Blokčejn

Šta je i čemu služi

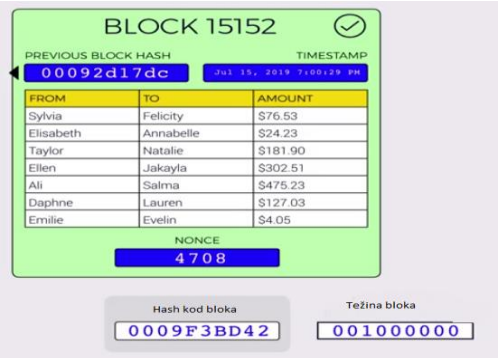
Blokčejn (Blockchain) je tehnologija koja omogućava deljeno (distribuirano) i proverljivo evidentiranje transakcija. Značaj blokčejn tehnologije je u tome što donosi poverenje u mreže ravnopravnih čvorova (peer to peer networks). Banke, na primer, postoje pre svega da bi služile kao garant transakcija. Pojava blokčejna omogućava trajno zapisane i proverljive transakcije, bez potrebe za centralnim autoritetom. Pri tome je evidentiranje i potvrđivanje pomenutih transakcija vrlo efikasno zahvaljujući upotrebi algoritama iz oblasti kriptografije. Dakle, blokčejn se može opisati kao otvorena, distribuirana glavna knjiga u koju se mogu beležiti transakcije na efikasan, proverljiv i trajan način. Jednom upisana transakcija, sačuvana je zauvek. Pod pojmom transakcije obično podrazumevamo plaćanje, ali to može biti i objavljivanje bilo kakvih podataka čiju istoriju i verodostojnost želimo da pratimo.

Distribuirani sistemi kao što je blokčejn su manje ranjivi od centralizovanih, jer ne postoji ključno mesto (centralni serveri) koje bi moglo da bude napadnuto, a čijim bi ispadanjem bila ugrožena funkcionalnost sistema.

Kako radi

Blokčejn se realizuje kao lista zapisa koji se zovu blokovi, a koji su povezani u lanac. Svaki blok sadrži:

- vremenski pečat (timestamp),
- podatke o transakcijama,
- kriptografsku heš vrednost prethodnog bloka,
- završni broj (nonce), koji služi kao dokaz rada (proof of work).



Sledi objašnjenje sadržaja bloka.

Da bi transakcija bila validna, ona mora imati digitalni potpis autora transakcije (u slučaju novčane transakcije, to je osoba koja plaća). Digitalni potpis je različit za svaku transakciju i praktično se ne može falsifikovati. Ovde i u daljem tekstu, reč „praktično“ znači da bi bilo potrebno previše vremena za potrebna računanja, ili bi (čak i da je to realno moguće uraditi dovoljno brzo) potrebno računanje bilo neuporedivo skuplje od koristi koju bi doneo falsifikat. Digitalnim potpisom platilac potvrđuje verodostojnost transakcije. Ovako overene transakcije se javno emituju, tako da svi zainteresovani mogu da ih slušaju i prikupljaju. Transakcije se dodaju na listu za novi blok po redosledu objavljivanja.

Heš vrednost je broj od 256 bita, koja se izračunava primenom heš funkcije na kompletan sadržaj bloka. Heš funkcija je svaka funkcija koja za proizvoljan sadržaj izračunava 256-bitni rezultat, a ima ove dve osobine:

- Čak i najmanjom izmenom sadržaja za koji se računa heš, dobija se potpuno drugačija vrednost;
- Inverznu funkciju je veoma teško, praktično nemoguće izračunati (izračunati blok za dati heš).

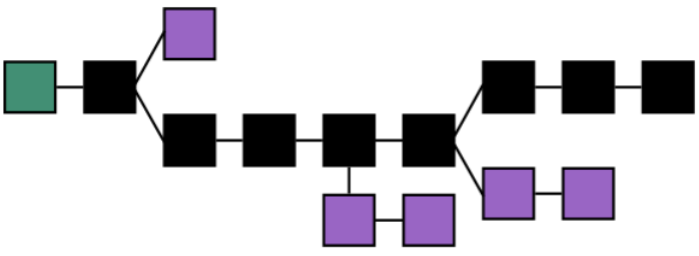
Najčešće korišćena heš funkcija se zove SHA256, ali mogla bi da posluži i bilo koja druga funkcija koja ima gore navedene osobine. Ove osobine su veoma važne, jer iz njih sledi da je praktično je nemoguće pogoditi kako treba da se dopuni određeni blok završnim brojem, tako da heš vrednost bude nekog specijalnog oblika (konkretno, da počinje sa N nula). Jedini način da se postigne da heš vrednost bloka počinje sa N nula je da se pokušava sa različitim vrednostima završnog broja za taj blok, dok se ne dogodi da heš vrednost ima traženu osobinu. Za N početnih nula (u binarnom zapisu) potrebno je u proseku 2^N pokušaja, što može biti veoma mnogo. Dakle, da bi neko kompletirao jedan blok i dobio heš vrednost tog bloka koja počinje sa N nula, potrebno je da obavi mnogo računanja i zato se završni broj koji kompletira blok naziva dokaz rada.

Reći da neka heš vrednost (u binarnom zapisu) počinje sa N nula, isto je što i reći da je ta heš vrednost manja od broja koji počinje sa N-1 nula i jedinicom, i nastavlja se nulama (to je broj 2^{256-N}). Ova granična vrednost od koje heš mora biti manji, naziva se težina bloka.

Svako može da sastavi novi blok sa transakcijama koje su do njega stigle, da izračuna završni broj i da emituje taj blok. Međutim, obični korisnici koji samo žele da obavljaju transakcije, ne moraju da slušaju pojedinačne transakcije, dovoljno je da slušaju blokove (o ovome će biti reči kasnije).

Korisnici koji slušaju pojedinačne transakcije i stvaraju blokove obično se nazivaju rudari. Kao nagradu za kreiranje bloka, rudar ima pravo da na početak bloka doda jednu specijalnu transakciju kojom on prema protokolu dobija određenu svotu praktično niotkuda. Svako može da izračuna heš vrednost za objavljeni blok i vidi da on počinje zahtevanim brojem nula, čime se potvrđuje da je kreator uložio rad u stvaranje bloka.

Moguće je da različiti rudari u najnoviji blok uključe različite transakcije, na primer zato što nisu primili informaciju o određenoj transakciji, ili zato što pokušavaju da varaju i ubace izmenjenu ili neobjavljenu (nepostojeću) transakciju. U takvoj situaciji pravilo nalaže da se za ispravan blok smatra onaj na koji se kasnije nadoveže najviše novih blokova. Na slici dole zeleni blok je inicijalni i od njega počinju svi lanci. Blokovi na koje se ne nadoveže dovoljno novih blokova nazivaju se siročići (orphan-blocks), na slici označeni ljubičasto. Kada se vidi da je neki blok siroče, on se na dalje ignoriše. Glavni lanac je najduži lanac blokova koji polazi od inicijalnog bloka i na slici su ti blokovi crni. Samo kreatori blokova u glavnom lancu dobijaju nagradu, jer samo ti blokovi ulaze u „glavnu knjigu“ (specijalne nagradne transakcije iz blokova siročića ne važe samim tim što njihovi blokovi nisu ušli u glavni lanac).



Kada više rudara radi na nalaženju odgovarajućeg završnog broja za isti blok (isti spisak transakcija i isti prethodni blok), oni će zajedno obaviti potreban broj pokušaja mnogo brže, tako da će blok biti kreiran za manje vremena. Naravno, to će doneti dobitak samo jednom od njih, ali u pricipu važi da što više ljudi (računara) priprema jedan isti blok, to će blok brže biti kreiran.

Ako bi neko pokušao da izmeni bilo koji deo nekog objavljenog bloka, dokaz rada bi postao nevažeći, jer bi se promenila heš vrednost tog bloka i ne bi počinjala potrebnim brojem nula. Tako bi blok postao nevažeći bilo da se izmeni neka transakcija (uključujući nagradnu), bilo samo redosled običnih transakcija, ili podatak o prethodnom bloku. Prema tome, radi bilo kakve izmene bloka potrebno je ponovo izračunati dokaz rada. Blokovima koji slede za ovim izmenjenim blokom bi takođe morali biti ponovo izračunati dokazi rada, jer se heš vrednost prethodnog bloka promenila. Da bi ovakva prevara mogla da uspe, prevarant bi u nastavku morao da kreira blokove brže nego rudari koji rade na lancu ispravnih blokova. Kako ogromna većina radi na ispravnim blokovima, prevarant bi morao da raspolaže računskom snagom većom od one kojom raspolaže ostatak sveta. Stoga ceo postupak dovodi do toga da izmenjeni blok izgubi vremensku trku sa ostalim objavljenim blokovima i završi kao siroče. Zahvaljujući ovome, produžavanjem glavnog lanca se ujedno potvrđuje ceo spisak svih prethodnih transakcija i celom sistemu se veruje (rudari samim svojim većinskim delovanjem određuju koji lanac je glavni).

Običan korisnik koji je zainteresovan za jednu određenu transakciju, treba putem odgovarajućeg softvera da sluša blokove i prati da li se data transakcija pojavljuje u nekom od njih. Da ne bi postao žrtva prevare (moguće je da prevarant neko vreme samo njemu šalje izmenjene blokove), dobro je da sačeka pojavu nekoliko novih blokova nakon onog koji sadrži očekivanu transakciju, kako bi se potvrdilo da blok od interesa pripada glavnom lancu.

Blokčejn mrežu čine svi korisnici koji su međusobno povezani u peer to peer mrežu. Čvorovi u mreži mogu biti:

- Teški čvorovi (full nodes) - čuvaju čitav blokčejn, i proveravaju i evidentiraju svaku transakciju
- Laki čvorovi (light nodes) - čuvaju samo završni deo blokčejna, za koji zahvaljujući radu teških čvorova veruju da je deo glavnog lanca.

Rudari se razlikuju od običnih čvorova po tome što oni ne čuvaju blokčejn, već prave nove blokove i prosleđuju ih čvorovima na proveru. Kada čvor dobije ispravan blok od rudara, on verifikuje dokaz rada (potvrđuje da je u kreiranje bloka uložen rad), uključuje blok u svoju lokalnu kopiju i prosleđuje ga nekolicini povezanih čvorova, koji takođe proveravaju blok, uključuju ga i emituju dalje. Na taj način se blok širi po celoj mreži i postaje neizmenjiv.

Primene (osim trgovine kriptovalutama)

- Ubrzo nakon osnivanja Bitcoina, postalo je očigledno da bi blokčejn tehnologija mogla da ima i mnogo širu primenu. Ustvari, blockchain može biti korišćen za bilo šta što podrazumeva i zahteva transakcije, koje treba zabeležiti na siguran način.
- Primena **u poslovanju** jeste realizacija koncepta pametnih ugovora (smart contracts) koji omogućuju direktnu razmenu digitalnih dobara, bez mogućnosti da jedna strana prevari drugu i ne ispuni svoj deo ugovora.

- Primena **u bankama**, gde već postoji servis za međubankarske transakcije, koji pretenduje da zameni SWIFT servis, efikasnije i sa značajno nižim troškovima po transakciji.
- Primena **u državnoj upravi**, gde kao primer možemo navesti matične i zemljišne knjige, tako da jednom upisani podaci postaju javno dostupni i proverljivi, distribuirani između građana i zainteresovanih strana.
- Primena **za elektronsko glasanje**, gde se svaki glas transparentno beleži i time se sprečavaju nepravilnosti.
- Primena **u zdravstvu**, za distribuirano čuvanje kartona pacijenata. U ovom slučaju treba koristiti lance sa zaštićenim pristupom podacima.
- Primena **u obrazovanju**, za proverljivost izdatih diploma i sertifikata, tako što bi škola koja ih izdaje objavila diplome kao transakcije i garantovala njihovu autentičnost.

Zanimljivosti

- Blokčejn je nastao 2008 godine. Prvi naučni rad koji opisuje ideju i daje uputstva za korišćenje, kao i prva verzija softvera potpisani su imenom Satoši Nakamoto. Zanimljivo je da se do sada o autoru ništa ne zna, tako da nije poznato ko je stvarni izumitelj.
- Visina nagrade za stvaranje bloka u glavnom lancu se vremenom smanjuje.
- Broj zahtevanih početnih nula u heš vrednosti bloka se vremenom povećava i trenutno je 19.
- Bitcoin blokovi mogu sadržati do oko 2000 transakcija, ali ovaj broj varira od blokčejna do blokčejna, i zavisi od veličine bloka. Bitcoin blok trenutno može biti veličine do 1MB.