

A large, stylized logo of the University of Bern, featuring a thick, curved line that forms a shape reminiscent of a stylized 'B' or a mountain peak. The line is colored in a gradient from orange at the bottom to pink at the top.

ALGEBRA BERNAYS

SVEUČILIŠTE



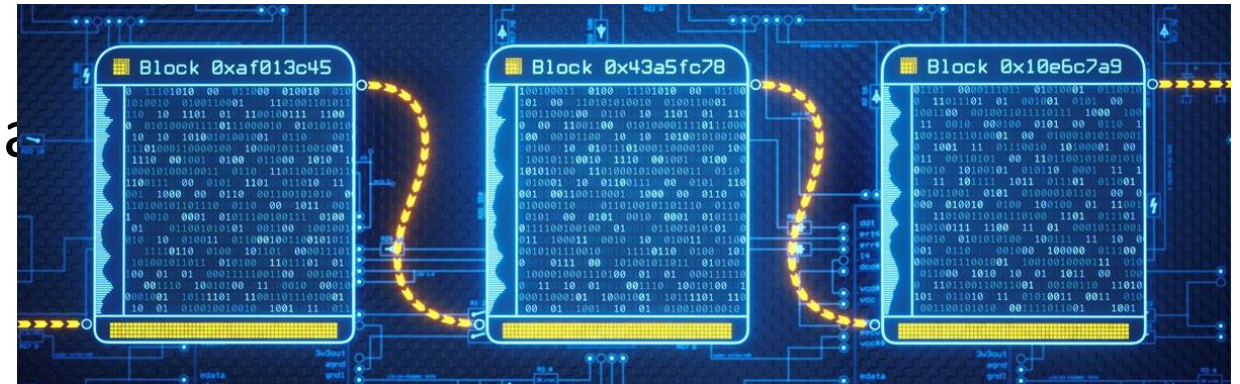
POSLOVNI INFORMACIJSKI SUSTAVI (PIS)

Blockchain /
Ulančani blokovi

Tomislav Bronzin, mag. ing. el.

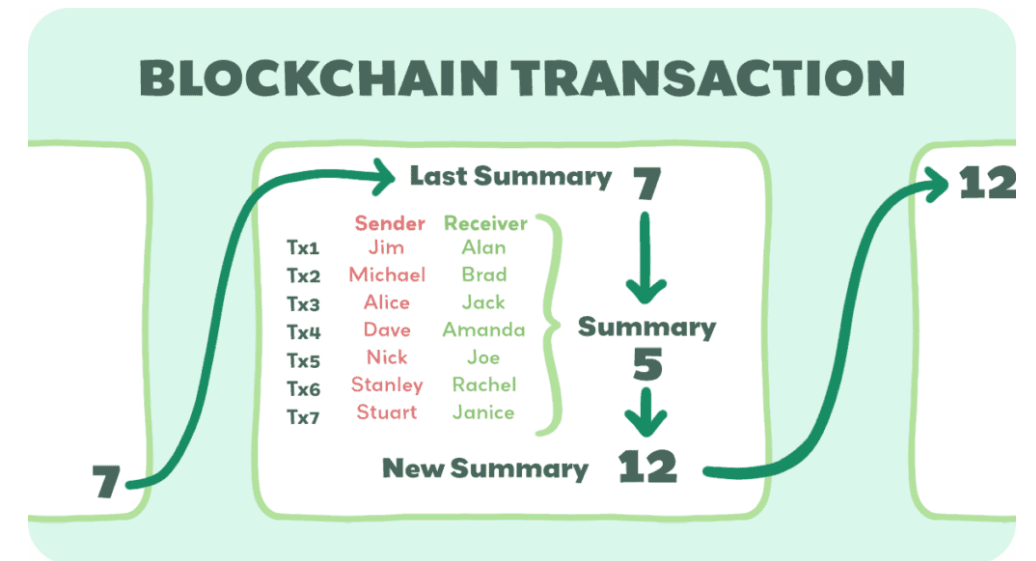
Blockchain – tehnologija povezanih (ulančanih) blokova

- Softverska tehnologija utemeljena na kriptografiji koja pohranjuje podatke
- Podaci su transakcije pohranjene u jedinicama koje se nazivaju blokovi
- Svaki blok ima neke podatke (blok) prije, a neke podatke (blok) poslije
- Funkcionira kao decentralizirana evidencija transakcija
- Vrlo sigurna tehnologija zbog svojih atributa peer-to-peer provjere i autentifikacije
- Ako netko pokuša promijeniti bilo koji podatak u bloku bez autorizacije, to automatski dovodi do lančane reakcije koja se odmah utvrđuje



Blockchain – tehnologija povezanih (ulančanih) blokova

- Radi se o međusobno povezanim blokovima podataka. Svaki blok ima:
 - Vremenski žig
 - Podatke o transakciji (imovini)
 - Svoju identifikacijsku oznaku (hash)
 - Identifikacijsku oznaku (hash) bloka na koji se nadovezuje
- Svaka službena izmjena poput potpisa postaje novi blok s vlastitom oznakom (*hashom*)



Blockchainovi kao distribuirane glavne knjige



Centralised



Decentralised



Distributed

Pohrana podataka u Blockchain okruženju

Funkcioniranje blockchain-a: Osnove

- **Kronološka glavna knjiga**
 - Transakcije su "pseudo-anonimne"
 - Transakcije su grupirane u "blokove"
 - Transakcije se bilježe i ovjeravaju podacima:
 - O vremenu
 - Iznosu i
 - Sudionicima
 - Kao da je javni bilježnik prisutan pri svakoj transakciji
- **Blockchain nije centraliziran**
 - Nema jednog vlasnika
 - Postoje stroga pravila o tome kako se mora održavati lanac povezanih blokova



Funkcioniranje blockchain-a: Održavanje

Proof of Work

vs

Proof of Stake



proof of work is a requirement to define an expensive computer calculation, also called mining



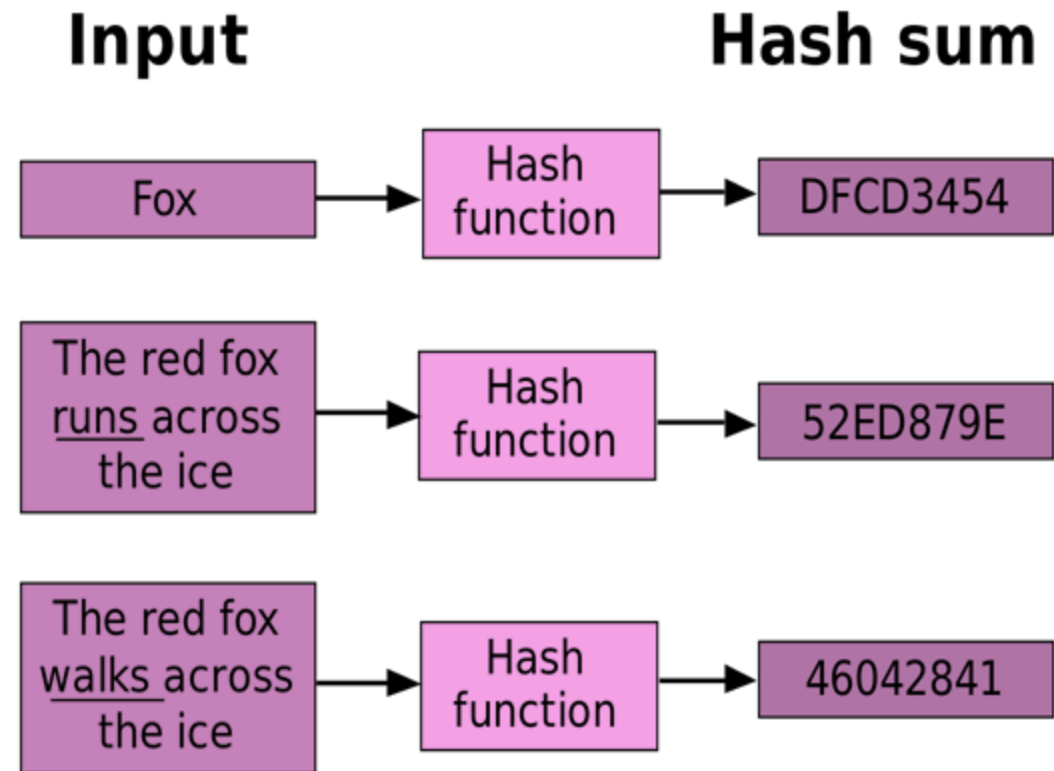
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

- Pojedinci koji održavaju i ažuriraju Blockchain su "rudari" i isplaćuje im se nagrada
- Rudari obrađuju transakcije na sljedeći način:
 - Rješavaju složeni matematički problem
 - Slanjem transakcije drugim čvorovima na provjeru

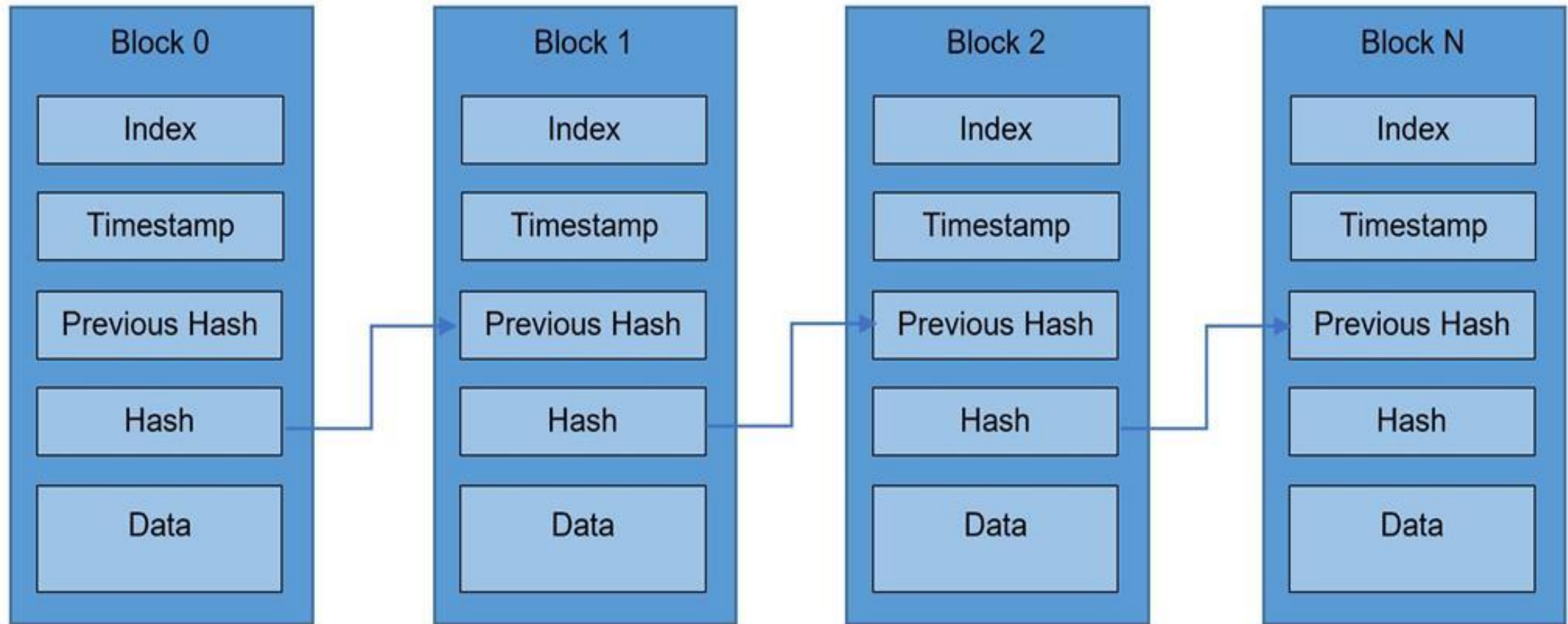
Funkcioniranje blockchain-a: Označavanje (Hashing)

Kada se svi rudari slože da je problem ispravno riješen, blok se dodaje u lanac i vidljiv je cijeloj mreži.

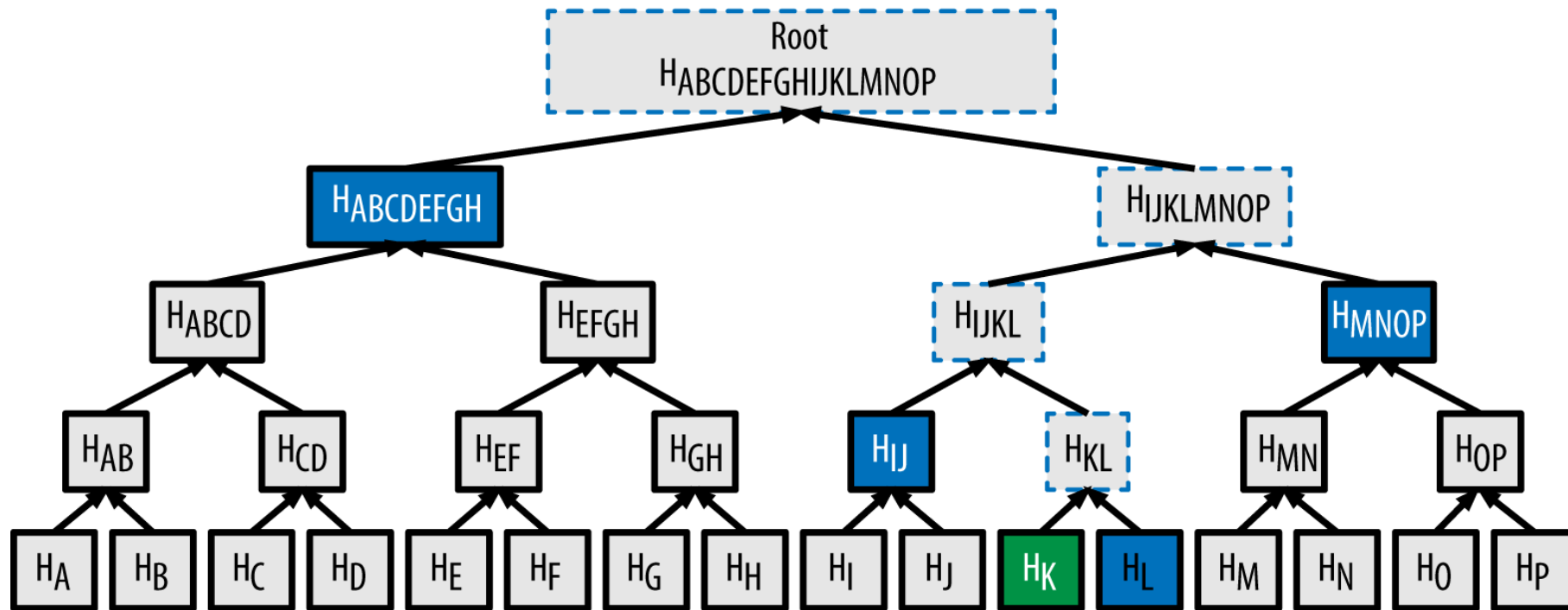
- Neprekinuti Hash (pečat) potvrđuje da je blok, a time i svaki blok prije njega, legitiman
- Rudari su motivirani da dodaju "valjane" transakcije zbog nagrade;
- Nevažeće transakcije se odbijaju i stoga se ne dodjeljuje nagrada



Povezani blokovi - lanac blokova

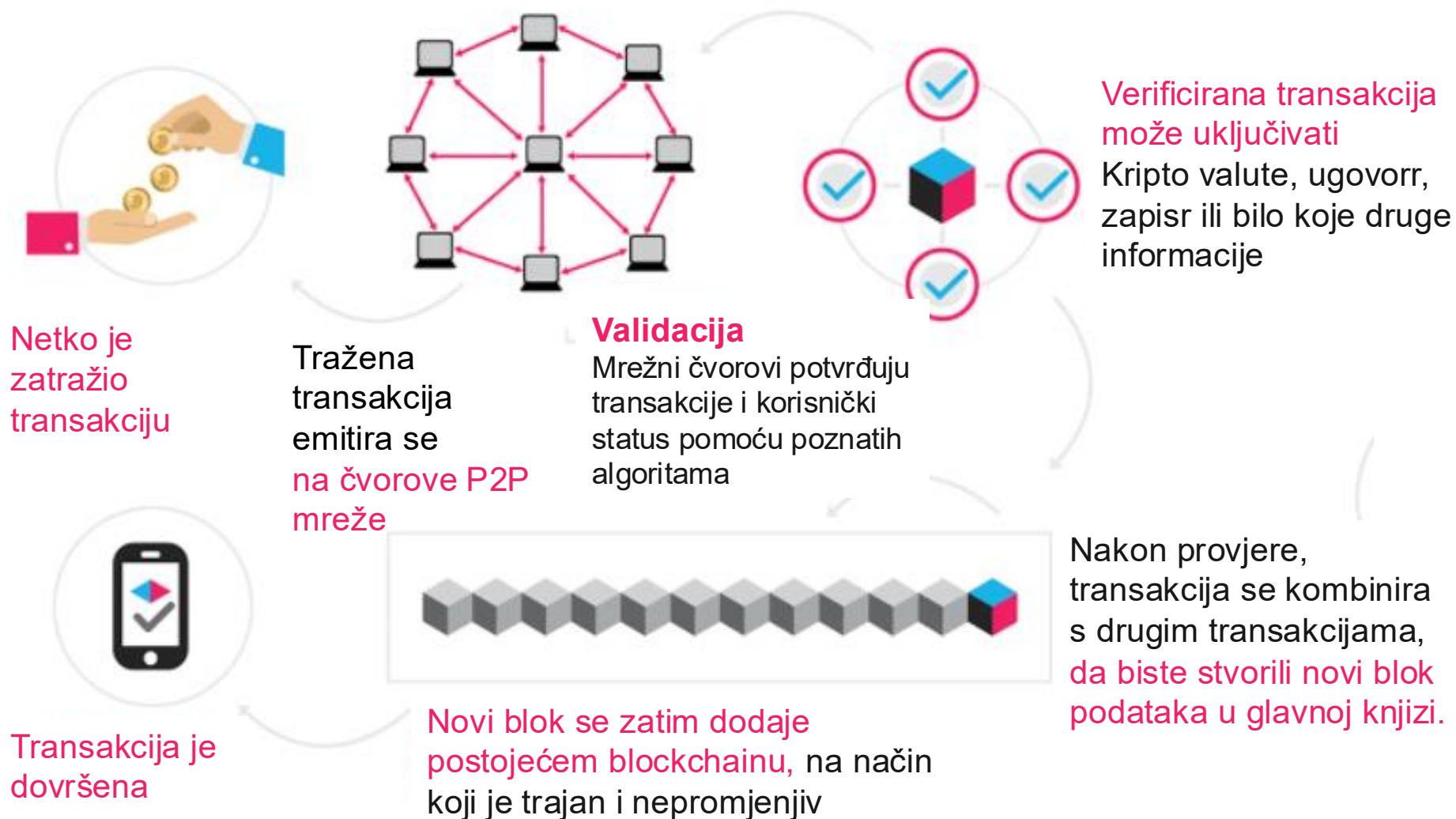


Merkleovo stablo (Merkle Tree)



Merkleovo stablo je struktura u obliku stabla, gdje čvorovi grana/listova sadržavaju oznaku (hash) dokumenta, a svaki pojedinačni čvor i srednji čvor sadržava će hash kombinacije djece-čvorova.

Funkcioniranje digitalne distribuirane glavne knjige



Blockchainovi: otvoreni-javni i zatvoreni

Permissionless/Otvoreni - javni

- Sustavi bez dopuštenja omogućuju svakome pristup i korištenje mreže bez potrebe za dopuštanjem
- Decentralizirani blockchaini bez povjerenja – svatko može obrađivati blokove
- Konsenzus se obično postiže putem Proof of Work-a
- Rudari plaćeni za validaciju
- Npr. **Ethereum, Bitcoin**

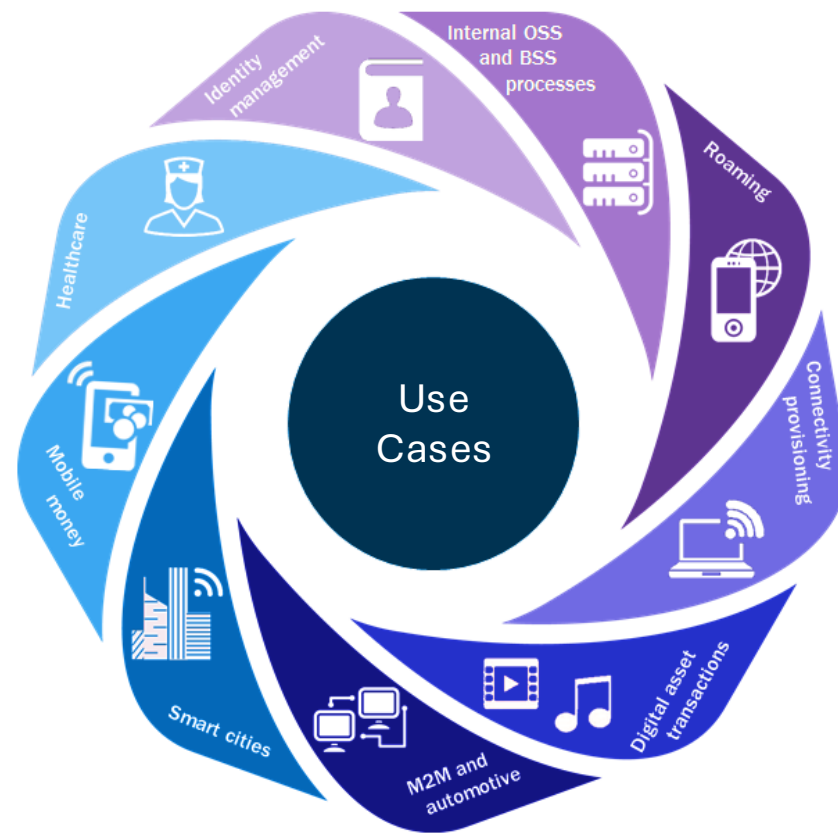
Permissioned/Zatvoreni

- Nije javno dostupan, korisnici se moraju identificirati (npr. digitalnim certifikatom)
- Korisnici moraju imati dozvolu za pristup
- Pouzdano: svi procesori blokova su poznati
- Manje obrade potrebno za konsenzus, dakle brže
- Npr. **Hyperledger**

Za što je blockchain?

Nepromjenjivo pohranjivanje digitalnog prikaza entiteta kako se njihovo stanje mijenja putem transakcija

- **Kriptovalute/mjesta pohrane vrijednosti** - Koje je stanje na mom računu?
- **Digitalni identitet** - Tko ste i kako ste se mijenjali kroz vrijeme?
- **Digitalni prikaz imovine/tokenizacija** - Tko je bio vlasnik ovog automobila tijekom vremena?
- **Praćenje porijekla hrane ili lijekova** - Iz koje zemlje i poštanskog broja dolazi ova piletina?



Pametni ugovori (primjena blockchaina)

- Pametni ugovor omogućuje pojedincima razmjenu podataka na pouzdan i beskonfliktna način bez oslanjanja na treću stranu poput banke, odvjetnika ili javnog bilježnika.
- To je samoautomatizirani računalni program koji može odraditi uvjete bilo kojeg ugovora.
- Uglavnom na temelju objektivnih uvjeta presedana
 - kriteriji „ako-onda“

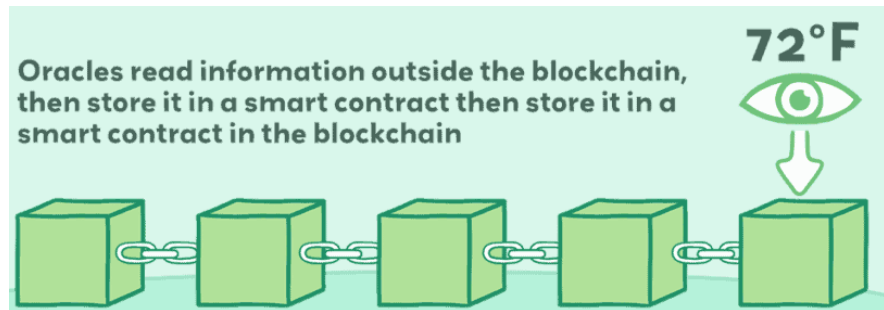


Blockchain Oracle-i

- Lanci blokova ne mogu pristupiti podacima izvan lanca
- Blockchain Oracles djeluju kao most između digitalnog i stvarnog svijeta
- Oni donose vanjske podatke u blockchain okruženje pružajući pametne ugovore s vanjskim informacijama.
- Podaci izvan blockchaina nazivaju se “off-chain”
- Podaci unutar blockchaina nazivaju se "on-chain"
- Svaki uređaj ili entitet koji povezuje deterministički blockchain s podacima izvan lanca naziva se blockchain proročište
- Smatraju se blockchain middlewareom jer služe kao poveznica između dva područja

Blockchain Oracle-i (2)

- Omogućite izvršavanje pametnih ugovora ovisno o stvarnim ulazima i izlazima
- Oracle mreža šalje podatke iz stvarnog svijeta u blockchain pametne ugovore
- Metoda povezivanja s postojećim naslijeđenim sustavima, izvorima podataka i naprednim izračunima

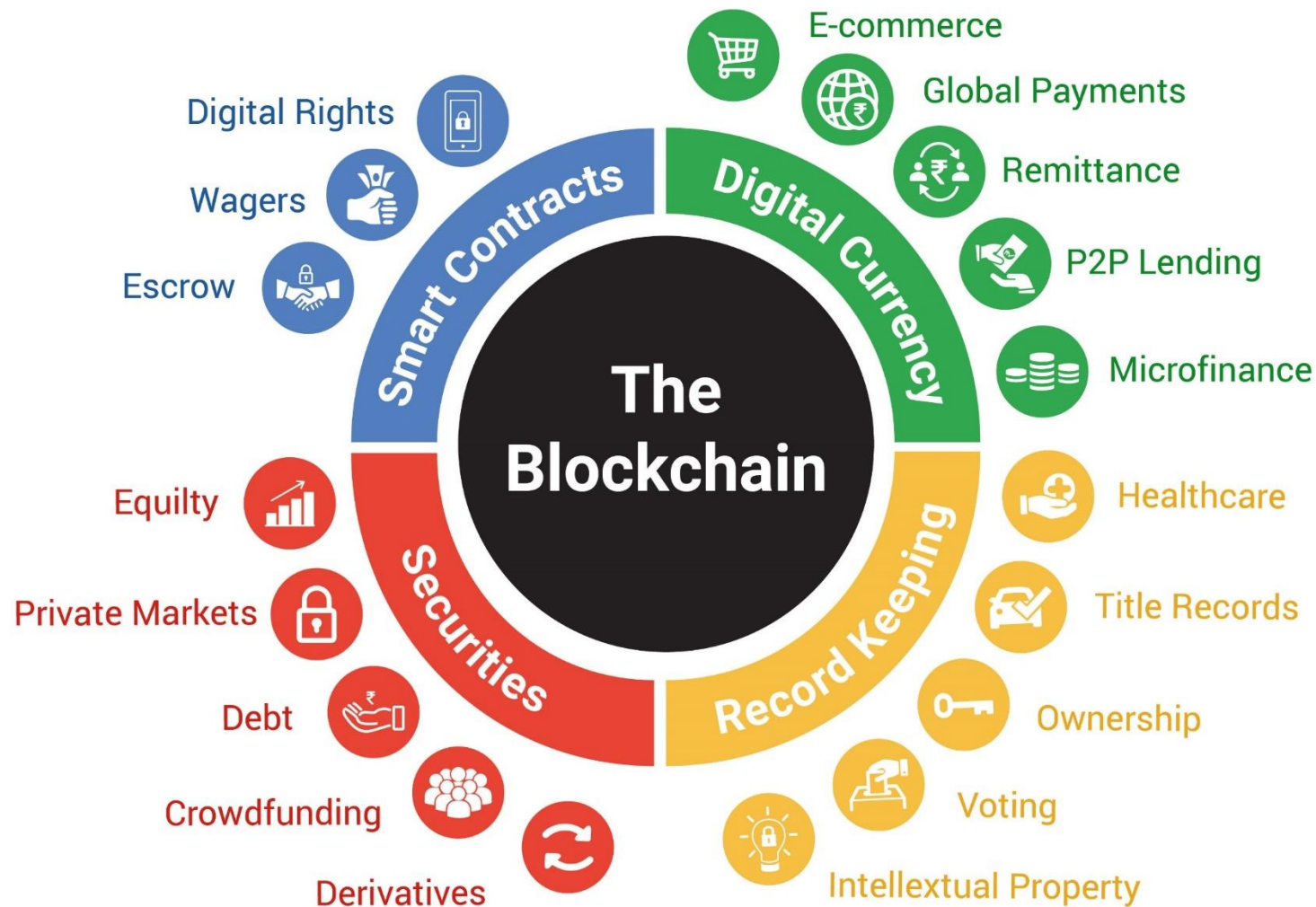


- Tipovi Oracle-a:
 - Softverski
 - Obraduju mrežne podatke kao što su tečajevi, informacije o letovima ili vremenska prognoza
 - Hardverski
 - U interakciji s fizičkim svijetom, poput RFID senzora u lancima opskrbe
 - Temeljeni na konsenzusu
 - Oni prikupljaju podatke iz više izvora kako bi postigli konsenzus, osiguravajući pouzdanost podataka

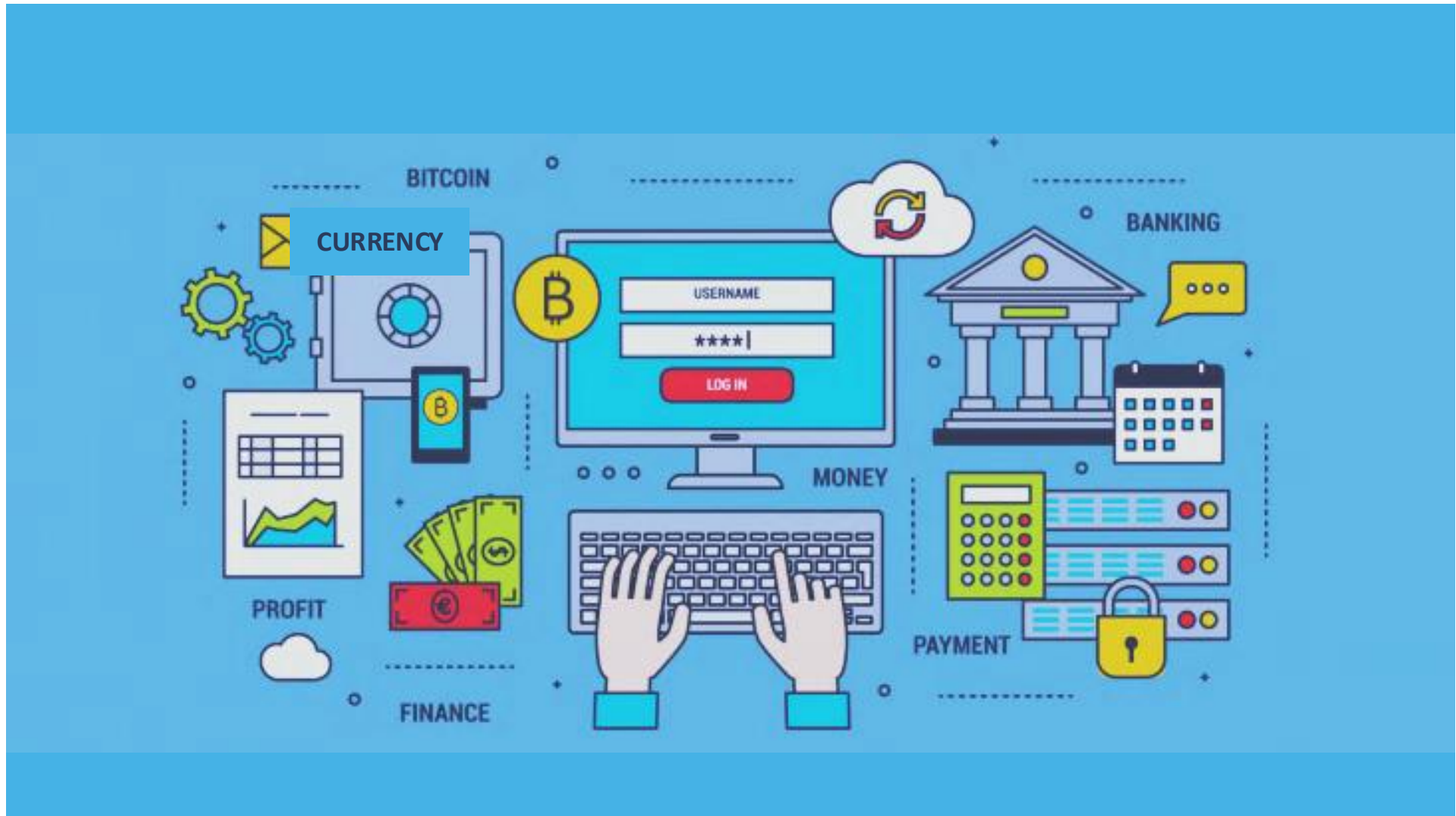
Mogućnosti upotrebe pametnih ugovora



Blockchain – primjene u industrijama



Blockchain u Financijama



Blockchain u Financijama

Plaćanja i doznake

- Transakcije se mogu odvijati izravno između dvije strane na besprijekornoj P2P osnovi.
- Primjena tehnologije za inozemne transakcije ima potencijal smanjiti rizik i troškove transakcija te poboljšati brzinu, učinkovitost i transparentnost.

Izdavanje, vlasništvo i prijenos financijskih instrumenata

- Tržište vrijednosnih papira temeljeno na blockchainu omogućuje trgovcima kupnju ili prodaju dionica izravno na burzama ili izravno drugim sudionicima na tržištu na P2P način bez posredničkih usluga koje pruža broker ili klirinška kuća.

Latencija kliringa i poravnanja

- Na blockchainu se cijeli životni ciklus trgovine, uključujući njezino izvršenje, kliring i namiru, može odvijati na razini trgovine, smanjujući latenciju nakon trgovine i smanjujući izloženost druge ugovorne strane.

Blockchain u Zdravstvu



Blockchain u zdravstvu

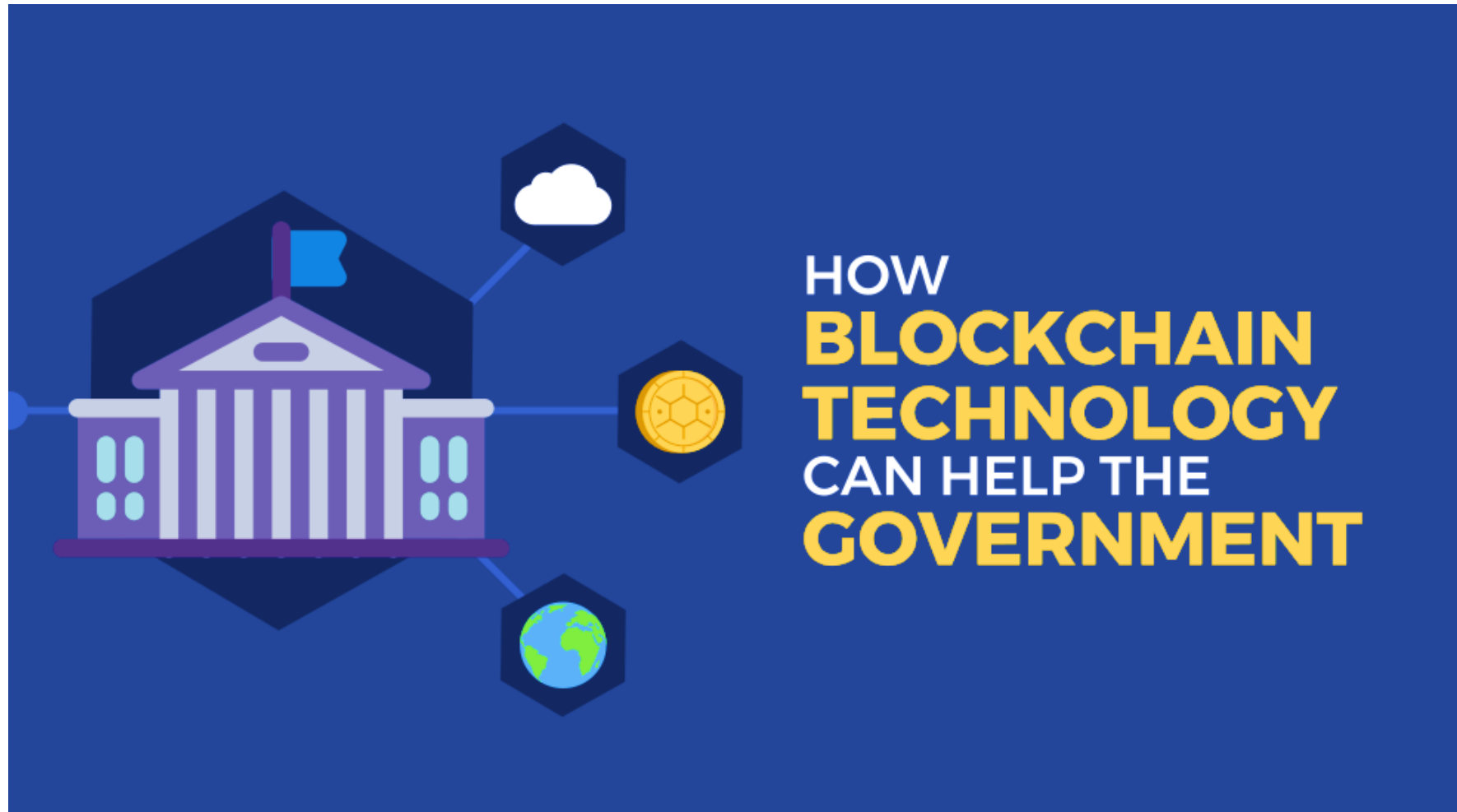
Ograničavanje troškova

- Blockchain se može filtrirati za identifikaciju i upozorenje o specifičnoj aktivnosti u lancu, praćenju, korištenju uzoraka, može uključivati podatke koji predstavljaju liječnika, potrošača, lijekove, procedure, sve se može tokenizirati i dodati u lanac.
 - Izgradnja baze pravila korištenjem najboljih praksi, ICD kodova, medicinskih postupaka i drugih troškova može se pratiti i revidirati korištenjem blockchaina.

Pametni ugovori

- Pametni ugovori bi automatski plaćali pružateljima usluga kada se uspostave uvjeti pružanja usluge, kao što su:
 - Potvrda da je uslugu primio registrirani pacijent Medicaida
 - Uslugu je pružio propisno registriran liječnik /davatelj usluga
 - Niti jedna strana nije na javnom popisu bivših sudionika bilo kakve prijevare

Blockchain u Vladi/Državnoj upravi



Blockchain u Vladi

Registracija imovine

- Okvir blockchaina omogućuje vladinim agencijama povećanje točnosti i učinkovitosti javno pohranjenih zapisa povezivanjem vlasništva nad imovinom s jednom, zajedničkom knjigom bez ometanja postojećih podataka registra.

Usluge identifikacije

- Blockchain omogućuje vladinim agencijama stvaranje jedinstvene, pouzdane zbirke digitalnih identifikacijskih dokumenata.
- Ovi dokumenti olakšavaju vladinim službenicima usklađivanje sukoba podataka i pružaju građanima kontrolu nad vlastitim identitetom.

Blockchain u Vladi (nastavak)

Sprječavanje prijevara i usklađenost

- Blockchain stvara dijeljenu i pouzdanu knjigu koja sekvencijalno dodaje kriptografski sigurne podatke.
- Glavna knjiga dostupna je samo pouzdanim stranama, što državnim administratorima daje sigurnost da rade s podacima koji su ažurni, točni i kojima je gotovo nemoguće manipulirati.

Lanac opskrbe

- Blockchain čini preciznu lokaciju objekta (i njegovu prateću digitaliziranu dokumentaciju) dijelom trajnog zapisa koji se može pratiti.
- Pružanje vladi pune vidljivosti lanca opskrbe

Pitanja



Primjeri pitanja za kontinuiranu provjeru

- Što je Blockchain tehnologija i kako funkcionira kao distribuirana glavna knjiga?
- Koje su razlike između centralizirane, decentralizirane i distribuirane pohrane podataka u blockchain okruženjima?
- Kako transakcije u blockchain tehnologiji ostaju pseudo-anonimne i koja su stroga pravila održavanja?
- Koja je razlika između Proof of Work i Proof of Stake u održavanju blockchaina?
- Kako proces raspršivanja potvrđuje transakcije i dodaje blokove u blockchain?
- Koje komponente čine blockchain strukturu i kako su međusobno povezane?

Primjeri pitanja za kontinuiranu provjeru

- Što je Merklovo stablo i kako funkcionira u blockchain tehnologiji?
- Kako funkcionira digitalna distribuirana knjiga i koji su koraci uključeni u provjeru transakcija?
- Koje su ključne razlike između blockchaina bez dopuštenja i s dopuštanjem?
- Koje su neke od ključnih primjena blockchain tehnologije?
- Kako pametni ugovori omogućuju pouzdanu razmjenu podataka bez posrednika?

Primjeri pitanja za kontinuiranu provjeru

- Koji su neki slučajevi upotrebe pametnih ugovora?
- Kako se blockchain tehnologija koristi u različitim industrijama?
- Koji su ključni aspekti blockchain tehnologije u financijskom sektoru?
- Kako blockchain tehnologija može koristiti zdravstvenom sektoru?
- Koje su potencijalne prednosti blockchain tehnologije za vladine operacije?



**ALGEBRA
BERNAYS**
SVEUČILIŠTE