Blockchain #6

Wallet

Prof. Byung Il Kwak

Review

- Bitcoin's block
- Bitcoin's transaction
  - UTXO
  - Transaction structure
- Public addresses
- Real-mining and confirmation of bitcoin
- Exchange markets
- Attacks on bitcoin

CONTENTS

- Wallet for cryptocurrency

Wallet for cryptocurrency

- Wallet
  - 비트코인 주소와 비밀키가 담겨있는 소프트웨어
  - 비트코인의 전송, 수취 및 보관하는데 사용됨

[Source https://kr.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin-wallets]

Wallet for cryptocurrency

- 지갑 기술 개요
  - 지갑의 역할
    - 개인 키 추적
    - 트랜잭션 송신, 수신, 저장
  - 지갑 양식
    - 스마트폰 앱
      - Mycelium, AirBitz
    - 온라인 웹 지갑
      - Blockchain.info, coinbase.com
    - 종이 지갑
      - Bitcoinpaperwallet.com
      - Bitaddress.org
    - 하드웨어 지갑
      - Trezor, KeepKey

Cold Storage

Wallet for cryptocurrency

- 개인키를 유실한 경우
  - 개인키를 분실하면, 블록체인에 기록된 해당 지갑의 UTXO는 영원히 사용할 수 없음.

≡ 매일경제 구독신청 로그인 회원가입

뉴스 오피니언 프리미엄 연예 스포츠 증권 부동산

경제 기업 사회 국제 부동산 증권 정치 IT·과학 문화 기획·연재 Special Edition 인기뉴스 암호화폐 오늘의 매경

"153조원 날아갈 판"...비트코인 370만개 비밀번호 몰라 못 찾는다

김승한 기자 | 입력 : 2021.01.13 14:30:32 수정 : 2021.01.13 16:36:48 5

비밀번호를 기억하지 못해 수천억원이 넘는 돈을 영원히 찾지 못한다면 어떤 기분일까. 암호를 분실해 디지털 지갑에 방치된 비트코인이 전세계 약 370만개에 달한다는 통계가 나왔다.

뉴욕타임즈는 12일(현지시간) 가상자산 시장 분석업체 체이널리시스(Chainalysis)를 인용해 현재 유통되는 1850만 비트코인 중 20%가 잠금을 해독하는 비밀번호를 찾지 못해 디지털지갑에 묶여있거나 분실됐다고 밝혔다. 약 1400억달러(약 153조원)에 달하는 수준이다.

분실된 디지털 키를 찾아주는 회사 월렛리커버리서비스(Wallet Recovery Services)는 최근 관련 요청건이 하루에 70건 이상 된다고 설명했다. 대부분 비트코인이 큰 가치가 없을 때 소유했다가 최근 시세가 다시 급등하자 찾으려는 사람들이다.

관련뉴스

빗썸·코인원·코빗, 은행 실명계좌 확보

3대 코인거래소 '휴~' 존폐 위기서 벗어났다.....

한국 투자자 또 호구되나...비트코인 급락에 다..

비트코인 '진짜 돈' 되자마자 비트코인 값 폭..

엘살바도르가 법정화폐로 도입한 날...비트코인..

인기뉴스

Wallet for cryptocurrency

- 브레인 월렛 (Brain Wallet)
  - 개인키를 랜덤하게 생성하지 않고 단어 목록이나 특정 문장 (passphrase)을 사용해서 개인키를 만드는 방식
    - 특정 문장에 double-SHA-256 해시 알고리즘을 적용하여, 256bit의 해시를 생성함
    - 작성 코드 (Python 사용) (bitcoin package 설치 필요)

```
import bitcoin.main as btc
passphrase = '기억하기 쉬운 단어들의 조합 또는 문장으로 작성'
private_key = btc.sha256(passphrase)
dprivate_key = btc.sha256(private_key)
public_key = btc.privkey_to_pubkey(dprivate_key)
address = btc.pubkey_to_address(public_key, 0)
```

Wallet for cryptocurrency

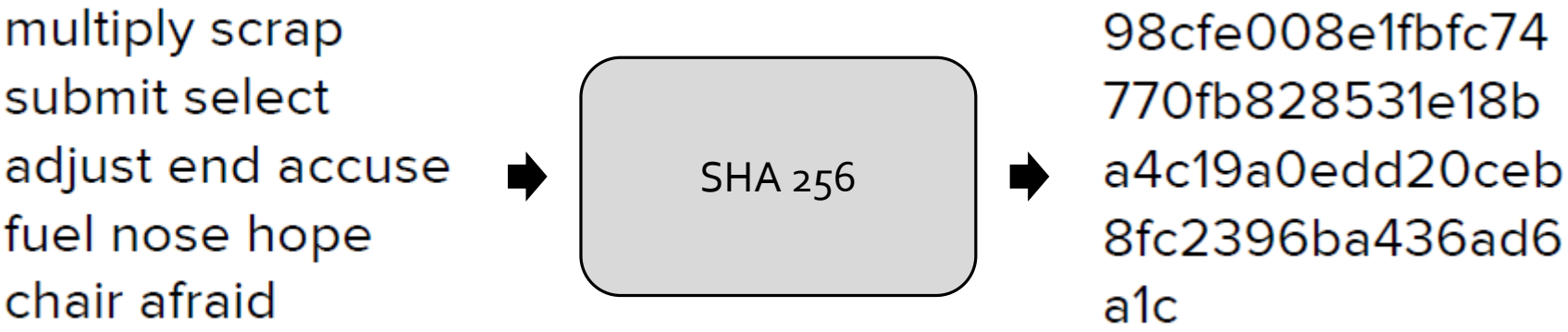
- 브레인 월렛 (Brain Wallet)

multiply	accuse
scrap	fuel
submit	nose
select	hope
adjust	chair
end	afraid

- 개인 키를 기억하는 편리하고 쉬운 방법
- 개인 키로 전환시킬 수 있는 쉬운 방법
- 사람들이 생각할 때, 어느정도 유추할 수 있는 범위가 있어 보안적인 측면이 다소 부족

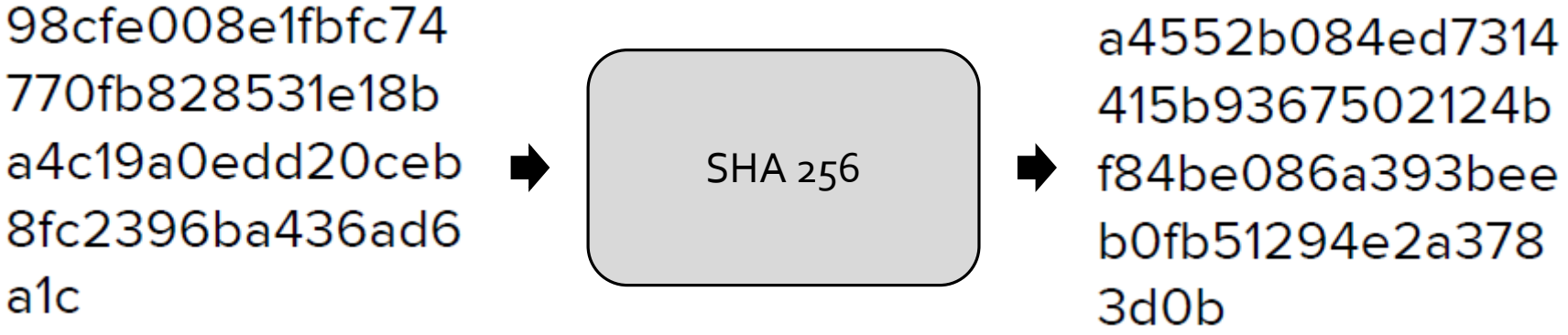
Wallet for cryptocurrency

- 브레인 월렛 (Brain Wallet)
  - 개인키 유도방법



Wallet for cryptocurrency

- 브레인 월렛 (Brain Wallet)
  - 개인키 유도방법



Wallet for cryptocurrency

- 베니티 월렛 (Vanity Wallet)
  - 지갑 주소의 특정 위치에 사용자가 원하는 문자열이 나타나게 하는것
  - 사용자 자신이나 다른 사람들이 지갑 주소를 알아보기 쉬움
    - 예) 인터넷 상점이나 사업체 등에서 회사명을 주소에 표시하는 것과 같음
  - 문자열이 나타날 때 까지 개인키를 반복해서 생성해야 함
    - 문자열이 길 경우, 시간이 오래 걸릴 수 있음
    - 문자열은 Base58Check 인코딩에 사용되는 문자열만 가능

Wallet for cryptocurrency

- 베니티 월렛 (Vanity Wallet)

```
import bitcoin.main as btc
For i in range(10000):
    while (1):
        privKey = btc.random_key()
        dPrivKey = btc.decode_privkey (privKey, 'hex')
    pubKey = btc.privkey_to_pubkey(privKey)
    address = btc.pubkey_to_address(pubkKey, 0)

    if address[1:4] == 'ABC':
        privKey, pubKey, address
```

256bit Random number 생성

개인키로 공개키 생성

공개키로 지갑 주소 생성

지갑 주소 앞부분이 원하는 문자열인지 확인

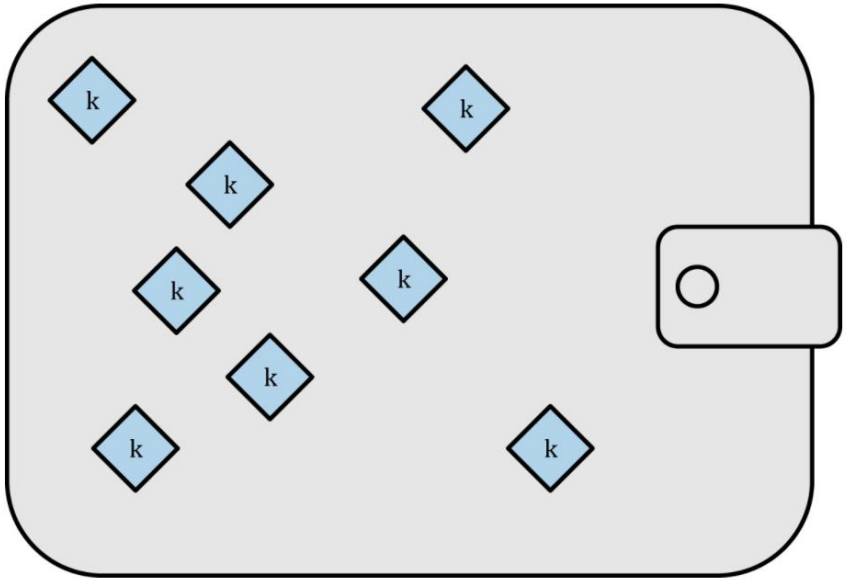
지갑 주소 앞부분이 원하는 문자열일 경우, privKey, pubKey, address 사용

Wallet for cryptocurrency

- 지갑의 유형과 키 관리
  - 비결정적 방식 (non-deterministic)
    - 개인키를 랜덤하게 생성
  - 결정적 방식 (deterministic)
    - 개인키를 공통 시드(seed)로부터 생성

Wallet for cryptocurrency

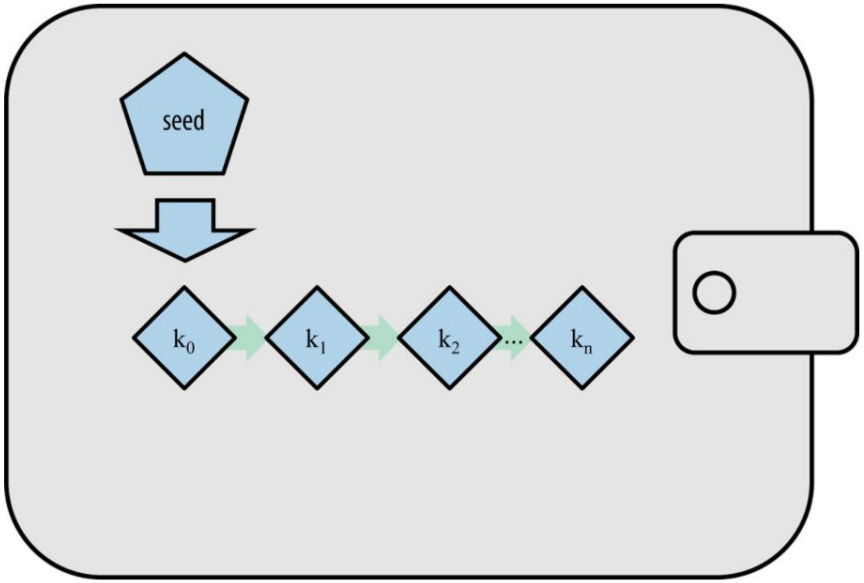
- 지갑의 유형과 키 관리
  - 비결정적 방식의 지갑 (Non-deterministic Wallet)
    - 개인키를 랜덤하게 생성 (무작위)
      - 무작위로 키를 생성하다 보니 한 번 생성된 이후에는 전부 복사본을 보관해야 함 (각 키들의 백업이 필수)
        - 분실의 위험이 있음



[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

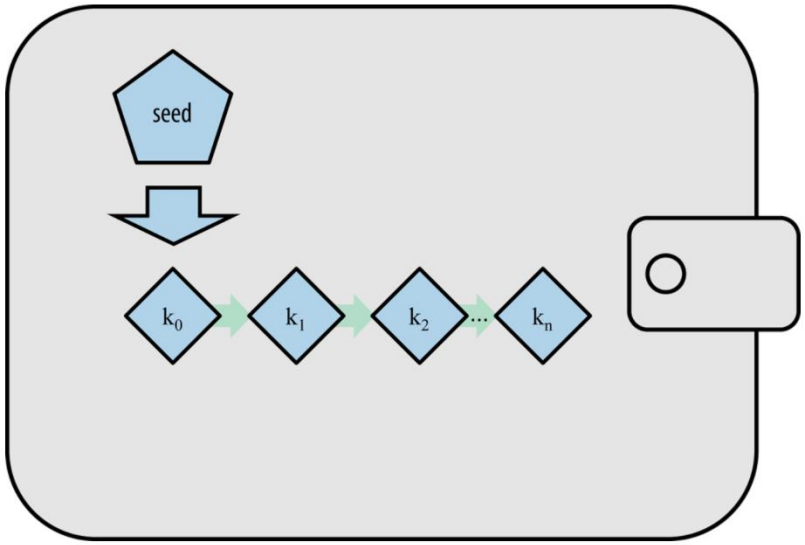
- 지갑의 유형과 키 관리
  - 결정적 방식의 지갑 (Deterministic Wallet)
    - 시드 값과 해시 함수를 이용해서 연쇄적으로 키를 생성
    - 이러한 키들은 시드 값을 시작으로 키 체인 (key chain)을 이룸
    - 각 키들은 서로 독립적이지 않고 관계를 형성함
      - 해시 함수의 확산 현상 (diffusion) 과정 때문에 그 관계가 드러나지 않음



[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

- 지갑의 유형과 키 관리
  - 결정적 방식의 지갑 (Deterministic Wallet)
    - 키 생성 방식
      - 초기 시드 (seed)의 해시 값으로 마스터키 (k_0)를 생성
        - 해당 마스터키 (k_0)의 해시 값으로 다음 키 (k_1)를 생성
        - 생성된 키 (k_1)의 해시 값으로 다음 키 (k_2)를 생성
        - …



[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

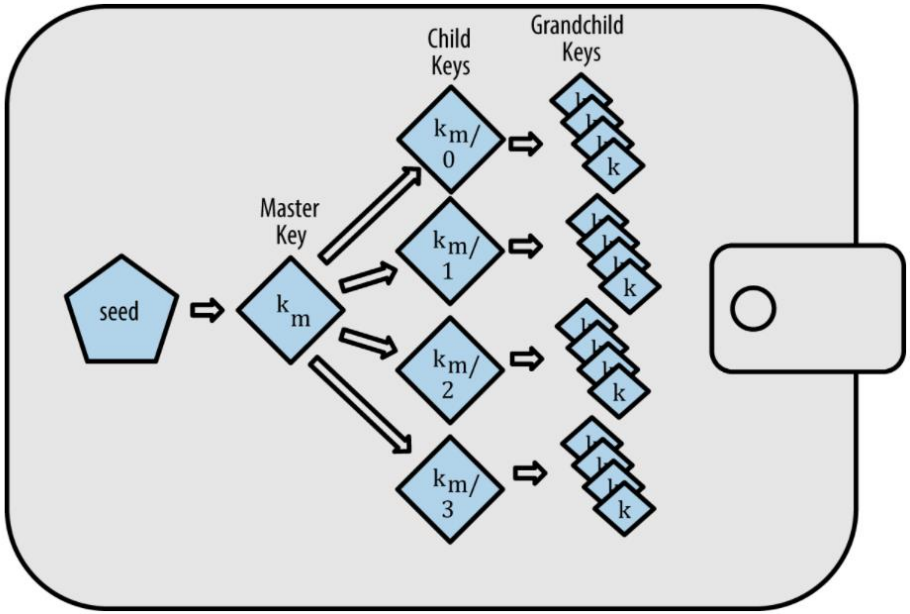
- 지갑의 유형과 키 관리
  - 결정적 방식의 지갑 (Deterministic Wallet)
    - 초기 시드 값만 잘 보관하거나 백업해 두게 되면, 나머지 키들은 언제든지 다시 만들 수 있다는 장점
      - 키를 많이 만들더라도, 일일이 백업할 필요가 없음
    - 이처럼, 결정적 방식의 지갑을 '**Type-1 형 지갑**'이라고 표현

[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

- 지갑의 유형과 키 관리
  - 계층 구조의 결정적 방식 지갑

    (Hierarchical Deterministic Wallets: HD Wallets, BIP-32)
    - 계층구조로 구성되며, 키와 지갑 주소를 관리함
    - 마스터 시드 (seed)로 마스터 개인키와 공개키를 생성
    - 상위 노드의 공개키로 하위 계층의 키와 주소를 생성



[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

- 지갑의 유형과 키 관리
  - 계층 구조의 결정적 방식 지갑의 특징
    - 하위 계층의 지갑 주소를 만들 때, 개인키를 사용하는 것이 아닌 **상위 계층의 공개키를 사용**한다는 점
      - 즉, 개인키가 없어도 지갑 주소를 만들 수 있음
    - 시드 값만 보관하면 하위 계층의 키와 주소들은 모두 원상복구 할 수 있어 백업 관리가 용이함

[Source https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch05.asciidoc]

Wallet for cryptocurrency

- 지갑 기술 - 산업 표준
  - 연상기호 코드 워드 (BIP-39)
    - 결정적 지갑을 추출하기 위해 seed로 이용한 난수를 표현하는 (인코딩) 영어 단어열
      - 연상기호 코드를 이용해 결정적 지갑을 실행하는 지갑 어플리케이션은 처음 지갑을 생성할 때 12 ~ 24개 단어로 구성된 단어열을 사용자들에게 보여줌
      - 사용되는 단어열은 지갑을 백업본
        - 동일한 지갑 어플리케이션 / 호환 가능한 지갑 어플리케이션에 있는 키 전부를 복원하고 재현하는 데 사용가능
        - 무작위 순열에 비해 쉽게 읽히고 정확하게 입력으로 인해 사용자들이 지갑을 백업하는 작업을 수월하게 함

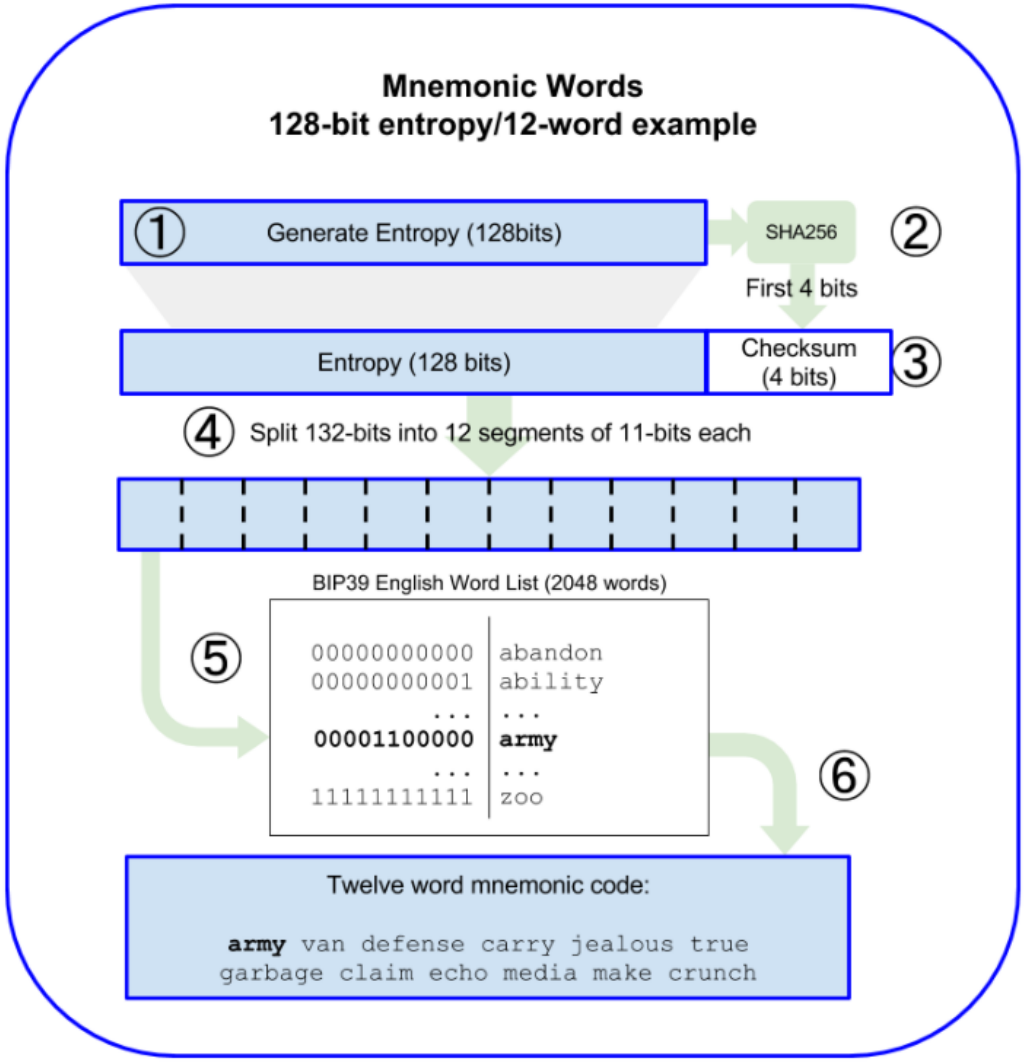
※'브레인월렛 (Brain Wallet)'과의 차이: '무작위로 생성된 단어' / '사용자가 선택한 단어로 구성'

Wallet for cryptocurrency

- 지갑 기술 - 산업 표준
  - 연상기호 코드 워드 (BIP-39)
    - 생성 과정
      - 1. 엔트로피 생성 후 연상기호 워드로 인코딩
      - 2. 연상기호로부터 seed 생성

Wallet for cryptocurrency

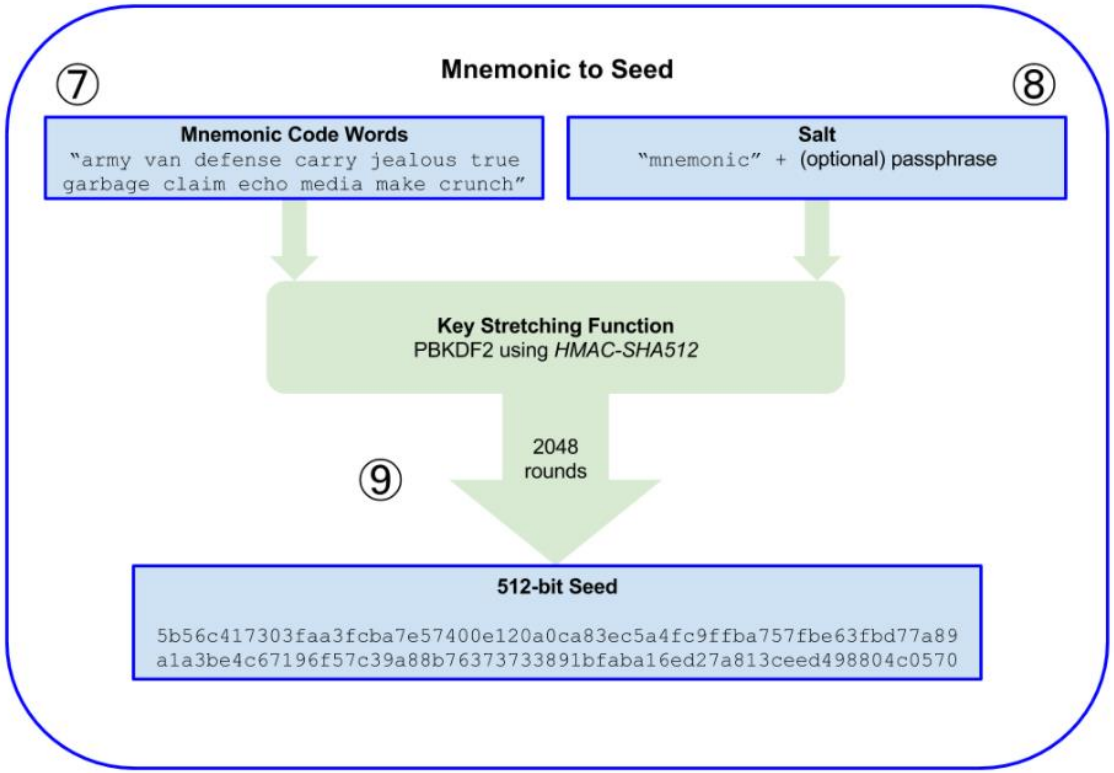
- 1. 엔트로피 생성 후 연상기호 워드로 인코딩



1. **128-256bit** 무작위열 **(엔트로피) 생성**
2. 생성된 열에 **SHA256 해시 적용 한 값의 초반 4bits**를 추출하여 **Checksum** 을 생성
3. 생성된 **Checksum** 값을 생성된 **entropy값 뒤에** 붙임
4. 해당 값을 11bit 단위로 분할
5. 미리 정해져 있는 단어사전의 **2048개에서 단어와 분할한 값들을 매칭**
6. **매칭된 단어들**이 **연상기호 코드**로 추출됨

Wallet for cryptocurrency

- 2. 연상기호로부터 seed 생성
  - 128-256 bit 길이의 연상기호 워드에 대해 PBKDF2를 사용하여 좀 더 길이가 긴 (512 bit) seed를 추출하는데 사용됨



7. PBKDF2 키 스트레칭에 대한 첫 번째 변수는 6단계에서 산출된 연상기호

8. PBKDF2 키 스트레칭에 대한 두 번재 변수는 솔트임

- 솔트에서 'mnemonic' 문자열 상수와 사용자가 제공하는 선택적 패스 프레이즈열이 연결되 있음

9. PBKDF2는 HMAC-SHA512 알고리즘으로 2,048회 해싱해서 연상기호와 솔트를 늘림

References

- Lecture slides from BLOCKCHAIN @ BERKELEY

- Mastering Bitcoin, https://github.com/bitcoinbook/bitcoinbook

Q & A