**SVEUČILIŠTE U SPLITU**

**FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE**

**ZAVRŠNI RAD**

**DECENTRALIZIRANE APLIKACIJE   
NA ETHEREUM BLOCKCHAIN-U**

**Ivo Kovačević**

**Split, srpanj 2018**

SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

Preddiplomski studij: **Računarstvo**

Oznaka programa: 120

Ime i prezime: **Kovačević Ivo**

Broj indeksa: 185-2015

**PRIJAVA ZAVRŠNOG RADA**

Radni naslov: Decentralizirane aplikacije na Ethereum blockchain-u

Zadatak: Potrebno je osmisliti i izraditi decentraliziranu aplikaciju za glasovanje. Aplikaciju izraditi u programskom jeziku Solidity. Izraditi potrebno korisničko sučelje. Objasniti prednosti i mane decentraliziranih aplikacija te njihovu moguću primjenu.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mentor: izv. prof. dr. sc. Damir Sedlar

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Predsjednik Odbora: prof. dr. sc. Maja Štula

Split, 02.03.2018.

SADRŽAJ

[1 UVOD 1](#_Toc513743306)

[2 ŠTO SU DECENTRALIZIRANE APLIKACIJE? 2](#_Toc513743307)

[2.1 Mane centraliziranih sustava/aplikacija 2](#_Toc513743308)

[2.2 Prednosti decentraliziranih sustava/aplikacija 3](#_Toc513743309)

[3 „BLOCKCHAIN“ – LANAC BLOKOVA 4](#_Toc513743310)

[3.1 Blok 4](#_Toc513743311)

[3.1.1 Podaci 4](#_Toc513743312)

[3.1.2 Ključ bloka 5](#_Toc513743313)

[3.1.3 Ključ prethodnog bloka 6](#_Toc513743314)

[3.1.4 Nastanak bloka i dodavanje na kraj lanca 6](#_Toc513743315)

[3.2 Karakteristike lanca blokova 6](#_Toc513743316)

[3.2.1 Distribuiranost 6](#_Toc513743317)

[3.2.2 Decentraliziranost 6](#_Toc513743318)

# UVOD

Korištenjem centraliziranih aplikacija nailazi se na razne probleme kao što su skalabilnost, sigurnost, preopterećenje centralnog sustava, pad centralnog sustava znači pad kompletne aplikacije.

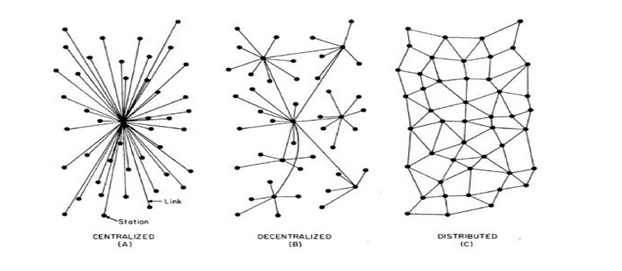
Sve ove probleme rješavaju nove decentralizirane aplikacije. One su pohranjene na puno čvorova te ukoliko jedan čvor prestane s radom, to neće utjecati na rad aplikacije. Sigurnost je također puno veća upravo zbog toga što jednom napisanu aplikaciju više nitko ne može modificirati pa čak ni sam autor aplikacije. To znači da se mogu programirati vrlo povjerljive aplikacije koje će onemogućiti prevaru jer se jednom napisani i dogovoreni kod više ne može mijenjati.

# ŠTO SU DECENTRALIZIRANE APLIKACIJE?

Danas najpoznatije i najrasprostranjenije aplikacije su centralizirane aplikacije. Postoji jedan centralni čvor o kojem ovisi rad kompletnog sustava. Centralni čvor upravlja svim drugim čvorovima te svi ostali čvorovi zavise o centralnom čvoru.

Kod distribuiranih sustava više čvorova rade zajedno kako bi ostvarili neku zadaću. Dakle nema centralnog čvora koji obavlja svu zadaću, nego je posao podijeljen na više čvorova.

U decentraliziranim sustavima posao se obavlja na svim čvorovima te je svaki čvor neovisan o drugim čvorovima. Prestanak rada jednog čvora ne znači i pad cijelog sustava.



Slika ‑ Razlika između centraliziranih, decentraliziranih i distribuiranih sustava

## Mane centraliziranih sustava/aplikacija

Glavna mana centraliziranih sustava je što rad sustava ovisi o jednom jedinom čvoru. Prestanak rada jednog centralnog čvora rezultira padom kompletnog sustava. To može biti veoma loše ukoliko se radi o aplikacijama kod kojih i sekunda prestanka rada znači ogromne materijalne gubitke.

Budući da o jednom čvoru ovisi rada cijelog sustava, preko toga čvora idu svi zahtjevi te se sav posao obavlja na tom čvoru. To znači da centralni čvor mora biti veoma moćno računalo koje će moći obaviti tako zahtjevan posao pouzdano, bez zastoja i grešaka. Ovakva organizacija sustava je izvediva kod jednostavnih i srednje složenih sustava. Kod složenih sustava poput Facebook-a, Google-a, Amazona itd. ovakva arhitektura ne bi donijela željene rezultate, stoga se ti sustavi distribuiraju.

Druga velika mana ovakvih sustava je ta što jedna korporacija (npr. Facebook) kontrolira ogromnu količinu podataka. Prilikom registracije na Facebook u zamjenu za besplatan servis, dijele se podaci korisnika. Korisnik nema uvid što se sve radi s tim podacima što otvara mogućnosti zlouporabe tih podataka.

Uzmimo za primjer Uber. Interni sustav Uber-a omogućuje praćenje svih vožnji u trenutnom vremenu na nekom području. Na temelju tih podataka može se zaključiti npr. tko će prenoćiti negdje samo jednu noć i ostale veoma povjerljive informacije.

Korisnici ukoliko žele podijeliti neke podatke na Internet moraju platiti određenoj „host“ organizaciji. Dakle, korisnici plaćaju dijeljenje vlastitih podataka raznim „host“ kompanijama.

Treća mana je što se ovakav sustav kontrolira od jedne strane.

## Prednosti decentraliziranih sustava/aplikacija

Nešto…

# „BLOCKCHAIN“ – LANAC BLOKOVA

„Blockchain“ nije ništa drugo nego lanac blokova koji sadrže informacije. Blokovi su povezani tako da svaki blok sadrži vlastiti ključ te ključ prethodnog bloka (Slika 3‑1).

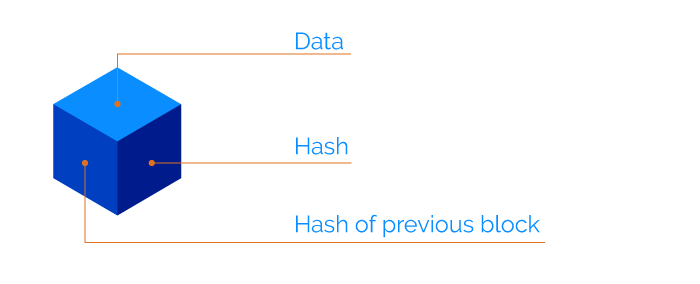


Slika ‑ Primjer lanca blokova

Lanac blokova možemo zamisliti kao već dobro poznate liste. Svaki član liste sadrži pokazivač na sljedećeg člana liste i neke podatke.

## Blok

Svaki blok unutar lanca se sastoji od podataka (engl. Data), vlastitog ključa (engl. Hash) te ključa prethodnog bloka (engl. Hash of previous block) kao što je prikazano na slici (Slika 3‑2).



Slika ‑ od čega se sve sastoji bok

### Podaci

Polje podaci mogu sadržavati proizvoljne podatke i ovise o vrsti lanca blokova. Npr. kod BitCoina polje podaci sadrži informacije o transakciji:

* Od koga? (engl. From) – označava pošiljatelja koji šalje određeni iznos.
* Kome? (engl. To) – označava primatelja koji prima taj isti iznos.
* Koliko? (engl. Amount) – odnosi se na iznos koji se šalje (npr. pošiljatelj šalje 2 BTC primatelju).

Kod Ethereum lanca moguće je u polje podaci pohranjivati i nešto što se zove pametni ugovor (engl. Smart contract). Upravo na tim pametnim ugovorima se temelje decentralizirane aplikacije koje su tema ovog rada. Pametni ugovori će detaljnije biti objašnjeni u poglavlju NAVEST BROJ POGLAVLJA!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.

### Ključ bloka

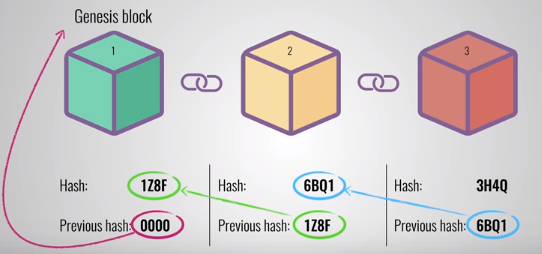
Ključ bloka (engl. Hash) se može zamisliti kao otisak prsta koji jedinstveno određuje svaki blok. Dakle, ne postoje dva bloka s istim ključem. Ključ se generira na osnovu funkcije koja uzima određene parametre vezane za taj blok te vraća jedinstveni ključ koji se potom dodjeljuje tom bloku.

f (razni parametri) 🡪 jedinstveni ključ.

Parametri ovisno o vrsti lanca mogu biti:

* Podaci bloka
* Ključ prethodnog bloka
* Trenutno vrijeme u sekundama (engl. Timestamp)
* Broj koji je potrebno pogoditi da ključ započinje određenim brojem nula (engl. Nonce)

### Ključ prethodnog bloka



Slika ‑ Povezanost blokova na osnovu ključa

### Nastanak bloka i dodavanje na kraj lanca

## Karakteristike lanca blokova

### Distribuiranost

### Decentraliziranost