L-Università ta' Malta
Faculty of Information & Communication Technology

Project Report

Manwel Bugeja

March 1, 2021

Contents

1 Pay-to-Public-Key-Hash (P2PK)

1.1 Overview

When using this script, the public key is stored as plaintext within the locking script. This is mostly used in coinbase transactions which was generated by mining software which is not up to date.

The following in an example of a P2PK locking script:

```
<Public Key A> OP_CHECKSIG
```

To unlock this, the following script must be submitted:

```
<Signature from Private Key A>
```

Together, they form the script which is validated transaction validation software. The script becomes:

```
<Signature from Private Key A> <Public Key A>
   OP_CHECKSIG
```

This script uses the CHECKSIG operater. This operator returns TRUE on the stack if the signature belongs to the correct key.

[1]

1.2 Problems

2 Pay-to-Public-Key-Hash (P2PKH)

This script is used for most of the transactions processed on the bitcoin network. Within this script, the locking script encrypts the output with a public key hash. This is known as a bitcoin address. When an output is spent, the lock on the output by a P2PKH is removed. This unlocking is done by handing over a public key and a digital signature that were created by the corresponding private key.

An example of a locking script is:

```
OP_DUP OP_HASH160 <Cafe Public Key Hash> OP_EQUAL
   OP_CHECKSIG
```

The corresponding unlocking script looks like:

```
<Cafe Signature> <Cafe Public Key>
```

The validation scripts of the previous two scripts looks like:

```
<Cafe Signature> <Cafe Public Key> OP_DUP OP_HASH160
    <Cafe Public Key Hash> OP_EQUAL OP_CHECKSIG
```

If the unlocking script has a valid signature that corresponds to the publid key hash set as an encumbrance, the script returns TRUE on the stack.

References

[1] A. M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly Media, 2014.