ΑΠΟΚΕΝΤΡΩΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

ASSIGNEMENT 1

BITCOIN

ΛΙΑΠΙΚΟΣ ΘΕΟΔΩΡΟΣ – Α.Μ.: 11

ΠΛΗΡΟΦΟΡΙΕΣ ΣΥΣΤΗΜΑΤΟΣ ΑΝΑΠΤΥΞΗΣ

Η εργασία ολοκληρώθηκε σε ΗΥ με Λειτουργικό Σύστημα Linux Mint19. Χρησιμοποιήθηκε γλώσσα προγραμματισμού Python 3.6.7 σε περιβάλλον ανάπτυξης (I.D.E.) Spyder 3.3.2.

Η συγγραφή της αναφοράς έγινε σε κειμενογράφο Libre Office Writer.

ΤΕΧΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΥΣΤΗΜΑΤΟΣ

Για τη συγκεκριμένη εργασία χρησιμοποιήθηκαν οι παρακάτω εξειδικευμένες βιβλιοθήκες:

- bitcoin-utils 0.3.2 (pip install bitcoin-utils)
- bitcoinrpc (pip install python-bitcoinrpc)

Δεν θυμάμαι αν κατά τη διάρκεια των 2 BitCoin Labs είχαμε εγκαταστήσει και άλλα εξειδικευμένα πακέτα. Αναλυτική παρουσίαση όλων των εγκατεστημένων πεκέτων της Python 3.x, κατά την ανάπτυξη του κώδικα της εργασίας, περιέχεται στο συνοδευτικό αρχείο *requirements.txt*.

Το περιεχόμενο του αρχείου ρυθμίσεων ~/.bitcoin/*bitcoin.conf* κατά τη διάρκεια των δοκιμών ήταν το ακόλουθο:

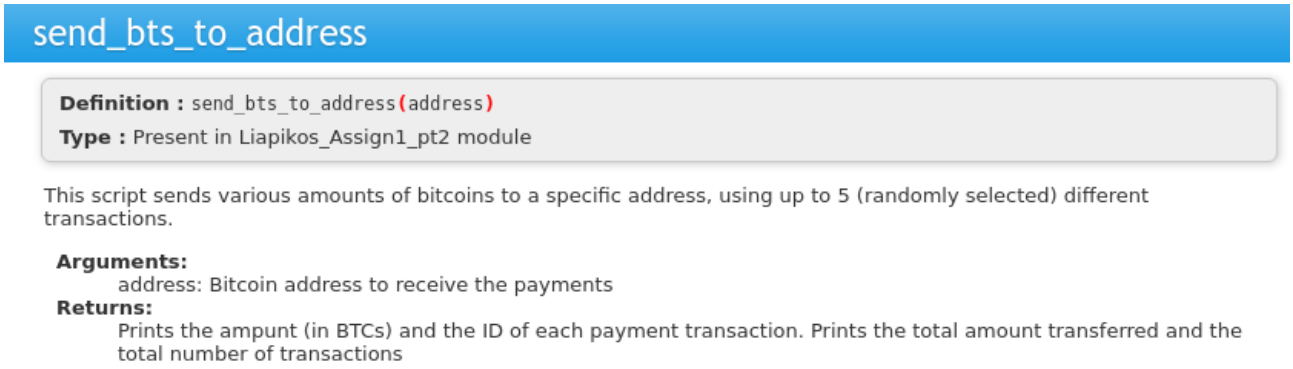
```
regtest=1
proxy=127.0.0.1:9050
server=1
daemon=1
rpcuser = my_name_is_bond
rpcpassword = james_bond
deprecatedrpc=signrawtransaction
```

ΠΕΡΙΓΡΑΦΗ ΠΡΟΓΡΑΜΜΑΤΟΣ

Το πρόγραμμα αναπτύχθηκε, σύμφωνα με τις οδηγίες της εκφώνησης, σε 2 μέρη που περιέχονται αντίστοιχα στα συνοδευτικά αρχεία *Liapikos_Assign1_pt1.py* και *Liapikos_Assign1_pt2.py*.

Ο κώδικας αναπτύχθηκε με τέτοιο τρόπο ώστε να ικανοποιεί τις απαιτήσεις (bullets) της εργασίας με τη σειρά που αυτές αναφέρονται στην εκφώνηση. Η κάθε απαίτηση διαχωρίζεται μέσα στο κώδικα με εμφανή επικεφαλίδα-σχόλιο.

Ο κώδικας είναι αναλυτικά σχολιασμένος σε κάθε σημείο, εξηγώντας το σκοπό των επιμέρους εντολών. Επιπλέον κάθε μέθοδος συνοδεύεται από συνοπτική τεκμηρίωση, σε κατάλληλο format, ώστε να προβάλλεται από το περιβάλλον ανάπτυξης, όπως στο παρακάτω παράδειγμα:



ΕΚΤΕΛΕΣΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

ΜΕΡΟΣ 1

Το πρώτο μέρος της εργασίας αποτελείται από μία μέθοδο που εκτελείται αυτόματα και σκοπό έχει τη δημιουργία μιας νέας P2SH BitCoin διεύθυνσης, όλα τα κεφάλαια της οποίας είναι δεσμευμένα (κλιδωμένα) από κατανάλωση μέχρι η αλυσίδα του blockchain να φτάσει σε κάποιο απόλυτο ύψος. Οι λειτουργίες που επιτελούνται είναι με τη σειρά οι ακόλουθες:

- Επιλέγει το BitCoin δίκτυο (regtest) και εκκινεί το proxy για την πραγματοποίηση RPC κλήσεων.
- Δημιουργεί μια νέα P2PKH διεύθυνση (το public κλειδί της)
- Ορίζεται το απόλυτο ύψος της αλυσίδας blockchain που οριοθετεί το κλείδωμα των κεφαλαίων της P2SH διεύθυνσης.
- Γίνεται έλεγχος της τιμής κλειδώματος σε σχέση με την τρέχουσα τιμή του ύψους της αλυσίδας blockchain και ειδοποιείται ο χρήστης, ανάλογα με την περίπτωση με το αντίστοιχο μήνυμα:

```
Current blockchain height: 0 blocks
Fund's lock is set to: 103 blocks
```

- ή

```
***BEWARE*** Given lock (103 blocks) is lower than current blockchain height (409 blocks)
```

- Ολοκληρώνεται η δημιουργία της νέας P2SH διεύθυνσης και το κλείδωμά της με το κατάλληλα δομημένο redeem script.
- Η νέα διεύθυνση εισάγεται στο πορτοφόλι (wallet) του χρήστη για να μπορεί να τη χειριστεί.
- Ο χρήστης ειδοποιείται με μήνυμα για την επιτυχή ολοκλήρωση της διαδικασίας με εκτύπωση της διεύθυνσης:

```
In [11]: runfile('/media/Personal Files/Theo Files/MSc/3. Αποκεντρωμένες Τεχνολογίες/Assignment 1/final/
Liapikos_Assign1_pt1.py', wdir='/media/Personal Files/Theo Files/MSc/3. Αποκεντρωμένες Τεχνολογίες/Assignment 1/
final')
Current blockchain height: 0 blocks
Fund's lock is set to: 103 blocks

Newly created P2SH address with absolute lock set to 103 blockchain height:
2N5st4iuxmrMVw8YKRPFytF987f2A2ceGoi
```

- Τέλος η μέθοδος επιστρέφει τα δεδομένα που είναι απαραίτητα για το δεύτερο μέρος της εργασίας, δηλ. το απόλυτο blocks κλειδώματος, το private key και την ίδια την P2SH διεύθυνση.

ΜΕΡΟΣ 2

Οι λειτουργίες που επιτελούνται είναι με τη σειρά οι ακόλουθες:

- Επιλέγει το BitCoin δίκτυο (regtest) και εκκινεί το proxy για τις RPC κλήσεις.
- Ανακτώνται τα απαραιτητα δεδομένα (ο απόλυτο blocks κλειδώματος, η P2SH διεύθυνση και το private key) μέσω της κλήσης και εκτέλεσης της κατάλληλης μεθόδου από το

Μέρος 1. Η μέθοδος εκτελείται εκ νέου, οπότε η διεύθυνση που δημιουργείται είναι διαφορετική από αυτή που δημιουργήθηκε αν είχε τρέξει πριν ο κώδικας του 1ου μέρους.

- Η P2SH διεύθυνση τροφοδοτείται με κάποια ποσά (κλειδωμένα), ώστε να τα χρησιμοποιήσει στη συνέχεια. Δημιουργείται και χρησιμοποιείται μέθοδος που εκτελεί τυχαίο αριθμό πληρωμών τυχαίων ποσών στη P2SH διεύθυνση, από τα κεφάλαια κάποιας άλλης διεύθυνσης του πορτοφολιού του χρήστη. Εκτυπώνονται τα στοιχεία των συναλλαγών και το τελικό αθροιστικό ποσό που μεταβιβάστηκε.
- Γίνεται εξόρυξη (mining) ενός block για να οριστικοποιηθούν οι συναλλαγές και ελέγχεται το mempool για το αν εχουν αυτές εκτελεστεί.
- Ελέγχονται τα διαθέσιμα UTXOs της P2SH διεύθυνσης. Η διαδικασία γίνεται με ειδική μέθοδο που ελέγχει τη διεύθυνση και επιστρέφει τα συνολικά UTXOs και το συνολικό ποσό BTCs στο οποίο αντιστοιχούν.
- Δημιουργείται μια νέα P2PKH διεύθυνση που θα λειτουργήσει ως παραλήπτης συναλλαγών από την P2SH διεύθυνση.

Ακολουθεί η διαδικασία δημιουργίας συναλλαγών από την P2SH προς την P2PKH διεύθυνση. Η εκφώνηση απαιτεί την χρήση όλων των διαθέσιμων κεφαλαίων, που πρέπει να προέρχονται από πολλαπλά UTXOs. Δεν κατάφερα να υπογράψω συναλλαγή από την P2SH διεύθυνση με πολλαπλά inputs, οπότε στη συνέχεια περιορίζομαι σε συναλλαγή με ένα input και συγκεκριμένα το πρώτο από τα UTXOs που επιστρέφονται παραπάνω.

- Υπολογίζεται η αμοιβή εξόρυξης (mining fees) της συγκεκριμένης συναλλαγής. Χρησιμοποιείται μέθοδος που υπολογίζει το μέγεθος της συναλλαγής (σε bytes) με εμπειρικό τύπο, που βασίζεται στο πλήθος inputs και outputs της συναλλαγής (1 και 1 αντίστοιχα). Στη συνέχεια υπολογίζει τη συνολική αμοιβή πολλαπλασιάζοντας με συντελεστή 50 satochis/byte, μια μέση τιμή που χρησιμοποιείται σήμερα.
- Δημιουργούνται το input και το output της συναλλαγής, χρησιμοποιώντας κατάλληλες τιμές για το sequence και το locktime, ανάλογα με τις τιμές που χρησιμοποιήθηκαν για το κλείδωμα της P2SH αρχικά. Δομείται η συναλλαγή συνδυάζοντας τα επιμέρους στοιχεία.
- Εκτυπώνεται η Raw Unsigned Transaction.
- Ξεκλειδώνεται το input της συναλλαγής. Αρχικά δημιουργείται εκ νέου το redeem script που χρησιμοποιήθηκε και στο 1ο μέρος. Με αυτό δημιουργείται η υπογραφή με την οποία υπογράφεται (ξεκλειδώνεται) το input.
- Εκτυπώνεται η Raw Signed Transaction.
- Εκτυπώνεται το ID της Raw Signed Transaction.
- Επικυρώνεται η συναλλαγή, ώστε να είμαστε βέβαιοι ότι αυτή θα γίνει αποδεκτή όταν αποσταλεί στους κόμβους του BitCoin. Χρησιμοποιείται έλεγχος, που επιτρέπει την συνέχιση εκτέλεσης του προγράμματος μόνο αν η επικύρωση είναι επιτυχής. Σε κάποιες περιπτώσεις η συναλλαγή απορρίπτεται (για διάφορους λόγους), οπότε το πρόγραμμα διακόπτει την εκτέλεσή του και ο χρηστης ειδοποιείται για τη αιτία απόρριψης:

```
Transaction verification:
Transaction rejected (reject-reason: missing-inputs). Transaction broadcast cancelled.

An exception has occurred, use %tb to see the full traceback.

SystemExit: 0
```

- Σε περίπτωση θετικής επικύρωσης, το πρόγραμμα προχωρά στην αποστολή της συναλλαγής στους κόμβους του BitCoin. Εκτυπώνει το συνολικό ποσό και τη διεύθυνση του παραλήπτη.
- Επιπλέον εξακρίβωση επιτυχούς συναλλαγής. Γίνεται εξόρυξη ενός block για να οριστικοποιηθεί η συναλλαγή. Για λόγους επίδειξης ελέγχεται το mempool πριν και μετά την εξόρυξη. Ελέγχονται τα ποσά που δέχτηκε η διεύθυνση του παραλήπτη και ειδοποιείται σχετικά ο χρήστης.

Μια τυπική έξοδος του προγράμματος, μετά την επιτυχή του εκτέλεση, είναι η ακόλουθη:

```
Reloaded modules: Liapikos_Assign1_pt1
Current blockchain height: 0 blocks
Fund's lock is set to: 103 blocks

Newly created P2SH address with absolute lock set to 103 blockchain height:
2My1bJx4fGBe74NYs8gyknZ336QRTNJW24s

Mining first 101 blocks

Payments to P2SH address:
Payment 1: 4.52736284 BTCs
ca3505d1f2957d937cdab1d919f80b04301d80a2676b05d59cfcc89c99417e8e
Payment 2: 4.68018450 BTCs
9776d21fc30e2cdca64f4177bf7c20626649741f24230e214e2a3e6f999bb758
Payment 3: 6.32034070 BTCs
aad2f9f485aa266dd21a9315b3301bff545c081e0bf813c91a1cfad97a3b6e71
Payment 4: 7.93067003 BTCs
456d1d29005a6f15f2c2b5281677cee2eebef1e6d0b7f747d798816dddcfa561
Total amount sent to P2SH address: 23.45855807 BTCs (4 TXs)

Pending transactions in mempool: 0

Total amount received by P2SH address: 23.45855807 BTCs

UTXOs for address 2My1bJx4fGBe74NYs8gyknZ336QRTNJW24s:
Found 4 UTXOs corresponding to 23.45855807 BTCs

Calculated fees for transaction: 0.00011200 BTCs

Raw Unsigned Transaction:
020000000158b79b996f3e2a4e210e23241f74496662207cbf77414fa6dc2c0ec31fd276970000000000feffffff015239e51b00000000197
6a914abd23027827d9513431b5d23d7ecbf11da40e60f88ac67000000

Raw Signed Transaction:
020000000158b79b996f3e2a4e210e23241f74496662207cbf77414fa6dc2c0ec31fd2769700000000894830450221 00a182b20b89a44edea
e22e3b85872c94fb7d4caeb24d40448600489913145cfa6022005f3121dba7ecf2db4da5bc95c4350804a9e1fc687f6f32770636649824dd0
20012103ae0b0aab66e9758504d36b55d1b4f2174700c3cd101cc240b771105c9d76d59e1d0167b17576a914ab2c398cb758cd655c16bbdf0
761e16dc1d3d7bb88acfeffffff015239e51b000000001976a914abd23027827d9513431b5d23d7ecbf11da40e60f88ac67000000

Raw Signed Transaction ID: fa514ebb3730a6b10e3ad17bb5f8f5faccb3a3c6d33c16a9966c41b5ad276dc1

Transaction verification:
[{'txid': 'fa514ebb3730a6b10e3ad17bb5f8f5faccb3a3c6d33c16a9966c41b5ad276dc1', 'allowed': True}]
Transaction seems ok!. Proceed to transaction broadcast.

Transaction sent successfully in blockchain: fa514ebb3730a6b10e3ad17bb5f8f5faccb3a3c6d33c16a9966c41b5ad276dc1
4.68007250 BTCs sent to address: mwBTdywB4BSCTfQ6bjs7fKJhXiFmPUie8z

Pending transactions in mempool before mining: 1
Pending transactions in mempool after mining: 0

Checking recipient P2PKH address for received BTCs:
Recipient address received 4.68007250 BTCs.
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Υλικό του μαθήματος
2. https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin/+packages
3. https://pypi.org/project/bitcoin-utils/
4. https://news.bitcoin.com/how-to-calculate-bitcoin-transaction-fees-when-youre-in-a-hurry/
5. https://github.com/jgarzik/python-bitcoinrpc
6. https://www.buybitcoinworldwide.com/fee-calculator/
7. https://bitcoinfees.earn.com/