

UNIVERZITET U SARAJEVU
ELEKTROTEHNIČKI FAKULTET SARAJEVO

DOMACA ZADACA 1

TEHNOLOGIJE SIGURNOSTI

Student: Mašović Haris

Indeks: 1689/17993

Odsjek: Računarstvo i Informatika

Datum:

02.11.2020

Potpis:

Zadaća 1

Prijem i slanje Bitcoin-a

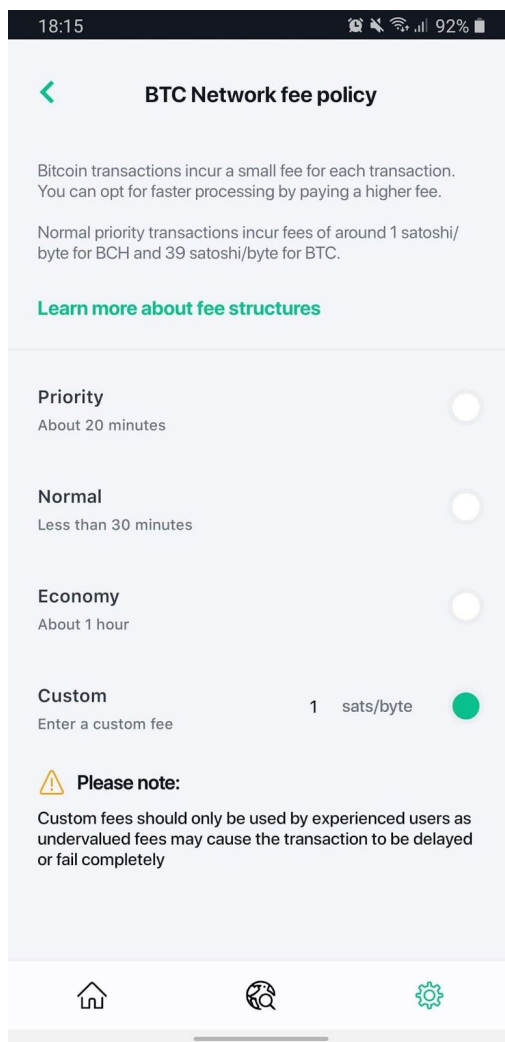
Potrebno je primiti i poslati Bitcoin-e i evidentirati transakcije kojim je ovo učinjeno. Asistent će jednom studentu iz grupe za vježbe poslati određen iznos Bitcoin-a. Taj student treba isti iznos (umanjen za trošak transakcije, ako je neophodan) poslati slijedećem studentu iz iste grupe i tako dok svi studenti iz grupe ne dobiju i pošalju Bitcoin-e. Posljednji student iz grupe treba Bitcoin-e poslati profesoru.

U izvještaju je potrebno navesti vlastitu Bitcoin adresu, adresu sa koje su dobiveni Bitcoin-i i adresu na koju su poslani. Na Blockchain je potrebno pronaći obje transakcije i sve tri adrese i prikazati ih u zadaći. Za svaku od transakcija je potrebno navesti koliki je bio njen trošak i koliko je trajalo dok nije potvrđena. Navedene vrijednosti je potrebno potkrijepiti dokazima u vidu ispisa sa lokacijama na kojim su pronađene.

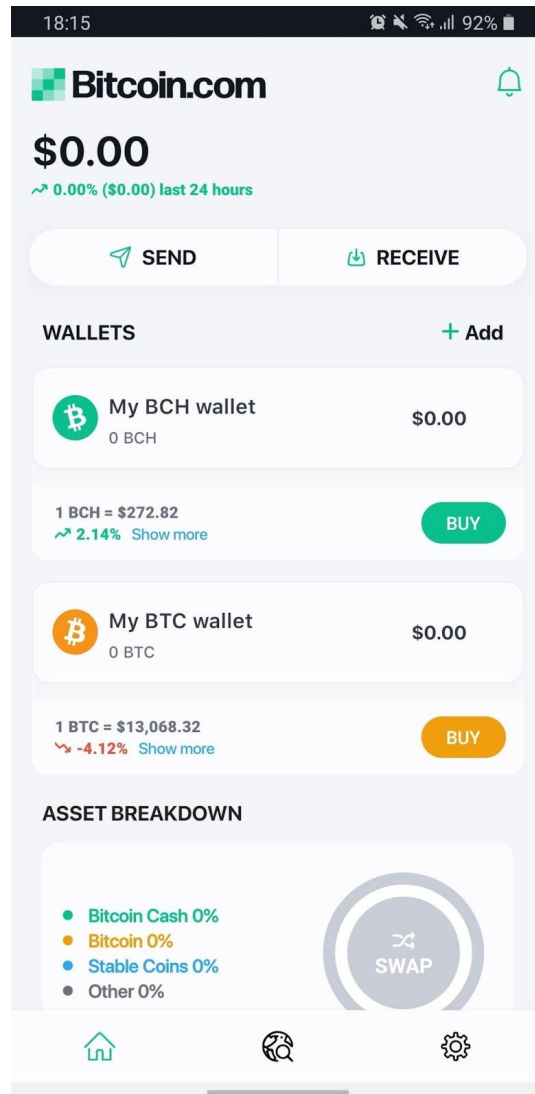
Zadaće se predaju putem Zamgera kao .pdf prilog.

Rok za predaju zadaća je petak 6.11.2020.

Prije svega treba postaviti custom fee vrijednost od 1 sats/byte kao sto je trazeno:



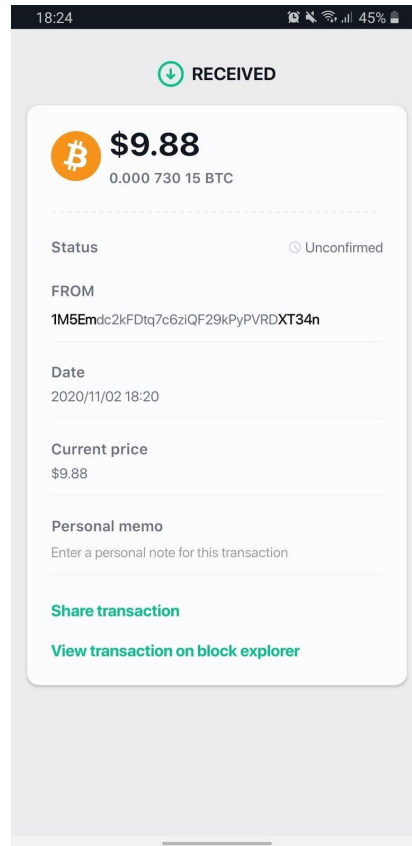
Pocetno stanje racuna je prikazano sljedecom slikom:



Transakcija na relaciji od kolege Irhada Omanovica ka meni je sljedeca:

- Adresa posiljaoca (kolega Irhad, ujedno i prva trazena adresa):
1M5Emdc2kFDtq7c6ziQF29kPyPVRDXT34n
- Adresa primaoca (moja adresa, druga trazena adresa):
16YgW8kiVUfoGVdXJeuZfRCAaZ47xE7Ymo
- Id transakcije:
4c7a8576ed26358f1994d366ec9cc253ba91d47da1a9111a9d1d922e92ea50a8

Prethodna transakcija se može prikazati sljedećim slikama (wallet + [ledger](#)):



Transaction

Confirmed

Transaction ID 4c7a8576ed26358f1994d366ec9cc253ba91d47da1a9111a9d1d922e92ea50a8

Transaction ID is an identifier which facilitates easy location of transactions on the blockchain.

Transaction ID is created by the SHA-256 hash function which takes a unique result (ID) from a given string of data.

Summary

[Hide details](#)

Coinbase	No	
Age	a day ago	
Date	November 8, 2020 2:54 PM	UTC+01:00
First Seen	November 2, 2020 6:20 PM	UTC+01:00
Block	655984	
Confirmations	184	
Fees	0.04 USD 0.04 USD	0.000 002 32 BTC
Fees per byte	< 0.01 USD < 0.01 USD	1.21 sat
Unix Timestamp	1604843680	
Total Input	11.09 USD 11.15 USD	0.000 732 47 BTC
Total Output	11.06 USD 11.11 USD	0.000 730 15 BTC
Size (kB)	0.191 kB	
Version	2	
Lock Time	0	



Now you can buy **Bitcoin**,
without even leaving your
wallet.

[Buy Bitcoin](#)

Inputs 1

Search inputs



Amount

0 1M5Emdc2kFDtq7c6z1QF29kPyPVR0XT34n 11.09 USD
11.15 USD

Outputs 1

Search outputs



Amount

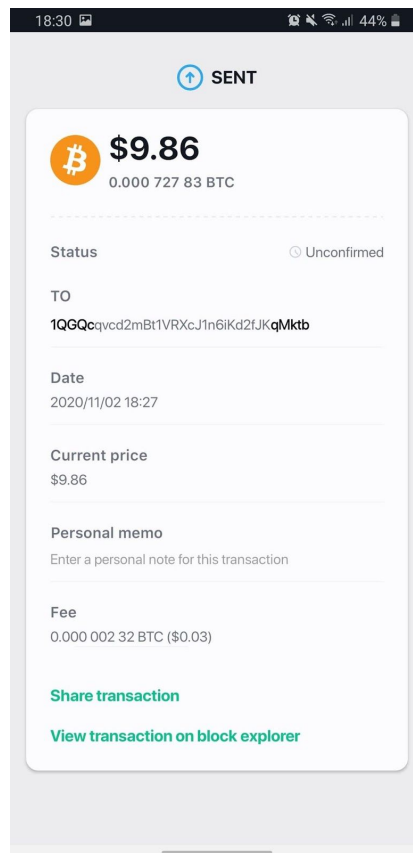
0 16YgW8kiVUfoGVdXJeuZFRCAaZ47xE7Ymo 11.06 USD
11.11 USD

- Trosak transakcije je bio 0.04 USD.
- 6 dana je bilo potrebno za potvrđivanje ove transakcije. Transakcija je obavljena 2. Novembra, a potvrđena 8. Novembra kao što se može vidjeti na slici iznad.

Nakon toga, ja sam poslao bitcoine kolegici Ajli Panjeti, svi bitni id-evi su sljedeći:

- Adresa posiljaoca: 16YgW8kiVUfoGVdXJeuZfRCAaZ47xE7Ymo
- Adresa primaoca (kolegica Ajla, treća tražena adresa):
1QGQcqvcd2mBt1VRXcJ1n6iKd2fJKqMktb
- Id transakcije:
ee16c50d7a793bcba3fb66ce7fc297d7b4d8887f2bdb02719faf6a0a8806e741

Prethodna transakcija se može vidjeti na sledecim slikama (wallet + [ledger](#)):



Transaction

Confirmed

Transaction ID [ee16c50d7a793bcb3fb66ce7fc297d7b4d8887f2bdb02719faf6a0a8806e741](#)

Summary

[Hide details](#)

Coinbase	No	
Age	a day ago	
Date	November 8, 2020 2:54 PM UTC+01:00	
First Seen	November 2, 2020 6:27 PM UTC+01:00	
Block	655984	
Confirmations	184	
Fees	0.04 USD 0.04 USD	0.00080232 BTC
Fees per byte	< 0.01 USD < 0.01 USD	1.21 sat
Unix Timestamp	1604843680	
Total Input	11.09 USD 11.11 USD	0.00073815 BTC
Total Output	11.05 USD 11.08 USD	0.00072783 BTC
Size (kB)	0.191 kB	
Version	2	
Lock Time	0	



Now you can buy **Bitcoin**,
without even leaving your
wallet.

[Buy Bitcoin](#)

Inputs 1

Search inputs



Amount

0 16YgW8kiVUfoGvdXJeuZfRCAaZ47xE7Ymo 11.09 USD
11.11 USD

Outputs 1

Search outputs



Amount

0 1QGQcqvcd2nBt1VRXcJ1n6iKd2fJKqkktb 11.05 USD
11.08 USD

- Trosak transakcije je bio: 0.04 USD.
- 6 dana je bilo potrebno za potvrđivanje ove transakcije. Transakcija je obavljena 2. Novembra, a potvrđena 8. Novembra, kao što se može vidjeti na slici iznad.

Finalnu listu transakcija mozemo vidjeti na sljedećoj slici:

