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

12. 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

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

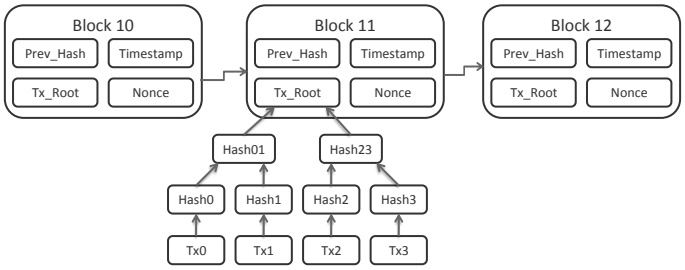
Napisati ovaj subsection

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

Blokovi su manji skupovi podataka koji se povezuju kako bi formirali krajnji lanac blokova (tj. blokčejn). Članovi distribuirane mreže (tj. korisnici blokčejna) objavljuju javno izmene koje žele da se dogode. Članovi zatim skupljaju veći broj izmena i spajaju ih da formiraju jedan blok. Svaki blok sadrži heš (dobijen pomoću kriptografski bezbedne heš funkcije) prethodnog bloka. Ovim je uspostavljen redosled blokova u lancu. Dodatno modifikacija nekog bloka postaje znatno teža jer ukoliko bi neki čvor u distribuiranoj mreži izmenio neki blok i tako izmenjen lanac prosledio dalje u mrežu ostali čvorovi bi lako videli da je blok izmenjen na sledeći način:
Neka je redosled blokova $b_0, b_1, ..., b_n$ i neka je pokušana izmena na bloku i i on je izmenjen u novi blok x: $b_0, b_1, ..., b_{i-1}, x, b_{i+1}, ..., b_n$. Uz svaki blok j je sačuvana heš vrednost h_j. Kada neki čvor dobije novi lanac blokova i njihove heš vrednosti vrši se verifikacija tako što čvor ponovo sračuna heš vrednosti blokova. Neka je heš funkcija f, onda se heš bloka j računa kao $h_j = f(h_{j-1}, b_j)$. Dakle na izmenjenom lancu bi bilo $h'_{i+1} = f(x, b_{i+1})$. Kako je blok $x \neq b_i$ jasno je da je $f(x, b_{i+1}) \neq f(b_i, b_{i+1})$ (tj. novosračunata vrednost h'_{i+1} će se razlikovati od dobijene vrednosti h_{i+1}). Slično je i za vrednosti $h'_{i+2}, h'_{i+3}, ...h'_n$ - kako je $h'_{i+1} \neq h_{i+1}$ onda će se i ostale vrednosti razlikovati.
Ovako je detektovana modifikacija na bloku i i utvrđeno je da je lanac nevalidan. Kako bi neko uspeo da izmeni jedan blok u lancu neophodno je da izmeni i ostale blokove i ponovo sračuna heš vrednosti kako bi dobio validan blokčejn.

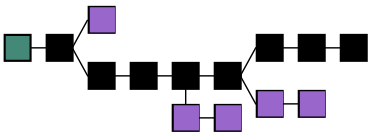
3.2 Decentralizacija

Umesto jednog centralnog autoriteta poput servera ili banke blokčejn koristi decentralizovanu, distribuiranu mrežu koja funkcioniše na "peer-to-peer"osnovi. "Peer-to-peer"komunikacija podrazumeva da se čvorovi u mreži ponašaju kao server i kao klijent, odnosno drugi čvorovi mogu tražiti podatke od njih, a i oni mogu tražiti podatke od drugih čvorova u mreži. Glavni izazov pri implementaciji distribuirane baze podataka je kome verovati da ima ispravnu verziju podataka - kako osigurati da mreža funkcioniše iako postoje čvorovi koji žele namerno da lažiraju podatke u svoju koristi ili ako postoje čvorovi koji ne funkcionišu ispravno. Suštinski, pitanje je kako da "pošteni" čvorovi dostignu koncenzus iako deo mreže ne sarađuje. Ovaj problem se često naziva "problem vizantijskih generala" (eng. Byzantine generals problem). Blokčejnovi najčešće koriste digitalne potpise zajedno sa algoritmom za postizanje koncenzusa poput "proof of work", "proof of stake" ili slično. Čime se postiže otpornost mreže čak do 50% nekooperativnih čvorova. "Proof of work" mehanizam funkcioniše tako što pri kreaciji bloka član mreže mora da uloži značajnu računarsku moć kako bi rešio težak algoritamski problem. Na primer u Bitcoin blokčejnu pri kreaciji novog bloga se vrše sledeći koraci:

1. Prikupljaju se transakcije koje će biti u novom bloku
2. Inicijalizuje se "nonce" vrednost na 0
3. Računa se heš vrednost transakcija koje treba staviti u blok, heš vrednosti prethodnog bloka i nonce vrednosti

4. Ukoliko tako dobijena heš vrednost počinje sa k nula, blok je validan i čvor ga prosleđuje ostatku mreže.
5. Inače uvećava se nonce vrednost za jedan i ponavo se računa heš vrednost dok se ne dobije k nula na početku.

Veruje se da se izlaz neke kriptografske heš funkcije ne može lako invertovati te se veruje da ne postoji efikasniji način od probanja velikog broja nonce vrednosti i ponovnog računanja heš vrednosti dok se ne dobije k nula na početku. Vrednost k se može povećavati i time postaje teže napraviti blok (što je poželjno kada mreža dovoljno poraste).
Iako neverovatno moguće je da se dva validna bloka kreiraju u slično vreme, ovo se naziva privremeno grananje blokčejna ("fork"). Ukoliko čvor primi blokčejn gde je došlo do grananja nastavlja sa kreacijom blokova samo odlučuje na koju granu će nadovezati sledeći blok. Kada se neka od grana produži novi blokčejn se oglašava mreži. U protokolu svakog blokčejna ugrađen je mehanizam kojim se razrešavaju grananja, najčešće se prihvata ona grana koja sadrži najviše blokova, a preostala grana se odbacuje.



Slika 2: Grananje u blokčejnu

Na slici 2 je prikazan primer grananja u blokčejnu. Crni blokovi predstavljaju aktuelni lanac, a ljubičasti blokovi predstavljaju bočne lance koji su eventualno odbačeni.
U kreaciji blokova najčešće ne učestvuju svi članovi mreže, već u slučaju "proof of work" mehanizma neki čvorovi biraju da se bave isključivo kreacijom blokova - ti čvorovi se nazivaju "mineri". U slučaju kriptovaluta mineri imaju inicijativu da kreiraju blokove zato što bivaju nagrađeni nakon uspešne kreacije bloka.
Digitalni potpisi, način povezivanja blokova u lanac pomoću kriptografskih heš funkcija i mehanizam za dostizanje koncenzusa u prisustvu nekooperativnih čvorova čine blokčejn pouzdanim načinom za čuvanje i upravljanje deljenom bazom podataka. Jedan od najpoznatijih načina da se blokčejn ipak prevari je ukoliko napadač uspe da obezbedi 51% mreže (tj. više nego što je potrebno za dostizanje koncenzusa). Ukoliko ovo uspe napadač može cenzurisati modifikacije blokčejna ili u slučaju kriptovaluta efektivno trošiti isti novac više puta. Napadač ne može praviti ilegalne izmene na blokčejnu - na primer čak iako upravlja 51% mreže to mu ne omogućava da lažira nečiji digitalni potpis ili doda nevalidnu transakciju u blok. Ako pokuša i ipak kreira nevalidan blok, zbog toga što napadač poseduje većinu mreže on će moći da nastavi da održava najduži lanac sa nevalidnim blokovima. Ostali učesnici mogu lako da detektuju da je blokčejn postao nevalidan i da prestanu da ga koriste, što nije u interesu napadača. Iako ne može vršiti nevalidne izmene na blokčejnu napadač

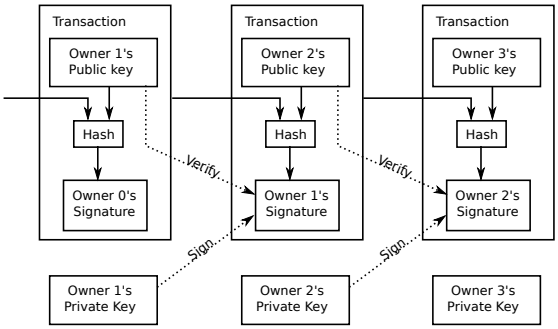
može odlučiti da neke izmene cenzuriše. Pošto napadač može da kreira svaki blok na lancu brže nego ostatak mreže on efektivno odlučuje koje izmene će biti uključene u lanac, a koje ne.

4 Primene

4.1 Kriptovalute

Ubedljivo najpoznatija primena blokčejn tehnologije, zbog koje je glavno i nastala, je u domenu digitalnih valuta. Ideja decentralizacije valute posebno je primamljiva u svetu finansija jer se odbacuje potreba za poverenjem u centralni autoritet kao što su banke ili državne vlade da bi se vrednost valute održala. Prva implementirana decentralizovana digitalna valuta - kriptovaluta koja je zasnovana na blokčejnu jeste čuveni Bitkoin.

Bitkoin u osnovi radi na principu transakcija - prenosa novca sa jednog na drugi đigitalni novčanik". Da bi sistem funkcionisao kao valuta, potrebno je da se vlasništvo novca koji se šalje može utvrditi. Ovo se postiže digitalnim potpisivanjem svake transakcije asimetričnom kriptografijom.

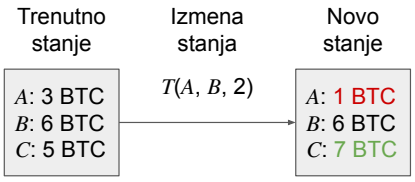


Slika 3: Transfer bitkoina

Takođe je potrebno osigurati da se isti novac ne može potrošiti dva puta (eng. double spending problem). Ovaj problem je rešen upravo upotrebom blokčejna, time što celu istoriju transakcija možemo smestiti i grupisati u pojedinačne blokove, a proof-of-work sistemom možemo osigurati koncenzus između korisnika o tome koja istorija transakcija je aktuelna.

4.2 Pametni ugovori

Nakon bitkoina primećen je mnogo opštiji način upotrebe blokčejn tehnologije. Posmatrajmo bitkoin protokol apstraktnije: kao sistem prelaska iz jednog stanja vlasništva novca u drugo. Na primeru sa dijagrama 4, ukoliko imamo osobe A, B i C sa 3, 6 i 5 bitkoina, ovo možemo predstaviti kao trenutno stanje. Ukoliko se izvrši transakcija gde osoba A pošalje 2 bitkoina osobi B, što bi predstavljalo neku funkciju izmene stanja $T(A, B, 2)$, dolazimo u novo stanje gde osoba A ima 2 manje, a osoba B 2 više bitkoina nego u prethodnom.

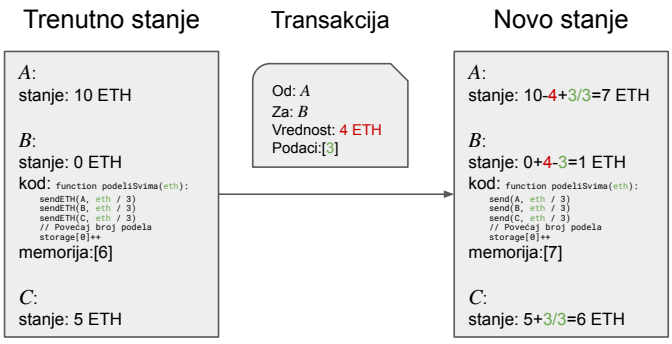


Slika 4: Promena stanja transkacijom

Posmatrajući protokol na ovaj način, jasno je da nema razloga ograničiti se na specifična stanja i funkciju izmene stanja kao što je ovde slučaj, već da ona mogu opisivati bilo koji željeni proces. Po ovom principu su nastali takozvani **pametni ugovori**.

Pametni ugovor kao pojam prvobitno je predstavljao bilo koji protokol ili program koji se automatski izvršava po odredbama nekakvog ugovora. Uzmimo kao primer automat za kafu. Svrha ove mašine je da automatski izvršava odredbe ugovora "Kupac će dobiti kafu ukoliko plati odgovarajuću sumu novca". Međutim, kada bi se desilo da se mašina hakuje ili pokvari i ne napravi kupcu kafu iako je u nju ubacio novac, odredbe ugovora ne bi bile zadovoljene. Da bi se izbeglo to da je potrebno verovati sistemu da će ispravno izvršiti odredbe, kao i eventualne troškove zbog posledica u ovakvim situacijama, pametne ugovore je idealno implementirati u okviru blokčejna, što nam omogućava **Ethereum**.

Danas sa pojavom Ethereum mreže se pojam pametnog ugovora uglavnom vezuje za bilo koji automatski proces koji se izvršava na blokčejnu. Ideja Ethereum protokola je da omogući decentralizovano izvršavanje bilo kakvog datog programa. Ovo se postiže različitim izmenama klasičnog bitkoin protokola. Glavna novina je što svaki đigitalni novčanik"uz svoju jedinstvenu adresu kao što je kod bitkoina takođe može imati memoriju i izvršivi kod u okviru sebe, nalik na prethodno opisano stanje i funkciju izmene stanja. Kod tj. izmena stanja se izvršava tako što se u transakcijama mogu dodati podaci koji predstavljaju ulazne vrednosti za taj proces (slika 5).



Slika 5: Promena stanja na Ethereum blokčejnu

Prilikom validacije blokova u ovako izmenjenom blokčejnu moguće je za svaku transakciju sa ulaznim podacima izvršiti odgovarajući kod naloga. Radeći ovo za svaki blok u najdužem lancu, dolazi se do krajnjeg decentralizovanog globalnog stanja za koji znamo da postoji koncenzus zbog ranije pomenutih svojstava blokčejna.

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.