Uvod u blokčejn

Različita značenja termina

- **Sam Bitcoin**, **Ethereum** i ostale kriptovalute
- **Određena blokčejn tehnologija** koja pruža osnovu za rad Bitcoina i drugih kriptovaluta
- **Ideja blokčejna** kao novog načina za beleženje podataka o transakcijama

Glavna knjiga

- Vođenje **računovodstvenih knjiga sa dvojnim unosima – dvojno knjigovodstvo** (engl. *double entry bookkeeping*)
- **Glavna knjiga** (engl. *ledger*) služi za beleženje transakcija, sa dugovanjima i potraživanjima u posebnim kolonama, kao i početnim i krajnjim stanjem računa
- Za transakciju se beleži - na teret kog računa (**debit**), u korist kog računa (**kredit**), kao i iznos

Izvor: https://en.wikipedia.org/wiki/Ledger#/media/File:Hauptbuch_Hochstetter_vor_1828.jpg

Distribuirana glavna knjiga

- **Distribuirana glavna knjiga** (engl. *distributed ledger*) ili **tehnologija distribuirane glavne knjige** (engl. *distributed ledger technology – DLT*) je način implementacije glavne knjige kod koga više nezavisnih "knjigovođa" u svojim kopijama beleže sve validne transakcije

- Usled postojanja više knjigovođa, neophodno je unapred dogovoriti:
  - **pravila** po kojima se utvrđuje koje **transakcije** su **validne**, kao i
  - **mehanizam postizanja dogovora** (**konsenzusa**) o tome koje će transakcije i u kom redosledu biti upisane
  - način na koji će se **razmenjivati poruke o transakcijama** između knjigovođa

Primer: Distribuirana glavna knjiga

- Stanje glavne knjige:

  Aca: $A = 5, B = 2, C = 3$
  Branka: $A = 5, B = 2, C = 3$
  Cveta: $A = 5, B = 2, C = 3$

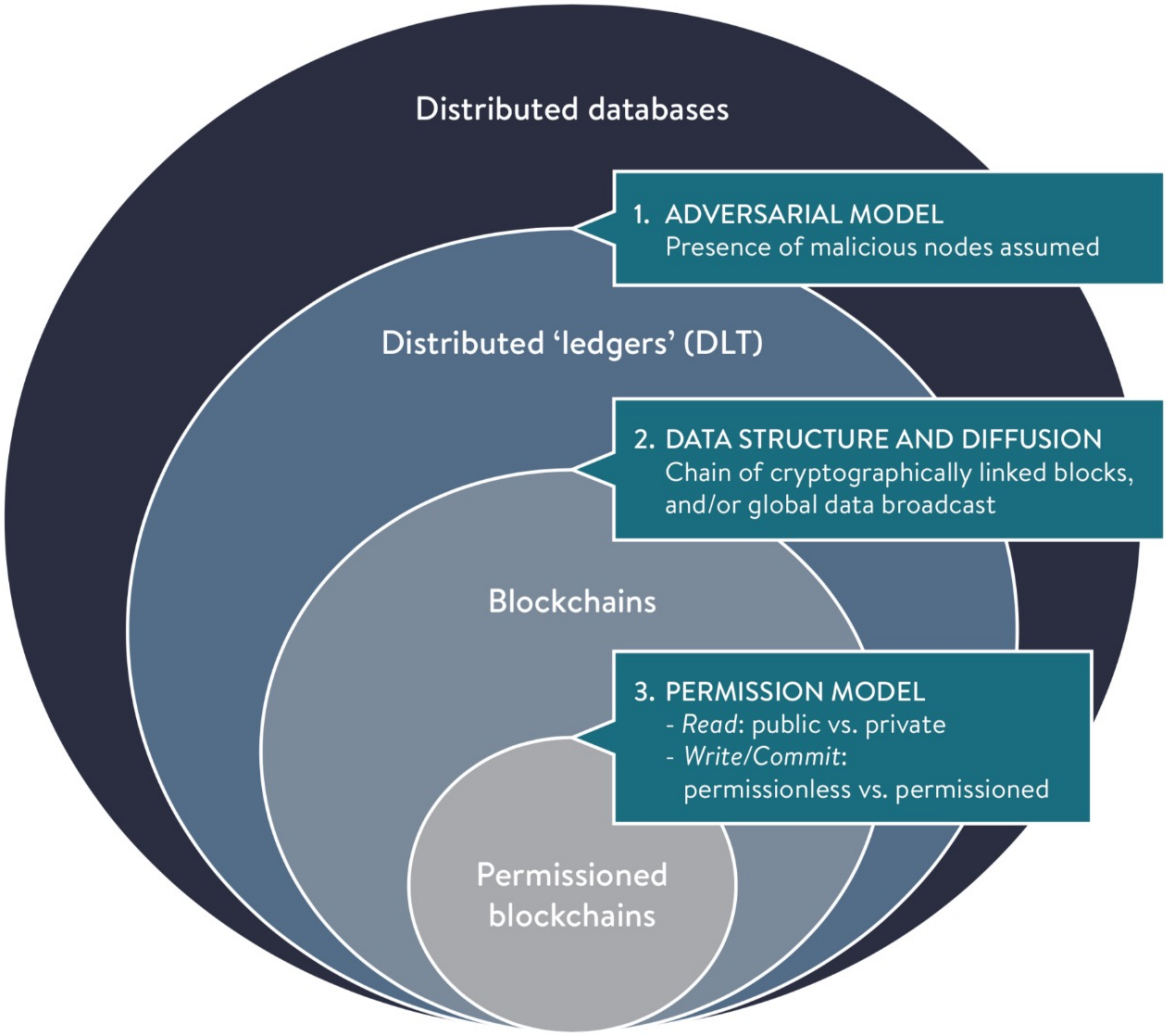
- Aca predlaže transakciju: Aca šalje Branki 2 dinara
- Predložena transakacija stiže do svih u mreži. Svi proveraju:
  - Da li A ima dovoljno sredstava za predloženu transakciju?
  - Da li ista sredstva trenutno nisu neophodna i za neku drugu predloženu transakciju?
- Ako su dogovorena pravila zadovoljena, svako upisuje predloženu transakciju u svoju kopiju glavne knjige, novo stanje svih kopija glavne knjige:

  Aca = 3, Branka = 4, Cveta = 3

Distribuirana baza, glavna knjiga i blokčejn

- **Distribuirana baza podataka** (engl. *distributed database*) je vrsta baze podataka kod koje se **podaci čuvaju u više čvorova** (računara)
- **Distribuirana glavna knjiga** (engl. *distributed ledger*) ili **tehnologija distribuirane glavne knjige** (engl. *distributed ledger technology* – DLT) je vrsta distribuirane baze podataka koja pretpostavlja moguće **prisustvo malicioznih korisnika** (čvorova), vrsta strukture podataka za pamćenje transakcija, razmeštena na više čvorova
- **Blokčejn** (engl. *blockchain*) je **distribuirana struktura podataka** koja implementira **distribuiranu glavnu knjigu**, a sastavljena je od **lanca kriptografski povezanih blokova** koji **sadrže grupe transakcija**. U opštem slučaju, vrši se **emitovanje** (engl. broadcast) **svih podataka** svim učesnicima u mreži
- **Tokenizacija** (engl. *tokenisation*) se odnosi na proces digitalnog predstavljanja tipično već postojećeg (off-chain) dobra (engl. *asset*) u DLT

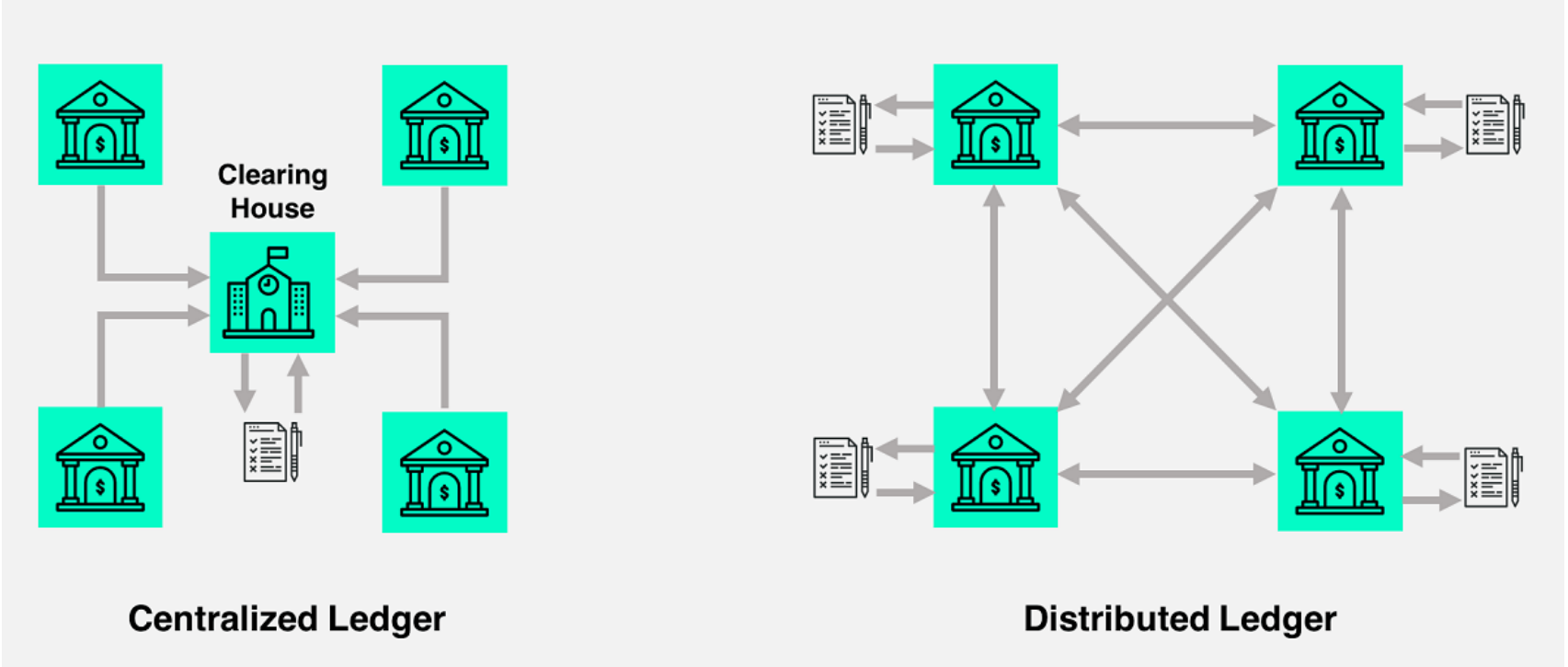
Distribuirana baza, glavna knjiga i blokčejn



Izvor: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-global-blockchain-benchmarking-study-2017.pdf

Distribuirana glavna knjiga – DLT

- **Centralizovana** i **distribuirana glavna knjiga**:



Izvor: https://tradeix.com/distributed-ledger-technology/

Distribuirana glavna knjiga – DLT

- **DLT** kao **sistem** sastoji se od **tri glavne komponente**:
  - **model podataka** (engl. *data model*) obuhvata trenutno stanje glavne knjige
  - **jezik transakcija** (engl. *language of transactions*) kojim se vrši promena stanja glavne knjige
  - **protokol** (engl. *protocol*) se koristi kako bi se među učesnicima u distribuiranom sistemu postigao konsenzus o tome koje će transakcije biti prihvaćene i u kom redosledu upisane u glavnu knjigu
- **DLT** je osnova za **novu generaciju transakcionih aplikacija** koje uspostavljaju **poverenje** (engl. *trust*), **odgovornost** (engl. *accountability*) i **transparentnost** (engl. *transparency*), pri tom **racionalizujući poslovne procese i pravna ograničenja kroz automatizaciju**

Distribuirana glavna knjiga – DLT

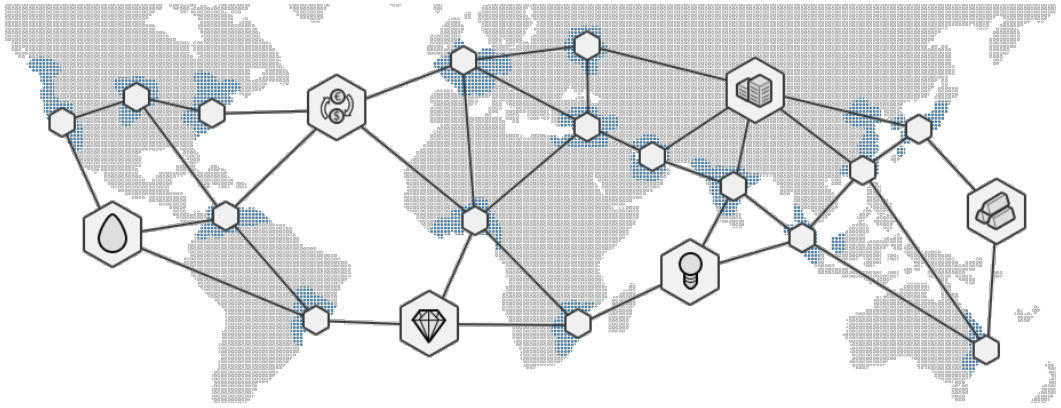
- Koncept DLT je postojao pre Bitcoina i blokčejn tehnologije. **Problem vizantijskih generala** (Lamport, Shostak i Pease,1982), opisuje kako "računarski sistemi moraju da se nose sa suprotstavljenim informacijama" u neprijateljskom (engl. *adversarial*) okruženju
- Dalja istraživanja dovela su do **prvog algoritma** (**PBFT**) za **visoko dostupne sisteme koji mogu da tolerišu vizantijske otkaze** sa malim povećanjem latencije (Castro i Liskov, 1999)
- Najranije identifikovano pojavljivanje koncepta blokčejna je u radovima Haber i Stornetta 1991. (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.8740), kao i Bayer, Haber i Stornetta 1992. (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.71.4891), koji su uveli pojam lanca kriptografski povezanih blokova podataka kako bi se efikasno i bezbedno postavljali vremenski otisci na digitalne podatke u distribuiranim sistemima korišćenjem kriptografskih heš funkcija i Merkleovih stabala (engl. *Merkle trees*)
- **Bitcoin blokčejn** je 2008. doveo do **konvergencije skupa tehnologija**, uključujući **vremenski otisak transakcija**, **P2P mreže**, **kriptografiju** (digitalne potpise), **deljenu moć izračunavanja**, zajedno sa **novim konsenzus algoritmom**

Blokčejn

- Glavna razlika između blokčejna i drugih distribuiranih baza podataka je u tome što je blokčejn projektovan kako bi se **postigao konzistentan i pouzdan dogovor o zapisu događaja** (npr. "ko je vlasnik čega") **između nezavisnih učesnika** koji mogu imati **različite motivacije i ciljeve**
- **Učesnici u blokčejn mreži postižu konsenzus o promenama stanja deljene baze podataka** (tj. transakcijama između učesnika) **bez potrebe da se veruje u integritet bilo kog učesnika mreže ili administratora**
- **Dogovor o stanju baze podataka** između učesnika u blokčejn mreži postiže se **mehanizmom konsenzusa**, koji osigurava da pogled na deljenu bazu podataka bude isti za svakog učesnika

Blokčejn

- **Kombinacija konsenzus mehanizma** sa **specifičnom strukturom podataka** omogućava da se primenom blokčejna reši tzv. **problem dvostruke potrošnje** (engl. *double spending problem*) – isti digitalni fajl se kopira i prenosi više puta – **bez zahteva za centralnom glavnom knjigom** ili **stranom koja bi sprečavala korisnike od dupliciranja ili potrošnje istog digitalnog fajla više puta**
- **Blokčejn** se, iz prethodnih razloga, može koristiti za **upravljanje prenosom dobara** (engl. *assets*) **ili drugih podataka bez potrebe za centralizovanim autoritetom** u koga svi moraju verovati



Blokčejn

- **Blokčejn** pruža **mehanizme** za:
  - **Spajanje transakcija u blokove** i njihovo beleženje
  - **Kriptografsko povezivanje blokova** u hronološkom redosledu
  - **Održavanje i pristup kopijama glavne knjige**
- Bitcoin kao **prva primena blokčejna** je **rešio problem štampanja valute** i **dvostruke potrošnje** u **digitalnom domenu**

Komponente blokčejn tehnologije

1. **Kriptografija**
   - kriptografske heš funkcije
   - Merkleova stabla
   - sistem sa javnim ključem

CRYPTOGRAPHY
Use of a variety of cryptographic techniques including cryptographic one-way hash functions, Merkle trees and public key infrastructure (private-public key pairs)

2. **P2P mreža**
   - javna ili privatna

P2P NETWORK
Network for peer discovery and data sharing in a peer-to-peer fashion

3. **Konsenzus mehanizam**
   - PoW, PoS, PoET,…
   - PBFT, SBFT

CONSENSUS MECHANISM
Algorithm that determines the ordering of transactions in an adversarial environment (i.e., assuming not every participant is honest)

4. **Glavna knjiga**
   - lanac kriptografski povezanih blokova

LEDGER
List of transactions bundled together in cryptographically linked 'blocks'

5. **Pravila važenja**
   - kako se ažurira glavna knjiga, koje transakcije su validne, itd.

VALIDITY RULES
Common set of rules of the network (i.e., what transactions are considered valid, how the ledger gets updated, etc.)

Izvor: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$FILE/ey-global-blockchain-benchmarking-study-2017.pdf