Blockchain

Specijalni Kurs

Pravi Rep je online na svim platformama

Sadržaj

1 Osobine blockchain-a

Blockchain tehnologija ima nekoliko ključnih osobina koje je čine jedinstvenom i pogodnom za razne aplikacije. Ove osobine omogućavaju decentralizovanu, sigurnu i transparentnu razmenu informacija i vrednosti.

1.1 Decentralizacija

Blockchain je distribuirana mreža u kojoj nema centralnog autoriteta. Svi učesnici (čvorovi) u mreži imaju jednak status i svi podaci su replicirani na svim čvorovima. Decentralizacija pruža sledeće prednosti:

- **Otpornost na cenzuru:** Nema centralne tačke koja bi mogla biti ciljana za cenzurisanje ili kontrolisanje podataka.
- **Veća sigurnost:** Napadač bi morao kompromitovati većinu čvorova kako bi uspeo da manipuliše podacima.
- **Povećana dostupnost:** Podaci su dostupni čak i ako neki čvorovi u mreži nisu funkcionalni.

1.2 Transparentnost

Sve transakcije i podaci u blockchainu su javno dostupni i mogu ih pregledati svi učesnici u mreži. Transparentnost pruža:

- **Verifikacija podataka:** Bilo ko može proveriti tačnost transakcija i integritet podataka.
- **Poverenje:** Transparentnost omogućava učesnicima da veruju sistemu bez potrebe za centralizovanim posrednikom.

1.3 Nepromenljivost (immutability)

Jednom kada su podaci zabeleženi na blockchainu, ne mogu biti izmenjeni ili obrisani. Nepromenljivost pruža:

- **Integritet podataka:** Podaci ostaju tačni i verodostojni kroz vreme.
- **Otpornost na manipulaciju:** Teško je ili nemoguće izmeniti podatke bez saglasnosti većine čvorova u mreži.

1.4 Sigurnost

Blockchain koristi kriptografske tehnike kako bi osigurao integritet i sigurnost podataka. Osnovni sigurnosni elementi uključuju:

- **Hash funkcije:** Koriste se za povezivanje blokova i zaštitu podataka unutar svakog bloka.
- **Kriptografija javnog ključa:** Omogućava bezbednu identifikaciju i verifikaciju transakcija.
- **Digitalni potpisi:** Osiguravaju autentičnost i integritet transakcija.

1.5 Konsenzus mehanizmi

Blockchain mreže koriste različite konsenzus mehanizme kako bi svi čvorovi postigli dogovor o stanju mreže. Najčešći mehanizmi uključuju:

- **Proof of Work (PoW):** Rudari rešavaju složene matematičke probleme kako bi dodali nove blokove u blockchain.
- **Proof of Stake (PoS):** Validatori se biraju na osnovu količine kriptovalute koju su uložili kao zalog.
- **Delegated Proof of Stake (DPoS):** Korisnici biraju delegate koji su odgovorni za verifikaciju i dodavanje novih blokova.

1.6 Automatizacija kroz pametne ugovore

Pametni ugovori su samoizvršavajući programi koji se automatski izvršavaju kada su ispunjeni određeni uslovi. Oni omogućavaju:

- **Automatizaciju poslovnih procesa:** Smanjuju potrebu za posrednicima i manuelnom verifikacijom.
- **Smanjenje troškova:** Automatizacija smanjuje operativne troškove.
- **Povećanje efikasnosti:** Brže i tačnije izvršavanje ugovora i transakcija.

Osobine blockchaina čine ga moćnim alatom za različite primene, od finansijskih transakcija do upravljanja lancem snabdevanja i pametnih ugovora. Njegove karakteristike omogućavaju sigurnu, transparentnu i efikasnu razmenu podataka i vrednosti u decentralizovanom okruženju.

2 Prednosti i mane blockchain-a

Blockchain tehnologija donosi mnoge prednosti, ali i određene izazove i mane koje treba uzeti u obzir. Razumevanje ovih aspekata pomaže u evaluaciji kada i kako koristiti blockchain tehnologiju.

2.1 Prednosti blockchain-a

- **Decentralizacija:**
  - Uklanjanje potrebe za centralnim posrednikom, što smanjuje rizik od centralne tačke neuspeha i cenzure.
  - Omogućava ravnopravno učestvovanje svih čvorova u mreži.
- **Transparentnost:**
  - Sve transakcije su javno dostupne i proverljive, što povećava poverenje korisnika.
  - Pruža mogućnost audita i praćenja svih aktivnosti u mreži.
- **Nepromenljivost:**
  - Podaci zapisani u blockchainu ne mogu biti izmenjeni ili obrisani, čime se osigurava integritet i trajnost podataka.
- **Sigurnost:**
  - Koristi kriptografske metode za zaštitu podataka i transakcija, čineći ih otpornim na falsifikovanje i neovlašćeni pristup.
- **Efikasnost kroz pametne ugovore:**

- Pametni ugovori omogućavaju automatizaciju i samostalno izvršenje ugovora, smanjujući potrebu za posrednicima i manuelnim procesima.

- **Povećana otpornost na napade:**
  - Distribuirana priroda mreže čini je otpornijom na DDoS napade i druge oblike centralizovanih napada.

2.2 Mane blockchain-a

- **Skalabilnost:**
  - Većina blockchain mreža trenutno ne može da obradi veliki broj transakcija po sekundi, što ograničava njihovu upotrebu za masovno usvajanje.

- **Visoki troškovi energije:**
  - Proof of Work (PoW) konsenzus algoritam, koji se koristi u mnogim blockchain mrežama, zahteva veliku količinu energije, što ima negativan uticaj na životnu sredinu.

- **Složenost i tehnička barijera:**
  - Implementacija i održavanje blockchain rešenja zahtevaju specifična tehnička znanja, što može biti prepreka za široko usvajanje.

- **Regulatorna nesigurnost:**
  - Pravna i regulatorna pitanja vezana za blockchain tehnologiju i kriptovalute još uvek nisu u potpunosti rešena u mnogim jurisdikcijama.

- **Privatnost:**
  - Iako je transparentnost prednost, ona može biti i mana kada je potrebna zaštita privatnosti korisnika i podataka.

- **Neadekvatnost za neke primene:**
  - Blockchain nije uvek najprikladnija tehnologija za sve vrste aplikacija, posebno one koje ne zahtevaju visoku sigurnost i decentralizaciju.

2.3 Zaključak

Blockchain tehnologija nudi mnoge prednosti, uključujući decentralizaciju, transparentnost, nepromenljivost, sigurnost i efikasnost kroz pametne ugovore. Međutim, postoje i značajni izazovi, kao što su problemi sa skalabilnošću, visoki troškovi energije, tehnička složenost, regulatorna nesigurnost i pitanja privatnosti. Razumevanje ovih aspekata ključno je za donošenje informisanih odluka o implementaciji blockchain rešenja.

3 Primene blockchain-a

Blockchain tehnologija je našla široku primenu u raznim industrijama zahvaljujući svojim osobinama kao što su decentralizacija, transparentnost, nepromenljivost i sigurnost. U nastavku su predstavljene neke od ključnih primena blockchain tehnologije.

3.1 Finansijske usluge

- **Kriptovalute:**
  - Najpoznatija primena blockchain tehnologije, omogućavajući kreiranje i razmenu digitalnih valuta poput Bitcoina i Ethereuma.
- **Plaćanja i transfer novca:**
  - Blockchain omogućava brze i jeftine međunarodne transfere novca bez potrebe za posrednicima kao što su banke.
- **Decentralizovane finansije (DeFi):**
  - DeFi platforme koriste pametne ugovore za pružanje finansijskih usluga kao što su pozajmljivanje, zaduživanje i trgovina bez posrednika.

3.2 Upravljanje lancem snabdevanja

- **Praćenje i sledljivost proizvoda:**
  - Blockchain omogućava transparentno praćenje porekla i kretanja proizvoda kroz lanac snabdevanja, smanjujući rizik od falsifikovanja i poboljšavajući efikasnost.
- **Automatizacija ugovora:**
  - Pametni ugovori mogu automatski izvršavati uslove ugovora između različitih strana u lancu snabdevanja, kao što su plaćanja i dostave.

3.3 Zdravstvo

- **Sigurno čuvanje medicinskih podataka:**
  - Blockchain može obezbediti sigurnu i nepromenjivu evidenciju medicinskih podataka pacijenata, omogućavajući lakši pristup i razmenu podataka između zdravstvenih institucija.
- **Praćenje lekova:**
  - Praćenje kretanja lekova od proizvođača do pacijenata kako bi se smanjila pojava falsifikovanih lekova.

3.4 Nekretnine

- **Tokenizacija imovine:**
  - Digitalizacija fizičke imovine, kao što su nekretnine, u obliku tokena koji se mogu lakše trgovati i prenositi.
- **Upravljanje vlasničkim pravima:**
  - Blockchain omogućava sigurnu evidenciju vlasničkih prava i istorije transakcija, smanjujući rizik od prevara i sporova.

3.5 Glasanje

- **Elektronsko glasanje:**
  - Blockchain tehnologija može obezbediti siguran i transparentan sistem za elektronsko glasanje, smanjujući rizik od prevara i povećavajući poverenje u izborni proces.

3.6 Autorska prava i intelektualna svojina

- **Zaštita autorskih prava:**
  - Blockchain može obezbediti nepromenjivu evidenciju o vlasništvu i distribuciji intelektualne svojine, kao što su muzika, umetnička dela i patenti.
- **Licenciranje i ugovori:**
  - Pametni ugovori mogu automatizovati proces licenciranja i naplate naknada za korišćenje intelektualne svojine.

3.7 Javna uprava

- **Transparentnost i odgovornost:**
  - Korišćenje blockchain tehnologije u javnoj upravi može povećati transparentnost i odgovornost, omogućavajući građanima lakši pristup informacijama i praćenje javnih sredstava.
- **Digitalni identitet:**
  - Blockchain može obezbediti siguran i verifikovan digitalni identitet građana, koji se može koristiti za različite javne i privatne usluge.

3.8 Igranje igara i digitalni svetovi

- **Digitalna imovina i kolekcionarski predmeti:**
  - Blockchain omogućava kreiranje i trgovinu digitalnom imovinom i kolekcionarskim predmetima unutar igara i virtualnih svetova, koristeći nefugibilne tokene (NFT).
- **Transparentna ekonomija u igrama:**
  - Korišćenje blockchaina za praćenje transakcija unutar igara povećava transparentnost i poverenje među igračima.

3.9 Zaključak

Blockchain tehnologija pruža širok spektar primena u raznim industrijama, zahvaljujući svojim osobinama kao što su decentralizacija, transparentnost, nepromenljivost i sigurnost. Od finansijskih usluga do javne uprave, blockchain može transformisati mnoge aspekte modernog društva, povećavajući efikasnost, sigurnost i poverenje.

4 Izazovi za usvajanje blockchain tehnologije

Iako blockchain tehnologija donosi mnoge prednosti, njeno široko usvajanje suočava se sa različitim izazovima. Razumevanje ovih izazova je ključno za pronalaženje rešenja koja će omogućiti efikasniju implementaciju i upotrebu blockchain tehnologije.

4.1 Skalabilnost

- **Ograničen kapacitet transakcija:**
  - Većina blockchain mreža može obraditi samo ograničen broj transakcija po sekundi (TPS), što nije dovoljno za masovno usvajanje u globalnim aplikacijama.
- **Zagušenje mreže:**
  - Povećanje broja korisnika i transakcija može dovesti do zagušenja mreže, što uzrokuje duže vreme potvrde transakcija i više naknade.

4.2 Energetska efikasnost

- **Visoki troškovi energije:**
  - Proof of Work (PoW) konsenzus algoritam, koji se koristi u mnogim blockchain mrežama, zahteva značajnu količinu energije, što ima negativan uticaj na životnu sredinu.
- **Ekoloski otisak:**
  - Velika potrošnja energije za rudarenje kriptovaluta stvara veliki ekološki otisak, što postavlja pitanja održivosti blockchain tehnologije.

4.3 Regulatorna nesigurnost

- **Nedostatak regulative:**
  - Mnoge jurisdikcije još uvek nemaju jasne regulative za blockchain tehnologiju i kriptovalute, što stvara pravnu nesigurnost za korisnike i investitore.
- **Promenljive regulative:**
  - Regulativni okvir može brzo da se menja, što stvara izazove za dugoročno planiranje i usvajanje blockchain tehnologije.

4.4 Sigurnost i privatnost

- **Zaštita podataka:**
  - Transparentnost blockchaina može biti izazov za zaštitu privatnosti korisnika, posebno kada su u pitanju osetljivi podaci.
- **Sigurnosni napadi:**
  - Iako je blockchain tehnologija inherentno sigurna, postoji rizik od napada kao što su 51% napad, gde jedan entitet kontroliše većinu mreže, ili napada na pametne ugovore.

4.5 Interoperabilnost

- **Kompatibilnost između različitih blockchain mreža:**
  - Postoji mnogo različitih blockchain mreža, ali nedostatak standardizacije i interoperabilnosti između njih može otežati razmenu podataka i vrednosti.

4.6 Tehnička složenost i nedostatak stručnjaka

- **Kompleksnost implementacije:**
  - Implementacija i održavanje blockchain rešenja zahteva specifična tehnička znanja i veštine, što može biti prepreka za mnoge organizacije.
- **Nedostatak stručnjaka:**
  - Nedostatak kvalifikovanih stručnjaka za blockchain tehnologiju može ograničiti sposobnost organizacija da efikasno usvoje i implementiraju blockchain rešenja.

4.7 Prilagodljivost i usvajanje od strane korisnika

- **Otpor prema promenama:**
  - Organizacije i pojedinci mogu biti otporni prema usvajanju novih tehnologija zbog navika, nepoznavanja tehnologije ili straha od rizika.
- **Korisinčko iskustvo:**
  - Trenutne blockchain aplikacije mogu imati složena korisnička sučelja i loše korisničko iskustvo, što može obeshrabriti širu upotrebu.

4.8 Zaključak

Usvajanje blockchain tehnologije suočava se sa značajnim izazovima kao što su skalabilnost, energetska efikasnost, regulatorna nesigurnost, sigurnost, interoperabilnost, tehnička složenost i prilagodljivost korisnika. Rešavanje ovih izazova ključno je za omogućavanje šire primene i ostvarivanje punog potencijala blockchain tehnologije.

5 Osnovni elementi blockchain-a

Blockchain tehnologija se sastoji od nekoliko ključnih elemenata koji zajedno omogućavaju njeno funkcionisanje kao decentralizovane, sigurne i transparentne baze podataka. Ovi osnovni elementi uključuju blokove, hash funkcije, konsenzus mehanizme, decentralizovanu mrežu, pametne ugovore i kriptografske ključeve.

5.1 Blokovi

Blokovi su osnovne jedinice u blockchain mreži. Svaki blok sadrži skup transakcija i druge važne informacije. Struktura bloka uključuje:

- **Zaglavlje bloka (Block Header):**
  - *Hash prethodnog bloka (Previous Block Hash):* Kriptografska hash vrednost prethodnog bloka, koja povezuje blokove u lanac.
  - *Merkle Root:* Hash vrednost korena Merkle drveta koje sažima sve transakcije u bloku.
  - *Vremenska oznaka (Timestamp):* Vreme kada je blok kreiran.
  - *Nonce:* Nasumični broj koji rudari menjaju dok ne pronađu validnu hash vrednost za blok.
  - *Poteškoća (Difficulty):* Nivo težine koji određuje koliko je teško pronaći validnu hash vrednost za novi blok.
- **Telo bloka (Block Body):**
  - *Transakcije (Transactions):* Lista svih transakcija uključenih u blok.

5.2 Hash funkcije

Hash funkcije su kriptografske funkcije koje uzimaju ulazne podatke i generišu jedinstvenu izlaznu vrednost fiksne dužine (hash). U blockchainu, hash funkcije se koriste za:

- **Povezivanje blokova:** Hash vrednost prethodnog bloka je uključena u zaglavlje sledećeg bloka, čime se formira lanac blokova.
- **Verifikaciju integriteta:** Bilo kakva promena podataka u bloku menja njegov hash, što omogućava detekciju manipulacija.
- **Merkle drvo:** Hash funkcije se koriste za kreiranje Merkle drveta, koje omogućava efikasnu i sigurnu verifikaciju transakcija unutar bloka.

5.3 Konsenzus mehanizmi

Konsenzus mehanizmi omogućavaju svim čvorovima u mreži da se slože oko stanja blockchaina. Najčešći konsenzus mehanizmi uključuju:

- **Proof of Work (PoW):** Rudari takmiče u rešavanju složenih matematičkih problema kako bi dodali nove blokove u blockchain.
- **Proof of Stake (PoS):** Validatori se biraju na osnovu količine kriptovalute koju su uložili kao zalog.
- **Delegated Proof of Stake (DPoS):** Korisnici biraju delegate koji su odgovorni za verifikaciju i dodavanje novih blokova.

5.4 Decentralizovana mreža

Blockchain funkcioniše kao decentralizovana mreža u kojoj svi čvorovi (nodes) imaju jednak status i svi podaci su replicirani na svim čvorovima. Prednosti decentralizacije uključuju:

- **Otpornost na cenzuru:** Nema centralne tačke koja bi mogla biti ciljana za cenzurisanje ili kontrolisanje podataka.
- **Povećana sigurnost:** Napadač bi morao kompromitovati većinu čvorova kako bi uspeo da manipuliše podacima.
- **Povećana dostupnost:** Podaci su dostupni čak i ako neki čvorovi u mreži nisu funkcionalni.

5.5 Pametni ugovori

Pametni ugovori (smart contracts) su samoizvršavajući programi koji se automatski izvršavaju kada su ispunjeni određeni uslovi. Oni omogućavaju:

- **Automatizaciju poslovnih procesa:** Smanjuju potrebu za posrednicima i manuelnom verifikacijom.
- **Smanjenje troškova:** Automatizacija smanjuje operativne troškove.
- **Povećanje efikasnosti:** Brže i tačnije izvršavanje ugovora i transakcija.

5.6 Kriptografski ključevi

Kriptografski ključevi se koriste za sigurnu identifikaciju i verifikaciju korisnika i transakcija u blockchain mreži. Postoje dva osnovna tipa ključeva:

- **Privatni ključ (Private Key):** Koristi se za potpisivanje transakcija i dokazivanje vlasništva nad sredstvima.
- **Javni ključ (Public Key):** Koristi se za verifikaciju digitalnih potpisa i identifikaciju korisnika.

5.7 Zaključak

Osnovni elementi blockchain-a, kao što su blokovi, hash funkcije, konsenzus mehanizmi, decentralizovana mreža, pametni ugovori i kriptografski ključevi, zajedno omogućavaju sigurno, transparentno i efikasno funkcionisanje ove tehnologije. Razumevanje ovih elemenata je ključno za pravilnu implementaciju i korišćenje blockchain-a u raznim industrijama.

6 Kriptografski elementi blockchain tehnologije

Blockchain tehnologija se oslanja na različite kriptografske elemente kako bi obezbedila sigurnost, integritet i autentičnost podataka. Ovi kriptografski elementi čine osnovu za funkcionisanje blockchain mreža. Ključni kriptografski elementi uključuju hash funkcije, kriptografiju javnog ključa, digitalne potpise i Merkle drveće.

6.1 Hash funkcije

Hash funkcije su kriptografske funkcije koje uzimaju ulazne podatke bilo koje veličine i generišu izlaznu vrednost fiksne dužine (hash). Osnovne karakteristike hash funkcija su determinističnost, efikasnost, otpornost na sudare, efektivna skrivenost i otpornost na preimage napade.

- **SHA-256:** Najčešće korišćena hash funkcija u blockchain tehnologiji, posebno u Bitcoin mreži. Generiše 256-bitnu (32-bajtnu) hash vrednost.
- **Povezivanje blokova:** Svaki blok u blockchainu sadrži hash prethodnog bloka, što formira lanac blokova i osigurava nepromenljivost.
- **Merkle drvo:** Hash funkcije se koriste za kreiranje Merkle drveta, koje omogućava efikasnu i sigurnu verifikaciju velikog broja transakcija.

6.2 Kriptografija javnog ključa (Asimetrična kriptografija)

Kriptografija javnog ključa koristi par ključeva - privatni ključ i javni ključ. Ova metoda omogućava sigurno šifrovanje i dešifrovanje podataka, kao i verifikaciju identiteta.

- **Privatni ključ:** Tajni ključ koji se koristi za potpisivanje transakcija. Vlasnik privatnog ključa ima kontrolu nad sredstvima povezanih sa odgovarajućim javnim ključem.
- **Javni ključ:** Javni ključ se deli sa drugim korisnicima i koristi se za verifikaciju digitalnih potpisa kreiranih pomoću privatnog ključa.
- **Elliptic Curve Digital Signature Algorithm (ECDSA):** Algoritam često korišćen u blockchain tehnologiji za generisanje digitalnih potpisa.

6.3 Digitalni potpisi

Digitalni potpisi omogućavaju verifikaciju identiteta pošiljaoca i integriteta podataka. U blockchain tehnologiji, digitalni potpisi osiguravaju da su transakcije autorizovane od strane vlasnika privatnog ključa.

- **Stvaranje potpisa:** Pošiljalac koristi svoj privatni ključ za generisanje digitalnog potpisa na osnovu podataka transakcije.
- **Verifikacija potpisa:** Primalac koristi javni ključ pošiljaoca za verifikaciju potpisa. Ako verifikacija uspe, primalac može biti siguran da transakcija dolazi od vlasnika privatnog ključa i da podaci nisu izmenjeni.

6.4 Merkle drvo

Merkle drvo je struktura podataka koja omogućava efikasnu i sigurnu verifikaciju velikog broja transakcija u bloku. Merkle drvo koristi hash funkcije za kreiranje hijerarhijske strukture transakcija.

- **Merkle koren (Merkle Root):** Hash vrednost na vrhu Merkle drveta koja predstavlja sažetak svih transakcija u bloku.
- **Merkle grane (Merkle Branches):** Putanja hash vrednosti od određene transakcije do Merkle korena, koja omogućava verifikaciju da je transakcija deo bloka.

6.5 Konsenzus algoritmi

Konsenzus algoritmi koriste kriptografske tehnike kako bi osigurali da svi čvorovi u mreži postignu dogovor o trenutnom stanju blockchaina. Najpoznatiji algoritmi uključuju:

- **Proof of Work (PoW):** Rudari rešavaju složene kriptografske probleme kako bi dodali novi blok u blockchain. SHA-256 je često korišćena hash funkcija u PoW.
- **Proof of Stake (PoS):** Validatori se biraju proporcionalno njihovom ulogu (stake) u mreži, a kriptografske tehnike osiguravaju sigurnost i validnost blokova.

6.6 Zaključak

Kriptografski elementi blockchain tehnologije, uključujući hash funkcije, kriptografiju javnog ključa, digitalne potpise, Merkle drveće i konsenzus algoritme, omogućavaju sigurnost, integritet i nepromenljivost podataka u blockchain mrežama. Razumevanje ovih elemenata ključno je za efikasnu implementaciju i korišćenje blockchain tehnologije.

7 Problem distribuiranog konsenzusa

Distribuirani konsenzus je ključni koncept u blockchain tehnologiji, koji omogućava postizanje dogovora o stanju mreže među mnogim distribuiranim čvorovima. Postizanje konsenzusa u decentralizovanim sistemima suočava se s brojnim izazovima i problemima, od kojih su najznačajniji problem bizantijskih generala, otpornost na napade i efikasnost.

7.1 Problem bizantijskih generala

Problem bizantijskih generala ilustruje izazov postizanja konsenzusa u distribuiranim sistemima gde učesnici mogu biti nepošteni ili zlonamerni. Problem se može opisati na sledeći način:

- **Scenarij:** Grupa generala Bizantijske vojske raspoređena je oko neprijateljskog grada i mora da se dogovori da li će napasti ili se povući. Da bi napad bio uspešan, svi generali moraju se složiti oko odluke.
- **Izazov:** Neki generali mogu biti izdajnici i mogu poslati kontradiktorne informacije kako bi ometali postizanje zajedničkog dogovora.

Rešenje ovog problema zahteva protokol koji omogućava poštenim generalima da postignu konsenzus čak i u prisustvu nepoštenih aktera. U blockchain kontekstu, ovaj problem se rešava korišćenjem različitih konsenzus mehanizama.

7.2 Konsenzus mehanizmi

Različiti konsenzus mehanizmi koriste se u blockchain mrežama kako bi se postigao distribuirani konsenzus. Najpoznatiji mehanizmi uključuju:

- **Proof of Work (PoW):**
  - Rudari rešavaju složene matematičke probleme kako bi dodali nove blokove u blockchain. Ovaj proces zahteva značajnu računalnu snagu, čime se otežava manipulacija mrežom.
  - **Prednosti:** Visok nivo sigurnosti i otpornosti na napade.
  - **Mane:** Visoka potrošnja energije i ograničena skalabilnost.
- **Proof of Stake (PoS):**
  - Validatori se biraju proporcionalno njihovom ulogu (stake) u mreži. Validatori osiguravaju blokove stavljanjem svoje kriptovalute kao zalog.
  - **Prednosti:** Veća energetska efikasnost i potencijal za bolju skalabilnost.
  - **Mane:** Rizik centralizacije i ekonomska nepravda prema manjim učesnicima.
- **Delegated Proof of Stake (DPoS):**
  - Korisnici biraju delegate koji su odgovorni za verifikaciju i dodavanje novih blokova. Delegati se biraju glasanjem.
  - **Prednosti:** Brža potvrda transakcija i veća skalabilnost.
  - **Mane:** Potencijalna centralizacija moći među delegatima.

- **Practical Byzantine Fault Tolerance (PBFT):**
  - Dizajniran za sisteme sa manjim brojem čvorova, PBFT omogućava konsenzus čak i u prisustvu bizantijskih (zlonamernih) čvorova.
  - **Prednosti:** Visoka efikasnost i niska latencija.
  - **Mane:** Nije skalabilan za veće mreže sa hiljadama čvorova.

7.3 Otpornost na napade

Jedan od ključnih izazova distribuiranog konsenzusa je otpornost na različite napade, kao što su:

- **51% napad:** Ako napadač kontroliše više od 50% računarske snage (u PoW) ili uloga (u PoS), može manipulisati mrežom i dvostruko potrošiti kriptovalutu.
- **Sybil napad:** Napadač stvara mnoge lažne identitete kako bi dobio neproporcionalan uticaj na mrežu.
- **DDoS napad:** Distribuirani napad uskraćivanjem usluge može ometati rad čvorova i destabilizovati mrežu.

7.4 Efikasnost i skalabilnost

Postizanje konsenzusa u velikim distribuiranim mrežama može biti izazovno zbog:

- **Vreme potvrde:** Veće mreže mogu imati duže vreme potvrde zbog potrebe za komunikacijom među velikim brojem čvorova.
- **Računarski resursi:** Konsenzus mehanizmi poput PoW zahtevaju značajne računalne resurse, što može biti neefikasno.
- **Propusnost:** Ograničeni broj transakcija koje mreža može obraditi u jedinici vremena može ograničiti skalabilnost.

7.5 Zaključak

Distribuirani konsenzus je ključni izazov za blockchain tehnologiju, a problemi kao što su bizantijski generali, otpornost na napade i efikasnost moraju biti rešeni kako bi blockchain mreže bile sigurne, skalabilne i efikasne. Različiti konsenzus mehanizmi pružaju različita rešenja za ove probleme, ali svaki ima svoje prednosti i nedostatke koje treba pažljivo razmotriti pri implementaciji blockchain sistema.

8 Konsenzus zasnovan na dokazu rada (Proof of Work)

Proof of Work (PoW) je jedan od najpoznatijih i najčešće korišćenih konsenzus algoritama u blockchain tehnologiji. PoW algoritam se koristi za postizanje distribuiranog konsenzusa i obezbeđivanje sigurnosti i integriteta blockchain mreže. Ovaj algoritam je prvi put implementiran u Bitcoin mreži, a kasnije je usvojen i u mnogim drugim kriptovalutama.

8.1 Osnovni koncept

Proof of Work funkcioniše tako što rudari (miners) takmiče u rešavanju složenih matematičkih problema. Prvi rudar koji reši problem ima pravo da doda novi blok u blockchain i bude nagrađen kriptovalutom. Proces rešavanja problema zahteva značajnu računarsku snagu, što otežava manipulaciju mrežom.

8.2 Kako funkcioniše PoW

1. **Kreiranje bloka:**

- Rudari prikupljaju transakcije koje su emitovane u mreži i formiraju blok transakcija.

2. **Hash funkcija:**

- Rudari koriste kriptografsku hash funkciju (npr. SHA-256) za generisanje hash vrednosti bloka.

3. **Poteškoća (difficulty):**

- PoW algoritam postavlja određeni nivo poteškoće koji rudari moraju zadovoljiti. Poteškoća se često podešava kako bi se obezbedilo da mreža može dodati novi blok otprilike svakih 10 minuta (u slučaju Bitcoina).

4. **Rješavanje problema:**

- Rudari iterativno menjaju jedan parametar u bloku, poznat kao "nonce", dok ne pronađu hash vrednost koja zadovoljava uslov poteškoće (npr. hash mora započeti s određenim brojem nula).

5. **Verifikacija:**

- Kada jedan rudar pronađe odgovarajući hash, on emitira blok u mrežu. Ostali čvorovi proveravaju validnost bloka i hash vrednosti.

6. **Dodavanje bloka:**

- Ako je blok validan, dodaje se u blockchain, a rudar koji je rešio problem dobija nagradu u obliku novokreirane kriptovalute (npr. novi bitcoini) i/ili naknade za transakcije unutar bloka.

8.3 Prednosti PoW

- **Sigurnost:**
  - PoW je vrlo siguran jer zahteva značajnu količinu računalne snage za kreiranje novog bloka, čineći napade poput đouble-spending"vrlo skupim i nepraktičnim.
- **Decentralizacija:**
  - PoW omogućava bilo kome s potrebnom računalnom opremom da učestvuje u mreži kao rudar, potičući decentralizaciju.

8.4 Nedostaci PoW

- **Visoka energetska potrošnja:**
  - Rješavanje PoW problema zahteva ogromne količine energije, što je ekološki neodrživo i skupo.
- **Centralizacija rudarenja:**
  - Vremenom, rudarenje može postati centralizovano u velikim rudarskim bazenima (pools), što može ugroziti decentralizaciju mreže.

8.5 Primjeri korišćenja PoW

- **Bitcoin:**
  - Najpoznatiji primjer PoW konsenzus algoritma. Bitcoin koristi SHA-256 hash funkciju za kreiranje novih blokova.
- **Ethereum:**
  - Ethereum je koristio PoW algoritam (Ethash) do prelaska na Proof of Stake (PoS) konsenzus mehanizam kroz nadogradnju poznatu kao Ethereum 2.0.

8.6 Zaključak

Proof of Work je moćan alat za postizanje konsenzusa u decentralizovanim mrežama, ali sa sobom nosi i izazove, posebno u kontekstu energetske efikasnosti. Iako ostaje temelj mnogih blockchain sistema, razvoj novih konsenzus mehanizama kao što su Proof of Stake (PoS) ukazuje na evoluciju u pravcu održivijih rešenja.

9 Koncenzus zasnovan na dokazu ulaganja (Proof of Stake)

Konzensus zasnovan na dokazu ulaganja (eng. *Proof of Stake*, PoS) je metod verifikacije transakcija i postizanja konsenzusa u blokčejn mrežama. Za razliku od tradicionalnog dokaza o radu (eng. *Proof of Work*, PoW), koji zahteva značajnu računarsku snagu za rešavanje složenih matematičkih problema, PoS se oslanja na količinu kriptovalute koju korisnik poseduje i koju je spreman da uloži (stakuje) kao zalog.

Osnovni principi PoS su:

- **Validacija transakcija:** U PoS sistemu, validatori (takođe poznati kao *stakers*) potvrđuju transakcije i dodaju nove blokove u blokčejn. Validatori su izabrani na osnovu količine kriptovalute koju su uložili, odnosno stakovali.
- **Izbor validatora:** Što više kriptovalute korisnik uloži, veća je verovatnoća da će biti izabran kao validator. Izbor može biti nasumičan, ali verovatnoća izbora raste s povećanjem uloga.
- **Nagrade:** Validatori dobijaju nagrade u obliku novih kriptovalutnih jedinica ili transakcionih naknada za uspešno dodavanje blokova u blokčejn.
- **Bezbednost:** PoS sistemi su dizajnirani tako da obeshrabre zlonamerne radnje. Ako validator pokuša da prevari sistem, može izgubiti deo ili celokupan uložen zalog.

PoS ima nekoliko prednosti u odnosu na PoW:

- **Energetska efikasnost:** PoS troši značajno manje energije jer ne zahteva intenzivnu računarsku obradu.
- **Decentralizacija:** PoS može povećati decentralizaciju jer ne zahteva skupe specijalizovane hardvere, omogućavajući većem broju korisnika da učestvuju u mreži.
- **Brže transakcije:** PoS može omogućiti brže potvrđivanje transakcija jer nije ograničen brzinom rešavanja matematičkih problema.

U zaključku, konsenzus zasnovan na dokazu ulaganja predstavlja alternativni pristup postizanju sigurnosti i verifikacije transakcija u blokčejn mrežama, sa značajnim prednostima u pogledu energetske efikasnosti i decentralizacije.

10 Stanje blockchain-a: model zasnovan na transakcijama i na računima

Blokčejn tehnologija koristi dva osnovna modela za praćenje stanja mreže: model zasnovan na transakcijama (eng. *Transaction-based model*) i model zasnovan na računima (eng. *Account-based model*). Ova dva modela se razlikuju u načinu na koji beleže i ažuriraju stanje kriptovaluta i ostalih digitalnih sredstava.

Model zasnovan na transakcijama

Model zasnovan na transakcijama, takođe poznat kao UTXO (eng. *Unspent Transaction Output*) model, koristi se u Bitcoin mreži. Osnovni principi ovog modela su:

- **Transakcije:** Svaka transakcija troši prethodne neiskorišćene izlaze (UTXO) kao ulaze i stvara nove izlaze. Izlazi predstavljaju količinu kriptovalute koja može biti potrošena u budućim transakcijama.
- **Stanje:** Stanje mreže se određuje kao skup svih neiskorišćenih transakcijskih izlaza (UTXO). Svaki UTXO je jedinstven i može biti potrošen samo jednom.
- **Verifikacija:** Da bi se verifikovala transakcija, potrebno je proveriti autentičnost ulaza, tj. da li su UTXO-ovi legitimni i neiskorišćeni.

Prednosti UTXO modela uključuju visoku sigurnost i jednostavnost verifikacije transakcija, dok su nedostaci složenost u praćenju stanja i veća potrošnja memorije.

Model zasnovan na računima

Model zasnovan na računima koristi se u Ethereum mreži. Osnovni principi ovog modela su:

- **Računi:** Svaki korisnik ima nalog (račun) koji sadrži informacije o stanju kriptovalute, kao i druge relevantne podatke (npr. pametni ugovori).
- **Transakcije:** Transakcije direktno menjaju stanja računa. Svaka transakcija prenosi određenu količinu kriptovalute sa jednog računa na drugi.
- **Stanje:** Stanje mreže se definiše kao skup stanja svih računa u mreži.
- **Verifikacija:** Verifikacija transakcija uključuje proveru potpisa i stanja računa pošiljaoca kako bi se osiguralo da ima dovoljno sredstava za izvršenje transakcije.

Prednosti modela zasnovanog na računima uključuju jednostavnost upravljanja stanjima i niže memorijske zahteve, dok su nedostaci složenija verifikacija i potencijalno niža sigurnost u poređenju sa UTXO modelom.

Zaključak

Oba modela imaju svoje prednosti i nedostatke i prikladni su za različite vrste aplikacija. Model zasnovan na transakcijama pruža veću sigurnost i jednostavnost verifikacije, dok model zasnovan na računima omogućava lakše upravljanje stanjima i niže memorijske zahteve. Izbor modela zavisi od specifičnih potreba blokčejn mreže i ciljeva koje želi postići.

11 Struktura blockchain lanca

Blockchain je distribuirana i decentralizovana baza podataka koja čuva kontinuirani lanac blokova. Svaki blok u lancu sadrži skup transakcija, a svi blokovi su povezani kriptografski putem hash funkcija. Struktura blockchain lanca može se opisati sledećim elementima:

- **Blok:** Osnovna jedinica u blockchainu. Svaki blok sadrži skup transakcija, hash vrednost prethodnog bloka, vremensku oznaku, nonce, i druge relevantne podatke. Struktura jednog bloka može se predstaviti sledećim elementima:
  - *Zaglavlje bloka (Block Header):* Sadrži meta podatke o bloku, uključujući:
    - **Hash prethodnog bloka:** Kriptografski hash vrednost prethodnog bloka u lancu.
    - **Merkle Root:** Kriptografski hash vrednost korena Merkle drveta, koje se koristi za efikasnu i sigurnu verifikaciju transakcija unutar bloka.
    - **Vremenska oznaka:** Beleži vreme kreiranja bloka.
    - **Nonce:** Nasumični broj koji rudari menjaju dok ne pronađu validnu hash vrednost koja zadovoljava uslove poteškoće (difficulty).

        * **Poteškoća (Difficulty):** Nivo težine koji određuje koliko je teško pronaći validnu hash vrednost za novi blok.
    - *Telo bloka (Block Body):* Sadrži sve transakcije uključene u blok.

- **Lanac blokova (Blockchain):** Sekvencijalni niz blokova, gde je svaki blok povezan sa prethodnim blokom putem hash vrednosti, formirajući kontinuirani lanac od prvog (genesis) bloka do trenutnog bloka. Struktura lanca osigurava integritet i nepromenljivost podataka jer je svaki blok kriptografski vezan za prethodni blok.
- **Genesis blok:** Prvi blok u blockchainu. Genesis blok nema prethodnika i često ima posebne atribute definisane tokom inicijalizacije blockchain mreže.
- **Hash funkcije:** Kriptografski algoritmi koji uzimaju ulazne podatke i generišu jedinstvenu fiksnu dužinu hash vrednosti. U blockchainu, hash funkcije se koriste za povezivanje blokova i osiguranje nepromenljivosti podataka.
- **Merkle drvo:** Struktura podataka koja omogućava efikasnu i sigurnu verifikaciju velikog broja transakcija. Koreni hash vrednost (Merkle Root) uključena je u zaglavlje bloka.

Struktura blockchain lanca osigurava decentralizaciju, transparentnost i sigurnost, omogućavajući distribuiranim mrežama da konsenzusom verifikuju i beleže transakcije bez potrebe za centralizovanim autoritetom.

12 Procesiranje transakcije

Procesiranje transakcije u blockchain mreži obuhvata nekoliko koraka koji osiguravaju validnost, sigurnost i integritet transakcija pre nego što budu trajno zabeležene u blockchainu. Glavni koraci procesiranja transakcije uključuju:

1. **Kreiranje transakcije:**
    - Korisnik inicira transakciju koja sadrži informacije o pošiljaocu, primaocu, iznosu kriptovalute, i digitalni potpis pošiljaoca.
    - Transakcija se zatim šalje u mrežu kako bi bila emitovana svim čvorovima (nodes).
2. **Verifikacija transakcije:**
    - Čvorovi u mreži primaju transakciju i proveravaju njenu validnost. Proverava se ispravnost digitalnog potpisa i da li pošiljalac ima dovoljno sredstava za izvršenje transakcije.
    - Ako je transakcija validna, dodaje se u mempool (memorijski bazen nepotvrđenih transakcija) gde čeka da bude uključena u blok.
3. **Formiranje bloka:**
    - Rudari ili validatori prikupljaju nepotvrđene transakcije iz mempool-a i formiraju novi blok. Blok sadrži zaglavlje bloka i telo bloka, koje uključuje sve prikupljene transakcije.
4. **Konsenzus mehanizam:**
    - Blockchain mreža koristi konsenzus algoritam (npr. Proof of Work ili Proof of Stake) kako bi odlučila koji čvor će dodati novi blok u blockchain.
    - U Proof of Work, rudari takmiče u rešavanju kriptografskog problema. Prvi rudar koji reši problem dodaje blok i emituje ga u mrežu.
    - U Proof of Stake, validatori su izabrani proporcionalno njihovom ulogu (stake) u mreži.
5. **Verifikacija i dodavanje bloka:**

- Kada je blok kreiran, emituje se u mrežu gde ga ostali čvorovi verifikuju proverom validnosti transakcija i hash vrednosti.
- Ako je blok validan, dodaje se u blockchain, a transakcije unutar bloka se smatraju potvrđenim.

6. **Ažuriranje stanja:**
   - Nakon dodavanja bloka u blockchain, svi čvorovi ažuriraju svoje kopije blockchaina i stanje računa ili UTXO-a (zavisno od modela) kako bi reflektovali nove transakcije.

Procesiranje transakcije u blockchain mreži obezbeđuje da sve transakcije budu transparentne, sigurne i nepromenljive, zahvaljujući decentralizovanoj prirodi i kriptografskim mehanizmima koji čine osnovu blockchain tehnologije.

13 Sadržaj transakcije i bloka

Blockchain transakcije i blokovi sadrže specifične informacije koje omogućavaju sigurno i transparentno beleženje podataka. Razumevanje strukture i sadržaja transakcija i blokova ključno je za shvatanje funkcionisanja blockchain tehnologije.

13.1 Sadržaj transakcije

Transakcija u blockchain mreži obuhvata sledeće elemente:

- **Ulazi (Inputs):**
  - *Identifikator prethodne transakcije (Transaction ID):* Hash vrednost prethodne transakcije iz koje se sredstva prenose.
  - *Indeks izlaza (Output Index):* Indeks specifičnog izlaza u prethodnoj transakciji koji se koristi kao ulaz.
  - *Digitalni potpis (Signature):* Kriptografski potpis vlasnika sredstava, koji dokazuje vlasništvo i autorizaciju prenosa sredstava.
  - *Javni ključ (Public Key):* Javni ključ pošiljaoca, koji omogućava verifikaciju digitalnog potpisa.
- **Izlazi (Outputs):**
  - *Iznos (Amount):* Količina kriptovalute koja se prenosi na adresu primaoca.
  - *Adresa primaoca (Recipient Address):* Kriptografska adresa primaoca sredstava.
- **Podaci (Data):**
  - *Podaci o transakciji (Transaction Data):* Dodatni podaci koji mogu biti uključeni u transakciju, kao što su oznake ili posebne instrukcije.
- **Identifikator transakcije (Transaction ID):**
  - *Hash vrednost transakcije (Transaction Hash):* Kriptografski hash koji jedinstveno identifikuje transakciju.

13.2 Sadržaj bloka

Blok u blockchain mreži sastoji se od sledećih elemenata:

- **Zaglavlje bloka (Block Header):**
  - *Hash prethodnog bloka (Previous Block Hash):* Hash vrednost prethodnog bloka u lancu, što omogućava povezivanje blokova i formiranje lanca.

- *Merkle Root:* Hash vrednost korena Merkle drveta, koja predstavlja sažetak svih transakcija unutar bloka i omogućava efikasnu verifikaciju transakcija.
- *Vremenska oznaka (Timestamp):* Vreme kreiranja bloka.
- *Nonce:* Nasumični broj koji rudari menjaju dok ne pronađu validnu hash vrednost koja zadovoljava uslove poteškoće (difficulty).
- *Poteškoća (Difficulty):* Nivo težine koji određuje koliko je teško pronaći validnu hash vrednost za novi blok.

- **Telo bloka (Block Body):**
  - *Transakcije (Transactions):* Lista svih transakcija uključenih u blok. Svaka transakcija sadrži ulaze, izlaze i dodatne podatke.

Sadržaj transakcija i blokova čini osnovu sigurnosti i integriteta blockchain mreže. Svaka transakcija mora biti validna i proverena od strane mreže pre nego što bude uključena u blok, a svaki blok mora biti kriptografski povezan sa prethodnim blokom, čime se osigurava nepromenljivost i verodostojnost podataka u blockchainu.

14 Merkle drvo (Merkle Tree)

Merkle drvo je struktura podataka koja se koristi u blockchain tehnologiji za efikasno i sigurno verifikovanje integriteta velikog broja transakcija. Ova struktura omogućava kompaktnu reprezentaciju i proveru podataka putem kriptografskih hash funkcija.

14.1 Osnovna struktura Merkle drveta

Merkle drvo je binarno drvo koje se sastoji od sledećih elemenata:

- **Listovi (Leaves):**
  - Svaki list predstavlja hash vrednost jedne transakcije. Transakcije se prvo hashiraju, a zatim se te hash vrednosti koriste kao listovi u drvetu.
- **Čvorovi (Nodes):**
  - Svaki čvor u drvetu (osim listova) predstavlja hash vrednost dva podčvora. Na ovaj način, čvorovi na višim nivoima drveta predstavljaju hash vrednosti kombinacija hash vrednosti sa nižih nivoa.
- **Koren drveta (Merkle Root):**
  - Najviši čvor u drvetu je koren drveta. Merkle root je hash vrednost koja predstavlja sažetak svih transakcija u bloku.

14.2 Kreiranje Merkle drveta

Kreiranje Merkle drveta uključuje sledeće korake:

1. **Hashiranje transakcija:**
   - Svaka transakcija u bloku se hashira koristeći kriptografsku hash funkciju (npr. SHA-256).
2. **Formiranje listova:**
   - Hash vrednosti transakcija postaju listovi Merkle drveta.
3. **Formiranje čvorova:**

- Svaki par listova kombinuje se i hashira kako bi formirao čvor na sledećem nivou drveta. Ako postoji neparan broj listova, poslednji list se duplira.

4. **Ponavljanje procesa:**
   - Proces kombinovanja i hashiranja se ponavlja sve dok se ne dođe do korena drveta.

14.3 Verifikacija transakcija

Merkle drvo omogućava efikasnu verifikaciju pojedinačnih transakcija bez potrebe za proverom celog skupa transakcija. Proces verifikacije uključuje sledeće korake:

1. **Putanja do korena (Merkle Path):**
   - Da bi se verifikovala određena transakcija, potrebno je obezbediti putanju do korena drveta, koja uključuje hash vrednosti svih čvorova koji su potrebni za rekonstrukciju Merkle root-a.
2. **Rekonstrukcija Merkle root-a:**
   - Korišćenjem hash vrednosti iz putanje, validatori mogu rekonstrisati Merkle root i uporediti ga sa onim koji je zapisan u zaglavlju bloka.
3. **Provera integriteta:**
   - Ako rekonstruisani Merkle root odgovara zapisanom Merkle root-u, transakcija je validna i nije izmenjena.

14.4 Prednosti Merkle drveta

- **Efikasnost:**
  - Merkle drvo omogućava proveru integriteta velikog broja transakcija sa minimalnim brojem hash operacija.
- **Bezbednost:**
  - Koristeći kriptografske hash funkcije, Merkle drvo osigurava da su sve transakcije u bloku nepromenljive i da bilo kakva izmena transakcije može biti lako detektovana.
- **Skalabilnost:**
  - Merkle drvo omogućava efikasno skaliranje blockchain mreže jer se proveravanje transakcija može obaviti bez potrebe za pristupom svim transakcijama.

Merkle drvo je ključna komponenta u blockchain tehnologiji, pružajući efikasan način za verifikaciju integriteta i nepromenljivosti transakcija.

15 Pametni ugovori

Pametni ugovori (smart contracts) su samoizvršavajući ugovori sa ugrađenim pravilima i uslovima koji su zapisani u programskom kodu. Ovi ugovori omogućavaju automatsko sprovođenje i izvršavanje ugovorenih obaveza bez potrebe za posrednicima, čime se povećava efikasnost i smanjuju troškovi.

15.1 Osnovni koncept pametnih ugovora

Pametni ugovori funkcionišu na sledeći način:

- **Programski kod:**
  - Ugovorni uslovi i pravila su zapisani u obliku programskog koda koji se izvršava na blockchain platformi.
- **Decentralizacija:**
  - Pametni ugovori se čuvaju i izvršavaju na decentralizovanoj blockchain mreži, što znači da nema centralnog autoriteta ili posrednika.
- **Automatizacija:**
  - Kada se ispune preduslovi definisani u pametnom ugovoru, ugovor se automatski izvršava. Ovo eliminiše potrebu za ručnom intervencijom.

15.2 Komponente pametnog ugovora

Pametni ugovor obuhvata sledeće komponente:

- **Adresa ugovora:**
  - Svaki pametni ugovor na blockchainu ima jedinstvenu adresu koja se koristi za interakciju s njim.
- **Stanje (State):**
  - Stanje pametnog ugovora obuhvata sve podatke koje ugovor čuva, kao što su salda, brojevi transakcija, i drugi relevantni podaci.
- **Funkcije:**
  - Pametni ugovori sadrže funkcije koje definišu kako korisnici mogu interagovati s ugovorom. Ove funkcije su implementirane u programskom kodu i izvršavaju se kada ih korisnici pozovu.

15.3 Izvršavanje pametnog ugovora

Proces izvršavanja pametnog ugovora uključuje sledeće korake:

1. **Inicijacija:**
   - Korisnik inicira transakciju koja poziva funkciju pametnog ugovora. Transakcija se šalje u blockchain mrežu.
2. **Verifikacija:**
   - Čvorovi u mreži verifikuju transakciju i proveravaju uslove definisane u pametnom ugovoru.
3. **Izvršavanje:**
   - Ako su svi uslovi ispunjeni, pametni ugovor se automatski izvršava, a rezultati se beleže u blockchain.

15.4 Prednosti pametnih ugovora

- **Efikasnost:**
  - Automatizacija procesa eliminiše potrebu za posrednicima, što smanjuje troškove i ubrzava transakcije.
- **Transparentnost:**
  - Kod pametnog ugovora i sve transakcije su javno dostupni na blockchainu, što omogućava transparentnost i verifikaciju.
- **Sigurnost:**
  - Pametni ugovori su zaštićeni kriptografijom i izvršavaju se na decentralizovanoj mreži, što smanjuje rizik od manipulacije i prevara.

15.5 Primeri upotrebe pametnih ugovora

Pametni ugovori se mogu koristiti u različitim oblastima, uključujući:

- **Finansije:**
  - Automatizacija plaćanja, kredita, i osiguranja.
- **Nekretnine:**
  - Ugovori o kupovini i zakupu nekretnina.
- **Lanac snabdevanja:**
  - Praćenje proizvoda kroz lanac snabdevanja i automatizacija isporuka.
- **Glasanje:**
  - Implementacija sigurnih i transparentnih sistema za elektronsko glasanje.

Pametni ugovori predstavljaju značajan napredak u tehnologiji i imaju potencijal da transformišu mnoge industrije kroz povećanje efikasnosti, sigurnosti i transparentnosti.

16 Skalabilnost blockchain-a, rollupovi, L1/L2 rešenja

Skalabilnost je jedno od glavnih izazova s kojima se suočava blockchain tehnologija. Kako bi se obezbedila efikasnost i brzina transakcija na blockchain mrežama, razvijena su različita rešenja, uključujući rollupove i Layer 1 (L1) i Layer 2 (L2) rešenja.

16.1 Skalabilnost blockchain-a

Skalabilnost blockchain-a odnosi se na sposobnost mreže da obradi veći broj transakcija u jedinici vremena. Trenutni problemi skalabilnosti uključuju:

- **Ograničeni broj transakcija:** Tradicionalne blockchain mreže poput Bitcoina i Ethereuma mogu obraditi ograničeni broj transakcija po sekundi (TPS), što nije dovoljno za masovno usvajanje.
- **Visoke naknade:** Kako se mreža zaguši, transakcijske naknade rastu, što čini male transakcije neisplativima.
- **Vreme potvrde:** Vreme potrebno za potvrdu transakcija može biti dugo, što smanjuje korisničko iskustvo.

16.2 Layer 1 (L1) rešenja

Layer 1 rešenja podrazumevaju promene i optimizacije na osnovnom blockchain protokolu kako bi se poboljšala skalabilnost. Neka od L1 rešenja uključuju:

- **Povećanje veličine bloka:** Povećanje veličine bloka omogućava većem broju transakcija da budu uključene u svaki blok.
- **Sharding:** Deljenje blockchain mreže na manje delove (shardove) koji mogu paralelno obrađivati transakcije, čime se povećava ukupni kapacitet mreže.
- **Poboljšanje konsenzus algoritama:** Razvoj efikasnijih konsenzus algoritama koji mogu brže postići dogovor među čvorovima, kao što su Proof of Stake (PoS) ili Delegated Proof of Stake (DPoS).

16.3 Layer 2 (L2) rešenja

Layer 2 rešenja se grade na vrhu osnovnog blockchaina (L1) i omogućavaju skaliranje transakcija van osnovnog lanca, čime smanjuju opterećenje osnovne mreže. Neka od L2 rešenja uključuju:

- **State Channels:** Dvosmerni kanali između korisnika koji omogućavaju brze i jeftine transakcije van lanca. Kada se kanal zatvori, konačni rezultat se beleži na blockchainu.
- **Plazma:** Framework za kreiranje child"blockchaina koji periodično šalju podatke nazad na osnovni lanac radi sigurnosti. Omogućava obradu velikog broja transakcija van glavnog lanca.
- **Rollupovi:** Tehnika koja agregira veliki broj transakcija u jedan "rollup"koji se zatim beleži na glavnom lancu kao jedna transakcija. Postoje dva glavna tipa rollupova:
  - **ZK Rollupovi (Zero-Knowledge Rollups):** Koriste kriptografske dokaze (zero-knowledge proofs) za verifikaciju transakcija van lanca. Validnost svih transakcija može se proveriti na lancu bez otkrivanja svih podataka.
  - **Optimistic Rollupovi:** Pretpostavljaju da su sve transakcije validne i proveravaju ih samo u slučaju spora ili sumnje. Ovaj pristup omogućava brže transakcije uz mogućnost izazova spornih transakcija.

16.4 Prednosti i izazovi L1 i L2 rešenja

- **Layer 1 (L1) rešenja:**
  - *Prednosti:* Direkno unapređenje osnovnog protokola može poboljšati sigurnost i decentralizaciju mreže.
  - *Izazovi:* Ove promene često zahtevaju hard forkove, što može izazvati neslaganja u zajednici i podelu mreže.
- **Layer 2 (L2) rešenja:**
  - *Prednosti:* Omogućavaju skaliranje bez promene osnovnog protokola, mogu se brže implementirati i ponuditi veći kapacitet za transakcije.
  - *Izazovi:* Kompleksnost implementacije, potreba za dodatnim sigurnosnim merama i interoperabilnošću sa osnovnim lancem.

Skalabilnost blockchain-a je ključna za masovno usvajanje i efikasnost mreže. Kroz kombinaciju Layer 1 i Layer 2 rešenja, blockchain tehnologija može prevazići trenutne ograničenja i omogućiti brže, jeftinije i sigurnije transakcije.

17 ERC20 tokeni i ERC721 tokeni

Ethereum blockchain omogućava kreiranje i upravljanje različitim vrstama tokena kroz upotrebu standarda. Dva najpoznatija standarda za tokene na Ethereum mreži su ERC20 i ERC721. Ovi standardi definišu skup pravila koja tokeni moraju slediti, što omogućava interoperabilnost i jednostavno integrisanje u različite aplikacije.

17.1 ERC20 tokeni

ERC20 (Ethereum Request for Comments 20) je standard za fungibilne tokene na Ethereum mreži. Fungibilni tokeni su identični i mogu se međusobno zamenjivati, slično kao što je to slučaj sa valutama (npr. jedan dolar je jednak svakom drugom dolaru).

17.1.1 Osnovne karakteristike ERC20 tokena

ERC20 standard definiše osnovne funkcionalnosti i metode koje svaki ERC20 token mora implementirati:

- **totalSupply:** Vraća ukupnu količinu tokena koja je ikada kreirana.
- **balanceOf:** Vraća trenutni balans određenog računa.
- **transfer:** Prenosi određenu količinu tokena sa trenutnog računa na drugi račun.
- **transferFrom:** Omogućava prenos tokena sa jednog računa na drugi, uz prethodno odobrenje.
- **approve:** Omogućava vlasniku računa da dozvoli drugom računu da troši određeni iznos tokena.
- **allowance:** Vraća preostali iznos tokena koji određeni račun može potrošiti u ime vlasnika računa.

17.1.2 Prednosti ERC20 tokena

- **Interoperabilnost:** Standardizacija omogućava da različiti tokeni budu kompatibilni sa novčanicima, berzama i drugim aplikacijama.
- **Jednostavnost kreiranja:** Razvojni programeri mogu lako kreirati i implementirati nove tokene koristeći postojeće šablone.
- **Široka primena:** ERC20 tokeni se koriste za različite svrhe, uključujući kriptovalute, vlasničke tokene i sredstva u decentralizovanim finansijama (DeFi).

17.2 ERC721 tokeni

ERC721 (Ethereum Request for Comments 721) je standard za nefugibilne tokene (NFT) na Ethereum mreži. Nefugibilni tokeni su jedinstveni i ne mogu se međusobno zamenjivati, što ih čini idealnim za reprezentaciju jedinstvenih predmeta poput digitalne umetnosti, kolekcionarskih predmeta i imovine u igrama.

17.2.1 Osnovne karakteristike ERC721 tokena

ERC721 standard definiše osnovne funkcionalnosti i metode koje svaki ERC721 token mora implementirati:

- **balanceOf:** Vraća broj tokena koje određeni račun poseduje.
- **ownerOf:** Vraća vlasnika određenog tokena.
- **safeTransferFrom:** Bezbedno prenosi token sa jednog računa na drugi, proveravajući da li je primaoc sposoban da primi NFT.
- **transferFrom:** Prenosi token sa jednog računa na drugi.

- **approve:** Odobrava drugom računu pravo da prenese određeni token.
- **getApproved:** Vraća račun koji je odobren za prenos određenog tokena.
- **setApprovalForAll:** Odobrava ili opoziva pravo drugom računu da prenosi sve tokene vlasnika.
- **isApprovedForAll:** Proverava da li je određeni račun odobren za prenos svih tokena vlasnika.

17.2.2 Prednosti ERC721 tokena

- **Jedinstvenost:** Svaki ERC721 token je jedinstven, što ga čini idealnim za reprezentaciju digitalne umetnosti, kolekcionarskih predmeta i druge jedinstvene imovine.
- **Sledljivost vlasništva:** Blockchain tehnologija omogućava transparentno i nepovratno praćenje vlasništva nad NFT-ovima.
- **Interoperabilnost:** ERC721 standard omogućava da NFT-ovi budu kompatibilni sa različitim platformama i aplikacijama.

17.3 Zaključak

ERC20 i ERC721 standardi omogućavaju kreiranje fungibilnih i nefugibilnih tokena na Ethereum mreži, pružajući osnovu za širok spektar aplikacija u decentralizovanim finansijama, digitalnoj umetnosti, igrama i mnogim drugim oblastima. Standardizacija tokena osigurava interoperabilnost i olakšava integraciju sa različitim platformama i aplikacijama.