FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

LABORATORIJSKA VJEŽBA 3

Uvod u Bitcoin mrežu

Sadržaj

1. Uvod

Da bismo bolje razumjeli ovu vježbu, važno je razlikovati između pojmova "Bitcoin" i "bitcoin". Iako se može činiti da su ova dva pojma ista, zapravo postoji velika razlika među njima. Pojam "Bitcoin" (s velikim početnim slovom) se odnosi na cijelu mrežu koja uključuje algoritme, protokole, čvorove i druge elemente. To je slično kao što pojam "Internet" (s velikim slovom) označava točno određenu globalnu računalnu mrežu i sve ono što je čini mogućom, dok se pojam "internet" (pisano malim slovom) odnosi na vrstu mreža.

S druge strane, pojam "bitcoin" (pisano malim početnim slovom) se koristi za opisivanje kriptovalute koja se koristi na blockchain mreži. To je važno razumjeti kako bismo bolje shvatili razliku između Bitcoin mreže kao cjeline i samog kriptovalutnog tokena.

Za shvaćanje Bitcoina ćemo koristiti Bitcoin Core dok ćemo za shvaćanje bitcoina koristiti blockchain.com explorer.

2. Bitcoin

Bitcoin mreža je decentralizirana računalna mreža koja omogućuje prijenos i pohranu digitalnih vrijednosti u obliku bitcoina. To je otvorena mreža koja se sastoji od računala diljem svijeta, a svako računalo u mreži naziva se čvorom.

Bitcoin mreža omogućuje prijenos bitcoina između korisnika bez posrednika kao što su banke ili drugi financijski posrednici. Umjesto toga, transakcije se verificiraju i obrađuju od strane korisnika na mreži koji se nazivaju "rudari" (mineri). Kada se transakcije verificiraju, one se trajno bilježe na javnoj knjizi poznatoj kao blockchain.

Blockchain je temeljni dio Bitcoin mreže, a sastoji se od niza blokova koji sadrže transakcije. Svaki blok povezan je s prethodnim blokom, stvarajući na taj način neizbrisivi lanac transakcija. Ovaj proces osigurava da se digitalne valute ne mogu ponovo koristiti, te da su transakcije sigurne, transparentne i pouzdane.

Bitcoin mreža koristi kriptografiju kako bi osigurala sigurnost i privatnost transakcija. Korisnici se identificiraju putem jedinstvenih digitalnih ključeva, koji su izuzetno teški za hakiranje. Također, Bitcoin mreža je programirana da ograniči količinu bitcoina koji se može stvoriti, te se to ograničenje procjenjuje na 21 milijun Bitcoina. Ilustracija Bitcoina je prikazana na slici 1.

Slika 1. Bitcoin mreža

Bitcoin mreža je podijeljena na dvije glavne mreže: glavnu mrežu i testnu mrežu (Testnet). Glavna mreža je stvarna Bitcoin mreža koja se koristi za slanje i primanje bitcoina, dok se testna mreža koristi za razvoj i testiranje novih rješenja bez stvarnog rizika od gubitka novca ili oštećenja Bitcoin mreže. Obje mreže koriste zasebni blockchain. Na datum 29.3.2023., veličina blockchaina glavne mreže je oko 497 GB dok je Testnet blockchain znatno manji i iznosi oko 28 GB. Važno je napomenuti da bitcoini koji su u opticaju na testnoj mreži nemaju nikakvu novčanu vrijednost.

2.1. Bitcoin core

Bitcoin Core je softverski projekt otvorenog koda koji predstavlja referentnu implementaciju Bitcoin protokola. To je glavni softver koji se koristi za upravljanje Bitcoin mrežom.
Ako imate Bitcoin Core instaliran na svom računalu, tada ste zapravo pokrenuli Bitcoin čvor. Bitcoin čvor je računalo ili uređaj u Bitcoin mreži koje je uključeno u proces potvrde transakcija i održavanja blockchaina. Svaki čvor u mreži ima kopiju cijele Bitcoin blockchain baze podataka i koristi se za potvrdu novih transakcija i stvaranje novih blokova koji se dodaju u blockchain. Vaš čvor će se povezati s drugim čvorovima u mreži kako bi razmjenjivali podatke o transakcijama i novim blokovima, što doprinosi održavanju Bitcoin mreže i osigurava njezinu sigurnost i stabilnost.

Bitcoin Core omogućuje korisnicima da upravljaju svojim Bitcoin novčanicima (walletima), koji su neophodni za primanje i slanje Bitcoina. Softver omogućuje korisnicima da pregledavaju svoje transakcije, potpisuju i verificiraju transakcije, te provjere stanje svojih Bitcoin novčanika.

Osim toga, Bitcoin Core predstavlja i važan čimbenik u održavanju sigurnosti i stabilnosti Bitcoin mreže. Softver se redovito ažurira kako bi se poboljšale njegove funkcionalnosti, popravili eventualni bugovi te osigurala sigurnost mreže.

Bitcoin Core također omogućuje rudarima da provode proces potvrđivanja transakcija i stvaranja novih blokova u blockchainu, koji se koristi za bilježenje svih Bitcoin transakcija. Trenutna verzija programa prikazana je na slici 2.

Slika 2. Bitcoin core

Zapravo, na slici je prikazan Bitcoin Core Test koji je posebna verzija Bitcoin Core softvera koja se koristi u svrhu testiranja i razvoja Bitcoin mreže. Ova verzija softvera omogućuje programerima da testiraju svoje aplikacije i softverska rješenja prije nego što ih implementiraju u stvarnom okruženju.

Bitcoin Core Test mreža je mreža identična glavnoj Bitcoin mreži, ali se koristi samo u svrhu testiranja i razvoja. Na ovoj mreži korisnici mogu testirati transakcije, slati Bitcoine, mijenjati postavke softvera i razvijati nove aplikacije bez stvarnog rizika od gubitka novca ili oštećenja Bitcoin mreže.

Ova testna mreža se koristi i za testiranje novih verzija Bitcoin Core softvera prije nego što se implementiraju u glavnu mrežu. Ovaj pristup pomaže u otkrivanju eventualnih bugova i poboljšava stabilnost i sigurnost glavne Bitcoin mreže.

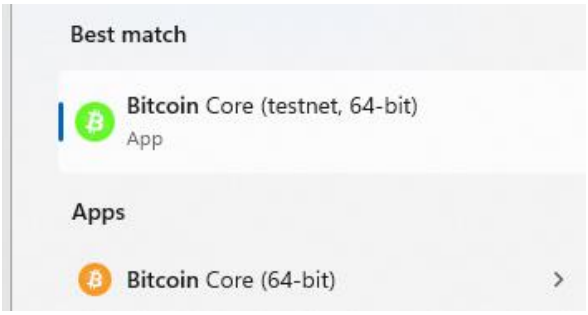
2.2 Slavina (eng. faucet)

Faucet za Bitcoin je web stranica ili aplikacija koja nudi besplatne Bitcoine korisnicima koji posjete njihovu stranicu. Ova vrsta web stranica je popularna među korisnicima koji žele dobiti mali broj Bitcoina bez ulaganja velikog novčanog iznosa.

Faucet web stranice obično nude korisnicima male količine Bitcoina, koje se obično izražavaju u satoshima - najmanjoj jedinici Bitcoina. Korisnici mogu posjetiti stranicu, ispuniti kratki captcha obrazac i dobiti nagradu u obliku malog broja satoshija. Iako su ove nagrade relativno male, mogu se akumulirati tijekom vremena i pomoći korisnicima da se upoznaju s kriptovalutama.

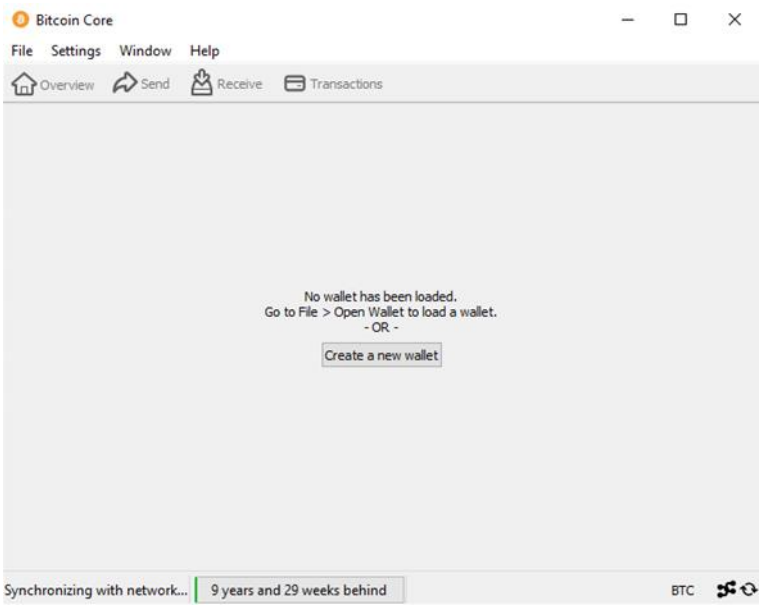
2.3. Pristup Bitcoin Testnetu putem programa Bitcoin Core

Bitcoin Core možete preuzeti sa poveznice https://bitcoin.org/en/bitcoin-core/. Nakon instalacije programa, računalo morate ostaviti upaljeno dok se ne skine čitav blockchain. Za potrebe ove laboratorijske vježbe, dovoljno je pokrenuti Bitcoin Core Test. Nakon što ste instalirali glavni program, instalirali ste i testnu verziju. Svakako pripazite koju verziju pokrećete. Razlika je u imenu i u boji kako je prikazano na slici 3.



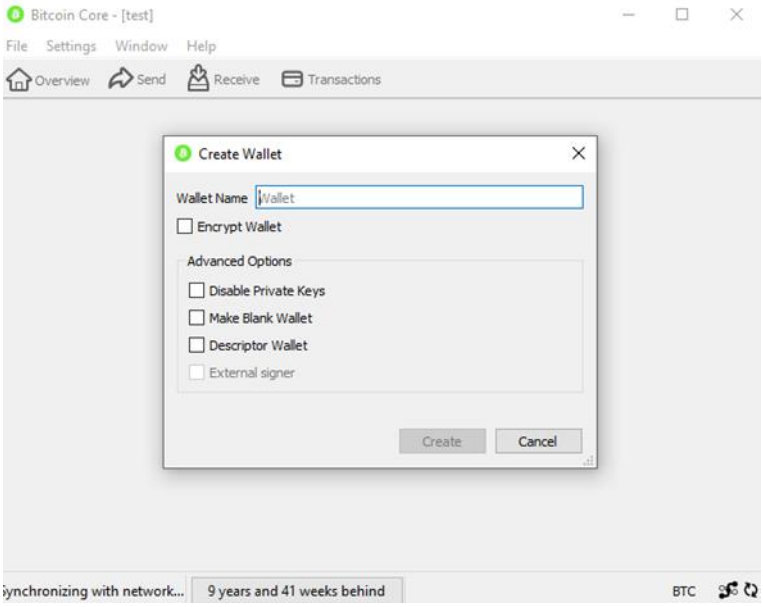
Slika 3. Razlika u inačicama Bitcoin Core programa

Verzija za testnu mrežu mora pohraniti oko 28 GB blockchaina na računalo a pohranjuje ga brzinom 2 Mbps. Nakon uspješno završene sinkronizacije blockchaina, dobiti ćete početni zaslon prikazan na slici 4.



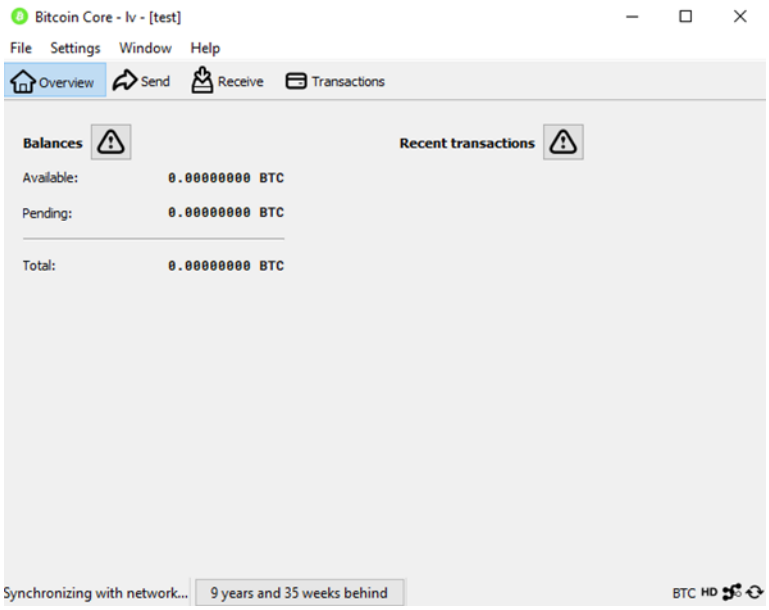
Slika 4. Početni zaslon Bitcoin Core programa

Nakon pokretanja programa, potrebno je kliknuti na gumb „Create a new wallet" kako bi kreirali svoj novčanik. Pritiskom gumba, vidimo ekran koji je vidljiv na slici 5.



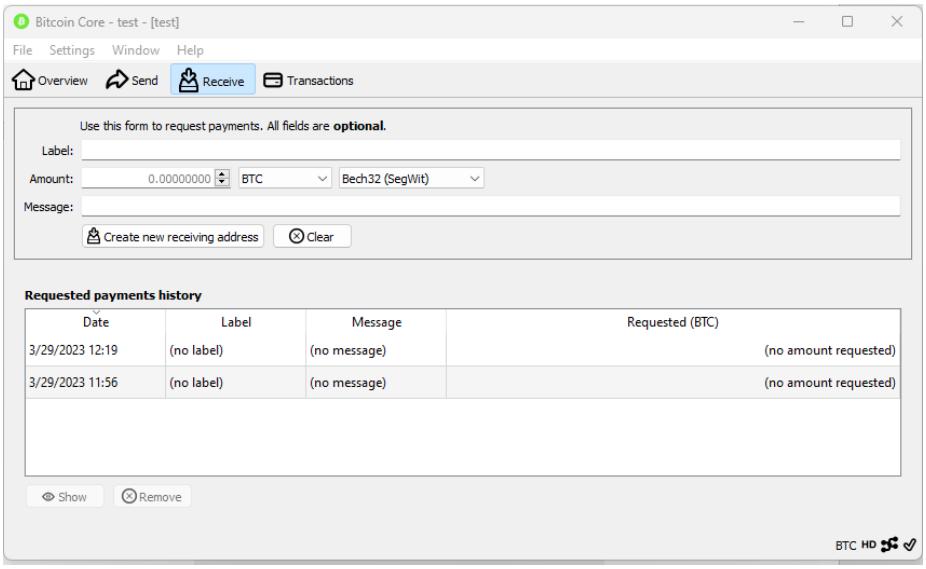
Slika 5. Kreiranje novčanika

U svrhu ovog testiranja, kreirati ćemo novčanik bez enkripcije stoga samo unesite proizvoljno ime. Nakon kreiranja novčanika, biti će nam vidljiv ekran kao na slici 6. Ukoliko niste i dalje završili sa sinkronizacijom blockchaina, vidjeti ćete znak uskličnika pokraj natpisa Balances i Recent transactions te nećete vidjeti daljnje rezultate potrebnu za dovršetak vježbe.



Slika 6. Kreirani novčanik

Kako bismo generirali novu adresu, potrebno je unutar programa pritisnuti karticu Recieve a potom gumb Creata new receiving address kako je vidljivo na slici 7.



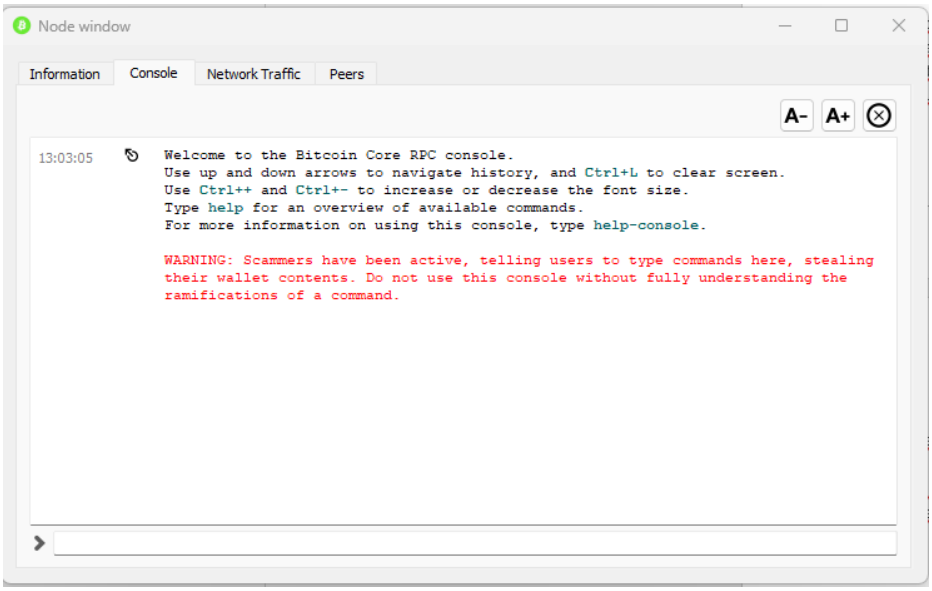
Slika 7. Generiranje adrese

Nakon generiranja adrese, otvara se prozor sa QR kôdom, adresom i imenom novčanika kako je prikazano na slici 8.

Slika 8. Adresa novčanika

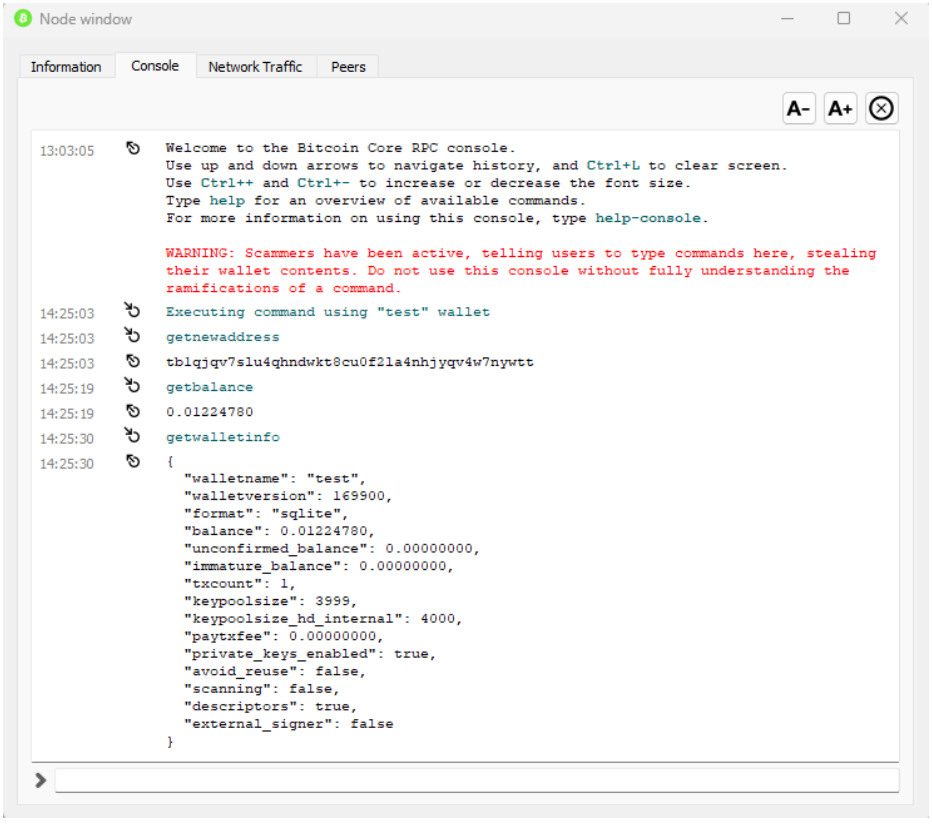
Možemo vidjeti da je dodijeljena adresa **tb1q35tqd68x3gq6ejpwhmwjqf0wtugngpqkdesw7r** . Naravno, adresa koja je dodijeljena vama će biti drugačija. Svakako ju kopirajte prije prelaska na slijedeći korak. Kako bismo napunili adresu testnim bitcoinom kojeg možemo prebaciti na drugu adresu i time ispuniti zadatak, koristimo faucet stranice. U ovom primjeru ćemo koristiti onaj sa poveznice https://coinfaucet.eu/en/btc-testnet/. Ova stranica nudi malu količinu bitcoina a može ju se koristiti samo jednom unutar 24 sata.

U otvoreni prozor na faucet, kopirajte adresu novčanika te stisnite gumb Get bitcoins. Ukoliko se vratite u Bitcoin Core, vidjeti ćete “pending” transakciju koja još mora biti potvrđena. Dok ćekate verifikaciju transakcije, možete uključite Bitcoin Core Console prikazan na slici 9 (na Win operativnom sustavu kratica je CTRL + T).



Slika 9. Bitcoin Core Console

Ovdje možemo pokrenuti neke jednostavne naredbe poput getnewaddress, getbalance, getwalletinfo, sendtoaddress. NJihovi rezultati su vidljivi na slici 10.



Slika 10. Jednostavne Console naredbe

3. bitcoin

Za razliku od Bitcoina kao mreže, bitcoin je kriptovaluta koja se koristi na istoj. Bitcoin je decentralizirana valuta, što znači da ne postoji centralna vlast koja bi je kontrolirala. Umjesto toga, transakcije se provode putem distribuirane mreže korisnika koji koriste softverske aplikacije za slanje i primanje bitcoina. Kao takva, bitcoin nema fizičko postojanje i ne ovisi o vladi ili centralnoj banci za svoju vrijednost.

Novi bitcoini se u mrežu dodaju procesom koji se naziva rudarenje. Rudari koriste računalnu snagu za rješavanje složenih matematičkih problema koji se koriste za potvrđivanje i obradu transakcija u mreži. Za svoj trud, rudari su nagrađeni novim bitcoinima.

Proof of Work (PoW) je algoritam konsenzusa koji se koristi u blockchain mrežama kriptovaluta, uključujući Bitcoin, kako bi se potvrdilo da su transakcije valjane i da se ne može desiti dvostruko trošenje. PoW algoritam zahtijeva da rudari potroše računalnu snagu na rješavanje matematičkih problema. Kada se problem uspješno riješi, rudari dobivaju nagradu u obliku novih bitcoina.

PoW zahtijeva puno računalne snage i troši puno energije, što znači da rudarenje može biti vrlo skupo. Međutim, PoW algoritam pruža visoku razinu sigurnosti, jer bi napadači trebali potrošiti ogromne količine resursa kako bi preuzeli kontrolu nad mrežom.

Bitcoin se može koristiti za kupovinu robe i usluga na trgovinama koje prihvaćaju ovu kriptovalutu kao način plaćanja. Također se može trgovati na različitim burzama kriptovaluta, što znači da se njegova vrijednost može mijenjati ovisno o ponudi i potražnji. Programski je određeno da postoji ukupno 21 milijun bitcoina. Trenutnim tempom, zadnji bi trebao biti izrudaren oko 2140. godine.

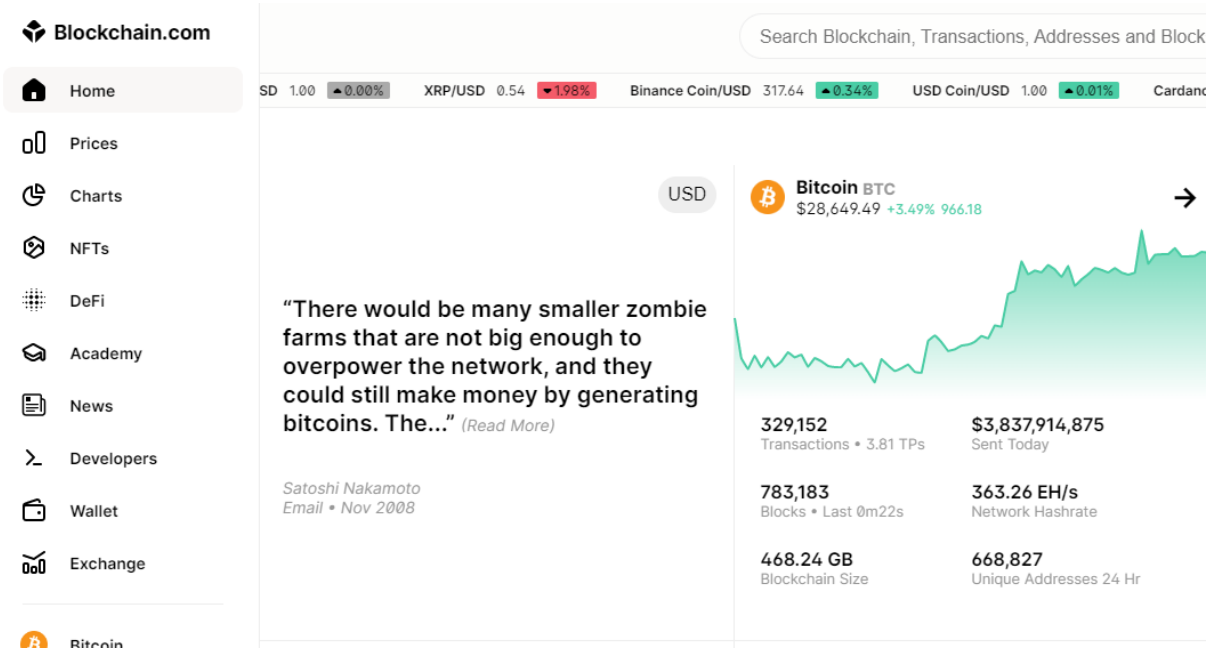
Stanje bitcoina, ka oi mnogih ostalih kriptovaluta možemo pogledati na mnogim servisima.

3.1. Blockchain.com explorer

Blockchain.com Explorer je alat za pregled i istraživanje blockchaina, te se koristi za pregledavanje transakcija, blokova i adresa na blockchain mreži kriptovaluta, kao što su Bitcoin i Bitcoin Cash. Pristupiti mu možemo na poveznici https://www.blockchain.com/explorer

Ovaj alat omogućava korisnicima da vide detaljne informacije o svakoj transakciji koja se odvija na blockchain mreži, uključujući iznos, vrijeme, hash vrijednost, i druge relevantne podatke. Također, korisnici mogu pregledati informacije o svakom bloku u blockchainu, kao što su veličina bloka, vrijeme stvaranja bloka i nagrada za rudarenje.

Blockchain.com Explorer je dostupan na webu i koristi se u cijelom svijetu kao jedan od najpopularnijih blockchain explorer alata. Korisnici mogu koristiti ovaj alat za praćenje svojih transakcija i provjeru potvrda, kao i za istraživanje i analizu podataka o blockchain mrežama. Prikaz početnog zaslona vidljiv je na slici 11.



Slika 11. Blockchain explorer

Sučelje je intuitivno i dostupne su sve informacije koje nas zanimaju. Potrebno je proučiti ovo sučelje kako biste mogli izvršiti zadatke laboratorijskih vježbi.

4. ZADACI

1. Na računalo instalirati Bitcoin Core, kreirati novčanik i na njega primiti iznos bitcoina sa neke od faucet stranica. Nakon što ste primili bitcoine, pošaljite proizvoljnu količinu bitcoina na neku novu i adresu iz svog novčanika. Iznos naknade postavite na 20sat/vB a broj konfirmacija 6. Screenshot transakcija unesite u dokument koji ćete predati putem Merlina.
2. U word dokumentu napravite izvještaj o stanju bitcoina na dan pravljenja izvještaja. Upišite najnižu i najvišu cijenu unutar 24 sata, također, izvještaj mora sadržavati i Market Cap, broj zadnjeg bloka, nagradu po bloku, broj coina u opticaju, maksimalan broj tokena, konsenzus, algoritam i datum Genesis bloka. Isto to napravite i za Shiba Inu.
3. (BONUS PITANJE ZA MAKSIMALAN BROJ BODOVA) Zašto Shiba Inu neće u dogledno vrijeme doseći vrijednost od 10 centi. Za potkrijepiti ovo pitanje koristite argumente iz izvještaja sa Blockchain Explorera.