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

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. 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.