Hand in five: Exercise 8.2
Group: IT03

Kasper Iverslien Borgbjerg (201808262) – 201808262@post.au.dk
Oliver Christensen (201808502) – 201808502@post.au.dk
Frederik Bay (201800246) – 201800246@post.au.dk

October 27, 2020

Kasper Iverslien Borgbjerg – 201808262 Oliver Christensen – 201808502
Frederik Bay Nørgaard – 201800246

1 Exercise 6.13 (Implement a Simple Peer-to-Peer Ledger)

1.1 How it is prompted

It is prompted through the terminal through the whole process.

A few terminal windows is opened and then we typed the following in:

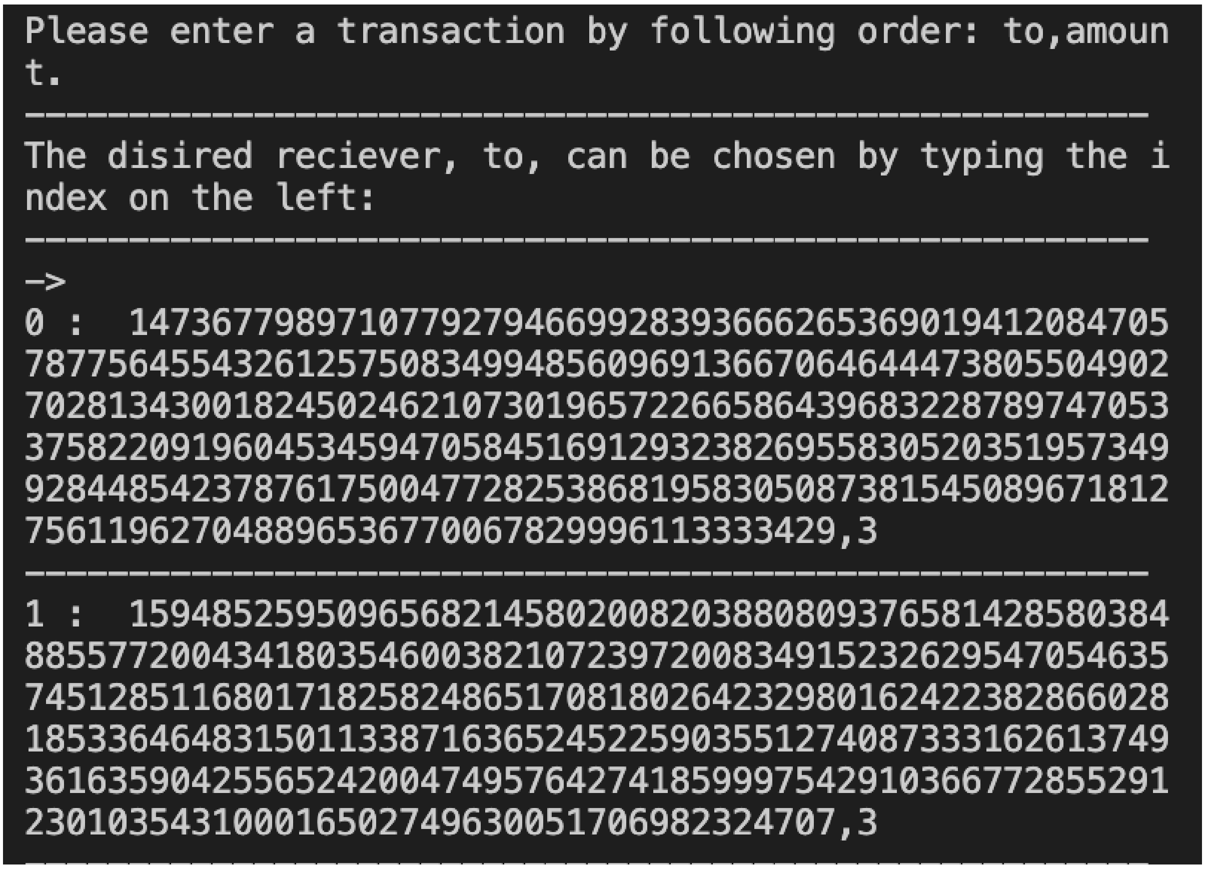
go run assignment613.go

This will prompt the command line, where you will type your localhost and a port ex. "localhost:58967".

If nothing is typed, it will open a port automatically.

When the first port has been opened, this can be connected to with other peers.

After this is done, an request for typing a transaction will appear. It will show a list of PK, which a transaction can be made to with an adhering index.



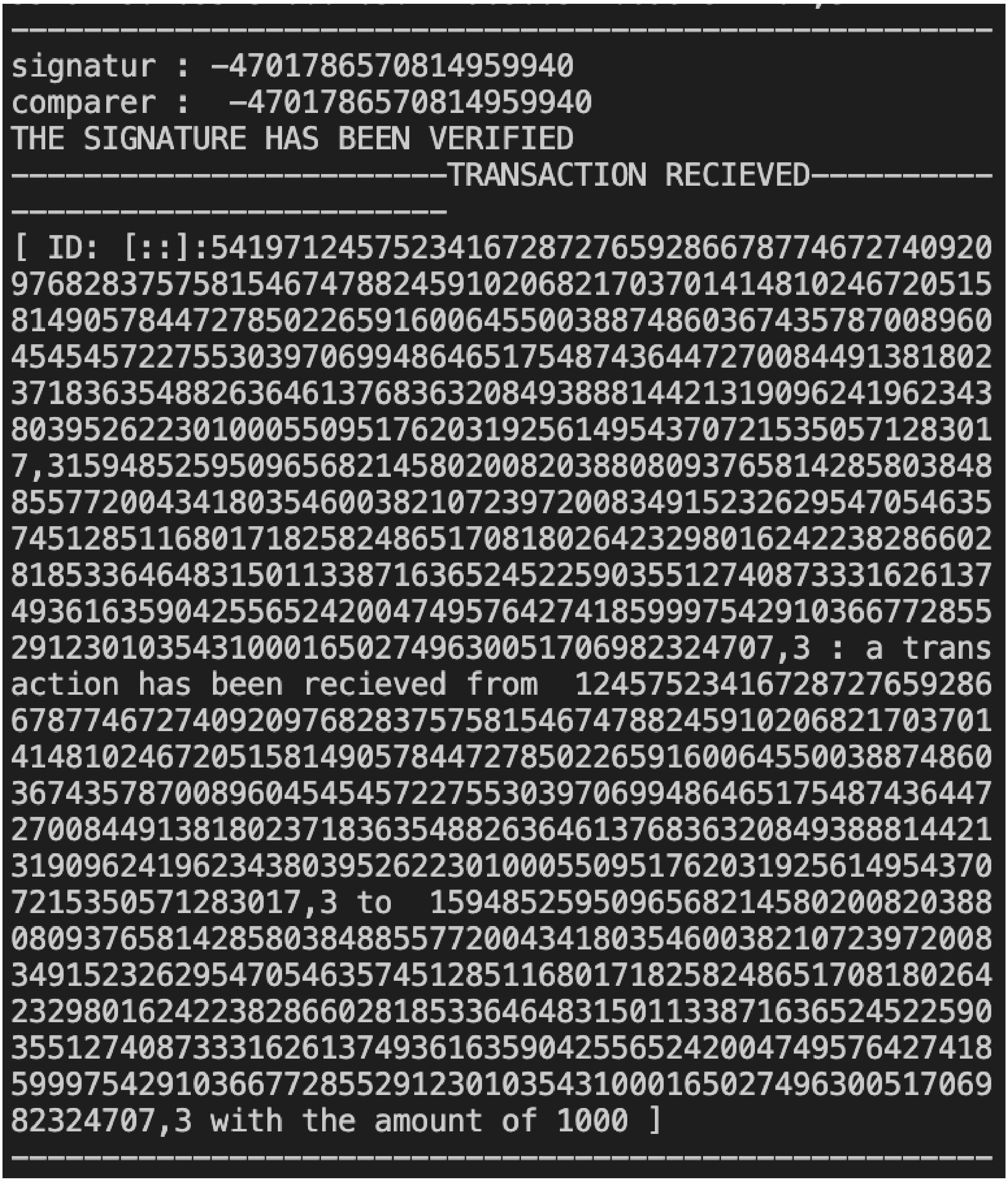
```
Please enter a transaction by following order: to,amoun
t.
------------------------------------------------------
The disired reciever, to, can be chosen by typing the i
ndex on the left:
------------------------------------------------------
->
0 :  14736779897107792794669928393666265369019412084705
7877564554326125750834994856096913667064644473805504902
7028134300182450246210730196572266586439683228789747053
3758220919604534594705845169129323826955830520351957349
9284485423787617500477282538681958305087381545089671812
756119627048896536770067829996113333429,3
------------------------------------------------------
1 :  15948525950965682145802008203880809376581428580384
8855772004341803546003821072397200834915232629547054635
7451285116801718258248651708180264232980162422382866028
1853364648315011338716365245225903551274087333162613749
3616359042556524200474957642741859997542910366772855291
230103543100016502749630051706982324707,3
------------------------------------------------------
```

Figure 1: Transaction request

By typing the index and the desired amount to be tranferred in the following order, as ex: "1,20000".

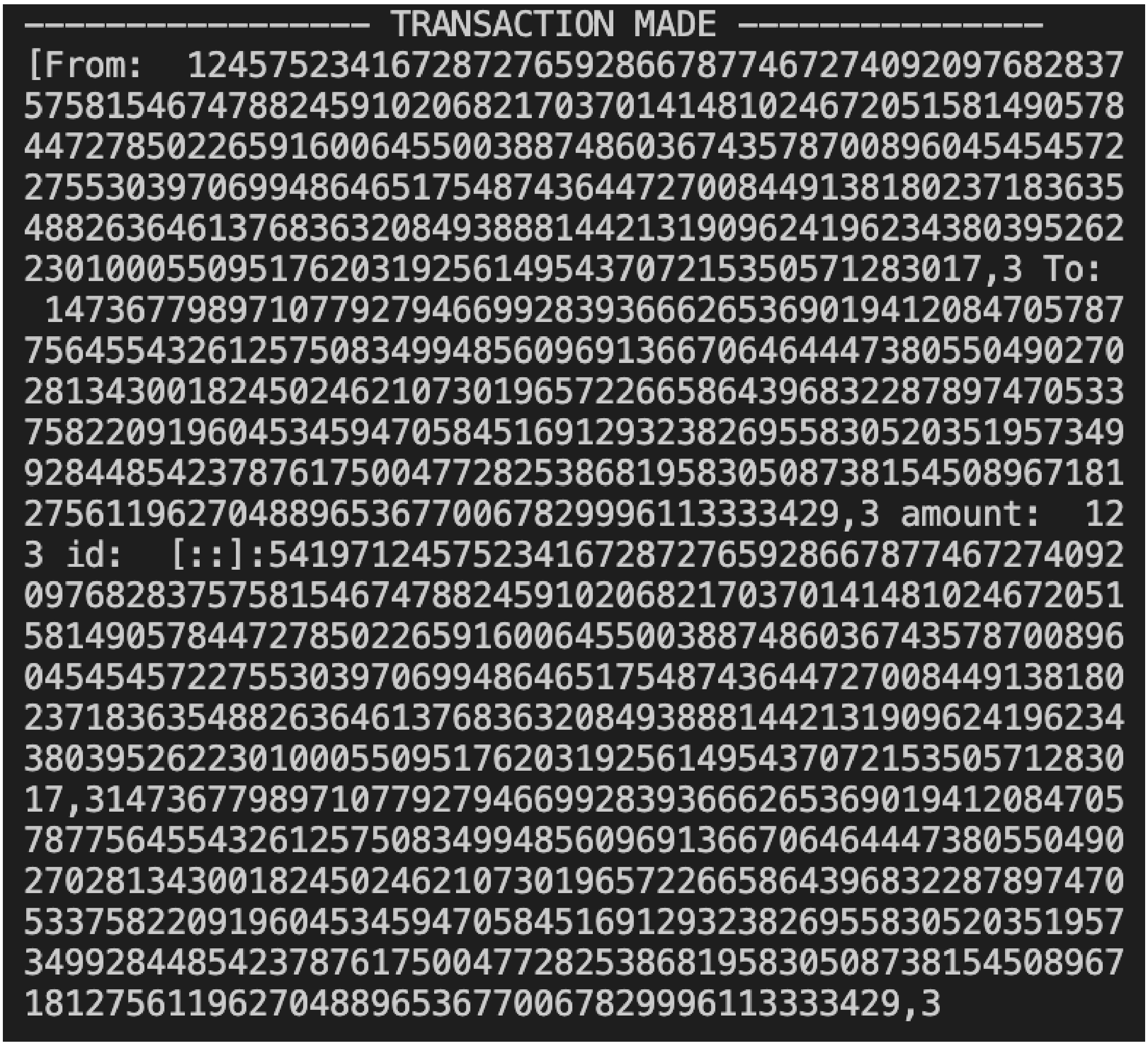
By doing this, it is insured that the reciever is possible to send to.

After the transaction has been approved, it will send it to the other peers, and they can verify it.



```
------------------------------------------------------
signatur : -4701786570814959940
comparer :  -4701786570814959940
THE SIGNATURE HAS BEEN VERIFIED
------------------------TRANSACTION RECIEVED----------
------------------------
[ ID: [::]:5419712457523416728727659286678774672740920
976828375758154674788245910206821703701414810246720515
814905784472785022659160064550038874860367435787008960
454545722755303970699486465175487436447270084491381802
371836354882636461376836320849388814421319096241962343
803952622301000550951762031925614954370721535057128301
7,3159485259509656821458020082038808093765814285803848
855772004341803546003821072397200834915232629547054635
745128511680171825824865170818026423298016242238286602
818533646483150113387163652452259035512740873331626137
493616359042556524200474957642741859997542910366772855
2912301035431000165027496300517069823247O7,3 : a trans
action has been recieved from  12457523416728727659286
678774672740920976828375758154674788245910206821703701
414810246720515814905784472785022659160064550038874860
367435787008960454545722755303970699486465175487436447
270084491381802371836354882636461376836320849388814421
319096241962343803952622301000550951762031925614954370
7215350571283017,3 to  1594852595096568214580200820388
080937658142858038488557720043418035460038210723972008
349152326295470546357451285116801718258248651708180264
232980162422382866028185336464831501133871636524522590
355127408733316261374936163590425565242004749576427418
599975429103667728552912301035431000165027496300517069
82324707,3 with the amount of 1000 ]
------------------------------------------------------
```

Figure 2: Transaction verified



```
----------------- TRANSACTION MADE ---------------
[From:  1245752341672872765928667877467274092097682837
575815467478824591020682170370141481024672051581490578
447278502265916006455003887486036743578700896045454572
275530397069948646517548743644727008449138180237183635
488263646137683632084938881442131909624196234380395262
23010005509517620319256149543707215350571283017,3 To:
 14736779897107792794669928393666265369019412084705787
756455432612575083499485609691366706464447380550490270
281343001824502462107301965722665864396832287897470533
758220919604534594705845169129323826955830520351957349
928448542378761750047728253868195830508738154508967181
2756119627048896536770067829996113333429,3 amount:  12
3 id:  [::]:541971245752341672872765928667877467274092
097682837575815467478824591020682170370141481024672051
581490578447278502265916006455003887486036743578700896
045454572275530397069948646517548743644727008449138180
237183635488263646137683632084938881442131909624196234
380395262230100055095176203192561495437072153505712830
17,314736779897107792794669928393666265369019412084705
787756455432612575083499485609691366706464447380550490
270281343001824502462107301965722665864396832287897470
533758220919604534594705845169129323826955830520351957
349928448542378761750047728253868195830508738154508967
1812756119627048896536770067829996113333429,3
```

Figure 3: transaction made

1.2 How it was tested

No automated testing was made to this program due to time issues.

The system was tested through the terminal with both small amounts of peers connected and severaly bigger amounts peers connected.

By enhancing and lowering the KeyGen's k, it would be visible when the KeyGen was small enough till the program would not verify the signature.

A few things still need to be implemented for the program to work to full extend. Therefore it is not able verify if the transaction is negative. But all other aspects was tested.

What was accomplished for the test, was that the program sometimes stops recieving and sending transactions after sending a few. Though, the loop of requesting a tranaction should work.

When converting the signature to a string and back we encounteret that it lost some data, when it was converted, this was found out in the testing phase, and solved by using the big.Int when converting.