

Assignment2: Bitcoin Transactions

컴퓨터공학과 2271104 최수희

1. 개요 (Introduction)

본 보고서는 DSA(Digital Signature Algorithm)를 활용하여 비트코인의 기본 거래 유형인 P2PK(Pay-to-PubKey)와 P2PKH(Pay-to-PubKey-Hash)의 스크립트 기반의 거래 로직을 구현하고 검증하는 과정을 다룹니다. 과제의 목표는 암호화 원리를 이해하고, ScriptSig와 ScriptPubKey의 구성 및 실행을 통해 거래의 유효성을 입증하는 것입니다.

2. 프로그램 실행 요구 사항 (Execution Requirements)

2.1 개발 환경 및 종속성

- Python 버전 : python 3.8 이상 (3.10 또는 3.11)
- 주요 라이브러리 : `cryptography` (DSA 키 생성 및 디지털 서명 구현에 사용됩니다.)
- 추가 라이브러리 : `hashlib` (표준 SHA-1 해시 함수 사용을 위해 Python 기본 모듈을 사용합니다.)
- 패키지 설치 : 활성화된 가상 환경 내에서 다음 명령으로 `cryptography` 를 설치해야 합니다.
 - `pip install cryptography`

2.2. 실행 방법

프로그램은 Task 별로 기능이 분리된 3개의 Python 파일로 구성되며, Task1 파일은 나머지 파일에 키 객체를 제공하는 모듈 역할을 합니다.

a. 파일 구성 : 다음 3개의 `.py` 파일이 같은 디렉토리에 위치해야 한다.

- `dsa_key_generation.py` : (Task1) 키 생성 및 객체 정의
- `p2pk_implementation.py` : (Task2) P2PK 구현 및 실행
- `p2pkh_implementation.py` : (Task3) P2PKH 구현 및 실행

b. 실행 명령어 : 가상 환경이 활성화된 터미널에서 Task2와 Task3 파일만 순차적으로 실행하면 됩니다. 각 파일은 `dsa_key_generation.py` 를 임포트하여 필요한 키 객체를 가져오고, 스크립트를 실행한다.

```
python p2pk_implementation.py
python p2pkh_implementation.py
```

3. 프로그램 예상 결과 및 검증 기준 (Expected Outcome)

프로그램의 검증 기준은 모든 스크립트 실행의 최종 결과가 True를 반환하는 것입니다. 이는 ScriptSig가 ScriptPubKey의 요구 조건을 성공적으로 만족시켜 거래가 유효하다는 것을 의미합니다.

| Task | 목표 | 예상 출력 | 검증 기준 |
|---------------|---|--|---|
| 1. DSA 키 쌍 생성 | P2PK 및 P2PKH에 사용할 DSA 키 쌍 2개 생성 | 두 쌍의 Private Key PEM 및 Public Key PEM 문자열 | 키 객체(<code>DSAPrivateKey</code> , <code>DSAPublicKey</code>)가 성공적으로 생성되었는지 확인 |
| 2. P2PK 구현 | "Blockchain Application Q1" 메시지에 대한 서명 및 P2PK 스크립트 실행 | ✅ OP_CHECKSIG 결과: <code>TRUE</code> (거래 성공) | 최종 스크립트 실행 결과가 <code>True</code> 인지 확인 |
| 3. P2PKH 구현 | "Blockchain Application Q2" 메시지에 대한 서명, | ✅ OP_EQUALVERIFY 성공: <code>Public Key Hash</code> 일치 확인. | OP_EQUALVERIFY와 OP_CHECKSIG가 모두 성 |

| | | |
|--------------------------------|---|--------------------------|
| SHA-1 해시 적용 및 P2PKH 스크립트 실행 | 및 ✔ OP_CHECKSIG 결과: TRUE (거래 성공!) | 공하여 최종 결과가 True 인지 확인 |
|--------------------------------|---|--------------------------|

Task2 실행

- 메시지를 SHA-256 알고리즘을 사용하여 개인 키로 서명하는 과정이 성공적으로 완료 (Task1)
- ScriptSig와 ScriptPubKey가 결합된 완전한 스크립트가 실행되어 서명 검증에 성공
- P2PK 거래의 유효성이 최종적으로 확인

```
soohe@DESKTOP-NSQMM3F MINGW64 /c/projects/blockchain/bitcoin
$ python p2pk_implementation.py

=====
✔ Task 1: DSA 키 쌍 2개 생성 완료
=====

[ Key Pair 1 (P2PK) ]
-----
1. Private Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPrivateKey object at 0x000...
2. Public Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPublicKey object at 0x000...

--- 개인 키 (Private Key PEM) ---
-----BEGIN PRIVATE KEY-----
MIICZQIBADCCAjkGByqGSM44BAEwggIsAoIBAQRo2JfNoLHzFkre9HqAW0tEB19
7x4DEAJx9EPgv3EXCd1hVoi2nzw0N650wB3Jfcsj1J05P4k4Rtcw6kyM9j1fT/DvV
BEeCV9roSfoJArZTcm24e1CPb3nueZ1r17C041KP3hd9sl1fz1eSc144J97Nhmq

dv8z1XD6KVKVHE1tL69wN3HzcEFpQd4xT1cXSnwfq/B5YjsiIzUdFzq/Rs4IwxU2
cGKXnJQgRS+y+1ss7iYKQmrF/f2TkVBlOpJla87FuWxyDcEu0jyVVs9QRHyZwaT
xg9P8wQjAiEAjbJ9afBYydfRaRLbB64BS0d5d4dJjD5c63B2KQ+rtE=
-----END PRIVATE KEY-----

--- 공개 키 (Public Key PEM) ---
-----BEGIN PUBLIC KEY-----
MIIDRjCCAjkGByqGSM44BAEwggIsAoIBAQRo2JfNoLHzFkre9HqAW0tEB197x4D
EAJx9EPgv3EXCd1hVoi2nzw0N650wB3Jfcsj1J05P4k4Rtcw6kyM9j1fT/DvVBEeC
V9roSfoJArZTcm24e1CPb3nueZ1r17C041KP3hd9sl1fz1eSc144J97Nhmq2D4z

rBt1rCItNwKw5syoGmhbnPUIhaeG0m1VMYBdhQbm73EOETyidHgyxwMS121Zsn
eh9iKIuf6Dm7U7ZuRtgoDGFq12ysaTW4T6Y=
-----END PUBLIC KEY-----

-----

[ Key Pair 2 (P2PKH) ]
-----
1. Private Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPrivateKey object at 0x...
2. Public Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPublicKey object at 0x...

--- 개인 키 (Private Key PEM) ---
-----BEGIN PRIVATE KEY-----
MIICZAIBADCCAjkGByqGSM44BAEwggIsAoIBAQR0c06c7EsvB4u71EEsg7DjjUQVX
apkcDxv4jILd3thL2smjMaMKR8I17gXOGzBXw/UdOxjyPaUJCjiUd3qJjhRqljs
mwqP57qmmaQHTfXh9YqkcNnO411Tq+HI9PCCd0n/aQS/e3GyZiKpes7/242SuR2v
uKAICR/k6zacQUcxhqBr95jyYrD/xi88ldJydOwYq1YN06wTpbWrvEohVuKMhd1J

VXp4pxneyfNDJ7670VRjAhHzk7z8o5WABQmN61py9sbCXI8eKnNkRZ/ZBPzBaAsr
inuG3LP1uhzHPbMhCjr1uTeVnOGifsZkXmycA8T+1Kxeig0ivDVL1Ahg50pC5DeW
rfpCF9o69Txp0t0RQ6sio3VcE5SguI0VrcStiHs4MteO3qiGMxs7w29zskPzbwE
xyAvIAQIAiBN6FRGfi2PVh0yBqLaFTa4x0LA6dqKo/9yom44BwlnEA==
-----END PRIVATE KEY-----

--- 공개 키 (Public Key PEM) ---
-----BEGIN PUBLIC KEY-----
MIIDRjCCAjkGByqGSM44BAEwggIsAoIBAQR0c06c7EsvB4u71EEsg7DjjUQVXapkc
Dxv4jILd3thL2smjMaMKR8I17gXOGzBXw/UdOxjyPaUJCjiUd3qJjhRqljsmwqP
s7qmmaQHTfXh9YqkcNnO411Tq+HI9PCCd0n/aQS/e3GyZiKpes7/242SuR2vuKAICR/
k6zacQUcxhqBr95jyYrD/xi88ldJydOwYq1YN06wTpbWrvEohVuKMhd1J0atC
```

```
OrRp4PinG7NSU7jQQ2gogAAGfDqgKRYrcr8X5HjVTnNxXzXEZ9xfcPHC8BPzpU
ztmu1juoltw/Zg+6+8xc5F2HbKDwi5Sux6riwJBaipbpWwYe1h0OfFMUkyP6vRpd
We7BNXB3fN2JiIzwJBncCCfBMJLHIhYI7t0=
-----END PUBLIC KEY-----
```

🚀 Task 2: P2PK 구현 및 실행

- ✅ 1. ScriptSig (Signature) 생성 완료 (SHA-256 사용).
- ✅ 2. ScriptSig 및 ScriptPubKey 구성 완료.

[실행] 완전한 스크립트 구성 및 실행 시작...

✅ OP_CHECKSIG 결과: TRUE (거래 성공!)

--- 최종 스크립트 실행 결과: True ---

Task3 실행

- 2가지 DSA 키 쌍 생성 (Task1)
- ScriptSig에서 제출한 공개 키를 SHA-1로 해시한 값이 ScriptPubKey에 미리 잠금 설정된 공개 키 해시 값과 일치함을 확인 (주소 일치 확인 완료)
- 서명과 공개키를 사용하여 서명이 유효함을 확인 (소유자 증명 완료)
- 위 2가지 조건이 모두 충족되어 거래가 유효함이 최종적으로 확인

```
soohe@DESKTOP-NSOMMBF MINGW64 /c/projects/blockchain/bitcoin
$ python p2pk_implementation.py
=====
✅ Task 1: DSA 키 쌍 2개 생성 완료
=====

[ Key Pair 1 (P2PK) ]
-----
1. Private Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPrivateKey object at 0x0000012BA949070>
2. Public Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPublicKey object at 0x0000012BA949070>

--- 개인 키 (Private Key PEM) ---
-----BEGIN PRIVATE KEY-----
MIICZAIBADCCAJkGBYqGSM4BAEwggIsAoIBAQCuokR0cB3XCz+2DF718nmnsD6y
aG6rsLb1KtZ9Go4ViBLEAwtt12wq3WfLwFgcETXRfDZ9HNVBae1k52BP36vi1tUs
-----END PRIVATE KEY-----
```

```
-----END PRIVATE KEY-----

--- 공개 키 (Public Key PEM) ---
-----BEGIN PUBLIC KEY-----
MIIDRjCCAjkGBYqGSM4BAEwggIsAoIBAQCuokR0cB3XCz+2DF718nmnsD6yaG6r
sLb1KtZ9Go4ViBLEAwtt12wq3WfLwFgcETXRfDZ9HNVBae1k52BP36vi1tUsdyoU
DmMzdPuziazq0v/UlCFBsm1zqNKI9orXZdCw0HQrdB+orzRKTR0TJBiuKBS1QXXw
MjpkOEYjoRsze8PV3TPv+oJezQNWkbtMirVTT31+ifKxDeayfLMwKB1aSMfXxyTR
fKZXQdXE2jAf96w3gR1eU7Owin8zhWgrLZxDmGxEadnSHP23Mw8WuSLS3WgVzLqf
cmtCd3UQ/M48nlyK5mP2gPoArxzgiFbdpkhpiE2ku6Lkrt3Quzy05dpAiEAiSv8
-----END PUBLIC KEY-----
```

```
-----
[ Key Pair 2 (P2PKH) ]
-----
1. Private Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPrivateKey object at 0x0000012BA9490070>
2. Public Key Object: <cryptography.hazmat.bindings._rust.openssl.dsa.DSAPublicKey object at 0x0000012BA9490070>

--- 개인 키 (Private Key PEM) ---
-----BEGIN PRIVATE KEY-----
MIICZQIBADCCAJkGBYqGSM4BAEwggItAoIBAQQJQWTTnG0Amaw9iJKEJx0v317b
-----END PRIVATE KEY-----
```

```
JTqUCC0uQypCGKjU42NpXoTwFh/d4P3EH9JJF2apTEUHG00aZH+BEW2ZsgNrjqo4  
orwVis0EIgIgfPg16cuCyUSQjdIG7pw31W2iudCFJQn7E0FhRL0I+D8=  
-----END PRIVATE KEY-----
```

```
--- 공개 키 (Public Key PEM) ---
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIIDSdCCAjoGByqGSM44BAEwggITaoIBAQDJQWTTnG0Amaw9iJKEJxOv317bp0Sy  
lsBmw1XHAZSybw/x7BIkIGBcZyyIyqBjwVAKXxv9FJS10RbqhzWY4+cyqYmftrvL  
rmSODMsf5oYZsP7yuvQ772B+1roVULqPtcGmZs4cibtovgJTLhX+GwMqiSNFGXH9  
/b9J6MBaYwmGyaVe4iXqrmvy/CpiTfz/t2SMZRF1D6JbnV39vJ5M1J+VsV4979eX  
UmXtj6dbbSHhJBrtPDzRw5NkhT4Yp11pB2AGkfvcDQWpM1Ki0iFhl/fVAiEAsjpy
```

```
4TcmRSvHsMX560050gLjgm5JYd0BGaqeTSH0e5La/viyeR9ycQE7BfmKJBiqRNOY  
gEJyMVxCNatwRGundIo1DuLsNweduXL7aVJLrQ==  
-----END PUBLIC KEY-----
```

```
=====
```

🏆 Task 3: P2PKH 구현 및 실행

- ✅ 1. ScriptSig (Signature) 생성 완료 (SHA-256 사용).
- ✅ 2. ScriptPubKey를 위한 Public Key Hash (SHA-1) 생성 완료.

[실행] ScriptPubKey 시작 (OP_DUP -> OP_HASH160 -> OP_EQUALVERIFY -> OP_CHECKSIG)...

- ✅ OP_EQUALVERIFY 성공: Public Key Hash 일치 확인.
- ✅ OP_CHECKSIG 결과: TRUE (거래 성공!)

--- 최종 스크립트 실행 결과: True ---

4. 결론 (Conclusion)

본 과제를 통해 DSA 알고리즘을 사용하여 개인 키와 공개 키 쌍을 생성하는 과정을 이해했습니다. 또한, 비트코인 거래의 가장 기본적인 두 가지 스크립트 유형인 P2PK와 P2PKH를 Python 코드로 구현하고, 디지털 서명(SHA-256)과 공개 키 해시(SHA-1)를 통한 스택 기반의 검증 로직을 성공적으로 시뮬레이션했습니다. 모든 Task의 스크립트가 유효성 검사를 통과하고 True를 반환함으로써, 비트코인 거래의 잠금(ScriptPubKey) 및 해제(ScriptSig) 매커니즘을 성공적으로 입증하였습니다.