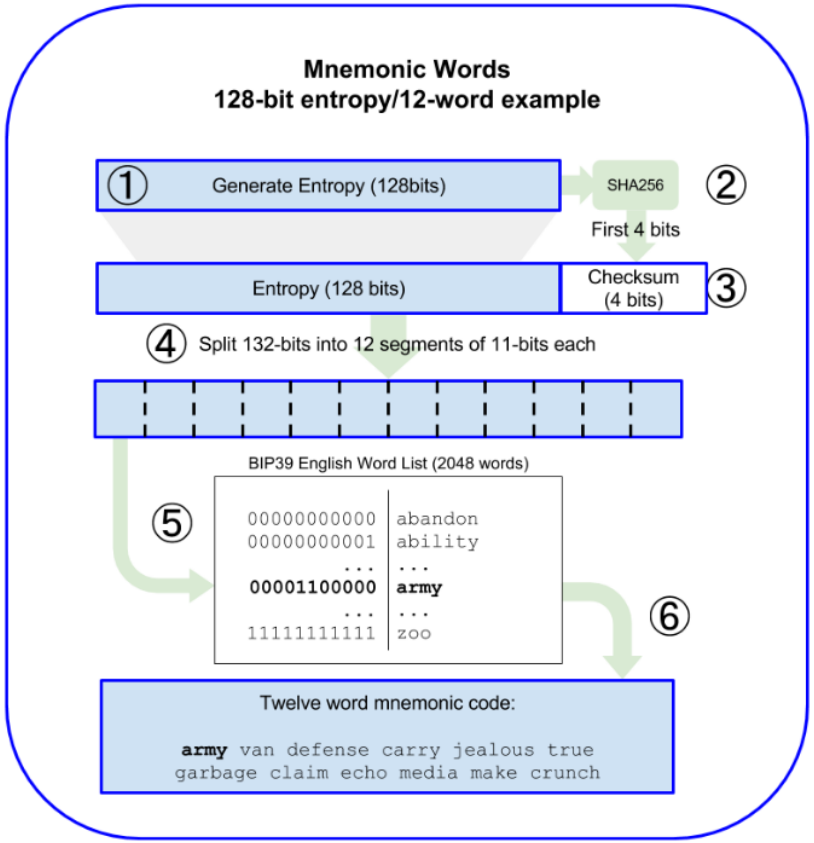


니모닉 코드

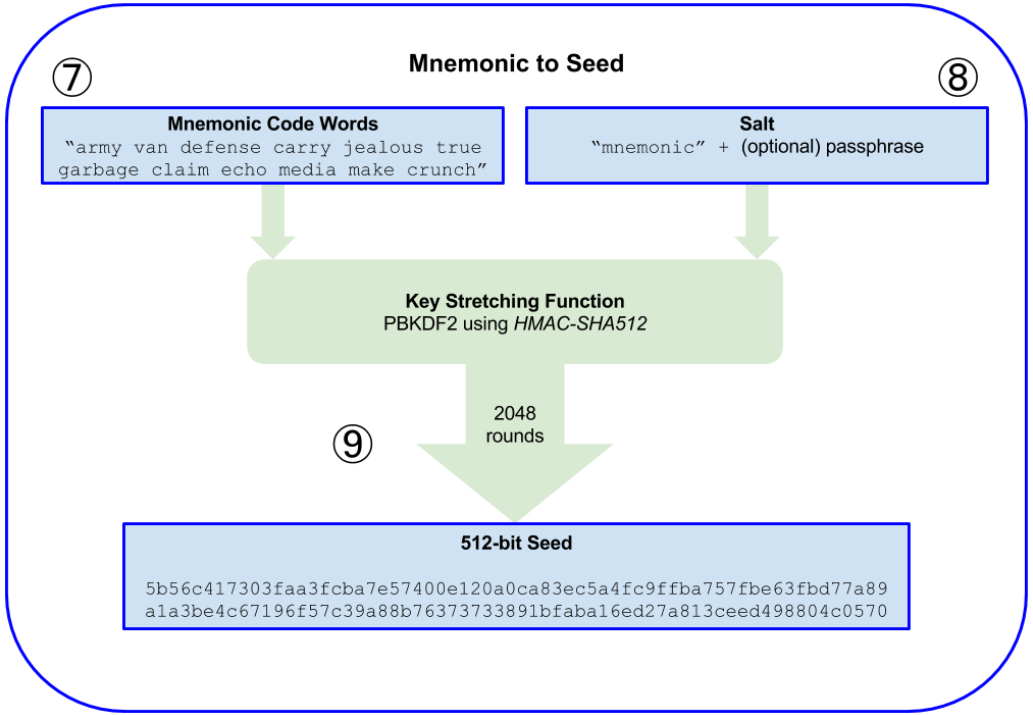
- 지갑을 쉽게 복구하기 위한 단어
- 니모닉 != 프라이빗 키
- 시드 만들기가 중요한 것



엔트로피에서 니모닉코드까지

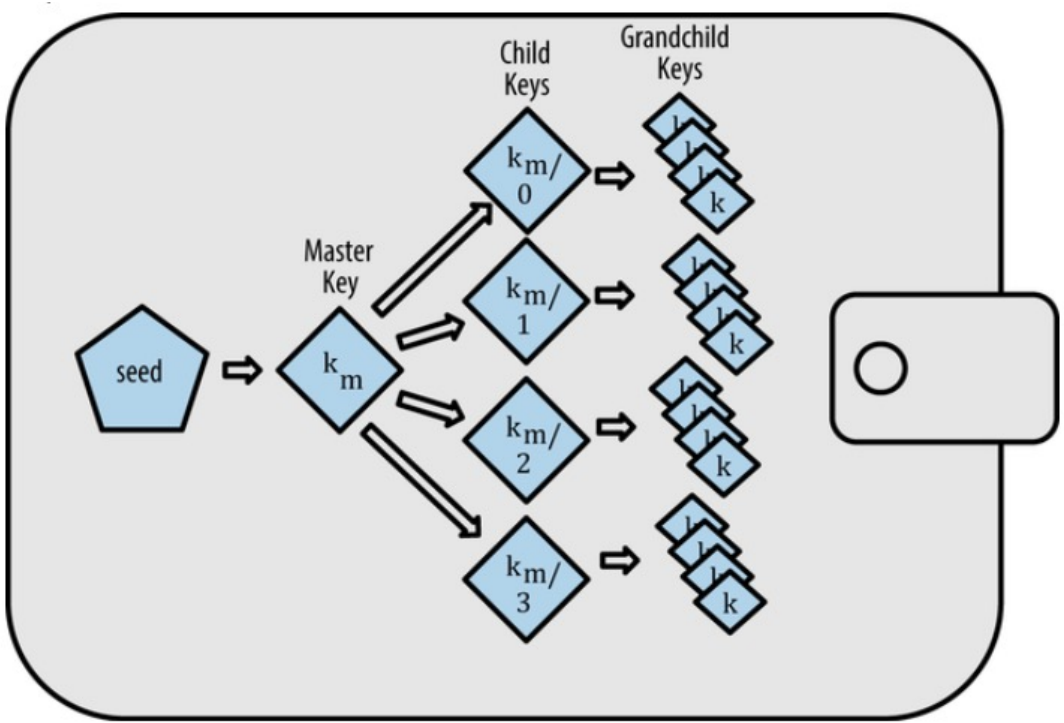


니모닉에서 시드까지

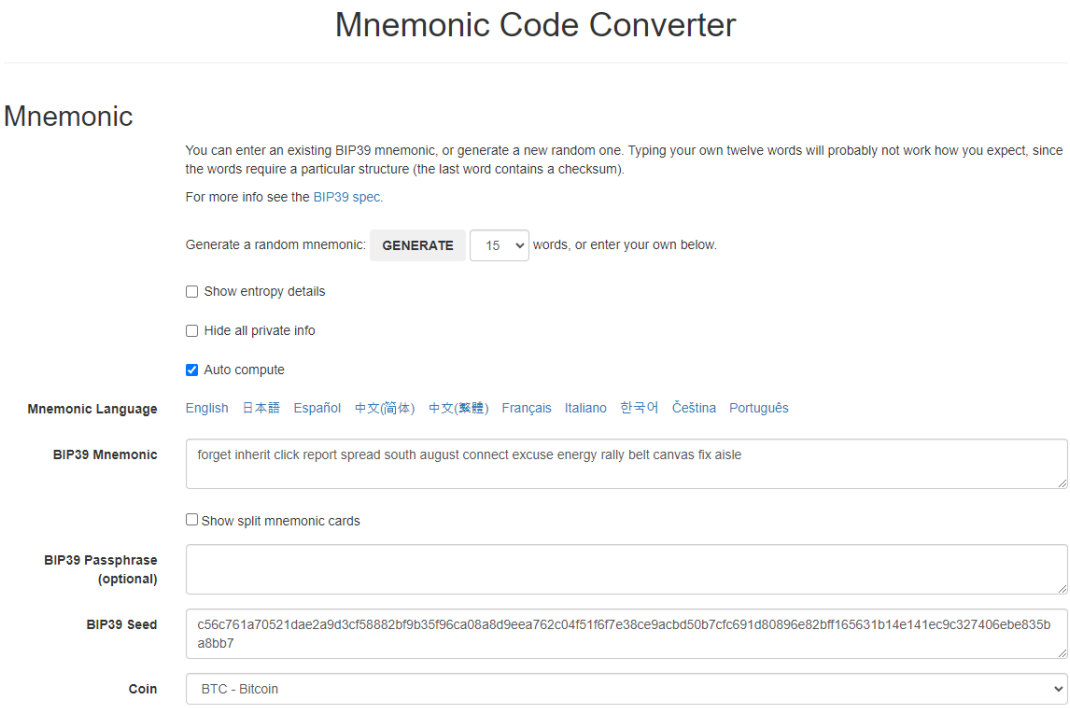

Mnemonic to Seed
⑦
⑧
Mnemonic Code Words
"army van defense carry jealous true garbage claim echo media make crunch"
Salt
"mnemonic" + (optional) passphrase
Key Stretching Function
PBKDF2 using HMAC-SHA512
⑨
2048 rounds
512-bit Seed
5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

HD 지갑

- 계층 결정적 지갑



HD 지갑



https://iancoleman.io/bip39