SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 000

Usporedba performanci Ethereum raspodijeljene knjige na raznorodnom sklopovlju

Jakov Buratović

Zagreb, svibanj 2020.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu `\izvornik`.

Zahvaljujem se mentoru doc. dr. sc. Igoru Čavraku na podršci i pomoći pri izradi ovog rada.
Zahvaljujem se i kolegi Ediju Sinovčiću koji se već dulje vrijeme bavi razvojem programskih rješenja koji koriste tehnologiju distribuirane knjige te mi je mogao odgovoriti i riješiti sve moje nedoumice.

SADRŽAJ

1. Uvod **1**

2. Tehnologija glavne raspodijeljene knjige **2**

3. Proof of Authoroty algoritam **4**

4. PoA mreža na raznovrsnom sklopovlju **5**

4.1. Sklopovlje i programska podrška 5

4.1.1. Cubieboard2 6

4.1.2. Raspberry Pi 1 model B 6

4.1.3. Raspberry Pi 3 model B 7

4.1.4. Prijenosno i stolno računalo 7

5. Zaključak **9**

Literatura **10**

1. Uvod

Ethereum mnogi znaju kao jednu od najpopularnijih kriptovaluta. Iako je to točno, Ethereum je mnogo više od same digitalne valute. To je programska potpora raspodijeljena na mreži računala na kojima je moguće razmjenjivati podatke i pokretati računalne programe bez centralnog poslužitelja. Podaci se repliciraju na svaki čvor u mreži. Određenim algoritmima konsenzusa se osigurava nepromjenjivost i pouzdanost. To omogućuje da mreža bude potpuno javna i sigurna. Posebnost je što svatko može koristiti mrežu i objavljivati sadržaj bez ikakvih posebnih dozvola.
Za razliku od Bitcoina i mnogih drugih implementacija tehnologije distribuirane knjige koji nude mogućnost pohrane podataka bez centralnog poslužitelja, Ethereum mreža omogućuje i izvođenje programskog koda u obliku pametnih ugovora.
U ovom radu je prikazano kako se može pokrenuti privatna mreža na različitom sklopovlju s naglaskom na ispitivanje najnižih zahtjeva sklopovlja. Dodatno, prikazat ću proces obavljanja transakcija i izvođenja programskog koda na čvorovima uz prigodni prikaz sa sučeljem u jednostavnoj web aplikaciji.
U prvom poglavlju ovog rada, objasnit će se osnove tehnologije distribuirane knjige i njene primjene.
Nakon toga će biti poglavlje usmjereno na Ethereum kao implementaciju navedene tehnologije te prikaz i opis njegovih algoritama konsenzusa.
Treće poglavlje je zaduženo za detaljan postupak kreiranja privatne mreže na raznorodnom sklopovlju s različitim operativnim sustavima.
U posljednjem poglavlju je na prethodno kreiranu mrežu dodan grafički prikaz aktivnosti mreže i transakcija u jednostavnoj web aplikaciji.

2. Tehnologija glavne raspodijeljene knjige

U nastavku ćemo tehnologiju glavne raspodijeljenje knjige (engl. *Distributed Ledger Technology*) referencirati kraće po kratici engleskog naziva, odnosno DLT.
DLT i blockchain se često poistovjećuju no to nije u potpunosti ispravno. Bitno je znati da je svaki blockchain DLT s određenim pravilima konsenzusa. DLT je baza podataka repliciranog sadržaja na svakom čvoru *peer-to-peer* mreže. Svaki čvor mora sadržavati identičnu kopiju kompletnog sadržaja baze podataka i konstantno se ažurira sa susjednim čvorovima.
Kod blockchaina se te promjene zapisuju u obliku transakcije u blokove koji formiraju neprekidan lanac. Odatle dolazi i sam naziv tehnologije. Prije nego što se novi blok transakcija poveže u postojeći lanac blokova, on mora biti potvrđen od većine čvorova prema poznatim pravilima konsenzusa koji se koristi u toj implementaciji mreže. Nakon što je blok povezan, sve transakcije zabilježene ostaju zauvijek i šanse za maliciozne izmjene su vrlo malene. Više o mogućim napadima će biti opisano u nastavku jer se razlikuju za ovisno o implementaciji.
Bitcoin je najpoznatiji primjer primjene blockchaina u široj populaciji. Njegova mreža je aktivna od siječnja 2009. godine kada je Satoshi Nakamoto potvrdio prvi blok (engl. *genesis*). Još uvijek nije poznato tko je Satoshi Nakamoto i je li to uopće stvarna osoba ili naziv za grupu ljudi koji su sudjelovali u tazvoju bitcoina. Problem koji bitcoin pokušava riješiti je centraliziranost ekonomskog sustava i plaćanja. Svaka transkacija u trenutnom sustavu mora proći kroz centralno sjedište, odnosno banku. To znači da korisnici moraju vjerovati centralnom sjedištu da će provesti transakcije kako korisnik želi i da se neće ponašati maliciozno. Također, korisnici moraju vjerovati u sigurnost centralnog sjedišta i mogućnost zaštite od napada od treće strane.
Za takav način je potreban velik broj ljudi, novca i kontrole što dovodi dodatna ograničenja kao što su čekanje na potvrdu transakcije dulje vrijeme, nemogućnost obavljanja transakcija vikendom i praćenje toka novca.

Bitcoin te probleme rješava na način da izbacuje centralno sjedište i umjesto njega koristi *Proof of Work* pravila konsenzusa koja osiguravaju pouzdanost bez povjerenja. Nakon bitcoina su se pojavili mnogi *forkovi* s manjim ili većim promjenama, obično u veličini samih blokova ili brzini potrvrđivanja istih. Oni su obilježili prvu generaciju kriptovaluta.

2013. godine ruski programer Vitalik Buterin predlaže Ethereum, novu javnu platformu koja koristi dorađeno izdanje Nakamotovog *PoW* konsenzusnog algoritma. Posebnost Ethereuma jest da on nije samo raspodijeljena platforma za transakcije, već raspodijeljeni virtualni stroj (engl. *Ethereum Virtual Machine -EVM*) koji može izvoditi kod poznat pod nazivom pametni ugovor (engl. *smart contract*).

3. Proof of Authoroty algoritam

4. PoA mreža na raznovrsnom sklopovlju

Glavni zadatak ovog završnog rada bio je postaviti vlastitu mrežu koristeći Ethereum platformu na raznorodnom sklopovlju te provjeriti koliko su visoki zahtjevi jedne takve mreže na hardver. Osim same mreže, dodane su još neke osnovne funkcionalnosti kako bi se što ovi laboratorijski uvjeti što više približili pravom svijetu te nam ponudili kvalitetnije rezultate. Tako recimo imamo postavljen pretražitelj blokova (engl. *Block explorer*) koji u realnom vremenu prikazuje putem web aplikacije trenutni blok i transakcije koje su se provele u tom bloku. Moguće je i pretraživati starije blokove putem njega.
Osim pretražitelja blokova, dodana je i još jedna web aplikacija koja nudi podatke o opterećenosti pojedinog čvora u mreži što je korisno za ovaj završni rad jer jednostavno možemo usporediti opterećenost na raznorodnom sklopovlju.
Posljednja funkcionalnost jest zapravo podizanje (engl. *deployment*) najjednostavnijeg pametnog ugovora kako bismo zapravo mogli vidjeti samu komunikaciju između čvorova i izvođenje programskog koda.

4.1. Sklopovlje i programska podrška

Ono što čini ovaj sustav zanimljivim i pristupačnim širokoj populaciji je mogućnost sudjelovanja u distribuiranoj mreži s vrlo različitim sklopovljem. To znači da korisnici u većini slučajeva neće morati ulagati novac u novi hardver.
U ovom radu su korištena tri uređaja s ARM procesorima, jedno prijenosno računalo s Intel 64 bitnim procesorom i stolno računalo s AMD 64 bitnim procesorom.

4.1.1. Cubieboard2

Cubieboard2 jest jednostavno računalo (engl. *single-board computer*) kompanije Cubietech. Ovo računalo jest otvoreno što znači da su svi podaci o sklopovlju dostupni javno. Cubieboard2 je njihov drugi proizvod, izravni nasljednik originalnog Cubieboarda.

Pogoni ga Allwinner A20 čipset kojeg čini dvojezgreni Cortex-A7 procesor takta 1 GHz s Mali400 grafičkim sklopom. Na ploči je integrirana radna memorija DDR3 kapaciteta 1 GB na taktu 480 MHz i memorija za pohranu od 4 GB. Memorija za pohranu je proširiva microSD memorijskom karticom. Ne postoji ugrađen modul za bežičnu povezivost putem Wifi-a pa je korišten Ethernet ulaz propusnosti 10M/100M. Ovo računalo je moguće napajati putem USB micro sučelja ili DC 5V ulaza.

Obzirom da je Cortex-A7 ARM procesor postoje razne mogućnosti kad je u pitanju odabir operativni sustav. Tvornički dolazi Android da unutarnjoj memoriji od 4 GB što nije odgovaralo potrebama ovog rada pa je bilo potrebno pronaći odgovarajuću distribuciju Linux operativnog sustava.

Odličan izbor se pokazala distribucija armbian koja je ponudila minimalnu instalaciju operativnog sustava za ovo računalo baziranu na Debian Linuxu. Dolazi s ažurnom verzijom Linux kernela 5.4 što znači da sa strane programske podrške postoje dobri uvjeti.

Nakon instalacije operativnog sustava, ažurirani su svi paketi, postavljena je statična IP adresa kako bi se bilo moguće udaljeno povezati na računalo putem SSH protokola.

4.1.2. Raspberry Pi 1 model B

Raspberry Pi je najraširenije jednostavno računalo. Model 1B jest prva generacija iz 2012. godine koja po današnjim standardima donosi vrlo ograničene performance.

Ovo računalo je dizajnirano oko Broadcom BCM2835 sustava na čipu (engl. *SoC*) koji sadrži ARM1176JZF-S procesor na ARMv6 arhitekturi i radnom taktu od 700 MHz. Usko grlo jest 256 MB radne memorije od kojih je samo 192 MB dostupno procesoru a ostatak je rezerviran za obradu multimedijskog sadržaja. Ne postoji nikakva ugrađena memorija za pohranu nego sva pohrana ide na SD karicu. Kao i kod Cubieboard2 računala, niti ovdje ne postoji ugrađeni Wifi modul pa su mogućnosti svedene na Ethernet ulaz ili USB adapter za Wifi. Računalo se napaja putem USB micro sučelja.

Obzirom da je Raspberry Pi vrlo raširen, operativni sustav je vrlo lako dostupan i redovno održavan. Korišten je službeni Raspbian operativni sustav koji je baziran na Debian Linux distribuciji. Raspbian dolazi u dvije varijante, s grafičkim sučeljem i

bez njega (engl. *headless*). Za ovaj rad je primjerenije odabrati opciju bez grafičkog sučelja kako ne bismo trošili resurse nepotrebno na prikaz slike i razne dodatne procese koji su porenuti s grafičkim sučeljem.
Nakon instalacije Raspbiana, paketi su ažurirani i kao i kod Cubieboard2 računala, postavljena je statična IP adresa i upaljen SSH servis.
Već prilikom ovog postavljanja se vidi da je u odnosu na Cubieboard2 ovo računalo dosta nižih performanci.

4.1.3. Raspberry Pi 3 model B

Ovaj model je najranije izdanje treće generacije Raspberry Pi računala. Sklopovljem je mnogo bliži Cubieboard2 računalu nego svom predhodniku prve generacije.
Pogoni ga četverojezgreni Broadcom BCM2837 64 bitni procesor radnog takta 1,2 GHz. Baziran je na armhf arhitekturi. BCM2837 ima ugrađeni modul za bežičnu povezivost putem Wifi-a i Bluetooth-a. Na ploči je 1 GB radne memorije i kao i njegov prethodnik nema memoriju za pohranu na ploči nego za to koristi microSD karticu. Napaja se putem USB Micro sučelja.
Ponovno je odabir operativng sustava raznovrstan zbog raširene arhitekture procesora no većina korisnika koristi službeni Raspbian. Odabrana je opcija bez grafičkog sučelja te su provedeni koraci kao i za prethodna dva računala.
Postavljanje sustava i postavki je značajno brže nego na Raspberry Pi 1 modelu što je očekivano obzirom na sklopovlje.

4.1.4. Prijenosno i stolno računalo

Prijenosno računalo kao i stolno računalo je u raširenijoj uporabi u kućanstvima i upravo takvim sklopovljem se može najvjernije prikazati kako gotovo bilo tko može sudjelovati u jednoj distribuiranoj mreži na Ethereum platformi.
Sklopovlje na korištenim računalima u ovom radu ne spada među najmoderniji sloj trenutno dostupnog sklopovlja no i dalje je mnogo snažnije nego na single-board računalima.
Prijenosno računalo pogoni Intel Pentium četverojezgreni procesor N3530 čiji radni takt seže do maksimalnih 2,58 GHz. Ugrađeno je 8 GB radne memorije i za pohranu se koristi SSD kapaciteta 500 GB. Ovaj procesor je 64 bitne arhitekture. Kao i većina prijenosnih računala danas i ovo posjeduje ugrađenu mrežnu karticu koja nudi bežićnu povezivost.
Stolno računalo pogoni AMD Phenom II X4 925 procesor čiji je takt podignut na 3,4

GHz. Arhitekture procesora je 64 bitna. Također ima 8 GB radne memorije na taktu 800 MHz. Podaci se pohranjuju na SSD od 250 GB.
Računalo je povezano putem Ethernet sučelja na usmjeritelj (engl. *Router*).
Na prijenosnom računalu je instaliran Xubuntu 20 operativni sustav dok je na stolnom računalu instaliran Ubuntu 19.10. Oba operativna sustava su redovno ažurirana i imaju postavljene statične IP adrese.

5. Zaključak

Zaključak.

LITERATURA

Usporedba performanci Ethereum raspodijeljene knjige na raznorodnom sklopovlju

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Performance Comparison of the Ethereum Blockchain on Heterogeneous Hardware

Abstract

Abstract.

Keywords: Keywords.