# Kako i zašto funkcioniše blockchain?

Seminarski rad u okviru kursa
Tehničko i naučno pisanje
Matematički fakultet

Lazić, Jovana
kontakt email adresa autora

Nikić, Ognjen
kontakt email adresa autora

Nešković, Ognjen
mi22009@alas.matf.bg.ac.rs

Sekešan, Pavle
kontakt email adresa autora

7. novembar 2022.

**Sažetak**

U radu su sažeto iznete osnove kriptografije potrebne za razumevanje i implementaciju blokčejna. Ukratko je predstavljena istorija blokčejna, kao i glavne ideje potrebne za realizaciju blokčejna koji se nalazi iza jedne od najpoznatijih kriptovaluta - Bitcoin. Dopuniti kasnije...

## Sadržaj

**1 Uvod** **2**

**2 Kriptografske osnove** **2**
2.1 Kriptografske heš funkcije . . . . . 2
2.2 Asimetrična kriptografija . . . . . 2

**3 Blokčejn** **2**
3.1 Blokovi . . . . . 3
3.2 Decentralizacija . . . . . 3

**4 Primene** **3**
4.1 Kriptovalute . . . . . 3
4.2 Pametni ugovori . . . . . 3

**5 Zaključak** **3**

**Literatura** **3**

# 1 Uvod

Napisati uvod - ukratko nešto o istoriji blokčejna, čemu služi, zašto je koristan, pomenuti osnovne ideje koje se koriste (heširanje, merkle stabla, asimetrična kriptografija (digitalni potpisi) itd.)

# 2 Kriptografske osnove

## 2.1 Kriptografske heš funkcije

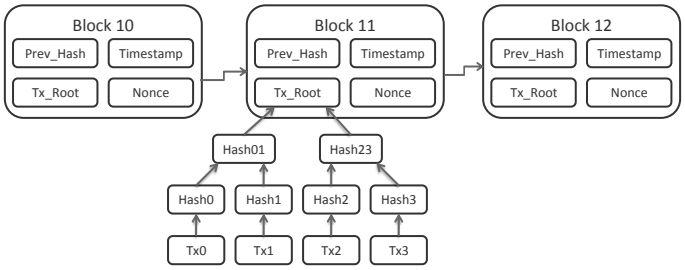
Napisati ovaj subsection

## 2.2 Asimetrična kriptografija

Napisati ovaj subsection

# 3 Blokčejn

Blokčejn je decentralizovan, distribuiran i najčešće javan skup podataka (najčešće transakcija ili drugih zapisa) [2] sačinjen od manjih jedinica podataka - "blokova". Blokovi su takvi da se dati blok ne može izmeniti bez promene svih blokova koji dolaze nakon njega. Ovim blokovi uspostavljaju "istoriju", odnosno sekvencu izmena na javnom skupu podataka.




Slika 1: Bitcoin blokčejn

Na primer u slučaju Bitcoin blokčejna (slika 1) blokovi sadrže, pored ostalog, heš prethodnog bloka i transakcije (preciznije merkle stablo izgrađeno nad transakcijama). Time što jedan blok sadrži heš bloka koji je kreiran pre njega je uspostavljen redosled blokova, pa i time redosled transakcija. Neke izmene nad skupom podataka moraju biti odobrene od strane pojedinca kome podaci pripadaju (na primer u slučaju transakcija) što se postiže metodama asimetrične kriptografije. Svi učesnici u distribuiranoj mreži mogu lako verifikovati da li su izmene u blokčejnu validne i složiti se sa izmenama ili glasati protiv njih. Kako bi se došlo do konsenzusa oko toga koja sekvenca izmena na blokčejnu je validna uvode se metode poput dokaza o izvršenom radu (proof of work), dokaza o posedovanju valute (proof of stake) itd. Metode za postizanje konsenzusa se biraju tako da se postigne veliki stepen otpornosti prema ne-kooperativnim agentima u distribuiranoj mreži. Zajedno sa javno dostupnim blokčejnom ovaj

sistem rešava jedan od značajnih problema digitalnih dobara poznat kao ”double spending”. [1]

### 3.1 Blokovi

Napisati ovaj subsection - apstraktnije opisati pojam bloka u blokčejnu generalno (ne samo kod bitkojna), način za postizanje konsenzusa (proof of work, proof of stake,...), forkovi

### 3.2 Decentralizacija

Napisati ovaj subsection - opisati kako blokčejn koristi peer to peer mrežu, sa konkretnim primerom (na primer kako bitkojn radi broadcast ili šta već), prednosti i mane decentralizacije generalno - double spending ako neko ima preko 51%, itd.

## 4 Primene

### 4.1 Kriptovalute

Napisati ovaj subsection

### 4.2 Pametni ugovori

Napisati ovaj subsection - pomenuti eth pošto btc nije turing complete

## 5 Zaključak

Napisati ovaj subsection

## Literatura


[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[2] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–2, 2014.