Odgovori na ispitna pitanja BLOCKCHAIN

1.Osobine blockchain-a

U današnje vreme, zbog jedinstvenih karakteristika blockchain tehnologije, ona se koristi u različitim aplikacijama širom različitih industrija i slučajeva upotrebe. Neke od važnih karakteristika blockchain tehnologije su:

1.Poboljšana sigurnost Blockchain tehnologija podržava poboljšanu sigurnost decentralizacijom svih informacija koje se čuvaju u blockchain mreži. Informacije ne mogu biti manipulisane, a heš jednog čvora povezan je sa prethodnim čvorom; promene u hešu jednog čvora dovode do promena u heševima svih čvorova.

2.Decentralizovana mreža Decentralizacija je jedna od glavnih karakteristika blockchain mreže. To znači da nema upravljanja ili centralnog autoriteta u blockchain mreži. Ovde, grupa čvorova vrši kontrolu nad celokupnom mrežom čineći je decentralizovanom. Blockchain mreža postavlja korisnike na određene pozicije. Dakle, korisnici mogu direktno koristiti blockchain mrežu putem interneta i čuvati svoje podatke na blockchain mreži jer mreži nije potreban centralni autoritet.

3.Nepromenljivost Podaci u blockchain mreži se smatraju trajnim zapisom transakcija. Jednom kada se blok doda u mrežu, ne može se menjati ili brisati. Svaki čvor proverava validnost transakcije kada je dodata u mrežu. U blockchain mreži, ako većina čvorova validira transakciju, tada se dodaje u javnu knjigu. Ovo obezbeđuje poverenje u blockchain mrežu.

4.Transparentnost Blockchain tehnologija je dizajnirana da transparentno kontroliše korisničke podatke. Blokovi podataka su dostupni svakom čvoru i čvorovi mogu koristiti podatke prema svojim potrebama.

5. Distribuirana knjiga Nezavisni računari ili čvorovi se koriste u distribuiranim knjigama kako bi delili, beležili i sinhronizovali transakcije u svojim elektronskim knjigama. Ovde, podaci se ne čuvaju centralno kao u tradicionalnoj knjizi. Obično, javna knjiga javno pruža sve informacije o transakciji i njenim učesnicima. Privatne blockchain mreže funkcionišu na nešto drugačiji način.

6. Konsenzus U blockchain mreži, algoritmi konsenzusa su osnovna karakteristika arhitekture te mreže. Ovi algoritmi konsenzusa pomažu mreži da donosi odgovarajuće

odluke na osnovu situacije. Ako postoji milion čvorova u mreži, algoritam konsenzusa je neophodan za validaciju određene transakcije. Dakle, sve odluke mreže su direktno ili indirektno pobednički scenario te mreže. Konsenzusni mehanizam je jedna od velikih snaga distribuirane knjige.

7. Brže poravnanje Tradicionalni bankarski sistemi su spori jer nekada treba dani da se završi transakcija. U poređenju sa ovim tradicionalnim sistemima, blockchain tehnologija podržava bržu tehniku poravnanja. Dakle, korisnici mogu završiti transakcije u kratkom vremenskom periodu, što ne čini ceo sistem sporim. Iako postoje slučajevi u kojima mreža ne podržava previše korisnika, kao i brže poravnanje, danas se blockchain koristi za brze transakcije, i može se koristiti za slanje novca vršnjacima.

8. Hronološki podaci Bockchain tehnologija je lanac blokova. Ovde, svaki blok čuva informacije o transakciji i povezan je sa prethodnim blokom putem kriptografskog heša. Sledeći blok sa istom vrednošću heša povezan je sa svojim prethodnim blokom. Ovi povezani blokovi u mreži formiraju hronološki lanac informacija, čime se beleži prenos vlasništva i uspostavlja poreklo.

9. Pametni ugovori Pametni ugovor je jedna od važnih karakteristika blockchain mreže. U blockchain mreži, to su programi, kodovi ili logike korišćeni za uslove, odredbe ili automatizovane zadatke mreže. Pametni ugovori su najkorisniji u dozvoljenom blockchainu. Oni pomažu u brzom završavanju bilo koje poravnanje. Pametni ugovori mogu automatizovati mnoge zadatke blockchain mreže**.**

2.Prednosti i mane blockchain tehnologije

Prednosti:

1. Integritet podataka: U blokčejn mreži, detalji transakcija koje se dodaju mreži ne mogu se izmeniti, tj. informacije su nepromenljive. Na ovaj način, blokčejn mreža podržava integritet podataka, kao i visoku bezbednost.
2. Verifikacija: Podaci se čuvaju na decentralizovan način, pa svi korisnici blokčejn mreže lako mogu da verifikuju tačnost podataka koristeći nulto-znanje dokaz.
3. Decentralizacija: Ovo je jedna od glavnih prednosti blokčejn mreže. Kako se hiljade uređaja koristi za čuvanje podataka u blokčejn mreži, čitav sistem, kao i podaci, visoko su otporni na bilo kakav tehnički kvar i zlonamerne napade. Najvažnije, ovi uređaji se nalaze na distribuiranoj mreži. Distribuirani i sinhronizovani podaci preko svih entiteta čine čitav sistem decentralizovanim i efikasnim.
4. Tragljivost: Tehnologija blokčejna je dizajnirana tako da može stvoriti neopozivu revizorsku stazu, čineći je pristupačnom i jednostavnom za praćenje bilo koje informacije iz te lance.

5. Bezbednost: Blokčejn mreža je obezbeđena jer je svaki entitet te mreže opremljen jedinstvenim hešom koji je povezan sa prethodnim čvorom. Takođe, enkripcijska tehnika blokčejna otežava hakovanje čitave blokčejn mreže hakerima i napadačima.
6. Brža obrada: Tradicionalni bankarski sistemi zahtevaju mnogo vremena za obradu i završetak transakcija. Međutim, nakon uvodjenja tehnologije blokčejna, brzina transakcija se značajno povećala, smanjujući vreme na gotovo minut ili čak sekundu.
7. Bez mešanja trećih strana: Danas, nijedna finansijska institucija ili vlada nema kontrolu nad bilo kojom kriptovalutom, koja se uglavnom operiše koristeći tehnologiju blokčejna. To implicira da nema mešanja treće strane u blokčejn mrežu.
8. Automatizacija: Pametni ugovori i dostupnost podataka na svakom čvoru smanjuju složenost procesa validacije. To dalje pomaže u automatizaciji procesa i poboljšanju brzine transakcija.

Mane:

1. Potrošnja energije: Potrošnja energije u blokčejn mreži tokom procesa rudarenja je relativno visoka. Ovo je uglavnom zato što kada se novi čvor doda u mrežu, mora biti komunikacije sa svim ostalim čvorovima istovremeno. Održavanje vođenja u realnom vremenu takođe je jedan od glavnih razloga za potrošnju energije.

2. Nezrelost: Ipak, blokčejn tehnologija je u ranoj fazi, tako da obični ljudi nemaju puno poverenja u nju zbog nedostatka znanja. Ljudi nisu spremni da ulažu u nju.

3. Vremenska zahtevnost: Da bi se dodao novi blok u blokčejn mrežu, rudari moraju izračunati vrednost nonce-a. U mnogim slučajevima, ovaj proces izračunavanja je veoma vremenski zahtevan, kao i troši mnogo resursa.

4. Pravne formalnosti i standardi: Danas mnoge zemlje rade na blokčejn tehnologiji. Međutim, to postaje prepreka za prihvatanje Bitkoina u mnogim zemljama od strane njihovih finansijskih institucija. Osim toga, pošto je blokčejn još u ranoj fazi, ne postoje specifični standardi.

5. Napadi sa 51%: Blokčejn mreža se smatra sigurnom. Međutim, mogu postojati neki sigurnosni napadi u blokčejn mreži, a napad sa 51% je jedan od najčešćih napada. Ovaj napad se događa kada entitet može da upravlja sa više od 50% čvorova blokčejn mreže, što mu omogućava da poremeti blokčejn mrežu namerno menjajući ili isključujući redosled transakcija.

6. Robusnost mreže: Sve aplikacije bazirane na blokčejnu imaju osnovnu poslovnu logiku. Ova logika opisuje kako aplikacije funkcionišu u smislu poslovnih zahteva, i to je fiksna logika koja se ne može preprojektovati nakon razvoja aplikacije.

7. Teškoće u razvoju: Primena složenih protokola za postizanje konsenzusa je veoma važna. Brza implementacija nije moguća, već je potrebno duboko poznavanje različitih programskih jezika kako bi se razvio aplikacija bazirana na blokčejnu.

8. Skladištenje: U blokčejn mreži, svaki blok ili transakcija se dodaje u lanac ili mrežu, što povećava veličinu baze podataka, a veličina knjiga raste tokom vremena. Trenutno, Bitkoin zahteva oko 200 GB prostora za skladištenje. Dakle, u mnogim slučajevima, to stvara problem za korisnike.

9. Skalabilnost: Skalabilnost se smatra jednim od glavnih nedostataka blokčejn tehnologije jer je veličina bloka blokčejn mreže fiksna. Ako je veličina bloka bilo koje blokčejn mreže 1 MB, može samo sačuvati manje detalja transakcija na određenom bloku.

3.Primene Blockchain tehnologije

1.Primene u Bankarstvu i finansijama

Blockchain tehnologija ima široku primenu u bankarstvu i finansijama, uključujući međunarodne plaćanja, kapitalna tržišta, trgovinske finansijske poslove, regulatornu usklađenost, zaštitu od pranja novca i osiguranje.

1. **Međunarodna plaćanja**: Santander One Pay FX koristi blockchain za brže i jeftinije međunarodne transfere.
2. **Kapitalna tržišta**: Blockchain poboljšava evidenciju trgovine i procese poravnanja na kapitalnim tržištima.
3. **Trgovinski finansijski poslovi**: Blockchain olakšava finansijske transakcije u trgovini, posebno van geografskih granica.
4. **Regulatorna usklađenost i revizija**: Blockchain osigurava sigurnost i integritet podataka, olakšavajući reviziju i računovodstvo.
5. **Zaštita od pranja novca**: Blockchain identifikuje korisnike i podržava KYC procedure.
6. **Osiguranje**: Blockchain smanjuje prevaru u osiguranju, pojednostavljuje potraživanja i pruža transparentnost kroz pametne ugovore. Na primer, openIDL podržava osiguravajuće usluge kroz IBM-ov blockchain.

2.Primene u poslovnim sektorima

1. **Upravljanje lancem snabdevanja**: Blokčejn omogućava praćenje robe u realnom vremenu tokom celog lanca snabdevanja, integrišući se sa ERP i IoT uređajima za transparentnost i bezbedno deljenje podataka.
2. **Zdravstvo**: U pametnom zdravstvenom ekosistemu, blokčejn čuva sigurno podatke o pacijentima, omogućavajući pristup podacima bez kompromitovanja privatnosti.
3. **Nekretnine**: Blokčejn olakšava proces kupovine i prodaje nekretnina, ubrzavajući proveru detalja i smanjujući šanse za prevaru.
4. **Mediji:** U industriji medija, blokčejn se koristi za upravljanje digitalnim pravima, autorskim pravima i distribuciju sadržaja, omogućavajući smanjenje troškova, eliminaciju prevare i zaštitu intelektualne svojine.
5. **Energija**: Blokčejn se istražuje u oblastima distribucije električne energije, trgovine energijom i istraživanja gasa, omogućavajući sigurnu i efikasnu transakciju snabdevanja energijom.

3.Primene u vladi

1. Upravljanje evidencijama: Blokčejn olakšava čuvanje podataka o građanima, kao što su bračni status, porodični detalji, datumi rođenja i imovina. To omogućava transparentnost i sigurnost, umesto tradicionalnog, vremenski zahtevnog procesa odlaska građana u vladine kancelarije.

2. Glasanje: Blokčejn omogućava transparentno i sigurno glasanje, sprečavajući manipulacije. Svaki glas je povezan sa jedinstvenim ID-om, a brojanje glasova je olakšano.

3. Porezi: Blokčejn čini proces prijave poreza efikasnijim, smeštajući informacije na privatnu blokčejn mrežu.

4. Nevladine organizacije (NGO): Blokčejn omogućava transparentno praćenje donacija, omogućavajući donatorima da vide kako se njihov novac koristi.

5. Usaglašenost/regulatorni nadzor: Blokčejn čuva ažurirane evidencije u realnom vremenu, što olakšava regulatorima i poslovnim profesionalcima praćenje usaglašenosti.

4.Ostale primene

1. **Veliki podaci**: za skladištenje velikih podataka, blokčejn je idealno rešenje zahvaljujući svojoj neizbrisivosti i proveri podataka na svakom čvoru mreže.
2. U kombinaciji sa **IoT uređajima**, blokčejn omogućava snimanje različitih fizičkih osobina, što je posebno korisno u dijagnostici grešaka.
3. **U poljoprivredi**, blokčejn se koristi za praćenje proizvoda, kao što su kafa, palmino ulje i soja, što pomaže u održavanju kvaliteta i bezbednosti proizvoda. Takođe se istražuje praćenje zemlje poljoprivrednika korišćenjem ove tehnologije.

4. Izazovi za usvajanje Blockchain tehnologiji

1. Cyber napadi: Istraživači su pokazali da blockchain tehnologija nije sigurna protiv različitih cyber napada.Na brimer, 2014. godine dogodio se napad na Bitcoin mrežu na MtGox, uzrokujući gubitak od oko 450 miliona dolara.

2. Duplo trošenje: Duplo trošenje se odnosi na korišcenje iste kriptovalute u nekoliko transakcija. To može biti problem jer se iskorišcava vremenski interval između početka i validacije dve različite transakcije.

3. Izazovi modifikacije podataka: U blockchain mreži je teško promijeniti informacije, što može dovesti do razdvajanja (forkinga) mreže, što može biti mekano ili tvrdo. Tvrdi forking može stvoriti mnoge izazove.

4.**Regulativa o Opstoj uredbi o zaštiti podataka (GDPR)**: Korištenje blockchain tehnologije može biti u sukobu s GDPR-om zbog decentraliziranosti mreže.

5. **Visoka potrošnja energije:** Neke operacije su jako neefikasne, jer se trosi velika kolicina energije

6. **Kompresija podataka**: Čvorovi u blockchain mreži moraju imati mehanizam za kompresiju podataka pre nego što ih sačuvaju na mreži.

7. **Brzina transakcija**: Broj transakcija u sekundi (TPS) je važan jer veći broj transakcija može podržati veće korisničke zahteve.

8. **Troškovi**: Implementacija blockchain tehnologije može biti skupa zbog potrošnje energije, tehnološke kompleksnost i nedostatka razvijenih programera.

9. **Usaglašenost i jasnoća regulatornih zahteva**: U većini slučajeva, blockchain tehnologija nije direktno podržana zakonima i propisima. To može otežati usvajanje u sektorima gde su transakcije vezane za pravne procese.

10. **Interoperabilnost**: Dve blockchain mreže nisu interoperabilne, ali istraživači rade na pronalaženju rešenja za komunikaciju između različitih blockchain mreža.

5.Osnovni elementi blockchain-a

1. Decentralizovano umrežavanje: Blockchain se oslanja na mrežu računara, nazvanih čvorovi blokčejna, koji doprinose računarskim resursima kako bi pomogli u skladištenju i obradi transakcija. Ovi računari rade autonomno i komuniciraju međusobno na način peer-to-peer (P2P), što znači da nema centralne autoritete.

2. Matematička kriptografija: Kriptografske metode osiguravaju sigurnost i integritet podataka u blockchainu. Kriptografski heševi se koriste za povezivanje podatkovnih blokova, a transakcije se šifruju kako bi se osiguralo da su verifikovane i da samo određeni korisnici mogu pristupiti određenim informacijama.

3. Distribuirani konsenzus: Odluke u blockchain mreži donose se na osnovu postignutog konsenzusa među učestvujućim čvorovima, umesto da postoji centralna autoriteta. Protokoli konsenzusa, poput Proof-of-Work i Proof-of-Stake, osiguravaju da je svaka transakcija ili blok dodat na blockchain ona jedina i jedina verzija istine koja je dogovorena od strane svih čvorova.

4.Transakciona evidencija: Blockchain je digitalna evidencija koja hronološki skladišti transakcije u blokovima koji se dodaju na način da se mogu samo dodavati. To omogućava transparentnost i nepovredivost podataka.

5. Pametni ugovori: Aplikacije koje se pokreću na blockchainu implementirane su kao "pametni ugovori", koji su programi koji automatski izvršavaju određene uslove bez ljudske intervencije. Ovi ugovori omogućavaju automatizaciju procesa i osiguravaju dosledno izvršenje uslova.

Ovi elementi čine osnovu blockchain tehnologije i omogućavaju njegovu sigurnost, transparentnost i decentralizaciju.

6.Kriptografski elementi blockchain mreze

Kriptografski elementi su ključni za funkcionisanje blockchain mreže na način koji obezbeđuje sigurnost i nepovredivost podataka. Osnovni koncept koji omogućava ovo je upotreba kriptografskih hash funkcija. U ovom kontekstu, hash funkcija je matematički algoritam koji uzima ulazni podatak bilo koje dužine i pretvara ga u jedinstveni string konstantne dužine, poznat kao hash vrednost. Za blockchain, ove hash vrednosti su ključne, jer omogućavaju jednostavnu proveru integriteta podataka.
Prvo, važno je razumeti kako prethodno-hashiranje (prethodna-hash) funkcioniše između blokova. Svaki blok u blockchainu sadrži informaciju o hash vrednosti prethodnog bloka. Ovo stvara lanac blokova, gde je svaki blok povezan sa prethodnim blokom putem hash vrednosti. Ovo povezivanje je ono što osigurava imutabilnost podataka: bilo kakva promena u prethodnom bloku automatski bi promenila hash vrednost, što bi se odrazilo na sve naredne blokove u lancu, jasno ukazujući na promene i čineći ih lako detektovanim.
Kada govorimo o kriptografskim hash funkcijama, naglasak je na njihovim ključnim osobinama. Prva je **otpornost na sudare**, što znači da je teško pronaći dva različita ulazna podatka koji će proizvesti istu hash vrednost. Ovo je od vitalnog značaja za blockchain, jer osigurava jedinstvenost svakog bloka. Druga važna osobina je **sakrivanje**, što znači da na osnovu hash vrednosti teško je odrediti originalni ulazni podatak. I konačno, treća osobina, poznata kao "**puzzle-friendly**", čini izazovnim pronalaženje odgovarajućeg ulaznog podatka koji će dati željenu hash vrednost. Kombinacija ovih osobina čini kriptografske hash funkcije idealnim alatima za osiguravanje integriteta podataka u blockchainu. Zahvaljujući ovim funkcijama, čak i uz teoretsku mogućnost promene blokova bez detekcije, praktično je nemoguće izvesti takvu manipulaciju. Time se postiže osnovna ideja blockchaina: nepovredivost podataka i poverenje među učesnicima mreže bez potrebe za centralizovanim autoritetom.

7.Problem distribuiranog konsenzusa

Problem distribuiranog konsenzusa, koji je suštinski ključan za funkcionisanje blockchain mreža, leži u postizanju sporazuma među različitim čvorovima o tome koji blok treba dodati u lanac. Različiti algoritmi konsenzusa nude različite pristupe ovom problemu, svaki sa svojim prednostima i manama.

Neki od najčešće korišćenih algoritama konsenzusa u blockchain tehnologiji su:

1. Proof of Work (PoW): Koristi se u Bitcoinu. Minerima je potrebno da reše kriptografski problem kako bi dodali blok u lanac. Iako je PoW siguran, troši velike količine energije i ima ograničenu skalabilnost.Osnovna ideja PoW-a je da se zahteva od korisnika, poznatih kao rudara, da reše kompleksan matematički problem kako bi mogli da dodaju blok transakcija u blockchain.

2.Proof of Capacity (PoC): PoC je skoro sličan PoW-u. Međutim, PoC se oslanja na kapacitet hard diska umesto na računarsku snagu rudara, stoga značajno štedi više energije od PoW-a. U PoC-u, rudari moraju da skladište ogromne skupove podataka, što se naziva parcela, kako bi dobili priliku da rudare novi blok. Dakle, rudari u PoC-u mogu povećati šansu za dodavanje novog bloka tako što čuvaju više parcela. PermaCoin je jedna od kriptovaluta koja koristi PoC. U PoC-u, vreme generisanja bloka je 4 minuta, i ima visoku latenciju

3. Proof of Stake (PoS): Umesto na računarsku moć, PoS se oslanja na vlasništvo nad kriptovalutom. Čvorovi sa više kovanica imaju veću verovatnoću da budu izabrani za dodavanje bloka. Iako je energetski efikasniji od PoW, PoS može dovesti do centralizacije moći.

4. Delegated Proof of Stake (DPoS): Sličan PoS-u, ali umesto da svi čvorovi imaju jednaku šansu, vlasnici tokena glasaju za "svedoke" koji će dodavati blokove. Ovo može poboljšati skalabilnost, ali takođe može dovesti do centralizacije.

5. Practical Byzantine Fault Tolerance (PBFT): Koristi se u privatnim blockchainima kao što je Hyperledger. Zahteva manje resursa od PoW-a i omogućava brz konsenzus, ali nije pogodan za javne mreže zbog ograničene skalabilnosti.

6.Leased Proof of Stake (LPoS): LPoS rešava problem centralizacije PoS-a, a princip rada LPoS-a je isti kao kod PoS-a. Ovaj algoritam konsenzusa podržava čvorove da učestvuju u verifikaciji novih blokova dodavanjem opcije iznajmljivanja. Ovo iznajmljivanje omogućava vlasnicima većeg bogatstva da iznajme svoje bogatstvo ili sredstva na određeno vreme. Čvorovi sa manjim bogatstvom ili saldo mogu uzeti iznajmljena sredstva i povećati šansu za dodavanje novog bloka. Zatim mogu proporcionalno deliti bogatstvo sa vlasnicima većeg bogatstva. Na taj način, čini čitavu mrežu decentralizovanom.

7.Proof of Activity (PoA): PoA je algoritam konsenzusa koji se zasniva na kombinaciji PoW-a i PoS-a. Ovde rudar pokušava da reši funkciju heširanja kako bi pronašao novi

blok kao kod PoW-a. Međutim, novi blok sadrži samo adresu rudara i zaglavlje bez transakcija, a zatim se detalji transakcije dodaju u novi blok. Ovde se set od 10 validatora bira za potpisivanje novog bloka na osnovu zaglavlja rešenog bloka kako bi se postigao konsenzus. Ova operacija se izvršava korišćenjem PoS-a koji je siguran protiv mnogih popularnih napada. Međutim, doživljava veće kašnjenje.

8. Консензус заснован на доказу рада (proof of work)

Dokaz rada: Markus Jakobson je prvi put predložio termin "Dokaz rada" 1999. godine. U PoW-u, sve čvorove mreže blockchaina pokušavaju da reše kriptografsku hash funkciju. Ovde se koristi SHA-256, koji generiše fiksnu vrednost heša od 256 bita. Da bi dodali čvor ili blok korišćenjem PoW-a, rudari pronalaze određeni broj koji rešava kriptografski problem. Ovaj proces je vremenski zahtevan i matematički težak jer rudari koriste pretraživanje brute force-a da bi pronašli broj koji rešava problem. Ovde, ciljni broj podržava težinu mreže. U Bitcoinu, ciljni broj je označen na takav način da proces rudarenja može da se odvija svakih 10 minuta. Napadači ili zlonamerni korisnici mogu da utiču na PoW-based blockchain mrežu ako dobiju kontrolu nad 25% računarske snage putem napada seljačkog rudarenja. Međutim, ovaj napad ne utiče na neprolaznost blockchain mreže. PoW je bio veoma popularan za kriptovalute tokom mnogih godina.

9. Консензус заснован на доказу улагања (proof of stake)

Ovaj algoritam konsenzusa je generalizovana forma PoW-a. U PoS-u, čvorovi se nazivaju validatori. Validatori validiraju izvršenje kako bi zaradili naknadu za transakcije. U ovom algoritmu konsenzusa, nema takmičenja između validatore za rešavanje računarskog problema. Čvor se bira koristeći lutriju za rudarenje novog bloka na osnovu količine stejkholdera. Izabrani čvor koristi digitalnu tehniku potpisa kako bi dokazao vlasništvo nad ulogom. Dakle, u PoS-u nije potrebna velika računarska snaga. Međutim, postoji novi problem jer čvor sa najvećom količinom uloga uvek dobija priliku da dodaju novi blok. Time, indirektno, ponovo postaje centralizovana mreža. Štaviše, u PoS-u, ako izabrani čvor deluje kritično, nema ništa da izgubi. Ovaj problem je poznat kao "ništa na kocki". U ovom algoritmu konsenzusa, sve kovanice su prisutne od prvog dana.

10. Стање блокчејна: модел заснован на трансакцијама и модел заснован на рачунима

Stanje blokčejna može se predstaviti na dva načina: modelom zasnovanim na transakcijama i modelom zasnovanim na računima.
U modelu zasnovanom na transakcijama, kao što je Uneseni izlaz transakcije (UTXO) koji je predložio Bitcoin, svaka transakcija može poslati vrednost jednom ili više primaoca. Ovaj model se sastoji od sledećih informacija:
Polje izlaza: Lista primačkih adresa i iznos fondova koji će biti poslat svakom od njih. Svaki izlaz prenosa naziva se UTXO transakcija.
Polje unosa: Lista UTXO transakcija koje će pružiti fond za transakciju. Ove UTXO-ove prethodno su poslale fondove pošiljaocu i trenutno nisu potrošene.

U modelu zasnovanom na računima, stanje se sastoji od informacija o saldima za svaku adresu. Kada postoji transakcija, saldo pošiljaoca i primaoca će odmah biti ažurirano i sačuvano u stanju. Stoga, kada se upita saldo računa za adresu, ono je trenutno dostupno bez ikakvog izračunavanja.

Ključna razlika je u načinu kako se obrađuju transakcije. U modelu zasnovanom na transakcijama, svaka transakcija može imati više izlaza i unosa, što zahteva pretragu stanja blokčejna da bi se utvrdilo da li su unosi UTXO-ovi zaista neiskorišćeni. Nasuprot tome, u modelu zasnovanom na računima, transakcija se sastoji od samo jedne primačke adrese i iznosa fondova koji se šalje, što omogućava bržu verifikaciju da li pošiljalac ima dovoljno fondova.

Oba modela imaju svoje prednosti i mane. Model zasnovan na transakcijama je kompleksniji i zahteva više resursa za verifikaciju transakcija, ali omogućava transparentnost i praćenje toka fondova. S druge strane, model zasnovan na računima je jednostavniji i brži za obradu transakcija, ali može biti manje transparentan i manje pogodan za složene operacije kao što su "pametni ugovori".

11. Структура блокчејн ланца

Struktura blockchain lanca je takva da se podaci organizuju u nizu blokova podataka, pri čemu svaki blok sadrži informacije o transakcijama, stanju blockchaina ako je primenjivo, i neophodne informacije u zaglavlju bloka. Ključne karakteristike svakog bloka su identifikator bloka (Block ID) i prethodni hash (Previous hash). Identifikator bloka se postavlja kao heš vrednost sadržaja bloka koristeći kriptografsku heš funkciju,

dok se prethodni hash postavlja na identifikator prethodnog bloka na koji je novi blok dodat. Ove informacije su od suštinskog značaja za očuvanje integriteta podataka u lancu. Validacija novog bloka zahteva proveru konzistentnosti prethodnog hasha i validnosti svih prethodnih blokova u lancu. Ova struktura omogućava da se detektuju promene u bilo kom delu lanca, čime se osigurava njegova pouzdanost i celovitost.

12. Процесирање трансакције

Procesiranje transakcija na blockchainu se sastoji od nekoliko koraka koji osiguravaju validnost i integritet transakcija u mreži. Evo detaljnog opisa procesa:

1. Inicijacija transakcije: Korisnik pokreće transakciju putem korisničkog sučelja koje može komunicirati s blockchain mrežom putem API poziva. Transakcija se sastoji od informacija kao što su adresa pošiljaoca, adresa primaoca i iznos koji se šalje.

2. Prijem transakcije od strane čvorova: Kada čvor na mreži prvi put primi transakciju, provodi nekoliko ključnih koraka:

2.1. Prosleđivanje transakcije: Transakcija se prosleđuje susednim čvorovima kako bi se osiguralo da svaki čvor ima informaciju o transakciji.

2.2. Verifikacija transakcije: Čvor proverava da li pošiljalac transakcije ima dovoljno sredstava za slanje. Ako je transakcija validna, stavlja je u mempool - privremenu listu čekanja za transakcije koje će biti uključene u novi blok.

2.3.Kreiranje bloka: Čvor formira novi blok koji uključuje validne transakcije iz mempool-a. Novi blok se dodaje na postojeći lanac blokova, pri čemu se uključuje informacija o prethodnom hash-u (vrednost hash-a prethodnog bloka).

2.4.Ažuriranje bloka: Novi blok se šalje susednim čvorovima kako bi ažurirali svoje kopije blockchaina.

3. Prijem bloka od strane čvorova: Kada čvor primi novi blok, sprovodi sledeće korake:

3.1.Prosleđivanje bloka: Blok se prosleđuje susednim čvorovima radi ažuriranja njihovih kopija blockchaina.

3.2.Validacija bloka: Čvor proverava validnost novog bloka. Ovo uključuje proveru konzistentnosti prethodnog hash-a i validnosti svake transakcije unutar bloka.

3.3.Umetanje bloka: Ako je blok validan, dodaje se na lanac blokova. U suprotnom, blok se ignoriše.

4. Konzensus Kako bi se osigurala konsistentnost blockchaina i rešili potencijalni problemi poput duple potrošnje ili različitih verzija blockchaina na različitim čvorovima, mreža koristi protokole konsenzusa. Ovi protokoli omogućavaju čvorovima da se slože o trenutnom stanju blockchaina, obezbeđujući da se samo jedan blok dodaje kao sledeći u lancu.

Ukratko, procesiranje transakcija na blockchainu uključuje slanje, primanje, verifikaciju i dodavanje transakcija u blokove, kao i validaciju i ažuriranje lanca blokova kako bi se održala konsistentnost mreže. Ovo je ključni deo tehnologije blockchaina koji omogućava decentralizovanu, sigurnu razmenu vrednosti.

13. Садржај трансакције и блока

Svaka **transakcija** u blokčeinu ima nekoliko atributa:

1. **Iznos**: Iznos je digitalna vrijednost koju pošiljatelj želi prenijeti.
2. **Ulaz**: Ulaz predstavlja detalje digitalne imovine koju pošiljatelj želi prenijeti. To uključuje identifikaciju digitalne imovine i njenu vrijednost.
3. **Izlaz**: Izlaz sadrži sve detalje računa primatelja. Ovo uključuje vrijednost digitalne imovine i identitet primatelja. Također uključuje pravila koja primatelj mora poštovati kako bi primio povezanu vrijednost.
4. **Hash transakcije ili ID**: Svaka transakcija ima jedinstveni hash ili ID koji podržava digitalni potpis na temelju kriptografije s javnim ključem.

Sadržaj **bloka** u Bitcoinu obuhvata nekoliko ključnih elemenata:
1. Veličina bloka: Ova vrijednost zauzima 4 bajta i označava ukupnu veličinu bloka u bajtovima.
2. Broj transakcija: Ovo je varijabilna vrijednost koja zauzima od 1 do 9 bajta, označavajući broj transakcija u bloku.
3. Transakcije: Ovaj dio sadrži listu transakcija koje su uključene u blok. Transakcije su varijabilne veličine.
4. Zaglavlje bloka: Ovo je ključni dio bloka koji sadrži važne informacije potrebne za kreiranje i validaciju bloka. Sastoji se od sljedećih polja:
4.1.Verzija: Ova vrijednost, zauzimajući 4 bajta, označava verziju softvera Bitcoin čvora koji je kreira.
4.2.Prethodni hash: Ovo je 32 bajta vrijednosti, koji predstavljaju hash (ID) prethodnog bloka u lancu.
4.3.Merkle korijen hash: Ovo je hash vrijednost od 32 bajta koja predstavlja hash vrijednost uključenih transakcija prema Merkle stablu.

4.4.Vremenska oznaka: Ovaj dio, zauzimajući 4 bajta, označava vrijeme kreiranja bloka u sekundama (Unix epoha).

4.5.Ciljna težina (Difficulty target): Ova vrijednost, zauzimajući 4 bajta, predstavlja prag koji se koristi za Bitcoin-ov Proof-of-Work algoritam.

4.6.Nonce: Ovaj broj, zauzimajući 4 bajta, predstavlja brojač koji se koristi u Bitcoin-ovom Proof-of-Work algoritmu.

ID bloka u Bitcoinu je hash vrijednost njegovog zaglavlja bloka, ne cijelog sadržaja bloka. Ova vrijednost dobiva se hashiranjem zaglavlja bloka dva puta kroz SHA256 algoritam. ID bloka zapravo nije uključen u strukturu podataka bloka, ali ga bilo tko može dobiti primjenom dvostrukog SHA256 hashiranja na zaglavlje bloka.

14. Меркле-дрво

Merkle tree je ključni koncept u blockchain tehnologiji koji omogućava efikasnu i sigurnu verifikaciju podataka. Osnovna ideja Merkle stabla je da se velika količina podataka organizuje u strukturu stabla kako bi se omogućila brza provera integriteta podataka.

Evo kako Merkle stablo funkcioniše u kontekstu blockchain-a:

1. Podaci: Prvo, transakcije ili podaci koji se skladište u blockchainu grupišu se u blokove. Svaki blok može sadržavati više transakcija.
2.Hashing: Za svaki blok, kreira se hash, koji je jedinstveni identifikator bloka. Hash funkcija obrađuje sve podatke u bloku i generiše jedinstveni string određene dužine.
3. Merkle stablo: Nakon što su podaci organizovani u blokove, kreira se Merkle stablo. To je binarno stablo gde su listovi hash vrednosti svake transakcije u bloku, a unutrašnji čvorovi predstavljaju hash vrednosti kombinacija parova listova.
4. Root hash: Kada se formira Merkle stablo, hash vrednost korena stabla (tj. hash vrednost najvišeg nivoa) naziva se "root hash" ili "Merkle root". Ova hash vrednost jedinstveno identifikuje sve podatke u bloku.
5. Verifikacija: Kako bi se proverila integritet podataka u bloku, dovoljno je da se proveri samo root hash. Kada se primi blok, korisnik može dobiti root hash od izvornika (npr. blockchain mreže) i uporediti ga sa root hash-om bloka koji je primio. Ako se root hash-ovi podudaraju, to znači da su podaci u bloku nepromenjeni.

Merkle stablo omogućava efikasnu proveru integriteta podataka jer omogućava da se velika količina podataka proveri sa samo jednom hash vrednošću. Osim toga, omogućava i brzo pronalaženje grešaka ili promena u podacima, što ga čini ključnim alatom u osiguravanju pouzdanosti i sigurnosti blockchaina.

15. Паметни уговори

Pametni ugovori su programski kodovi napisani koristeći visokonivojski programski jezik (na primer, Solidity, Viper, Flint, Bamboo). Najpopularniji jezik za pametne ugovore je Solidity. Ovi ugovori se koriste na blokčejn mrežama kako bi automatizovali izvršenje određenih uslova ili događaja. Na primer, mogu se koristiti za automatizaciju procesa plaćanja ili za stvaranje decentralizovanih aplikacija (DApps).
Solidity je Turing-potpun jezik, što znači da može simulirati bilo koju računsku operaciju. Ovo ga čini veoma moćnim, ali istovremeno može biti izvor problema ako nisu pažljivo napisani i testirani. Za razliku od toga, Script, programski jezik Bitcoina, nije Turing-potpun. To znači da je mnogo lakši i pogodniji za Bitcoinovu jednostavnu svrhu - digitalnu valutu.

Kada se pametni ugovor implementira, on se šalje kao transakcija na blokčejn mrežu kako bi se izvršio na svakom čvoru. Svaki čvor mora imati okruženje za izvršavanje bajtkoda pametnog ugovora. Na Ethereumu, ovo se naziva Ethereum Virtualna Mašina (EVM). EVM je gde žive svi Ethereum nalozi i pametni ugovori. Održava konsenzus za blokčejn.

Iako je jezik pametnog ugovora na Ethereumu Solidity koji je Turing-potpun, EVM je kvazi-Turing-potpuna mašina. To znači da teorijski može izvršiti svaki pametni ugovor, ali će se izvršenje zaustaviti i biti vraćeno ako premaši granicu alokacije resursa koju je odredio implementator.

Pametni ugovori su transparentni jer je izvorni kod javno dostupan. Međutim, iako je kod vidljiv, to ne garantuje da neće imati grešaka ili sigurnosnih propusta. Zbog toga je važno da se pametni ugovori sertifikuju od strane pouzdanih revizora pametnih ugovora kako bi se smanjio rizik od grešaka nakon što su već u upotrebi.

16.Скалабилност блокчејна, ролапови, L1/L2

Skalabilnost blockchain-a je sposobnost sistema da održi i obrađuje povećanu količinu transakcija ili podataka.
Rollup je tehnologija koja se koristi za poboljšanje skalabilnosti i performansi blockchain-a, posebno Ethereum blockchain-a. Ideja iza rollup-a je da se grupišu više transakcija u jedan zapis ili "rolap", koji se zatim beleži na glavnom blockchain-u. Ova grupisanja transakcija omogućavaju smanjenje opterećenja na glavnom blockchain-u, što rezultira bržim i jeftinijim transakcijama.

Postoje dva osnovna tipa rollup-a:

1. Zasnovan na stanju (State-based rollup):

- Ovaj tip rollup-a grupiše transakcije na osnovu promena stanja koje one prouzrokuju u blockchain-u. Ovo značajno smanjuje količinu podataka koju treba čuvati na glavnom blockchain-u.
- Rollup kontrakt na L1 čuva podatke o svim transakcijama, dok samo konačno stanje ili "rolap" ide na glavni blockchain.

2. Zasnovan na transakcijama (Transaction-based rollup):

- Ovaj tip rollup-a se fokusira na čuvanje samih transakcija, ali samo njihovih potpisa i osnovnih informacija, dok se sami podaci o izvršenim transakcijama smeštaju van glavnog blockchain-a. Ovo omogućava brže verifikacije transakcija jer se samo potpisi proveravaju na glavnom blockchain-u.
- Rollup kontrakt na L1 čuva samo osnovne informacije o transakcijama i njihove potpise, dok se sami podaci čuvaju izvan blockchain-a.

Rollup tehnologija pruža značajne prednosti, uključujući poboljšanu skalabilnost, smanjenje troškova transakcija i povećanje brzine obrade. Ovo čini rollup jednim od ključnih rešenja za prevazilaženje izazova sa kojima se suočavaju blockchain mreže, posebno u pogledu efikasnosti i performansi.

1. Layer 1 (L1)

- L1 se odnosi na osnovni sloj blockchain-a, tj. na samu osnovnu tehnologiju ili protokol. To su primarni blockchaini poput Bitcoina, Ethereuma, ili drugih sličnih sistema. Na L1 se izvršavaju sve glavne transakcije i operacije, uključujući slanje i primanje sredstava, izvršavanje pametnih ugovora itd.
- Karakteristike L1 blockchain-a često uključuju visok stepen decentralizacije, sigurnost putem konsenzusa, ali ponekad mogu patiti od ograničenja skalabilnosti, što rezultira sporijim transakcijama i povećanim troškovima.

2. Layer 2 (L2):

- L2 se odnosi na slojeve koji se nadovezuju na osnovni blockchain (L1) i omogućavaju dodatne funkcionalnosti i skalabilnost. To su rešenja koja se grade "iznad" osnovnog sloja, a često se koriste za obradu većeg broja transakcija van samog glavnog blockchaina.
- Rešenja na L2 mogu uključivati različite tehnologije poput sidechainova, rollup-ova, state channels, plasma tehnologija itd.

- Glavni cilj L2 rešenja je poboljšanje performansi i skalabilnosti, smanjenje troškova i povećanje brzine transakcija, dok istovremeno zadržavajući visok nivo sigurnosti i decentralizacije koji se nalazi na L1.

U suštini, L2 rešenja pružaju alternativne puteve za obradu transakcija izvan osnovnog blockchaina, čime se oslobađa opterećenje i smanjuju troškovi transakcija na L1, dok se istovremeno održava integritet i sigurnost celokupnog sistema.

17. ERC20 токени, ERC721 токени

Naravno, evo detaljnijeg objašnjenja. ERC20 i ERC721 su standardi tokena na Ethereum mreži koji definiraju način kako se tokeni mogu kreirati i interakcionirati unutar Ethereum ekosistema.

ERC20 je standard za zamjenjive tokene, što znači da svaki token te vrste može biti zamjenjen za drugi token iste vrste, bez ikakvih dodatnih karakteristika ili osobina koje bi ih razlikovale. Ovaj standard je često korišten za implementaciju kriptovaluta i drugih digitalnih sredstava, jer omogućava jednostavnu razmjenu i transfer tokena među korisnicima i platformama.

S druge strane, ERC721 je standard za nezamjenjive tokene (NFT). Za razliku od zamjenjivih tokena, svaki NFT je jedinstven i neponovljiv. To znači da svaki token koji se kreira prema ERC721 standardu ima svoje jedinstvene karakteristike i ne može biti zamijenjen za drugi token jednake vrste. Ovaj standard se često koristi za digitalno predstavljanje jedinstvenih predmeta ili imovine, kao što su umjetnička djela, kolekcionarski predmeti ili virtualne nekretnine.

Implementacija ovih standarda omogućava širok spektar aplikacija unutar Ethereum ekosistema, uključujući kriptovalute, digitalnu imovinu, igre, umjetnost i druge oblike tokenizacije. Kroz ove standarde, korisnici mogu stvarati, razmjenjivati i trgovati različitim vrstama tokena unutar Ethereum mreže, što doprinosi raznovrsnosti i fleksibilnosti blockchain ekonomije.