# Fakultet tehničkih nauka

**Elementi razvoja softvera**



Dokumentacija

Blockchain

Nikola InđićPR149/2020 Veljko AleksićPR93/2020

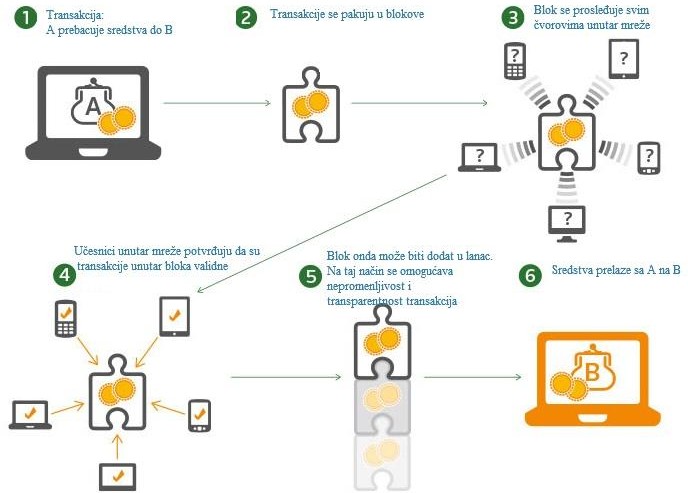
Milica NuždićPR149/2020 Marijana KolarovPR158/2020

# Blockchain – OPIS

Blockchain se sastoji od blokova koji su nanizani, odnosno povezani u lanac gde svaki od blokova ima niz zapisa. Blokovi se povezuju algoritmom koji koristi hash funkciju. Vezu između blokova je vrlo teško hakovati, jer je to ujedno algoritam koji koristi kriptografiju visokog nivoa .

Svaki blok u lancu ima konačnu količinu podataka ili transakcija koju može napajati. U trenutku kada se blok popuni, kreira se novi koji će biti povezan s blokom koji mu prethodi i s onim koji će tek biti kreiran u budućnosti.

# DIJAGRAM



# STRUKTURA BLOCKCHAIN-A

## Struktura bloka

Kako i samo ime govori, blockchain se sastoji od niza blokova koji su lančano povezani. Blok je struktura podataka koja sadrži informacije. U samom zaglavlju bloka susrećemo se s tehničkim informacijama o njemu samom i sa svim informacijama vezanim uz povezivanje s drugim blokovima koji su takođe deo blockchaina. Hash prethodnog bloka je konačni izlazni rezultat nakon dvostruke primjene hash funkcije SHA- 256. Napomenimo kako hash samog bloka nije deo strukture bloka, on se uobičajno računa samo kada ima potrebe za takvom akcijom.

## Povezivanje blokova

Zaglavlje bloka sadrži tehničke informacije, i ima referencu na prethodni blok. Ti podaci su vrlo bitni za svaki blok u lancu tj.treba znati gdje pripada i u kom redosledu. Kada bi došlo do narušavanja tog redosleda, naprimer usled nekog pokušaja napada na blockchain, vrlo lako bi pomoću referenci na prethodni blok vratili na prvobitno stanje. Korišćenjem hash funkcije dobijamo i validaciju podataka. Svaki korisnik koji ima pristup podacima nekog bloka ili barem samo zaglavlju tog pojedinog bloka koristeći kriptografske funkcije, u mogućnosti je odrediti hash tog bloka. Blok koji nastaje kasnije u lancu, sadrži u sebi hash bloka koji je nastao neposredno pre njega. Ukoliko bi neko pokušao napraviti izmenu u podacima odredjenog bloka, morao bi menjati sve hasheve od tog trenutka nadalje.

## Hash funkcije

Argument hash funkcija su podaci proizvoljne dužine, ali rezultat je fiksne. Cela blockchain tehnologija je zasnovana na iskorišćavanju svojstva hash-eva. Hash nekog bloka je vrlo lako izračunati ali je vrlo teško, odnosno nije moguće otkriti koji se podaci kriju u pozadini izračunatog hasha. Dovoljno je da nekoj ulaznoj informaciji ili rečenici izmjeniti samo jedno slovo, hash te informacije će u potpunosti izgledati drugačije.

## Rudar (Miner)

Funkcija rudara je ta da prihvata nove validirane nove podatke u lancu, kreira blokove od tih zapisa i smešta ih u blockchain. Novi blokovi se dodaju u blockchain pomoću rešavanja algoritma, kada se transakcije validiraju rudar koji je obavio taj posao i utrošio svoje resurse na izvršavanje iste, nagradjuje se odredjenim delom bitcoina.

# NAČIN FUNKCIONISANJA BLOCKCHAIN-A

1. Želja da se izvršiti transakcija sa tačke A na tačku B - transakcije se ne moraju odnositi samo na kripto valute, može se raditi o dokumentima, tablicama, slikama, odnosno o bilo kojim informacijama u digitalnom obliku.

2. Transakcija generiše blok – blok je potrebno validirati.

3. Blok se šalje svima na mreži – transakcija je vidljiva svima.

4. Transakcija se verificira unutar mreže - verifikacijom se proverava imaju li strane koje vrše transakciju. Verifikacija može biti izvršena odmah, ali i ne mora.

5. Blok se dodaje u „public leadger“ - time se stvara trajan zapis transakcije i ti se podaci više ne mogu menjati.

6. Transakcija prema tački B je izvršena – željena transakcija je izvršena.

Blockchain je baza podataka koja se ne nalazi na jednom mestu, već je čine manje baze (blokovi) koje su međusobno digitalno povezani, a koji sadrže informacije o digitalnim transakcijama bilo koje vrste. Prilikom njihove razmene nema nikakvog regulatora osim same mreže koja sadrži informacije o svim transakcijama koje su ikada izvedene. Kada se razmena izvrši, ona se sa drugim podacima i informacijama koje se prenose kriptografski povezuje sa blokom. Tada na scenu stupa proces “izvlačenja ruda” tj. minig koji se obavlja pomoću računara velike snage – izvlačeći postojeću “rudu” i stvarajući nove blokove. Svakoj obavljenoj trasakciji pripisuje se vremenska odrednica, dok se sama transakcija po hronološkom redu dodaje već postojećem lancu blokova i sa njim se povezuje uz pomoć čvora.

# BITCOIN

Bitcoin je danas jedna od najpopularnijih kripto valuta. Prva transakcija, odnosno plaćanje dogodilo se 2010. godine kada su dve pizze plaćene sa 10.000 jedinica bitcoina. Bitcoin ima unapred ograničen broj jedinica koje mogu biti izdane, kao i sve ostale kripto valute. Kod bitcoin-a se radi o 21 milijun jedinica. Do danas je izdano oko 17,5 miliona jedinica, a ostalih 3,5 miliona će se izdati u narednih 20-ak godina. Ovaj vremenski rok se može promeniti. S vremenom rudarenje postaje sve teže jer je verifikacija blokova sve komplikovanija. Ali treba uzeti u obzir napredak tehnologije pa postoji mogućnost da će preostale jedinice biti izdane i pre.