BLOCKCHAIN FOR AGRIFOOD EDU

Modul 2

Gradniki blokovne verige in mehanizem veriženja blokov

Co-funded by the European Union

Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Zanje ne moreta biti odgovorna niti Evropska unija niti EACEA

Opis modula

Modul »Gradniki blockchaina in blockchain mehanizma« vključuje principe ustvarjanja blockchaina (kaj je blok in kaj je veriga), osnovne značilnosti tradicionalnega, decentraliziranega in porazdeljenega koncepta podatkovnih baz ter lastnosti in zahteve kriptografije in hash funkcij in ima kot rezultat. Vključena je tudi razlaga razlike med dokazilom o delu in dokazilom o stanju ter glavne prednosti blockchaina v modulu.

Učni cilji

Diplomanti modula bodo pridobili temeljna teoretična znanja s področja kreiranja blockchaina in zahteve za kriptografske in razpršilne funkcije. Znanje je določeno s študijo primera, potrjeno s kvizom.

- Rezultati so:
- **Modul z učnim gradivom**
- **Študija primera**
- **Interaktivna dejavnost**
- **Kviz**

Vsebina

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Zanje ne moreta biti odgovorna niti Evropska unija niti EACEA

Vsebina

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Zanje ne moreta biti odgovorna niti Evropska unija niti EACEA

Vsebina

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Zanje ne moreta biti odgovorna niti Evropska unija niti EACEA

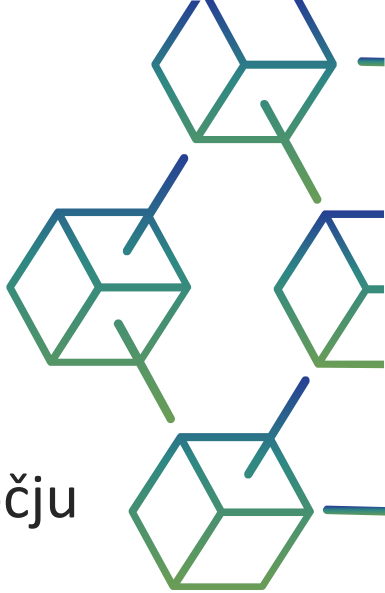
01

UVOD V MODUL 2
Gradniki blokovne verige in mehanizem veriženja blokov

Uvod
Kaj je tehnologija veriženja blokov?

- Blockchain tehnologija je napreden mehanizem baze podatkov, ki omogoča pregledno izmenjavo informacij znotraj poslovnega omrežja. Blockchain baza podatkov shranjuje podatke v blokih, ki so med seboj povezani v verigi.
- Podatki so kronološko dosledni, ker verige ne morete izbrisati ali spremeniti brez soglasja omrežja. Posledično lahko s tehnologijo veriženja blokov ustvarite nespremenljivo ali nespremenljivo knjigo za sledenje naročilom, plačilom, računom in drugim transakcijam.
- Sistem ima vgrajene mehanizme, ki preprečujejo nepooblaščene vnose transakcij in ustvarjajo doslednost v skupnem pogledu na te transakcije.

Uvod
Gradniki blokovne verige in mehanizem veriženja blokov



- Blockchain gradniki in blockchain mehanizem so ključni koncepti na področju digitalnega ekosistema in kriptovalut.
- Blockchain je tehnologija, ki omogoča beleženje transakcij in dogodkov v decentraliziranem in nespremenljivem sistemu.
- Osnovni gradniki blockchaina so naslednji elementi:
- Bloki
- Porazdeljena knjiga
- Kriptografija
- Mehanizem soglasja
- Nespremenljivost

Uvod
Gradniki blokovne verige in mehanizem veriženja blokov

BLOKI

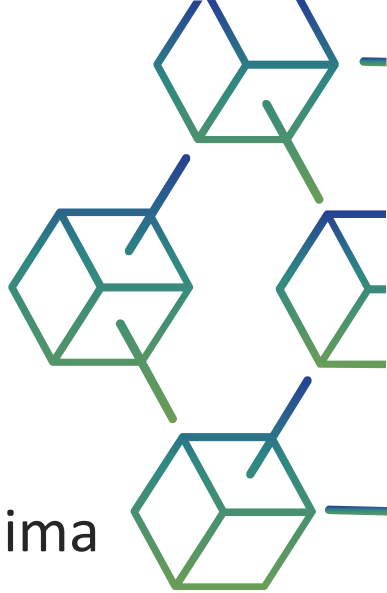
Blockchain je sestavljen iz verige blokov, kjer vsak blok vsebuje seznam transakcij in edinstveni identifikator (hash) prejšnjega bloka. To zagotavlja celovitost podatkov.

DISTRIBUIRANA KNJIGA

Blockchain je shranjen na tisočih računalnikih (vozliščih) po vsem svetu. Vsako vozlišče ima kopijo celotnega blockchaina, kar poveča njegovo odpornost na izpade in napade.

Uvod

Gradniki blokovne verige in mehanizem veriženja blokov



KRIPTOGRAFIJA

Asimetrična kriptografija se uporablja za zaščito transakcij. Vsak udeleženec ima zasebni in javni ključ, ki omogoča preverjanje in podpisovanje transakcij.

MEHANIZEM SOGLASJA

Blockchain zahteva, da vozlišča dosežejo soglasje o veljavnih transakcijah. To se običajno doseže z različnimi algoritmi soglasja, kot sta dokazilo o delu (PoW) ali dokazilo o deležu (PoS).

NESPREMENLJIVOST

Ko so podatki shranjeni v verigi blokov, jih ni mogoče enostavno spremeniti. To zagotavlja zaupanje in preglednost.

Uvod

Gradniki blokovne verige in mehanizem veriženja blokov

- Mehanizem veriženja blokov zagotavlja celovitost podatkov in nesporne transakcije.
- Blockchain ima široke aplikacije, ki presegajo kriptovalute, vključno s financami, dobavno verigo, zdravstvom in številnimi drugimi industrijami.
- Njena prihodnost je odvisna od sposobnosti skupnosti in podjetij za inovacije in uporabo svojega potenciala za reševanje resničnih problemov in premik digitalnega sveta.

02

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

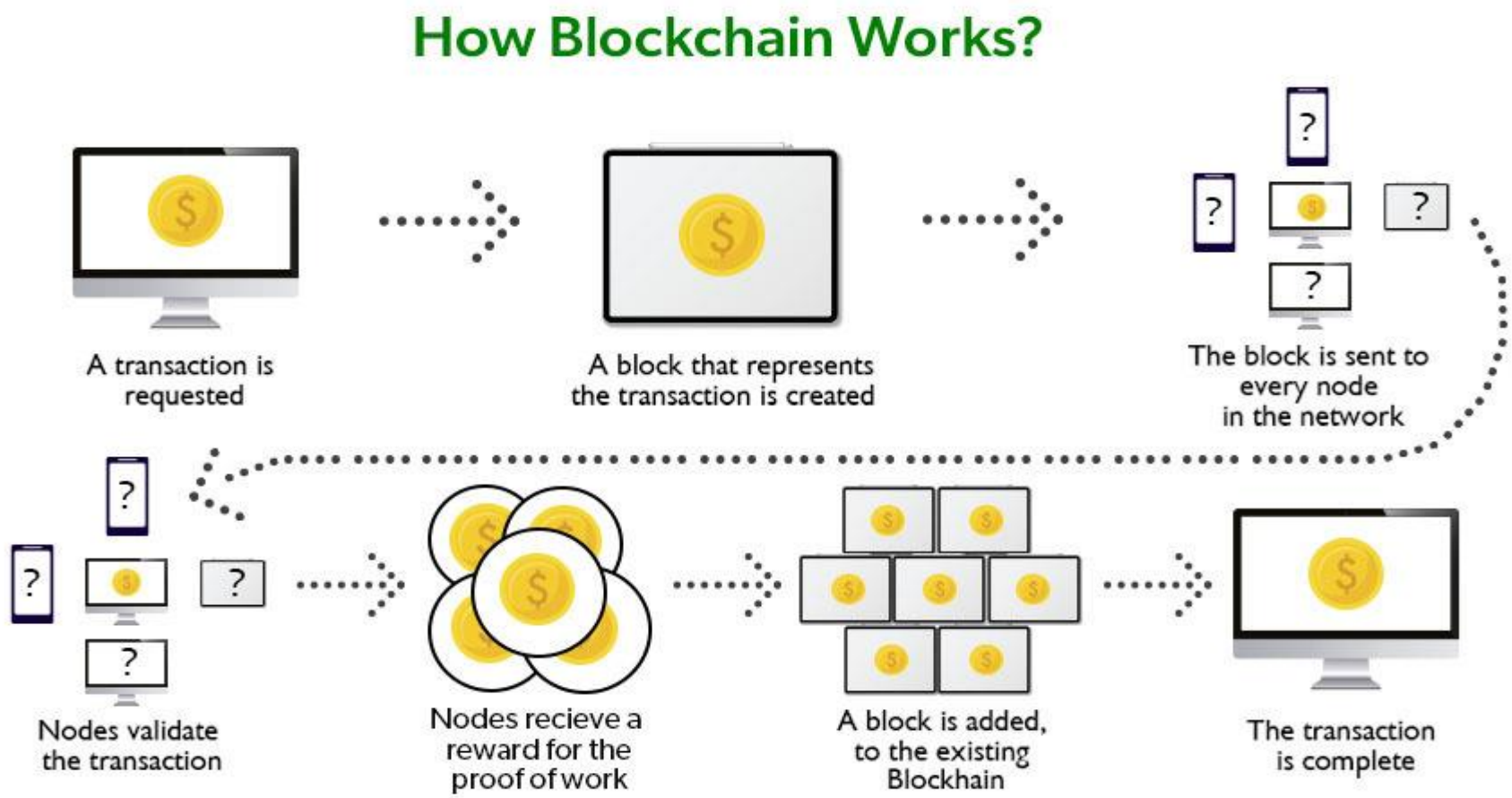
- Kako deluje blockchain?
- Vsaka transakcija ali vnos podatkov, znan kot "blok", je varno povezan s prejšnjim s kriptografskim razprševanjem, kar ustvarja neprekinjeno in nedovoljeno verigo informacij.
- Ker blokade ni mogoče spremeniti, je edino potrebno zaupanje na točki, ko uporabnik ali program vnese podatke. Ta vidik zmanjšuje potrebo po zaupanja vrednih tretjih osebah, ki so običajno revizorji ali drugi ljudje, ki dodajajo stroške in delajo napake.

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

Blockchain je sestavljen iz programov, imenovanih skripte, ki izvajajo naloge, ki bi jih običajno opravljali v bazi podatkov: vnos in dostop do informacij ter njihovo shranjevanje in shranjevanje nekje. Distribuira se veriga blokov, kar pomeni, da se na številnih računalnikih shrani več kopij in da se morajo vse ujemati, da bi bile veljavne.

Blockchain zbira podatke o transakcijah in jih vnese v blok, kot celica v preglednici, ki vsebuje informacije. Ko je poln, se informacije izvajajo prek algoritma šifriranja, ki ustvari šestnajstiško število, imenovano hash

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija



Slika 1: Kako deluje blockchain(vir: https://www.geeksforgeeks.org/how-does-the-blockchain-work/)

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

Transakcijski proces v verigi blokov lahko povzamemo na naslednji način:
1 Olajšanje transakcije
2 Preverjanje transakcije
3 Oblikovanje novega bloka
4 Algoritem soglasja
5 Dodajanje novega bloka v blockchain
6 Transakcija zaključena

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

Razpršitev se nato vnese v naslednjo glavo bloka in šifrira z drugimi informacijami v bloku. To ustvari vrsto blokov, ki so veriženi skupaj.

Transakcije sledijo določenemu procesu, odvisno od verige blokov, na kateri potekajo. Na primer, na Bitcoinovi verigi blokov, če začnete transakcijo z denarnico za kriptovalute - aplikacijo, ki zagotavlja vmesnik za blockchain - začne zaporedje dogodkov.

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

1. **Olajšanje transakcije:** nova transakcija vstopi v omrežje verige blokov. Vse informacije, ki jih je treba posredovati, so dvakrat šifrirane z javnimi in zasebnimi ključi.
2. **Preverjanje transakcije:** Transakcija se nato prenese v omrežje računalnikov peer-to-peer, distribuiranih po vsem svetu. Vsa vozlišča v omrežju bodo preverila veljavnost transakcije, na primer, če je na voljo zadostno stanje za izvedbo transakcije.
3. **Oblikovanje novega bloka:** V tipičnem blockchain omrežju je veliko vozlišč in veliko transakcij se preveri hkrati. Ko bo transakcija preverjena in razglašena za zakonito transakcijo, bo dodana v mempool. Vse preverjene transakcije na določenem vozlišču tvorijo mempool in takšni večkratni mempooli tvorijo blok.

Osnovne komponente: bloki, kriptografsko razprševanje, decentralizacija

6. **Algoritem soglasja:** Vozlišča, ki tvorijo blok, bodo poskušala dodati blok v omrežje blockchain, da bo trajen. Če pa lahko vsako vozlišče na ta način dodaja bloke, bo to motilo delovanje blockchain omrežja.
7. **Dodajanje novega bloka v blockchain:** Ko novo ustvarjeni blok dobi svojo hash vrednost in je overjen, je zdaj pripravljen za dodajanje v blockchain. V vsakem bloku je razpršilna vrednost prejšnjega bloka in tako so bloki kriptografsko povezani med seboj, da tvorijo blockchain. Na odprti konec verige blokov se doda nov blok.
8. **Transakcija končana:** Takoj ko je blok dodan v verigo blokov, je transakcija zaključena in podrobnosti o tej transakciji so trajno shranjene v verigi blokov. Vsakdo lahko pridobi podrobnosti transakcije in potrdi transakcijo.

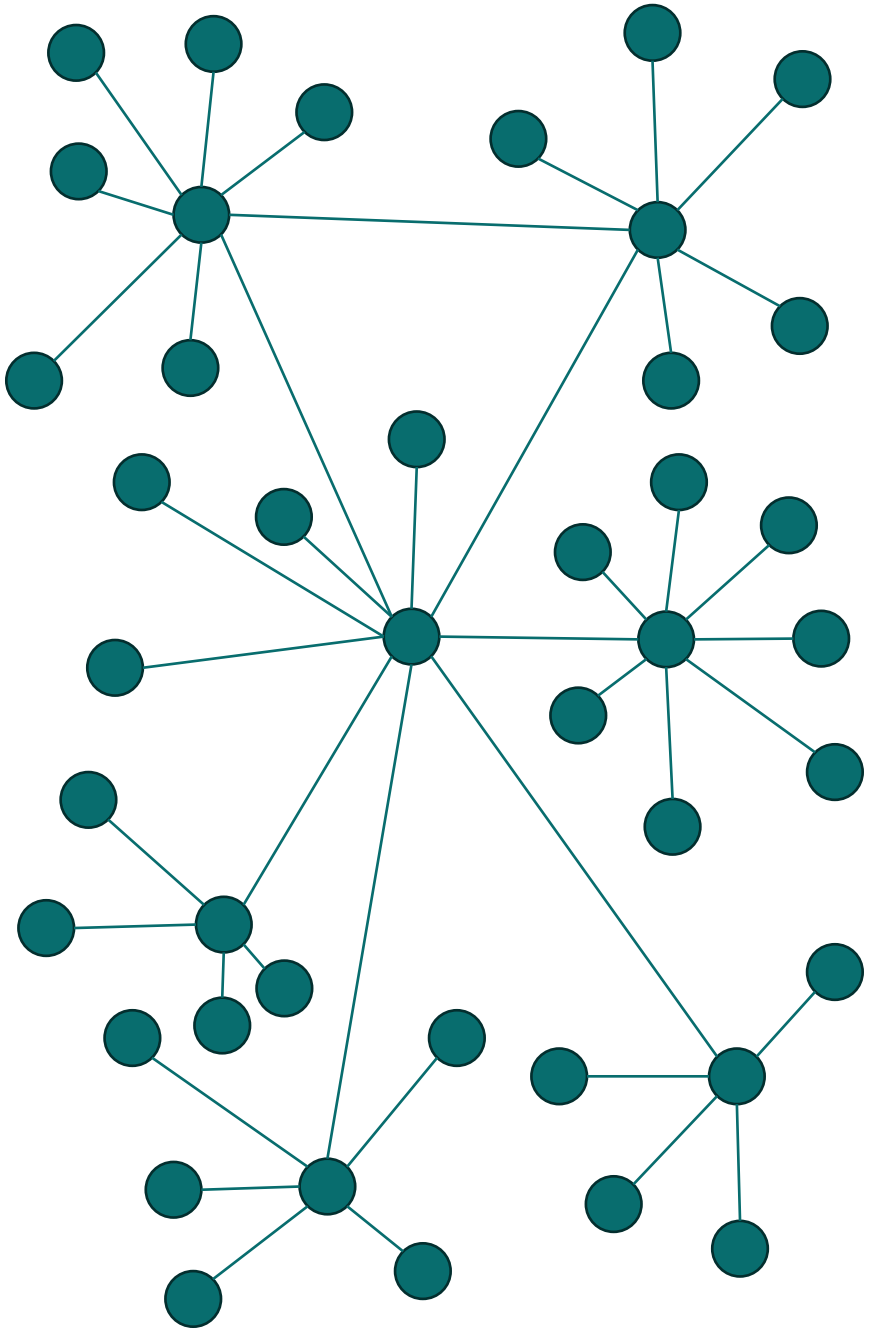
Primerjava s tradicionalnimi bazami podatkov

- Tradicionalne baze podatkov so centralizirane, spremenljive in optimizirane za hitro obdelavo podatkov, medtem ko so blokovne verige decentralizirane, nespremenljive in osredotočene na zagotavljanje zaupanja in preglednosti prek mehanizmov soglasja. Izbira med obema je odvisna od posebnih potreb posamezne vloge.
- Centralizacija proti decentralizaciji
- Struktura podatkov
- Nadzor dostopa
- Mehanizem soglasja
- Nespremenljivi podatki v primerjavi z spremenljivimi podatki
- Hitrost in razširljivost transakcij
- Primeri uporabe

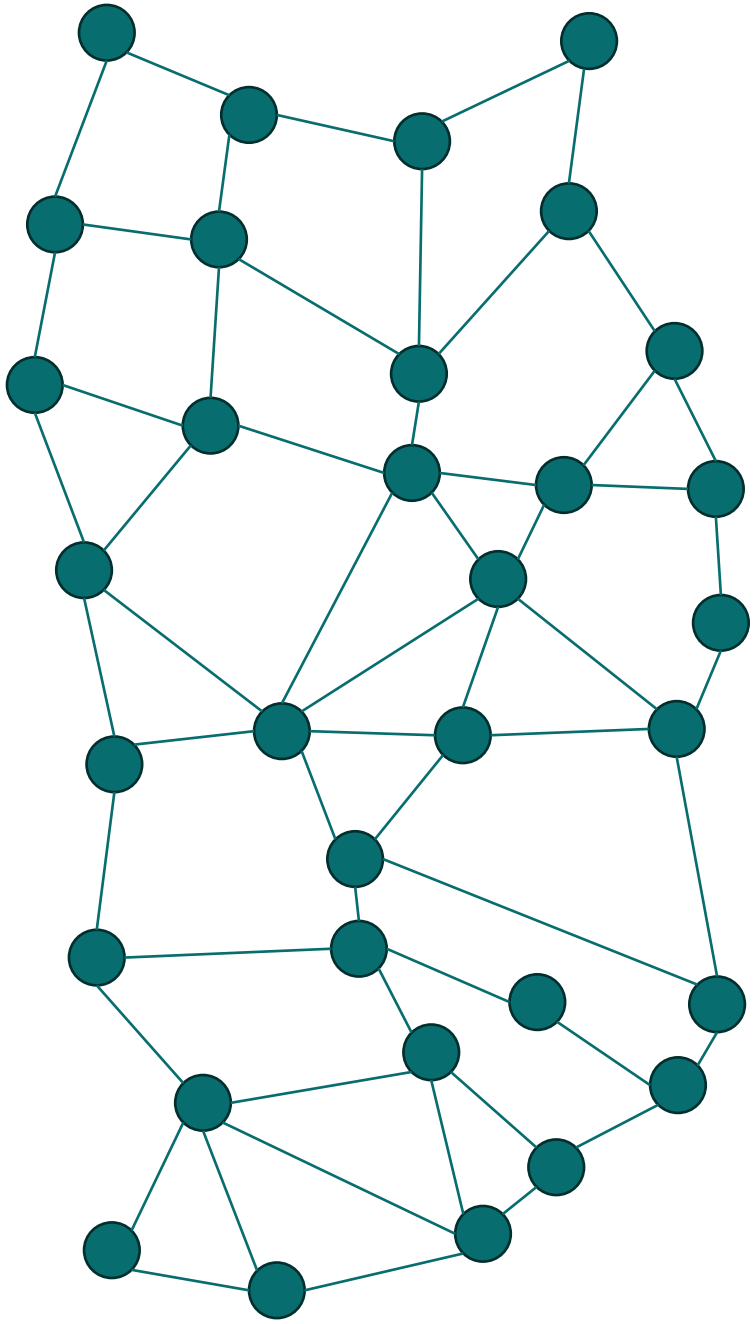
Primerjava s tradicionalnimi bazami podatkov

- **Centralizacija proti decentralizaciji**
- **Tradicionalne baze podatkov:** Tradicionalne baze podatkov so centralizirani sistemi, kjer ima en subjekt (npr. podjetje ali organizacija) nadzor nad bazo podatkov. Za upravljanje in shranjevanje podatkov se zanašajo na osrednji strežnik ali gručo strežnikov.
- **Blockchain:** Blokovne verige so decentralizirana omrežja, kjer se podatki distribuirajo po več vozliščih (računalnikih) v omrežju. Ni osrednjega organa ali enotne točke nadzora, zaradi česar so odporni proti cenzuri in nedovoljenim posegom.

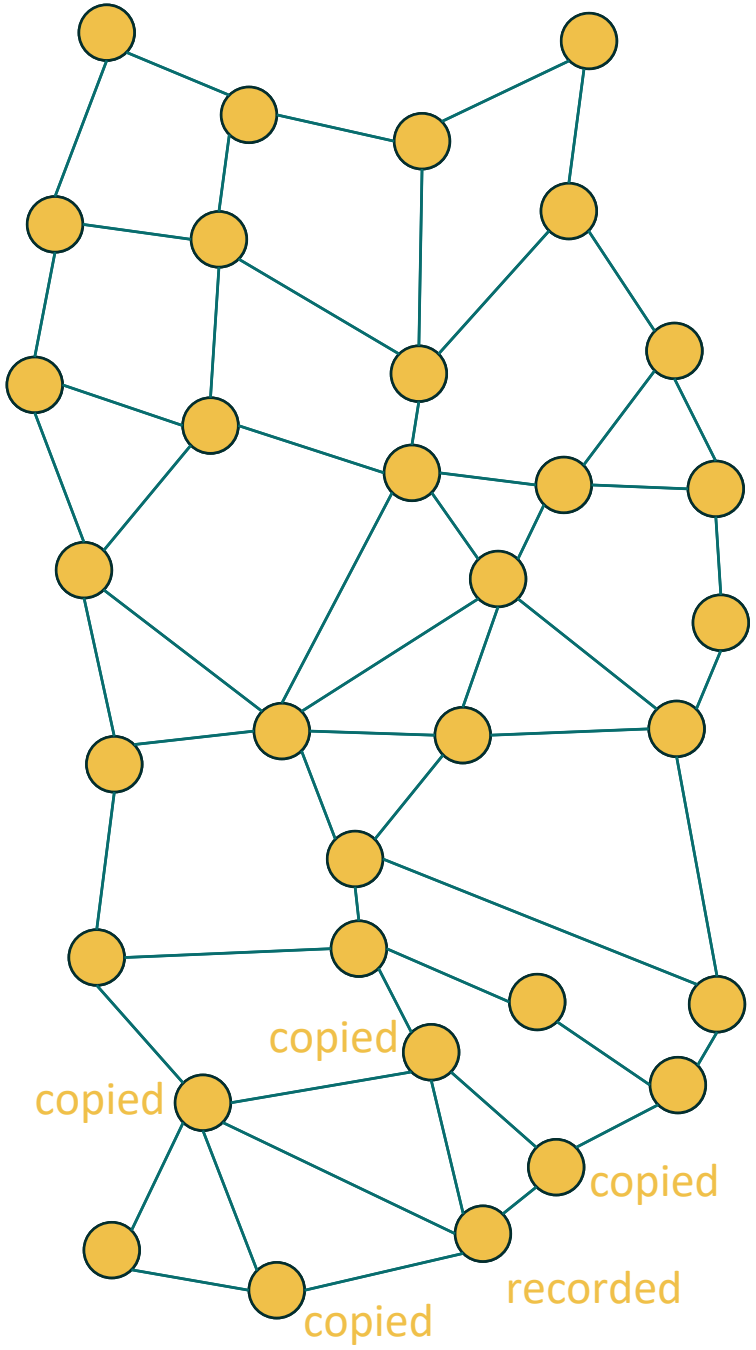
Centralizirano
Vsa vozlišča so povezana pod enim organom.



Decentralizirano
Noben strežnik oblasti ne nadzoruje vozlišč, vsi imajo indivitualno entiteto.



Razdeli
Vsako vozlišče je neodvisno
in med seboj povezano.

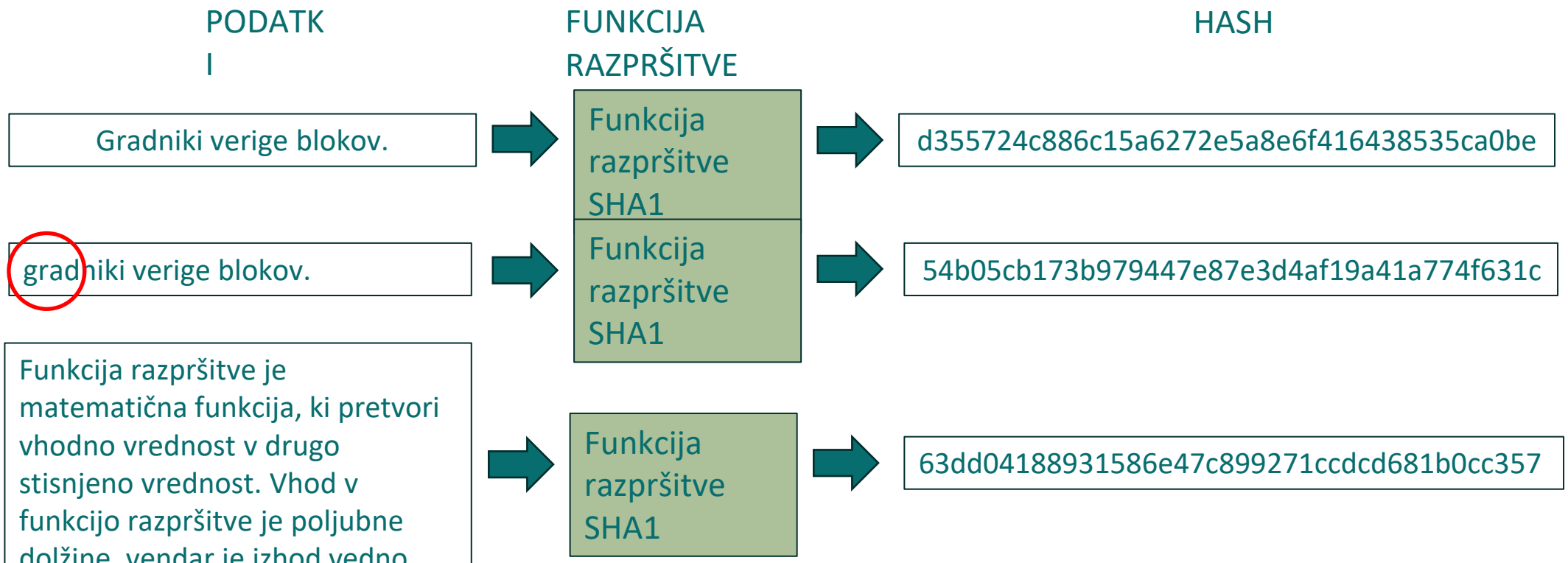


Transakcije v porazdeljenem omrežju
Transakcija se zabeleži v vozlišče in kopira drug na drugega.

Funkcija razpršitve

Funkcija razpršitve je matematična funkcija, ki pretvori vhodno vrednost v drugo stisnjeno vrednost. Vhod v funkcijo razpršitve je poljubne dolžine, vendar je izhod vedno fiksne dolžine.
Hash funkcije so izjemno uporabne in se pojavljajo v skoraj vseh aplikacijah za informacijsko varnost.

Edinstven izhod razpršilne funkcije



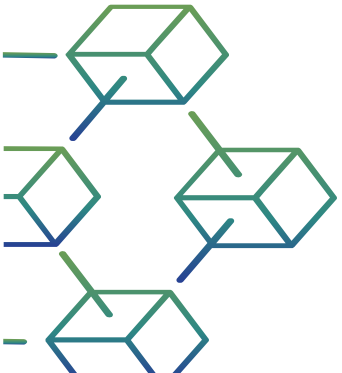
Funkcija razpršitve je matematična funkcija, ki pretvori vhodno vrednost v drugo stisnjeno vrednost. Vhod v funkcijo razpršitve je poljubne dolžine, vendar je izhod vedno fiksne dolžine.

SHA1 v tem času ni dovolj

Gradniki verige blokov.

Funkcija razpršitve SHA3-512

33322d615333e9faa2109c35997cf144876cc75ba76059454b28c81d2fa1c286a68679a00afb
baa71e9170ffc3bdaf6fbef5035a31b4f40a354502dd985368d4

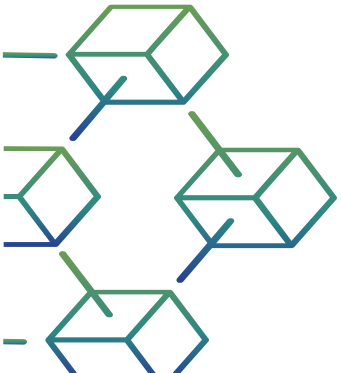


Odpornost pred sliko

Ta lastnost pomeni, da bi moralo biti računsko težko obrniti funkcijo razpršitve.

Z drugimi besedami, če je funkcija razpršitve h ustvarila razpršilno vrednost z, potem bi moral biti težaven postopek najti katero koli vhodno vrednost x, ki se razprši na z.

Ta lastnost ščiti pred napadalcem, ki ima samo razpršilno vrednost in poskuša najti vnos.



Odpornost proti trkom

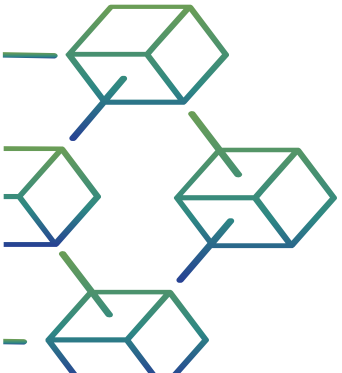
Ta lastnost pomeni, da bi moralo biti težko najti dva različna vhoda katere koli dolžine, ki imata za posledico isto razpršitev. Ta lastnost se imenuje tudi funkcija razpršitve brez trkov.

Z drugimi besedami, za funkcijo razpršitve h je težko najti dva različna vhoda x in y, tako da je h(x) = h(y).

Ker je funkcija razpršitve funkcija stiskanja s fiksno dolžino razpršitve, funkcija razpršitve ne more imeti trkov. Ta lastnost brez trkov samo potrjuje, da bi bilo te trke težko najti.

Ta lastnost napadalcu zelo otežuje iskanje dveh vhodnih vrednosti z isto razpršitvijo.

Če je funkcija razpršitve odporna proti trčenju, je druga odporna pred sliko.



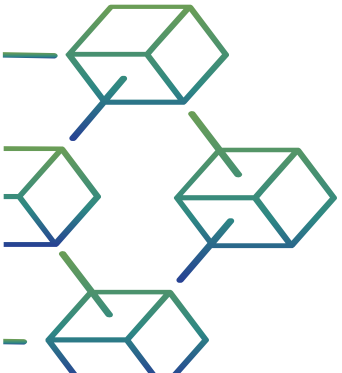
Source: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Druga odpornost pred sliko

Ta lastnost pomeni, da je glede na vhod in njegovo razpršitev težko najti drugačen vhod z isto razpršitvijo.

Z drugimi besedami, če funkcija razpršitve h za vhodni x povzroči razpršilno vrednost h(x), potem bi moralo biti težko najti katero koli drugo vhodno vrednost y, tako da je h(y) = h(x).

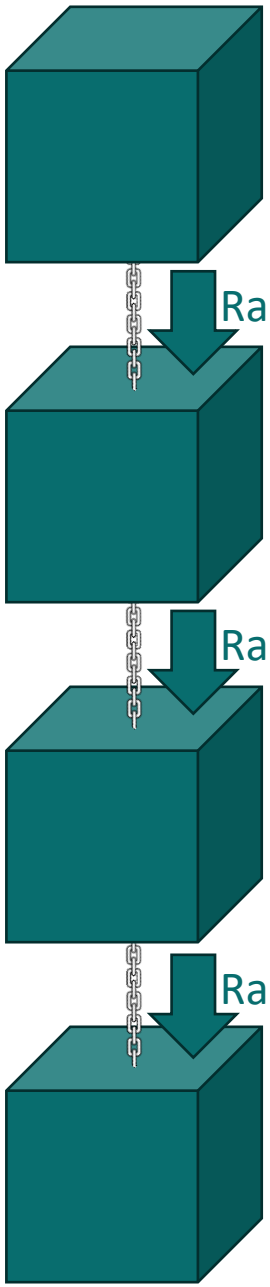
Ta lastnost razpršilne funkcije ščiti pred napadalcem, ki ima vhodno vrednost in njeno razpršitev ter želi nadomestiti drugačno vrednost kot zakonito vrednost namesto izvirne vhodne vrednosti.



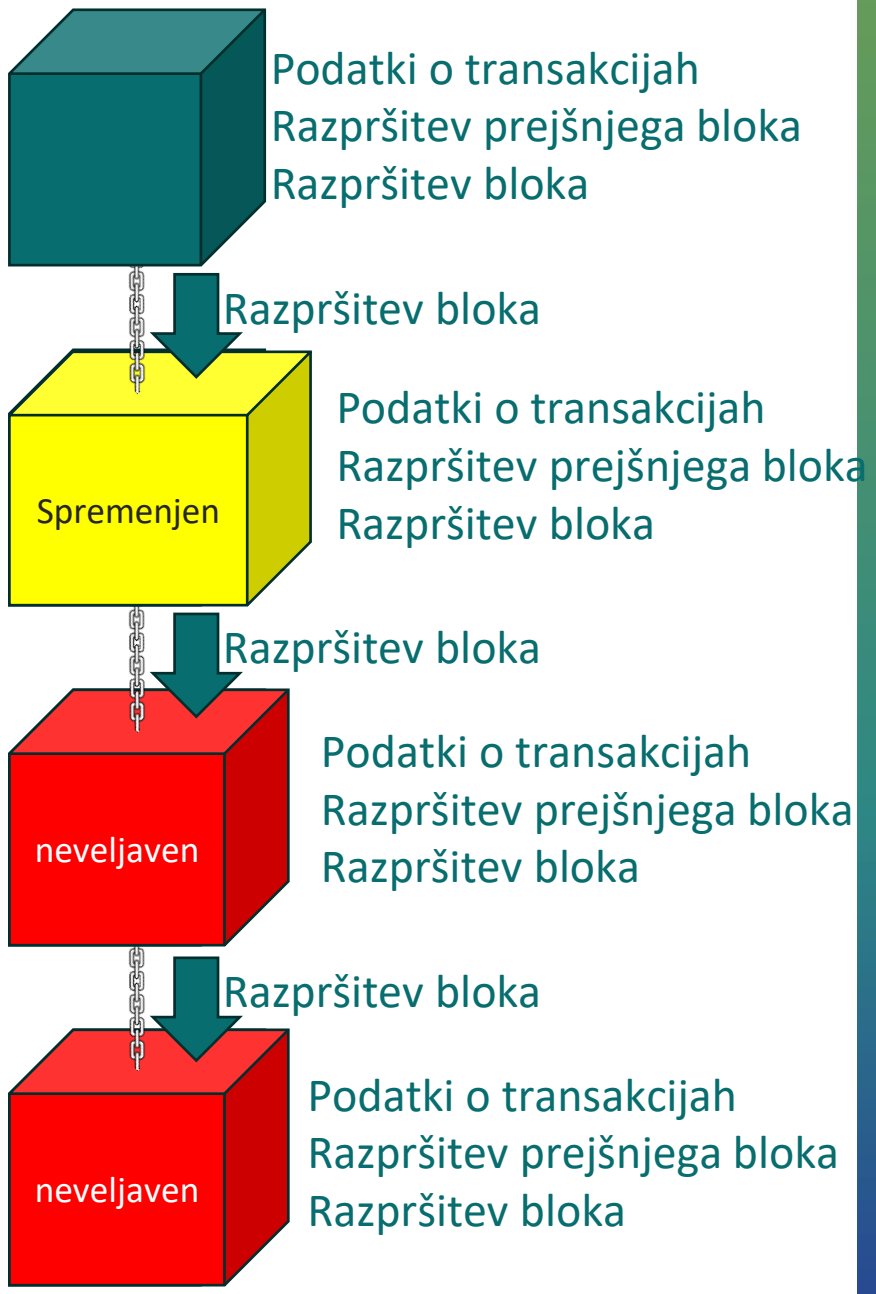
Blockchain

Blok = podatki + razpršitev prejšnjega bloka + razpršitev

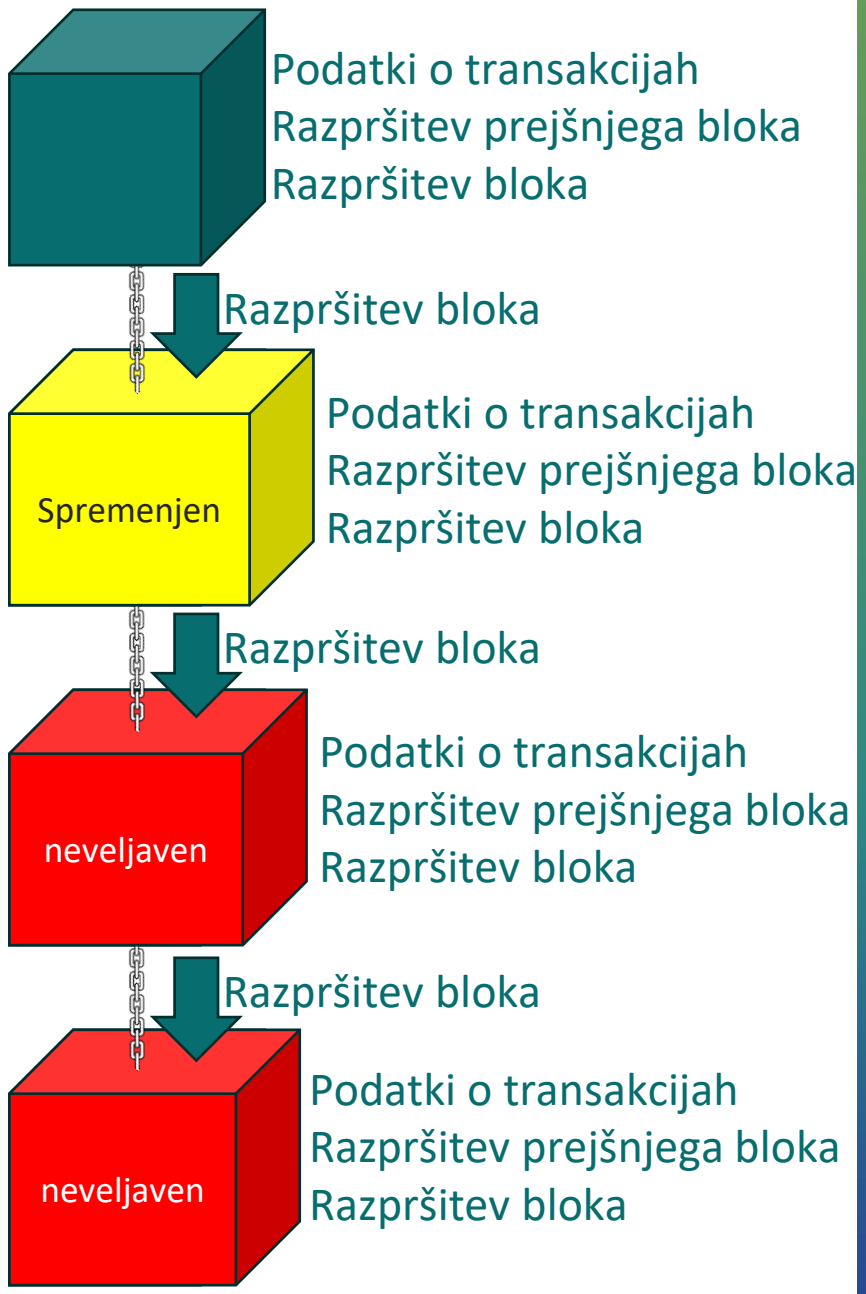
Veriga = veriga med bloki



Vse transakcije so zabeležene v "blokih"



Če je en blok (ena transakcija v enem bloku) spremenjen Vrednost razpršilne funkcije je drugačna



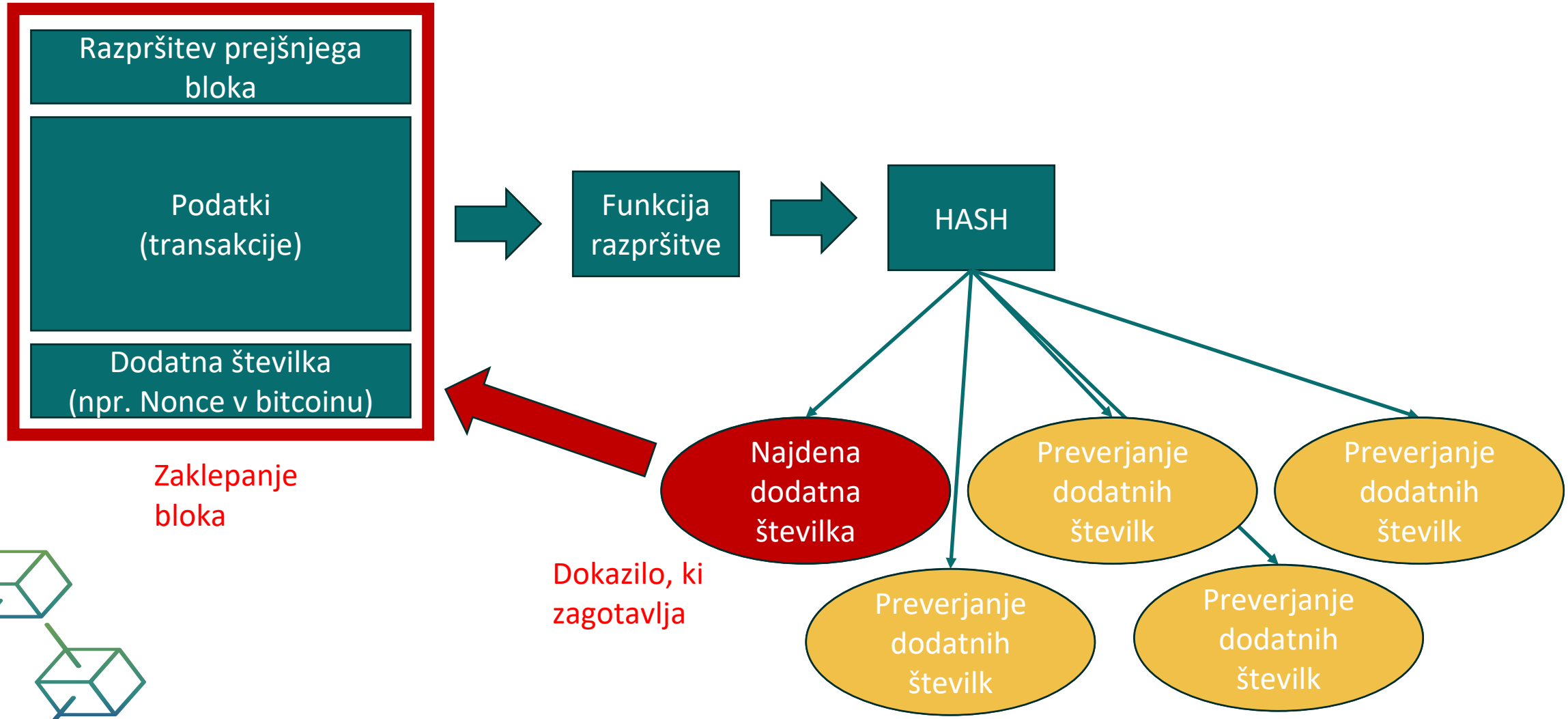
Če želi heker spremeniti en blok (podatke v enem bloku), mora spremeniti vse naslednje bloke in vse kopije blokov v porazdeljenem omrežju
Skoraj nemogoče (potrebuje ogromno računalniško moč, elektriko itd.)

Dokazilo o delu

Dokazilo o delu (PoW) je oblika kriptografskega dokaza, pri katerem ena stranka (preverjevalec) dokaže drugim (preveriteljem), da je bila porabljena določena količina določenega računskega napora.

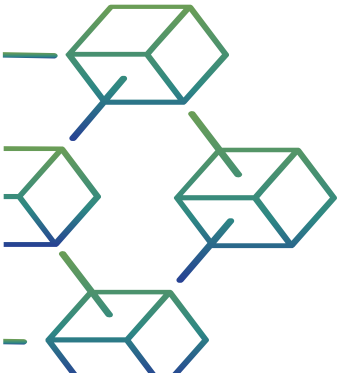
Preveritelji lahko naknadno potrdijo te izdatke z minimalnim naporom z njihove strani.

Dokazilo o delu



Dokazilo o deležu

Protokoli dokazila o deležu (PoS) so razred mehanizmov soglasja za blokovne verige, ki delujejo tako, da izberejo validatorje sorazmerno z njihovo količino imetij v povezani kriptovaluti.
To se stori, da bi se izognili računalniškim stroškom shem dokazila o delu.



3 ravni blockchaina

1. Blockchain 1.0: izvor sodobnega blockchaina
2. Blockchain 2.0: pametne pogodbe
3. Blockchain 3:0: Decentralizirana aplikacija na ravni podjetja

Primerjava s tradicionalnimi bazami podatkov

Struktura podatkov
Tradicionalne zbirke podatkov: Tradicionalne zbirke podatkov uporabljajo tabele za strukturirano organiziranje podatkov, običajno po vnaprej določeni shemi.
Blockchain: Blokovne verige uporabljajo strukturo knjige, kjer so podatki organizirani v bloke, vsak blok pa vsebuje seznam transakcij ali vnosov podatkov. Struktura je običajno manj toga, kar omogoča večjo prilagodljivost podatkovnih tipov in formatov.

Primerjava s tradicionalnimi bazami podatkov

Nadzor dostopa
Tradicionalne zbirke podatkov: nadzor dostopa upravlja centraliziran organ, dovoljenja pa je mogoče dodeliti ali preklicati različnim uporabnikom ali vlogam.
Veriženje blokov: nadzor dostopa se pogosto upravlja s kriptografskimi ključi. Uporabniki imajo nadzor nad svojimi zasebnimi ključi, kar jim omogoča interakcijo z blockchainom, ne da bi se zanašali na osrednji organ. Javne verige blokov so običajno brez dovoljenj, zasebne verige blokov pa imajo lahko različne ravni nadzora dostopa.

Primerjava s tradicionalnimi bazami podatkov

Mehanizem soglasja
Tradicionalne baze podatkov: Tradicionalne podatkovne baze se ne zanašajo na mehanizem soglasja med več stranmi. Predpostavljajo, da so podatki, shranjeni v bazi podatkov, točni.
Blockchain: Blokovne verige uporabljajo mehanizme soglasja (npr. dokazilo o delu, dokazilo o deležu) za potrditev in dogovor o stanju knjige. To zagotavlja, da imajo vsi udeleženci v omrežju skupen in dogovorjen pogled na podatke.

Primerjava s tradicionalnimi bazami podatkov

Nespremenljivi podatki v primerjavi z spremenljivimi podatki
Tradicionalne baze podatkov: Podatke v tradicionalnih bazah podatkov lahko pooblaščeni uporabniki spreminjajo ali brišejo s potrebnimi dovoljenji.
Blockchain: Ko so podatki zabeleženi v verigi blokov, so običajno nespremenljivi in odporni na spremembe. Ta nespremenljivost je ključna značilnost tehnologije veriženja blokov.

Primerjava s tradicionalnimi bazami podatkov

Hitrost in razširljivost transakcij
Tradicionalne baze podatkov: Tradicionalne baze podatkov so pogosto optimizirane za visoke hitrosti transakcij in jih je mogoče enostavno prilagoditi z dodajanjem več strežnikov ali virov.
Blockchain: Javne blokovne verige, zlasti tiste, ki uporabljajo dokazilo o delu, imajo lahko počasnejše hitrosti obdelave transakcij in izzive glede razširljivosti. Vendar pa se razvijajo različne rešitve in tehnologije za izboljšanje razširljivosti blockchaina.

Primerjava s tradicionalnimi bazami podatkov

Primeri uporabe
Tradicionalne baze podatkov: Tradicionalne baze podatkov so zelo primerne za aplikacije, ki zahtevajo visoko prepustnost, nizko zakasnitev in centraliziran nadzor, kot so bančni sistemi in platforme za e-poslovanje.
Blockchain: Blokovne verige so najbolj primerne za aplikacije, ki zahtevajo decentralizacijo, zaupanje, preglednost in varnost, kot so kriptovalute, sledenje dobavni verigi, sistemi glasovanja in pametne pogodbe.

03

Katere so ključne komponente blockchain tehnologije?

Katere so ključne komponente blockchain tehnologije?

- Blockchain arhitektura ima naslednje glavne komponente:
- Porazdeljena knjiga
- Pametne pogodbe
- Kriptografija javnega ključa

Katere so ključne komponente blockchain tehnologije?

1. Porazdeljena knjiga

Porazdeljena knjiga je zbirka podatkov v skupni rabi v omrežju verige blokov, ki shranjuje transakcije, na primer datoteka v skupni rabi, ki jo lahko urejajo vsi člani ekipe. V večini urejevalnikov besedil v skupni rabi lahko vsakdo s pravicami za urejanje izbriše celotno datoteko. Vendar pa imajo tehnologije distribuirane knjige transakcij stroga pravila o tem, kdo lahko ureja in kako urejati. Ko so vnosi zabeleženi, jih ne morete izbrisati.

Katere so ključne komponente blockchain tehnologije?

2. Pametne pogodbe

Podjetja uporabljajo pametne pogodbe za samostojno upravljanje poslovnih pogodb, ne da bi potrebovala pomoč tretje osebe. To so programi, shranjeni v sistemu blockchain, ki se samodejno zaženejo, ko so izpolnjeni vnaprej določeni pogoji. Izvajajo če-potem čeke, tako da je transakcije mogoče zanesljivo zaključiti. Na primer, logistično podjetje ima lahko pametno pogodbo, ki samodejno izvede plačilo, ko blago prispe v pristanišče.

Katere so ključne komponente blockchain tehnologije?

3. Kriptografija javnega ključa

Kriptografija javnega ključa je varnostna funkcija za edinstveno identifikacijo udeležencev v omrežju blockchain. Ta mehanizem ustvari dva nabora ključev za člane omrežja. Eden od ključev je javni ključ, ki je skupen vsem v omrežju. Drugi je zasebni ključ, ki je edinstven za vsakega člana. Zasebni in javni ključi sodelujejo pri odklepanju podatkov v knjigi.

Katere so ključne komponente blockchain tehnologije?

3. Kriptografija javnega ključa

John in Jill sta na primer dva člana mreže. John posname transakcijo, ki je šifrirana z njegovim zasebnim ključem. Jill jo lahko dešifrira s svojim javnim ključem. Tako je Jill prepričana, da je John opravil transakcijo. Jillov javni ključ ne bi deloval, če bi bil Johnov zasebni ključ spremenjen.

04

Kakšne so prednosti tehnologije veriženja blokov?

Kakšne so prednosti tehnologije veriženja blokov?

- Tehnologija veriženja blokov prinaša številne prednosti upravljanju transakcij s sredstvi. Nekaj jih navajamo v naslednjih pododdelkih:
- **Napredna varnost**
- **Izboljšana učinkovitost**
- **Hitrejše nadziranje**

Kakšne so prednosti tehnologije veriženja blokov?

1. Napredna varnost

Blockchain sistemi zagotavljajo visoko raven varnosti in zaupanja, ki jo zahtevajo sodobne digitalne transakcije. Vedno obstaja strah, da bo nekdo manipuliral z osnovno programsko opremo, da bi sam ustvaril ponarejen denar. Toda blockchain uporablja tri načela kriptografije, decentralizacije in konsenza, da ustvari zelo varen osnovni programski sistem, ki ga je skoraj nemogoče spreminjati. Ni ene same točke neuspeha in en uporabnik ne more spremeniti zapisov transakcij.

Kakšne so prednosti tehnologije veriženja blokov?

2. Izboljšana učinkovitost

Transakcije med podjetji lahko trajajo veliko časa in ustvarijo operativna ozka grla, zlasti kadar gre za skladnost s predpisi in regulativne organe tretjih oseb. Preglednost in pametne pogodbe v blokovni verigi omogočajo hitrejše in učinkovitejše poslovne transakcije.

05

Kakšna je razlika med bazo podatkov in verigo blokov?

Kakšne so prednosti tehnologije veriženja blokov?

3. Hitrejše nadziranje

Podjetja morajo biti sposobna varno ustvarjati, izmenjevati, arhivirati in rekonstruirati e-transakcije na revizijski način. Blockchain zapisi so kronološko nespremenljivi, kar pomeni, da so vsi zapisi vedno urejeni s časom. Zaradi te preglednosti podatkov je obdelava revizij veliko hitrejša.

Kakšna je razlika med bazo podatkov in verigo blokov?

Blockchain je posebna vrsta sistema za upravljanje baz podatkov, ki ima več funkcij kot običajna baza podatkov. Nekatere pomembne razlike med tradicionalno bazo podatkov in blockchainom opisujemo na naslednjem seznamu:

- Blokovne verige decentralizirajo nadzor, ne da bi pri tem škodovale zaupanju v obstoječe podatke. To v drugih sistemih baz podatkov ni mogoče.
- Podjetja, ki sodelujejo v transakciji, ne morejo deliti svoje celotne baze podatkov. Toda v omrežjih blockchain ima vsako podjetje svojo kopijo knjige, sistem pa samodejno vzdržuje doslednost med obema knjigama.
- Čeprav lahko v večini sistemov baz podatkov urejate ali brišete podatke, lahko v verigi blokov vstavljate samo podatke.

06

Kako se blockchain razlikuje od oblaka?

Kako se blockchain razlikuje od oblaka?

Izraz oblak se nanaša na računalniške storitve, do katerih je mogoče dostopati prek spleta. Do programske opreme kot storitve (SaaS), izdelka kot storitve (PaaS) in infrastrukture kot storitve (IaaS) lahko dostopate iz oblaka.

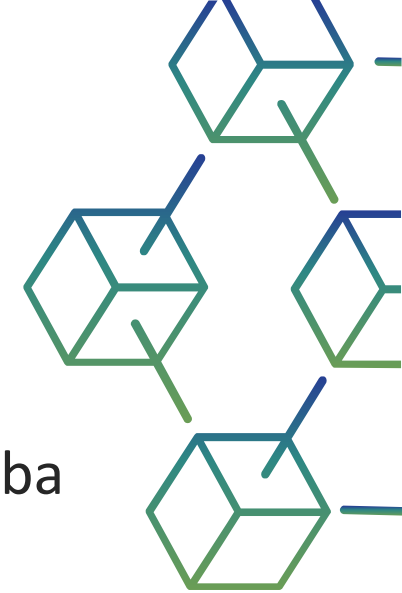
Ponudniki storitev v oblaku upravljajo svojo strojno opremo in infrastrukturo ter vam omogočajo dostop do teh računalniških virov prek interneta. Zagotavljajo veliko več virov kot le upravljanje baz podatkov.

Če se želite pridružiti javnemu omrežju blockchain, morate zagotoviti vire strojne opreme za shranjevanje kopije glavne knjige. V ta namen lahko uporabite tudi strežnik iz oblaka. Nekateri ponudniki storitev v oblaku ponujajo tudi popolno verigo blokov kot storitev (BaaS) iz oblaka.

07

Kaj je blockchain kot storitev?

Kaj je blockchain kot storitev?



Blockchain as a Service (BaaS) je upravljana blockchain storitev, ki jo tretja oseba zagotavlja v oblaku. Lahko razvijete aplikacije veriženja blokov in digitalne storitve, medtem ko ponudnik storitev v oblaku zagotavlja infrastrukturo in orodja za gradnjo blokovnih verig.

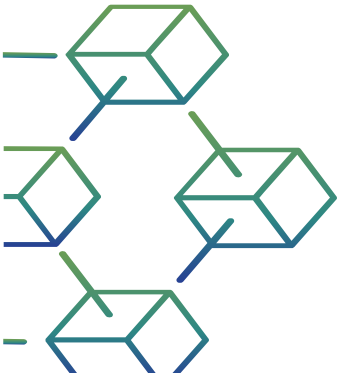
Vse kar morate storiti je, da prilagodite obstoječo tehnologijo veriženja blokov, zaradi česar je sprejemanje blockchaina hitrejše in učinkovitejše.

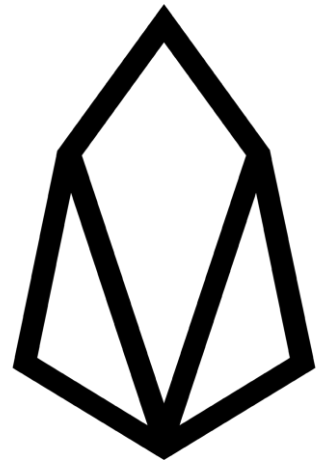
08

Primer uporabe

Kriptovaluta – prva široko uporabljena veriga blokov

- Sodobne kriptovalute uporabljajo blockchain
  - Bitcoin
  - Litecoin
  - Ethereum
  - XRP
  - EOS
  - NEO
  - Stellar
  - Monero
  - Dash
  - …



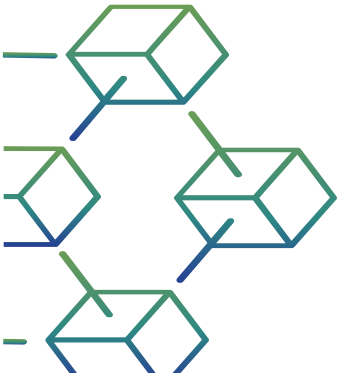


09

Sklep

Sklep

Blockchain tehnologija je napreden mehanizem baze podatkov, ki omogoča pregledno izmenjavo informacij znotraj poslovnega omrežja. Blockchain je sestavljen iz verige blokov, kjer vsak blok vsebuje seznam transakcij in edinstveni identifikator (hash) prejšnjega bloka. To zagotavlja celovitost podatkov. Blokovne verige so decentralizirana omrežja, kjer se podatki distribuirajo po več vozliščih (računalnikih) v omrežju. Ni osrednjega organa ali enotne točke nadzora, zaradi česar so odporni proti cenzuri in nedovoljenim posegom. Blockchain je shranjen na tisočih računalnikih (vozliščih) po vsem svetu. Vsako vozlišče ima kopijo celotnega blockchaina, kar poveča njegovo odpornost na izpade in napade.



Video

- How does a blockchain work – Simply Explained [6:00]
- Blockchain In 7 minutes [7:03]
- Blockchain Explained [10:23]
- What is a Blockchain? (Animated + Examples) [8:27]
- Blockchain Technology Explained (2 Hour Course) [1:54:53]
- Blockchain Basics & Cryptography [1:17:37]

Povezave

- BlockChain Principles, Type & Application & Why You Should Care About It?
- Design principles for blockchain
- Principles of Blockchains
- Principles of Successful Blockchain Deployments
- Basic blockchain security
- Blockchain Design – Explore The Blockchain Principles
- Blockchain Technology: Principles and Application in Medical Imaging

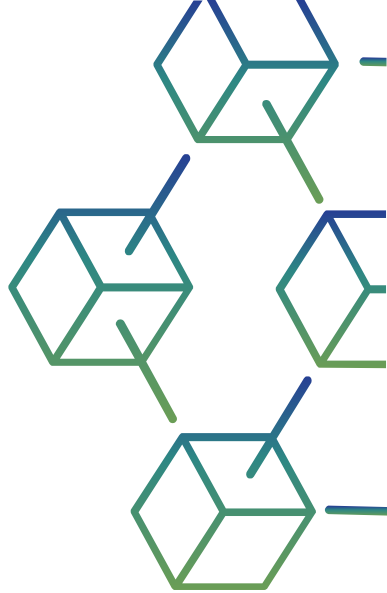
10

Interaktivna učna dejavnost

Naredite 5 blokov pod verigo blokov

1. Uporaba spletnega orodja za razpršitev https://emn178.github.io/online-tools/sha256.html
2. Uporabite SHA256 in naredite razpršitve 5 blokov – vsebina je na naslednjem diapozitivu

Naredite 5 blokov pod verigo blokov



1. Vsebina 1. bloka:
   2023-01-01T10:34:12+1,Jonh Newman,Jane Newman,236.23,EUR
   E3B0C44298FC1C149AFBF4c8996FB92427AE41E4649B934Ca495991B7852B855
2. Vsebina 2. bloka:
   2023-01-01T10:35:28+1,Steve Johnson,Richard McCay,100,00,EUR
   Uporabite razpršitev iz funkcije razpršitve 1. bloka
3. Vsebina 3. bloka:
   2023-01-01T10:35:33+1,Charles Tann,Elisabeth Bronson,100,00,EUR
   Uporabite razpršitev iz razpršilne funkcije 3. bloka
4. Vsebina 4. bloka:
   2023-01-01T10:35:59+1,Roger Blackburn,Lisa Tann,50,00,EUR
   Uporabite razpršitev iz razpršilne funkcije 3. bloka
5. Vsebina 5. bloka:
   2023-01-01T10:36:01+1,Richard Moss,Edward Morris,85,00,EUR
   Uporabite razpršitev iz razpršilne funkcije 4. bloka

Poskusite:

1. Naredite enake majhne spremembe v 2. bloku in primerjajte nove hashe
2. Uporabite drugačno funkcijo razpršitve– zgornji meni– Hash
    1. SHA1
    2. SHA2-512
    3. SHA3
    4. ...
3. Uporabite svojo vsebino bloka za ima funkcijo

11

Kviz

Kviz

1. Kaj je ključna zahteva za varno funkcijo razpršitve:
    a) Odpornost proti trčenju
    b) Redundance
    c) Predvidljivost
    d) Linearnost

Kviz

2. Kaj je značilnost centralizirane arhitekture baze podatkov?
   a) Enotna točka nadzora in pooblastila
   b) Porazdeljeno shranjevanje podatkov v več vozliščih
   c) Avtonomno odločanje vsakega vozlišča
   d) Visoka odpornost na cenzuro in nedovoljene posege

Kviz

3. Kaj je ključna značilnost decentralizirane arhitekture baze podatkov?
   a) Več "osrednjih" vozlišč
   b) Enotna točka nadzora in pooblastila
   c) Centralizirano odločanje z določenim vozliščem
   d) Nizka redundanca in toleranca napak

Kviz

4. Kaj je opredeljujoča značilnost porazdeljenega sistema zbirke podatkov?
   a) Podatki so shranjeni v več vozliščih v omrežju
   b) Centraliziran nadzor in avtoriteta nad celotno bazo podatkov
   c) Pomanjkanje odvečnih delavcev za večjo uspešnost
   d) Omejena razširljivost zaradi arhitekture z enim vozliščem

Kviz

5. Kaj najbolje opisuje razpršitev v kontekstu računalništva in kriptografije?

   a) Izhod fiksne velikosti, ki ga ustvari funkcija razpršitve in predstavlja edinstven digitalni podpis vhodnih podatkov

   b) Niz spremenljive dolžine, ki se uporablja za shranjevanje podatkov v podatkovnih bazah

   c) Programski konstrukt za optimizacijo pridobivanja podatkov v algoritmih

   d) Metoda šifriranja v realnem času za zaščito komunikacijskih kanalov

Kviz

6. Katera komponenta je odgovorna za vzdrževanje kronološkega in nespremenljivega zapisa transakcij v verigi blokov?
   a) Blok
   b) Vozlišče
   c) Pametna pogodba
   d) Algoritem soglasja

Kviz

7. **Kaj je ključni razlikovalec med blockchainom in tradicionalno bazo podatkov?**

   a) Blockchain ponuja decentraliziran in porazdeljen nadzor, medtem ko so tradicionalne baze podatkov običajno centralizirane

   b) Tradicionalne podatkovne baze omogočajo hitrejšo obdelavo transakcij v primerjavi s počasnejšo naravo blockchaina

   c) Blokovna veriga temelji na enotni točki nadzora, medtem ko tradicionalne podatkovne baze za nadzor uporabljajo porazdeljeno omrežje

   d) Tradicionalne podatkovne baze so same po sebi odporne na nedovoljene posege, medtem ko je blockchain bolj dovzeten za manipulacijo podatkov.

Kviz

8. Kje je bila prvič implementirana blockchain tehnologija?
    a) Finance in kriptovalute
    b) Zdravstvena in zdravstvena dokumentacija
    c) Družbeni mediji in mreženje
    d) E-poslovanje in spletna trgovina na drobno

https://blockchainforagrifood.eu/

Hvala

Imate vprašanja?

Co-funded by the European Union

Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Zanje ne moreta biti odgovorna niti Evropska unija niti EACEA