**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](#_Toc514255644)

[2 ŠTO SU DECENTRALIZIRANE APLIKACIJE? 2](#_Toc514255645)

[2.1 Mane centraliziranih sustava/aplikacija 2](#_Toc514255646)

[2.2 Prednosti decentraliziranih sustava/aplikacija 3](#_Toc514255647)

[3 „BLOCKCHAIN“ – LANAC BLOKOVA 4](#_Toc514255648)

[3.1 Blok 4](#_Toc514255649)

[3.1.1 Podaci 4](#_Toc514255650)

[3.1.2 Identifikator bloka 5](#_Toc514255651)

[3.1.3 Identifikator prethodnog bloka 6](#_Toc514255652)

[3.2 Karakteristike i mehanizmi lanca blokova 8](#_Toc514255653)

[3.2.1 Dokaz o radu (engl. Proof of work) 8](#_Toc514255654)

[3.2.2 Distribuiranost 9](#_Toc514255655)

[3.2.3 Decentraliziranost 10](#_Toc514255656)

[3.3 Kako ustvari radi lanac blokova? 11](#_Toc514255657)

[4 DECENTRALIZIRANE APLIKACIJE 18](#_Toc514255658)

# UVOD

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

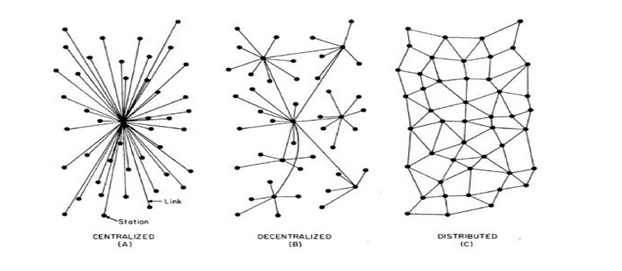
Sve ove probleme rješavaju nove decentralizirane aplikacije. One su pohranjene na puno čvorova te ukoliko jedan čvor prestane s radom, to neće utjecati na rad aplikacije. Sigurnost je također puno veća upravo zbog toga što jednom napisanu aplikaciju više nitko ne može modificirati pa čak ni sam autor 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 rad 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 identifikator te identifikator prethodnog bloka (Slika 3‑1).

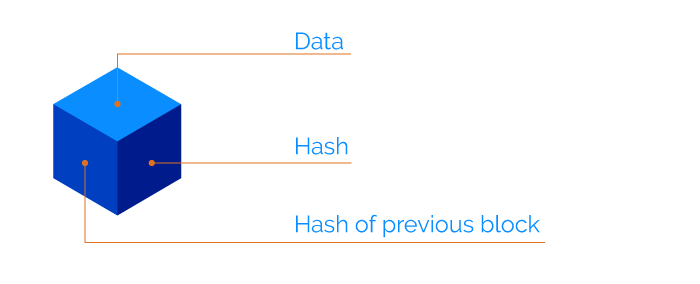


Slika ‑ Primjer lanca blokova

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 identifikatora (engl. Hash) te identifikatora 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!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.

### Identifikator bloka

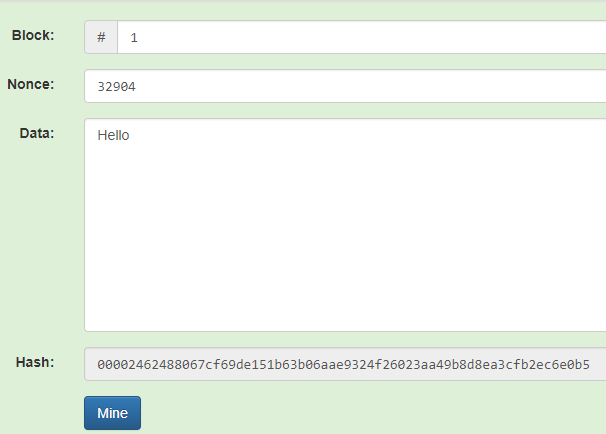
Identifikator bloka (engl. Hash) se može zamisliti kao otisak prsta koji jedinstveno određuje svaki blok. Dakle, ne postoje dva bloka s istim identifikatorom. Identifikator se generira na osnovu funkcije koja uzima određene parametre vezane za taj blok te vraća jedinstveni identifikator koji se potom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

f (razni parametri) 🡪 jedinstveni identifikator.

Parametri ovisno o vrsti lanca mogu biti:

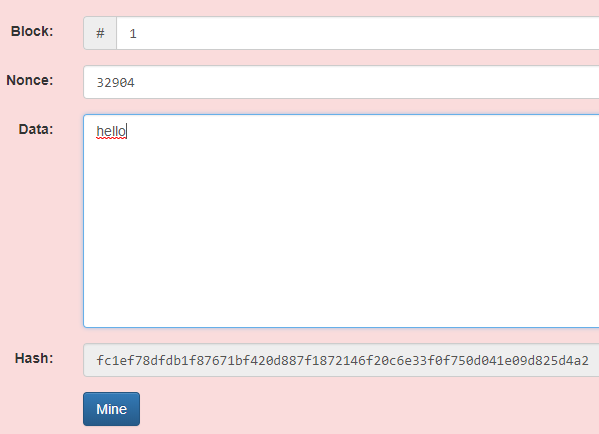
* Podaci bloka
* Identifikator prethodnog bloka
* Trenutno vrijeme u sekundama (engl. Timestamp)
* Broj koji je potrebno pogoditi da identifikator započinje određenim brojem nula (engl. Nonce)

Na slici (Slika 3‑3) vidimo jednostavan primjer određivanja identifikatora bloka na osnovu rednog broja bloka, broja koji je potrebno pogoditi da bi identifikator započinjao s određenim brojem nula (engl. Nonce) i podatka kojeg unosima (engl. Data).



Slika ‑ Određivanje identifikatora bloka na osnovu podataka u bloku

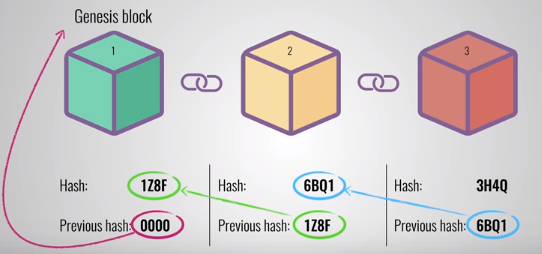
Ukoliko samo malo promijenimo neki od podataka na osnovu kojih se generira identifikator (engl. Hash), identifikator će se skroz promijeniti te on više neće biti ispravan (Slika 3‑4). Sada je potrebno opet pogoditi identifikator da počinje s određenim brojem nula. Ovaj mehanizam se naziva dokaz o radu (engl. Proof of work).



Slika ‑ Identifikator bloka se promijenio prilikom promjene podatka unutar bloka

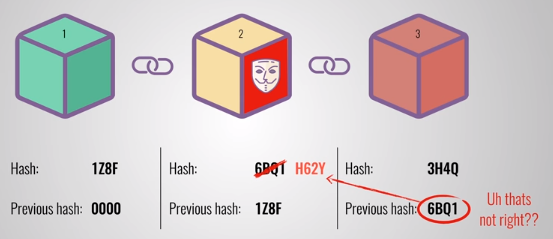
### Identifikator prethodnog bloka

Svaki blok (osim prvog bloka u lancu) sadrži identifikator (engl. Hash) prethodnog bloka (Slika 3‑5). Na taj se način blokovi povezuju u lanac blokova (engl. Blockchain).



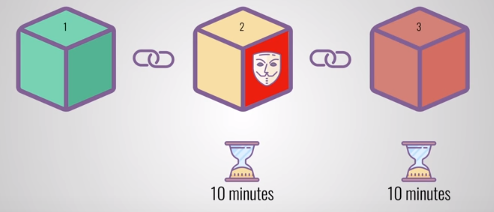
Slika ‑ Primjer povezanosti blokova

Ukoliko se promjeni bilo koji podatak unutar bloka, promijenit će se i identifikator bloka. Posljedica toga bit će puknuće lanca blokova jer slijedeći blok više ne sadrži ispravan identifikator prethodnog bloka (Slika 3‑6). Na slici vidimo da blok 3 više ne sadrži ispravan identifikator bloka 2 jer se bloku 2 promijenio identifikator zbog mijenjanja nekih podataka unutar bloka tj. došlo je do pucanja lanca.



Slika ‑Primjer puknuća lanca blokova

Da bi se riješio ovaj problem i skup blokova opet povezao u neprekidni lanac potrebno je ponovno proračunati identifikator svakog bloka počevši od mijenjanog pa nadalje. Moderna računala mogu proračunati oko 100 000 identifikatora po sekundi (engl. Hash). Da bi se usporilo nastajanje novih blokova, postoji nešto što se zove dokaz o radu (engl. Proof of work) što će biti detaljnije objašnjeno u poglavlju 3.2.1. Kod BitCoina je potrebno oko 10 minuta za stvoriti novi blok (Slika 3‑7).



Slika ‑Vrijeme potrebno za nastanak novog bloka

## Karakteristike i mehanizmi lanca blokova

### Dokaz o radu (engl. Proof of work)

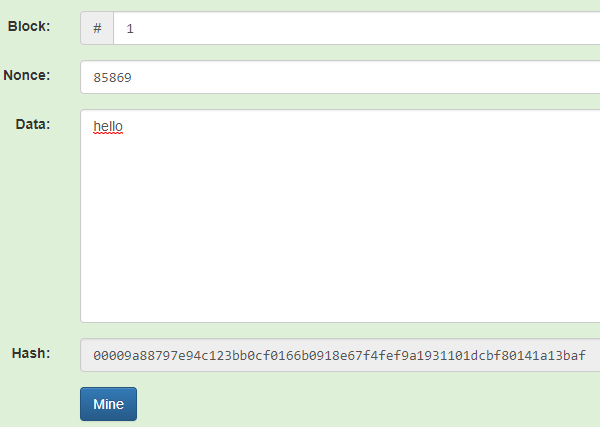
Dokaz o radu je mehanizam koji usporava nastanak novih blokova. Razlog tome je sprječavanje raznih napada na mrežu kao što su spamanje, lažne transakcije, mijenjanje sadržaja pojedinog bloka itd. što se postiže zahtijevanjem određene količine računalnog posla koje uzima određeno vrijeme.

Uzmimo za primjer da imamo blok koji sadrži transakciju gdje osoba X šalje osobi Y 20 kuna. Da ne postoji dokaz o radu, osoba Y bi mogla promijeniti iznos u bloku tako da umjesto 20 kuna napiše 200 kuna jer bi tada vrlo brzo mogla ponovno proračunati identifikator (engl. Hash) toga bloka i svih slijedećih blokova te bi lanac bio konzistentan. Upravo zbog toga što postoji dokaz o radu, ovakva mijenjanja sadržaja bloka su onemogućena jer bi trebala enormna količina računale snage da ponovno proračuna identifikator tolike količine blokova.

Dokaz o radu nam daje određena pravila i ograničenja pri određivanju identifikatora bloka. Identifikator bloka je ispravan jedino i samo ako počinje s određenim brojem nula. Broj nula s kojim identifikator mora započinjati se mijenja s vremenom kako bi se postiglo da za stvaranje svakog bloka treba otprilike 10 minuta (kod BitCoin-a).

Na slici (Slika 3‑8) prikazan je pronalazak ispravnog identifikatora bloka što rješava problem iz poglavlja 3.1.2 (Slika 3‑4). Vidimo da identifikator započinje s određenim brojem nula (u primjeru radi jednostavnosti uzeto je da je taj broj 4) te se identifikator smatra ispravnim.

Možemo uočiti i da se promijenilo polje „Nonce“. Taj je broj trebalo pogoditi da dobijemo identifikator sa slike koji počinje s 4 nule.

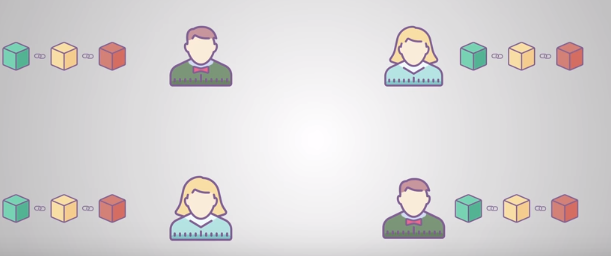


Slika ‑ Pronalazak ispravnog identifikator bloka nakon mijenjanja podataka u bloku

### Distribuiranost

Lanci blokova imaju svojstvo distribuiranosti tj. svima je omogućeno sudjelovanje koristeći P2P mrežu.

Upravo svojstvom distribuiranosti postiže se još jedan nivo sigurnosti ovakvog sustava. Razlog je u tome što svaki sudionik na mreži može nadgledati transakcije. Svi sudionici na mreži imaju vlastitu kopiju lanca blokova (Slika 3‑9).

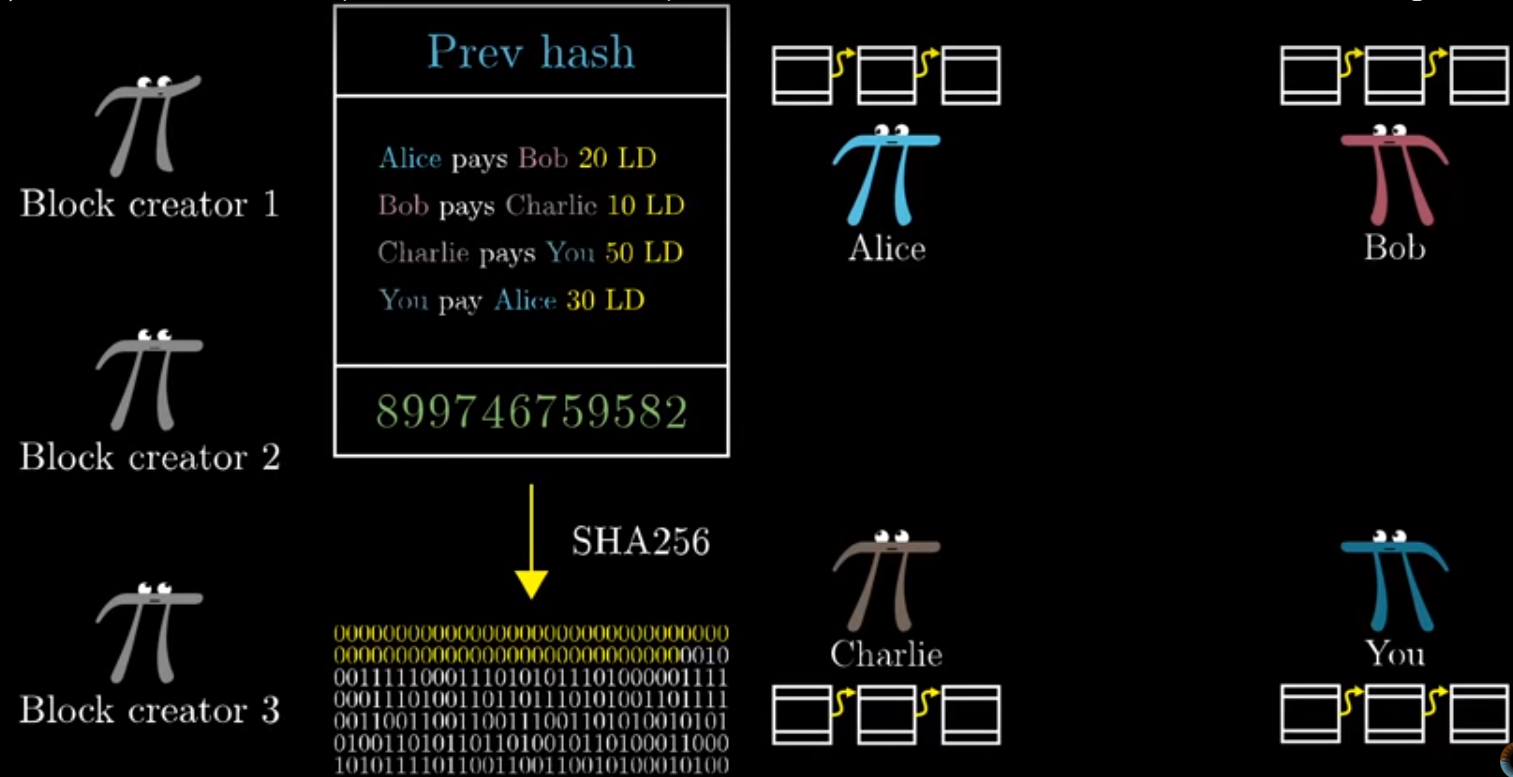


Slika ‑ Svaki sudionik na mreži ima vlastitu kopiju lanca blokova

Ukoliko neki od sudionika pokuša prevariti ostale npr. promjenom neke od transakcija želi dobiti veći iznos, svi ostali sudionici na mreži će vidjeti da se njihov lanac blokova razlikuje od lanca blokova zlonamjernog sudionika te će znati kako je ta njegova namjera zlonamjerna te će biti nevažeća. Da bi se zlonamjernom sudioniku ostvarila njegova namjera on mora imati više od 50% računalne snage kako bi imao većinu u tom distribuiranom svijetu sudionika. Iako vrlo lako moguće zvuči činjenica da neki sudionik ima više od 50% računalne snage (vlade, vojska itd.) u stvarnom svijetu je gotovo nemoguća. Upravo na tome se temelji velika sigurnost ovakvog sustava.

Distribuiranost se može promatrati iz dva pogleda. Prvi je već navedeni da je svima omogućeno sudjelovanje i nadgledanje transakcije i novih blokova, a drugi se odnosi na rudare (engl. Miner).

Na mreži se osluškuju transakcije te kada se nakupi određen broj transakcija one se spreme u jedan blok. Dakle, svaka transakcija se ne sprema u vlastiti blok, nego se više transakcija spremi u jedan blok što značajno ubrzava proces transakcija na mreži. Potom rudari, koji osluškuju te transakcije nastoje pogoditi ispravni identifikator (engl. Hash) bloka. Svi rudari koji sudjeluju u pogađanju ispravnog identifikatora se međusobno natječu te je pobjednik onaj koji prvi pogodi ispravni identifikator tako da on započinje s odgovarajućim brojem nula kao što je već objašnjeno u poglavlju 3.2.1. Rudar koji je pogodio ispravni identifikator potom dobiva određenu nagradu za svoj rad. Taj se uspješno napravljeni blok potom emitira na mrežu. Svi sudionici koji sudjeluju na mreži taj blok dodaju na kraj svog lanca (Slika 3‑10).



Slika ‑ Rudari (engl. Block creator/Miner) te sudionici (Alice, Bob, Charlie, You)

### Decentraliziranost

Decentraliziranost ovakvog sustava proizlazi iz toga što svaki sudionik na mreži posjeduje kopiju lanca blokova. Ukoliko jedan od čvorova prestane s radom to ne predstavlja nikakav problem za normalno funkcioniranje sustava zbog toga što svi ostali sudionici na mreži imaju taj isti lanac blokova.

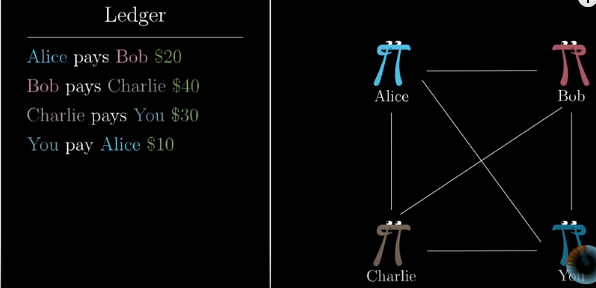
Dakle, u decentraliziranom sustavu svi čvorovi sustava imaju iste podatke i rade isti posao te nestanak jednog čvora nema nikakve posljedice na rad sustava.

## Kako ustvari radi lanac blokova?

U prethodnim poglavljima objašnjeni su razni pojmovi decentralizirane mreže. Svi ti pojmovi mogu izazvati pomutnju budući da se radi o sasvim novoj tehnologiji i načinu razmišljanja.

Stoga će se u ovom poglavlju na konkretnom primjeru BitCoin-a pokazati kako ustvari radi lanac blokova (engl. Blockchain).

Za početak uzmimo da imamo jednu knjigu u kojoj pišemo sve transakcije koje se događaju na mreži.

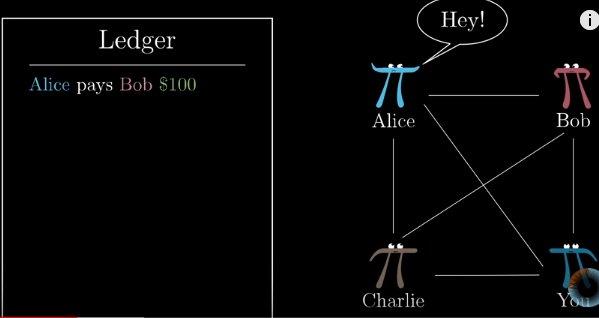


Slika ‑ Primjer javne knjige transakcija

Neka imamo vrlo jednostavan protokol koji se sastoji od pravila:

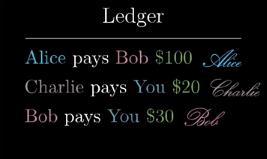
* Svatko može dodati transakciju u javnu knjigu
* Ne smije se uplatiti više nego što se posjeduje

Što sprječava nekoga da doda transakciju koja ide u njegovu korist bez da druga strana to odobri? Npr. Bob stavi da mu Alice treba platiti 100$ bez da Alice to odobri.



Slika ‑ Bob dodaje transakciju bez odobrenja Alice

Problem se riješi uz malo kriptografije tj. digitalnog potpisa.



Slika ‑ Dodavanje potpisa kako bi se odobrile transakcije

Ideja se sastoji od toga da postoji nešto što sudionici mogu dodati pored transakcije, označavajući kako su vidjeli i odobrili transakciju.

Što nas sprječava da kopiramo nečiji potpis?

Ključ je u tome što se potpis (engl. Signature) generira na osnovu privatnog ključa (engl. Private key) i ostalog sadržaja bloka. Dakle samo osoba s privatnim ključem može generirati ispravan potpis.

Svaki sudionik na mreži posjeduje vlastiti par privatnog/javnog ključa. Javni ključ se podijeli sa svim sudionicima na mreži, dok se privatni ključ ne govori nikome i strogo je povjerljiv. Na osnovu javnog ključa (engl. Public key) drugi sudionici znaju od koga dolaze transakcije te na koju adresu uputiti transakciju.

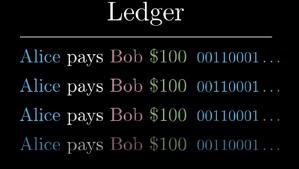
Generiranje ključa možemo zamisliti kao funkciju koja kao parametre prima neke podatke te privatni ključ a vraća jedinstveni potpis. Upravo zbog toga što podatke bloka uzima kao parametar rješava problem da se neki potpis kopira na drugu poruku.

Kako bi se provjerila ispravnost potpisa koristi se funkcija koja za parametre uzima podatke bloka, potpis i javni ključ te kao rezultat vraća točno/netočno (engl. True/false) ovisno o tome je li potpis ispravan ili netočan.

Potpis se sastoji od 256 bitova, što znači da će biti gotovo nemoguće pogoditi nečiji potpis „na sreću“ bez da se posjeduje privatni ključ. S 256 bitova moguće je napraviti 2256 kombinacija, a to je nezamislivo velik broj (od 78 znamenki). Zaključujemo da je gotovo nemoguće pogoditi taj broj.

Zaključak je: samo osoba koja ima privatni ključ može generirati taj potpis.

Što sprječava nekog da nakon prve potvrde samo kopira tu transakciju n puta budući da poznaje potpis koji je odobrio tu transakciju (Slika 3‑14)?



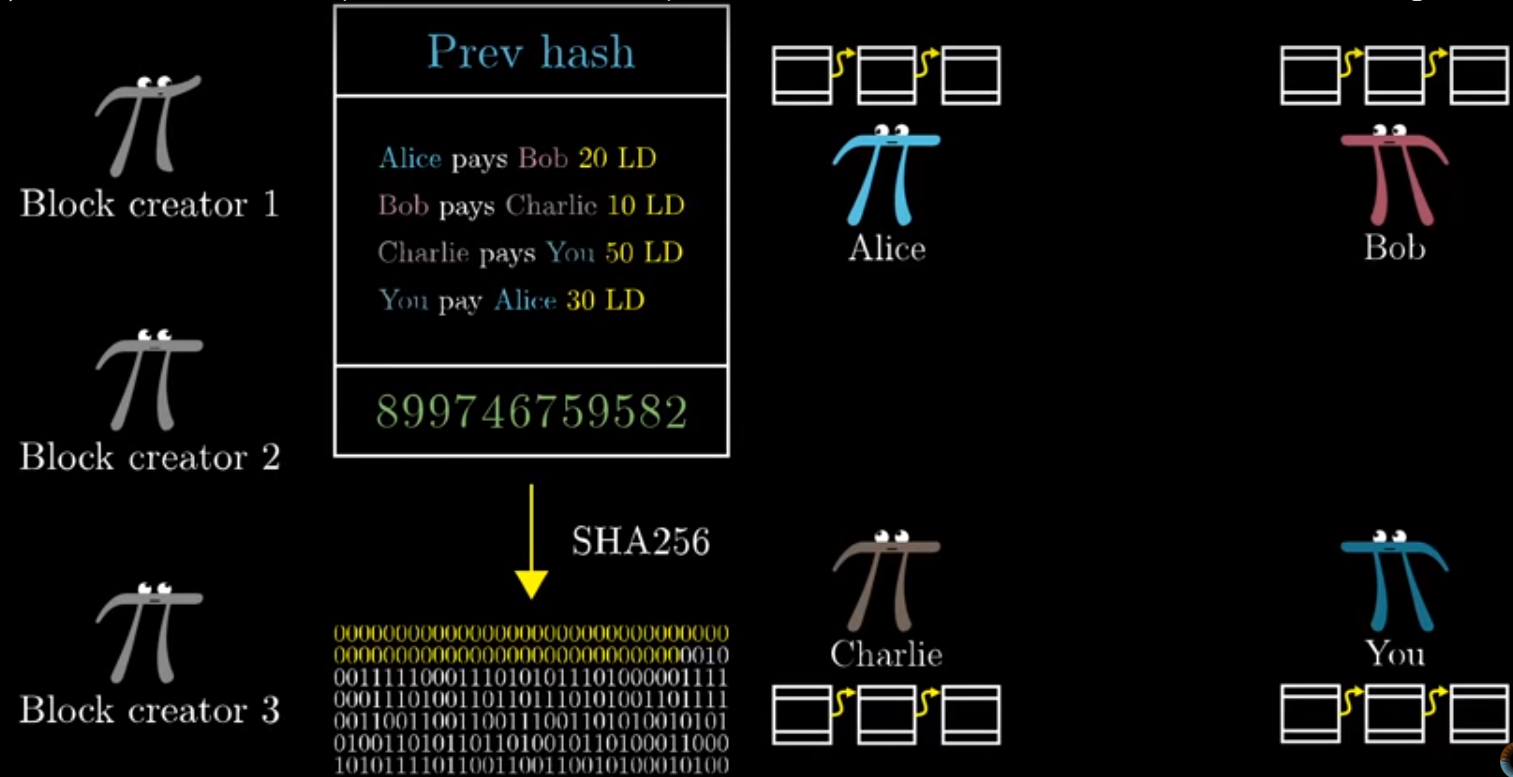
Slika ‑ Kopiranje transakcije n puta nakon što se potpiše kao ispravna

Trik je u tome što svaka transakcija nosi svoj ID što znači da signature nikad neće biti isti.

Slijedeći pojam je decentraliziranost. Svaki sudionik ima svoju kopiju javne knjige. Kada neki sudionik želi napraviti transakciju, transakcija se emitira svim ostalim sudionicima na mreži koji tu čuju i upišu u svoju javnu knjigu. Ukoliko se ne učini nešto više ovo je veoma loš sistem. Kako biti siguran da se svi slažu koja je javna knjiga ispravna? Kako biti siguran da svi ostali sudionici slušaju transakcije koje dolaze? Npr. netko vam uplati 20 kuna i kako biti siguran da su svi ostali sudionici „čuli“ da vam je poslano 20 kuna te da će te tih 20 kuna moći koristiti i njima raspolagati?

Problem je riješen tako da se vjeruje onoj „javnoj knjizi“ na koju je potrošeno najviše računalnog rada (engl. Computation work). Dakle, računalni rad predstavlja mjeru kome vjerovati. Vjeruje se uvijek onom zapisu koji ima najviše računalnog rada – dokaz o radu (engl. Proof of work).

Dakle, slušaju se sve transakcije koje se potm stavljaju u blok te se traži valjani identifikator za taj blok. Identifikator bloka da bi bio prihvatljiv mora započinjati s određenim brojem nula. Nakon što se nađe identifikator, taj se blok šalje svim sudionicima na mreži da ga dodaju na kraj svoje kopije lanca blokova (engl. Blockchain).



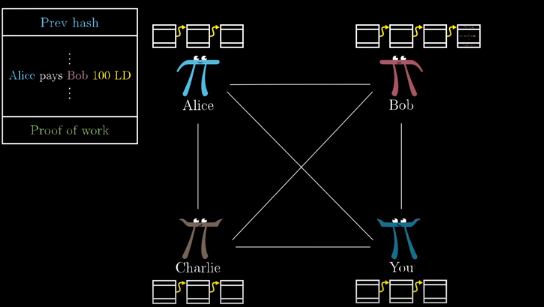
Slika ‑ Rudari (engl. block creator) pogađaju ispravni identifikator za blok koji se potom emitira sudionicima

Rudari (engl. Block creator/Miner) slušaju sve transakcije i probaju otkriti valjani identifikator prije ostalih rudara. Rudar koji prvi otkrije valjani identifikator dobije nagradu. Nagrada je određeni broj „novčića“ koji se prikupe od takse uzete od svake transakcije.

Svi ostali sudionici na mreži (Alice, Bob, Charlie, You) ne slušaju na sve transakcije nego samo na blokove koji se emitiraju od strane rudara.

Sada, kada smo objasnili osnovne pojmove vezane uz lanac blokova, na primjeru ćemo pokazati pokušaj prevare.

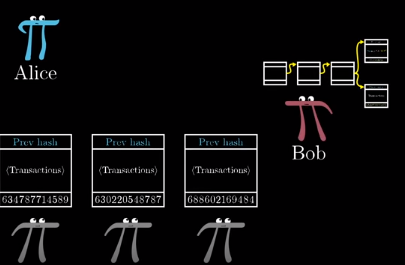
Uzmimo za primjer da Alice pošalje Bobu 100 kuna bez da svoju transakciju emitira mrežom.



Slika ‑ Alice plaća Bobu 100 kuna bez da svoju transakciju emitira svima na mreži

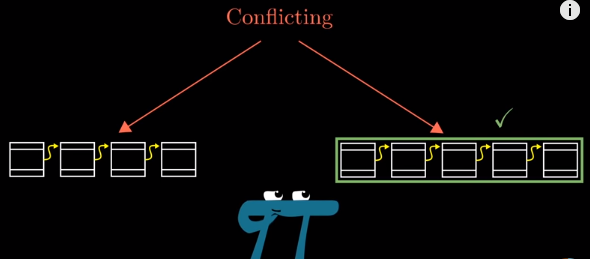
Da bi bilo moguće da blok pošalje samo Bobu, Alice treba pogoditi ispravni identifikator bloka prije svih ostalih rudara. Sasvim je moguće da Alice pogodi identifikator prije svih ostalih te da Bob doda taj blok na kraj svog lanca. Svi ostali sudionici na mreži tada neće znati za tu transakciju i vjerovat će da Alice ima tih 100 kuna.

Problem za zlonamjernog sudionika se skriva u tome što će Bob i dalje slušati emitirane blokove od svih rudara na mreži. U jednom trenutku nastat će konflikt između dva lanca blokova te će se lanac od Boba početi granati (Slika 3‑17).



Slika ‑ Grananje Bobovog lanca uslijed pokušaja prevare

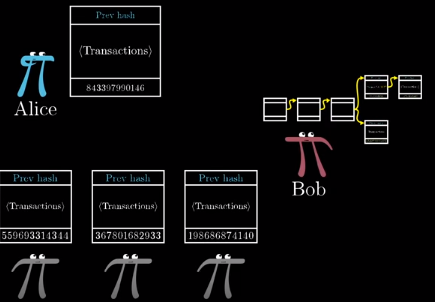
Pravilo glasi da se uvijek vjeruje dužem lancu jer je u njega uloženo više računalnog rada (Slika 3‑18).



Slika ‑ Uvijek se vjeruje lancu u kojeg je uloženo više rada

Trenutno, Bob ne zna koji je dio lanca ispravan jer su obe grane lanca jednake duljine stoga Bob i dalje nastavlja slušat emitirane blokove.

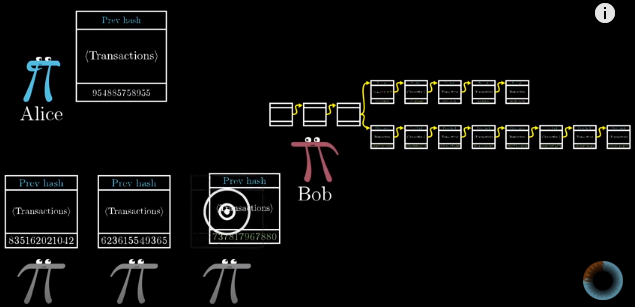
Da bi Alice uspjela u svom naumu mora i dalje pogađati ispravne identifikatore blokova prije svih ostalih rudara.



Slika ‑ Alice mora nastaviti pogađati identifikator prije svih ostalih rudara

Alice će možda pogoditi identifikator nekoliko puta prije ostalih rudara ukoliko ima toliko sreće, ali svakako neće moći održati lanac dužim dugoročno. Sve dok Alice nema najmanje 50% računalne snage u odnosu na sve ostale rudare gotovo je nemoguće da se to dogodi.

Dakle, svi ostali rudar koji rade zajedno će brže tržiti identifikator bloka nego Alice koja radi sama te će njihov lanac biti duži i Bob će zaključiti kako je Alicina grana lanca pokušaj prevare. Potom će odbaciti tu granu lanca i sve se vraća u normalu.



Slika ‑ Bob prati sve blokove dok ne postane očito koji je lanac ispravan

Zaključujemo da ukoliko se dogodi konflikt ne donosimo zaključke o ispravnosti odmah na temelju sljedećeg bloga nego se pričeka još par blokova te se odluči koji je lanac ispravan. S ovim zaključkom, objedinjeni su svi važni pojmovi i sigurnosni aspekti lanca blokova te su pokazani na konkretnom primjeru.

# DECENTRALIZIRANE APLIKACIJE