Blockchain tehnologija – Pitanja i odgovori

Pitanja i odgovori

1. Pitanje: Objasnite zašto decentralizirani sustav nužno mora biti distribuiran, dok distribuirani sustav ne mora biti decentraliziran.

Odgovor: Decentralizirani sustav nema središnju točku kontrole, pa se podaci i donošenje odluka moraju nalaziti na više neovisnih čvorova, što nužno zahtijeva distribuiranu arhitekturu. Distribuirani sustav može imati više čvorova, ali i dalje centralnu kontrolu. Primjer decentraliziranog i distribuiranog sustava je Bitcoin mreža, dok je primjer distribuiranog, ali ne decentraliziranog sustava infrastruktura Googleovih podatkovnih centara.

—

2. Pitanje: Što sprječava zlonamjerni čvor da izmijeni podatke u starom bloku? Objasnite ulogu hash pokazivača.

Odgovor: Svaki blok sadrži hash prethodnog bloka, čime nastaje lanac hash pokazivača. Izmjena starog bloka mijenja njegov hash i čini sve sljedeće blokove nevažećima. Napadač bi morao ponovno izračunati Proof-of-Work za sve sljedeće blokove i nadmašiti ostatak mreže, što je praktično neizvedivo.

—

3. Pitanje: Koja je funkcija Merkle stabla unutar zaglavlja bloka?

Odgovor: Merkle stablo omogućuje učinkovitu i sigurnu provjeru pripadnosti transakcije bloku pomoću Merkle root hash-a. Umjesto pohrane svih transakcija u zaglavlje, pohranjuje se samo jedan hash, čime se smanjuje količina podataka i povećava skalabilnost.

—

4. Pitanje: Objasnite proces generiranja Bitcoin adrese iz javnog ključa.

Odgovor: Bitcoin adresa nastaje hashiranjem javnog ključa pomoću SHA-256 i RIPEMD-160 algoritama, dodavanjem verzijskog bajta i kontrolne sume te kodiranjem rezultata u Base58Check formatu, koji smanjuje mogućnost pogreške pri unosu.

—

5. Pitanje: Što predstavlja UTXO model i kako čvor provjerava stanje sredstava?

Odgovor: UTXO model temelji se na neiskorištenim izlazima prethodnih transakcija. Čvor provjerava UTXO set i zbraja sve neiskorištene izlaze povezane s korisnikovim adresama kako bi provjerio ima li dovoljno sredstava za transakciju.

—

6. Pitanje: Objasnite otpornost na koliziju hash funkcija.

Odgovor: Otpornost na koliziju znači da je računalno neizvedivo pronaći dva različita ulaza koji daju isti hash. Ovo je ključno za sprječavanje krivotvorenja podataka i očuvanje integriteta blockchaina.

—

7. Pitanje: Objasnite tehnički proces Proof-of-Work.

Odgovor: Rudar traži nonce takav da hash zaglavlja bloka bude manji od ciljne vrijednosti zadane težinom mreže. Time se osigurava da je u blok uložen značajan računalni rad.

—

8. Pitanje: Što se događa kada dva rudara istovremeno pronađu valjani blok?

Odgovor: Dolazi do privremenog račvanja lanca. Mreža prihvaća obje grane dok jedna ne dobije sljedeći blok i postane dulja, nakon čega se druga grana odbacuje.

—

9. Pitanje: Kako prilagodba težine osigurava prosječno vrijeme bloka od 10 minuta?

Odgovor: Mreža periodično prilagođava težinu rudarenja ovisno o brzini stvaranja prethodnih blokova, čime se održava stabilno prosječno vrijeme generiranja blokova.

—

10. Pitanje: Usporedite PoW i PoS s aspekta Sybil napada.

Odgovor: U PoW-u se troši računalna snaga, dok se u PoS-u zalaže kapital u obliku kriptovalute. U oba sustava napad postaje ekonomski skup.

—

11. Pitanje: Što je 51% napad?

Odgovor: 51% napad znači kontrolu većine hash rate-a mreže, što omogućuje privremene reorganizacije lanca i double-spend napade, ali ne i krađu tuđih sredstava bez privatnih ključeva.

—

12. Pitanje: Objasnite koncept Gas-a u Ethereumu.

Odgovor: Gas predstavlja mjernu jedinicu računalnog rada potrebnog za izvršavanje pametnih ugovora te sprječava beskonačne petlje ograničavanjem resursa.

—

13. Pitanje: Što je Oracle u pametnim ugovorima?

Odgovor: Oracle je posrednik koji pametnim ugovorima dostavlja vanjske podatke jer ugovori sami ne mogu dohvatiti podatke s weba bez narušavanja deterministočnosti.

—

14. Pitanje: Što sadrži novčanik?

Odgovor: Novčanik sadrži privatne ključeve ili seed phrase, javne ključeve i adrese, ali ne i stvarna sredstva.

—

15. Pitanje: Razlika između hot i cold novčanika?

Odgovor: Hot novčanik je povezan s internetom, dok cold novčanik nije. Privatni ključ je izložen internetu samo kod hot novčanika.

—

16. Pitanje: Što znači non-custodial novčanik?

Odgovor: Korisnik sam upravlja privatnim ključevima i snosi punu odgovornost za gubitak sredstava u slučaju gubitka seed phrase-a.

—

17. Pitanje: Objasnite Self-Sovereign Identity.

Odgovor: SSI omogućuje korisnicima potpunu kontrolu nad vlastitim digitalnim identitetom bez središnjeg posrednika, za razliku od federativnih identiteta.

—

18. Pitanje: Zašto velike datoteke ne spremamo na blockchain?

Odgovor: Zbog visokih troškova pohrane, ograničenog prostora i problema skalabilnosti.

—

19. Pitanje: Opišite strukturu jednog bloka.

Odgovor: Blok se sastoji od zaglavlja (hash prethodnog bloka, Merkle root, timestamp, nonce) i tijela s transakcijama.

—

20. Pitanje: Kako su blokovi povezani?

Odgovor: Povezani su pomoću hash-a prethodnog bloka.

—

21. Pitanje: Razlika između punog i laganog čvora?

Odgovor: Puni čvor pohranjuje i verificira cijeli blockchain, dok lagani čvor pohranjuje samo zaglavlja blokova.

—

22. Pitanje: Razlike između blockchaina i klasične baze podataka?

Odgovor: Blockchain je decentraliziran, nepromjenjiv i temeljen na konsenzusu, dok je klasična baza centralizirana i promjenjiva.

—

23. Pitanje: Gdje su spremljeni podaci blockchain mreže?

Odgovor: Na diskovima svih punih čvorova u mreži.

—

24. Pitanje: Što je mempool?

Odgovor: Mempool je privremena memorija u kojoj se nalaze nepotvrđene transakcije.

—

25. Pitanje: Mogu li dva bloka imati isti hash?

Odgovor: U praksi ne, zbog otpornosti hash funkcija na koliziju.

—

26. Pitanje: Što je visina bloka?

Odgovor: Visina bloka je njegov redni broj u lancu.

—

27. Pitanje: Što je visina blockchaina?

Odgovor: Visina blockchaina je najveća visina bloka u lancu u određenom trenutku.

—

28. Pitanje: Koliko prostora zauzima Bitcoin ili Ethereum blockchain?

Odgovor: Bitcoin zauzima više od 500 GB, dok Ethereum zauzima više od 1 TB, ovisno o klijentu.

—

29. Pitanje: Što je blockchain explorer?

Odgovor: Blockchain explorer je alat za pregled blokova, transakcija, adresa i stanja mreže.

—

30. Pitanje: Može li se blockchainu pristupati bez vlastitog punog čvora?

Odgovor: Da, putem API-ja i RPC servisa poput Infure ili Alchemyja.