Report

Mybitcoinwallet은 3개의 클래스로 나뉘어져 있다. Cipher, wallet, user이다.

Cipher class: 개인키를 암호화하는 클래스

암호화는 pem 형태의 개인키 seed를 유저의 특정 비밀번호를 sha256을 통해 해쉬화한 값과 xor해서 저장한다. 복호화 또한 마찬가지로 해쉬와 파일을 xor해서 pem 형태의 개인키를 얻는다.

wallet Class: 비트코인 월렛 클래스

클래스 메소드: \_\_init\_\_, genprivkey, exportprivtoFile, getkeyfromFile, qrcode\_create, sendBT, history

클래스 변수: self.crypto, self.c self.testnetVal, self.priv\_ecc, self.priv, self.pub, self.addr

genprivkey: self.priv\_ecc = ecdsa.SigingKey.generate()로 새로운 키를 만든 뒤 이 키를 sha256으로 해싱해서 self.priv, 비트코인의 프라이빗 키로 사용한다. 그 뒤 cryptos.Bitcoin의 함수들을 사용해서 address까지 생성해서 각 변수들을 self 에 저장한다.

User class: 유저 인터페이스를 위한 클래스

Installation Guide

-파이썬 3.7.0 이상에서 작동.

-pip install cryptos, pip install ecdsa를 통해 dependency 설치 후 python wallet.py 를 통해 실행

User Guide:

프로그램 실행 후 help 명령어를 통해 확인