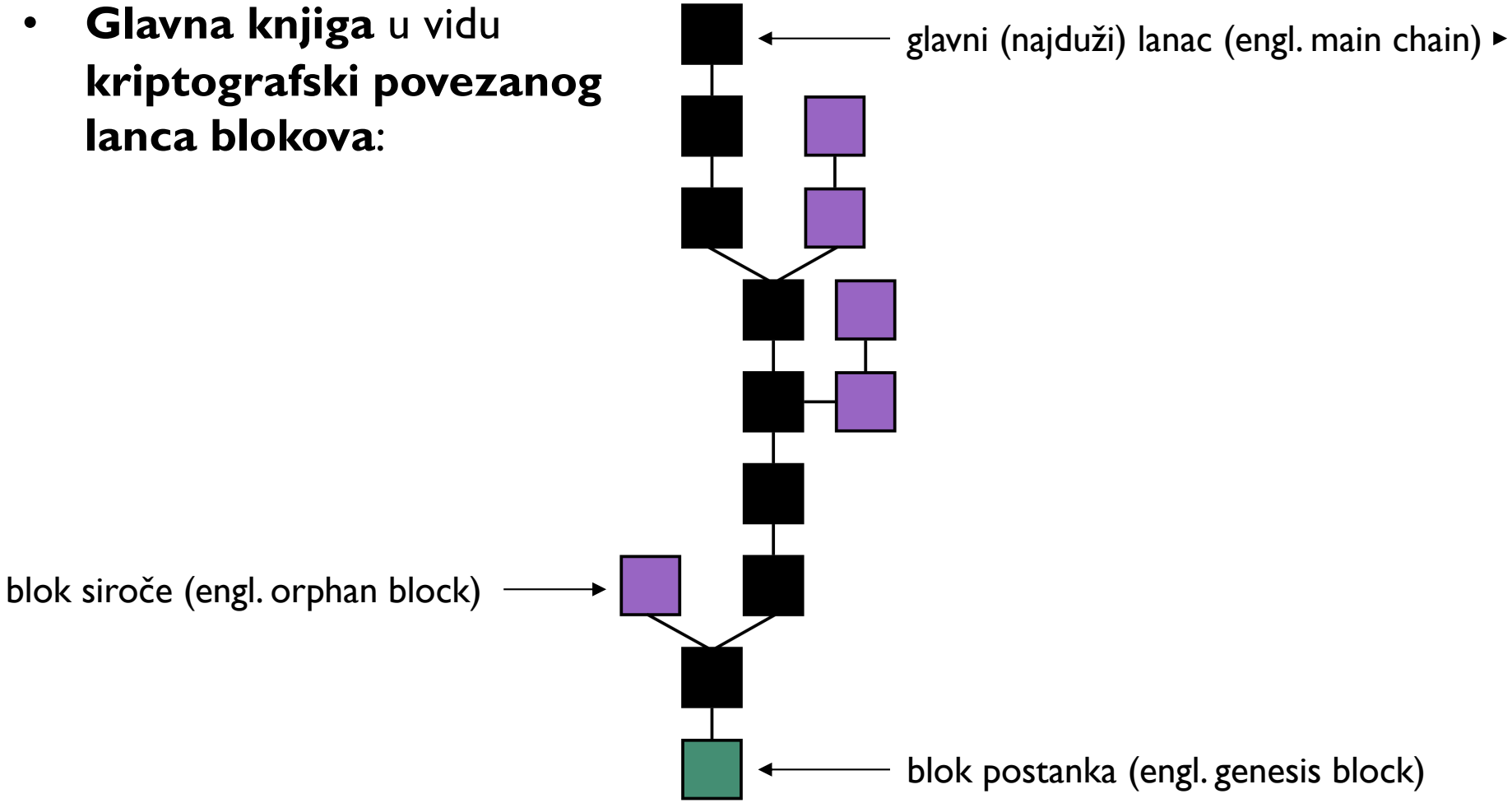
Uvod u blokčejn (nastavak)

Lanac blokova

- **Glavna knjiga** u vidu **kriptografski povezanog lanca blokova**:



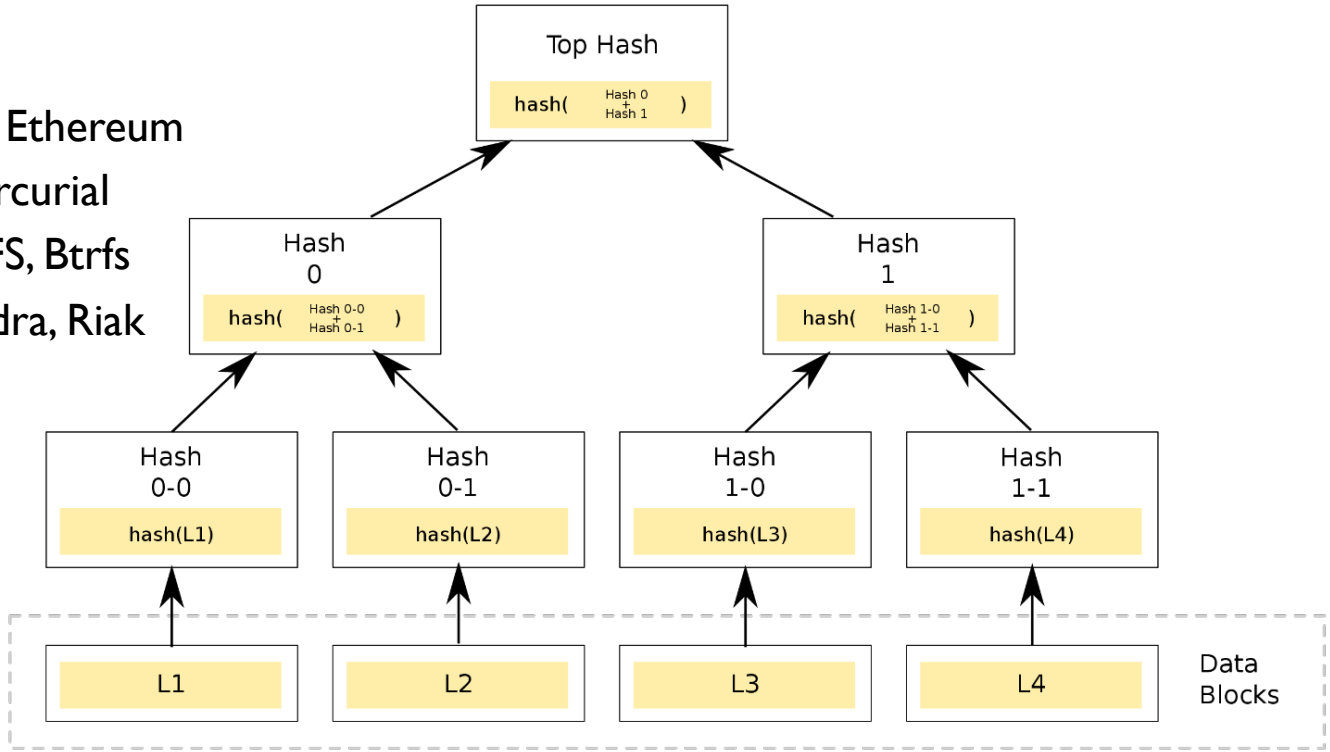
Izvor: https://en.wikipedia.org/wiki/Blockchain

Blok

- **Blok** (engl. *block*) je skup transakcija koje se u kompletu istovremeno dodaju u lanac. Svaki blok sadrži određeni broj transakcija
- **Postavljanje vremenskog otiska** (engl. *timestamping*) je ključno svojstvo blokčejn tehnologije. Svaki blok sadrži vremenski otisak i svaki novi blok se referencira na prethodni. Zajedno sa **kriptografskim heševima**, ovakav lanac blokova sa vremenskim otiscima pruža neizmenjiv zapis svih transakcija u mreži, počev od prvog (tj. *genesis*) bloka
- Blok, tj. **zaglavlje** (engl. *header*) bloka, tipično sadrži **četiri metapodatka**:
  - **referencu na prethodni blok** u vidu **kriptografskog heša**
  - **nons** (engl. *nonce*), slučajni broj koji se koristi samo jedanput
  - **vremenski otisak**
  - **koren Merkleovog stabla** za transakcije uključene u blok

Merkleovo stablo

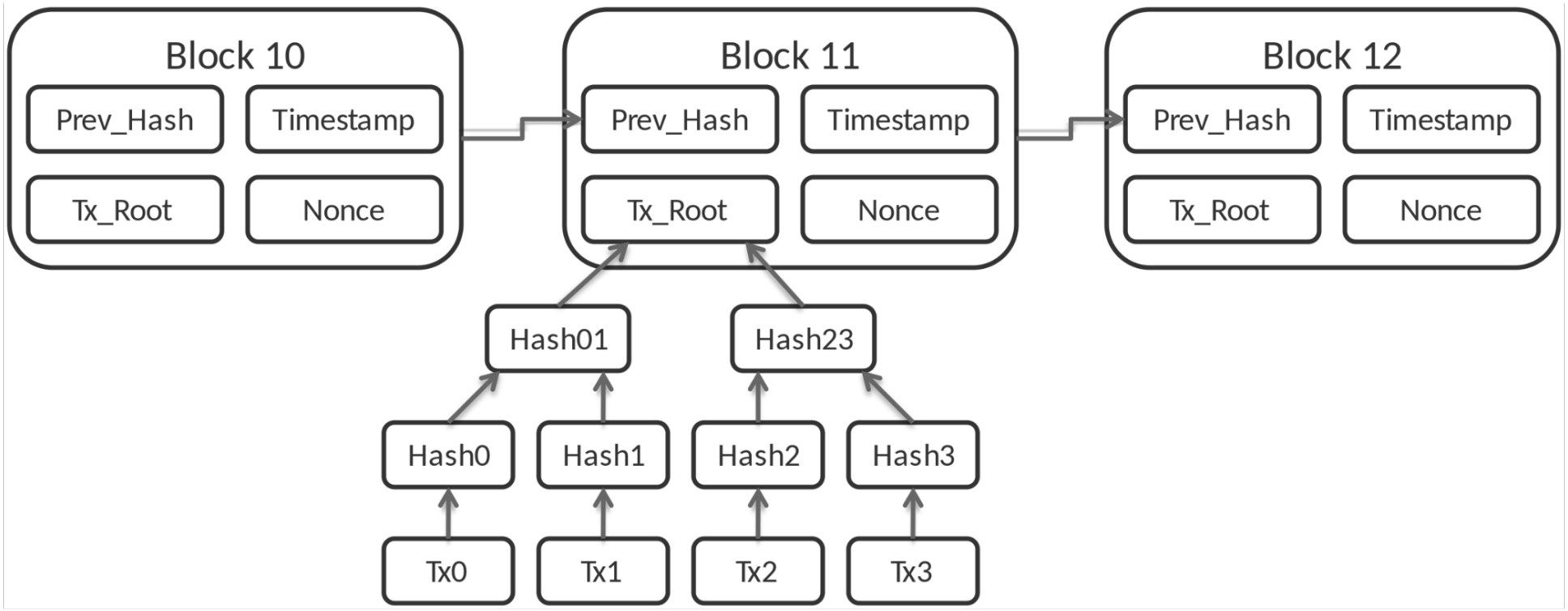
- **Merkleovo stablo** (engl. *Merkle tree* – Ralph Merkle 1979.) ili **heš stablo** je stablo u kome je svaki **terminalni čvor** (list) označen **hešom bloka podataka**, a svaki **neterminalni čvor** je označen **kriptografskim hešom oznaka njegovih potomaka**. Heš stabla omogućavaju efikasnu i bezbednu verifikaciju sadržaja velikih struktura podataka
- **Primene**:
  - Bitcoin, Ethereum
  - Git, Mercurial
  - IPFS, ZFS, Btrfs
  - Cassandra, Riak



Izvor: https://en.wikipedia.org/wiki/Merkle_tree

Primer: Bitcoin lanac blokova

- Primer globalne strukture Bitcoin lanca blokova:



Izvor: https://en.wikipedia.org/wiki/Blockchain

Primer: Princip rada blokčejna

- Aca, Branka, Cveta i Dušan su učesnici u jednoj blokčejn mreži. Stanje računa (glavne knjige) je Aca = 5, Branka = 3, Cveta = 7, Dušan = 4.
- Dušan hoće da izvrši transakciju kojom šalje učesniku Cveti iznos od 3 BTC.

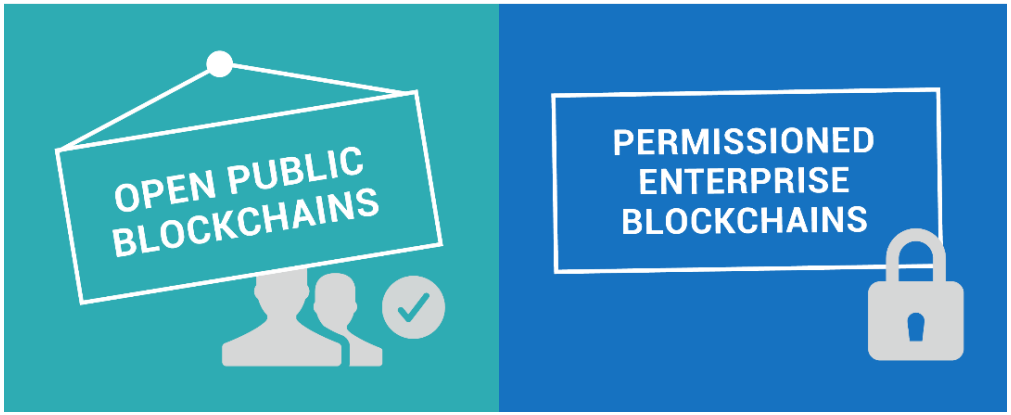
a) Ko mora da predloži tu transakciju i digitalno je potpiše?
b) Ko proverava da li je transakcija validna?
    i) Šta moramo prvo proveriti?
    ii) Da li je transakcija validna i ako Dušan u istom trenutku predlaže transakciju kojom šalje Aci iznos od 4 bitkoina? Kako vremenski otisak uz transakciju utiče na odluku po ovom pitanju?
c) Ko upisuje blokove sa validiranim transakcijama u svoju kopiju glavne knjige?

Pametni ugovori

- **Pametni ugovor** (engl. *smart contract*) je **samo-izvršavajući računarski program** koji **automatski izvršava unapred definisane akcije** (npr. izvrši se plaćanje kada neki događaj okine (engl. *trigger*) pametni ugovor) kada se **određeni uslovi unutar sistema ispune**
- **Funkcionalnost pametnih ugovora** odnosi se na stepen funkcionalnosti DLT radnog okruženja ili mreže u smislu **složenosti izračunavanja** koja može **izvesti na lancu** (engl. *on-chain*)
  - **sa pamćenjem stanja** (engl. *stateful*) – **sekvencijalni**: logički-optimizovani sistem sa širokim funkcionalnostima pametnih ugovora na nivou protokola, pamti interno stanje, podržava iteracije i rekurziju, otežana verifikacija
  - **bez pamćenja stanja** (engl. *stateless*) – **kombinacioni**: transakciono-optimizovani sistem koji ne podržava složena izračunavanja na osnovnom nivou, nema internog stanja, lakša verifikacija

Tipovi blokčejn mreža

- Osnovna **podela blokčejn P2P mreža na osnovu mogućnosti pristupa**:
  - **javne** (engl. *public*), **bez kontrole pristupa** (engl. *permissionless*), tj. sa slobodnim pristupom – bilo ko se može pridružiti mreži
  - **privatne** (engl. *private*), **sa kontrolom pristupa** (engl. *permissioned*), zahteva prethodnu verifikaciju učesnika u mreži koji su obično međusobno poznati
- **Izbor** između javnih i privatnih blokčejna **zavisi od slučaja korišćenja**



Tipovi blokčejn mreža

- Osnovna **podela blokčejn mreža na osnovu mogućnosti pristupa**:

Blockchain types			Read	Write	Commit	Example
	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

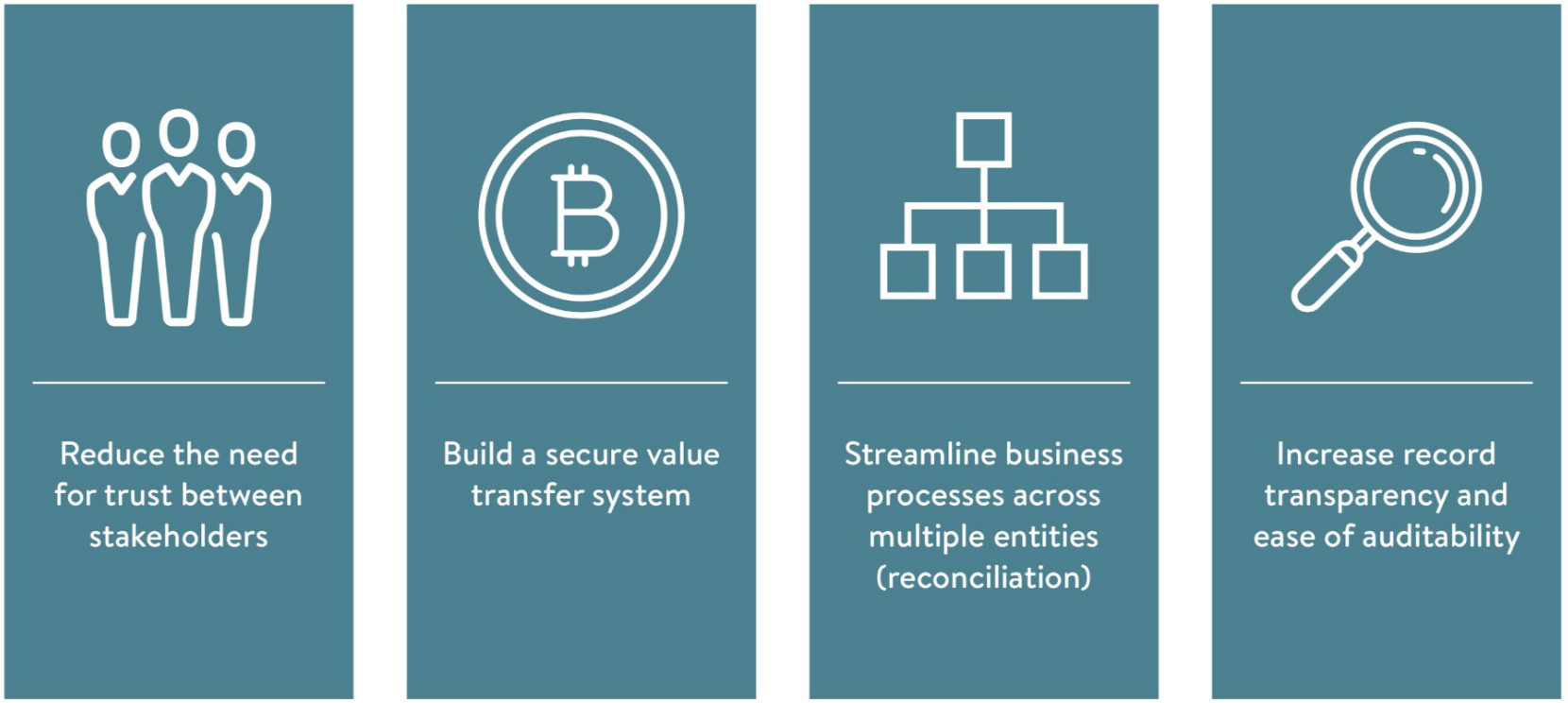
* *Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model).*

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

Primene blokčejna

"Blockchains can help us advance from a 'don't be evil' world to a 'can't be evil' world."

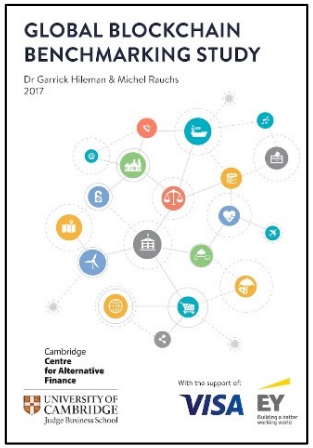
Muneeb Ali, Blockstack
(https://blockstack.org)

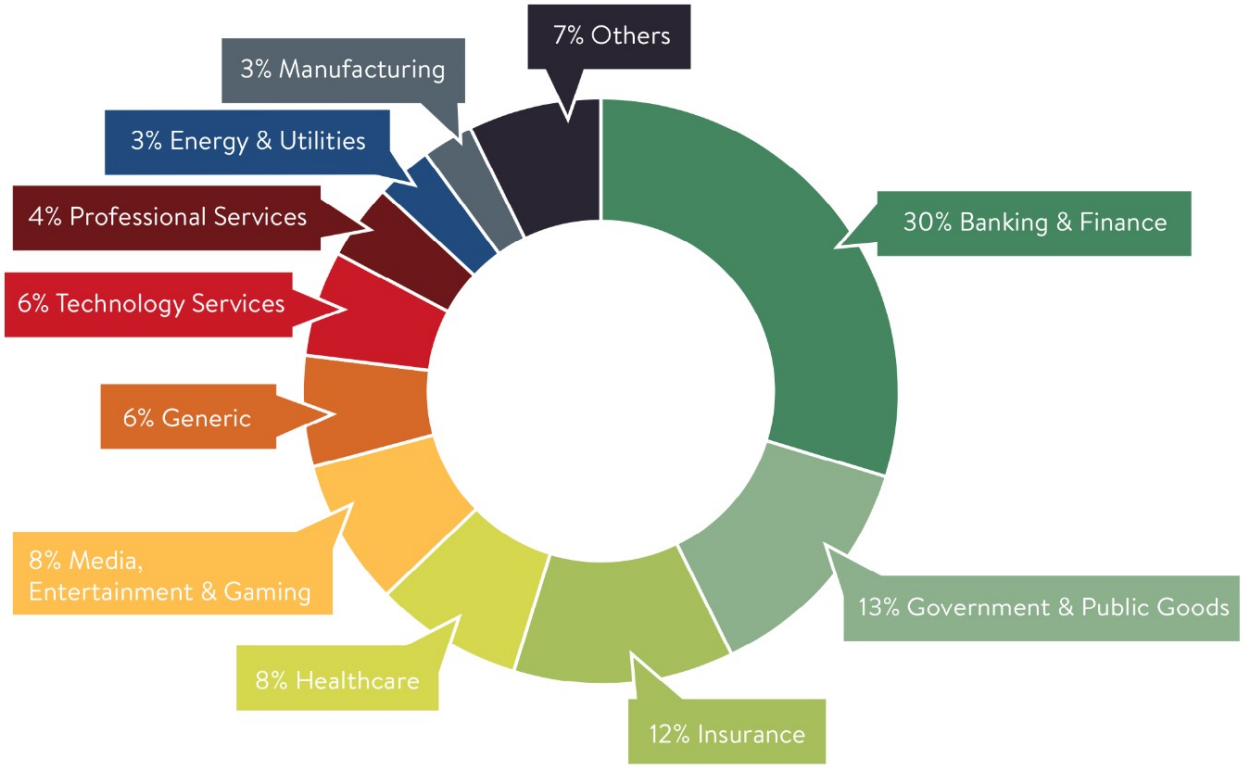


Izvor: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-global-blockchain-benchmarking-study-2017.pdf

Primene blokčejna

- Raspodela slučajeva korišćenja blokčejna prema granama privrede:





Note: This figure is based on a list of 132 use cases, grouped into industry segments, that have been frequently mentioned in public discussions, reports, and press releases.[33]

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

Mitovi o blokčejnu

MYTH

Blockchains are 'trustless'

REALITY

Blockchains always require some degree of trust

MYTH

Blockchains are immutable or 'tamper-proof'

REALITY

Transactions on a blockchain network can be reversed by network participants under specific circumstances

MYTH

Blockchains are 100% secure

REALITY

Blockchains are not automatically more secure than other systems

MYTH

Blockchains are 'truth machines'

REALITY

GIGO ('garbage in, garbage out') applies to every blockchain that uses non-native digital assets and/or external data inputs

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

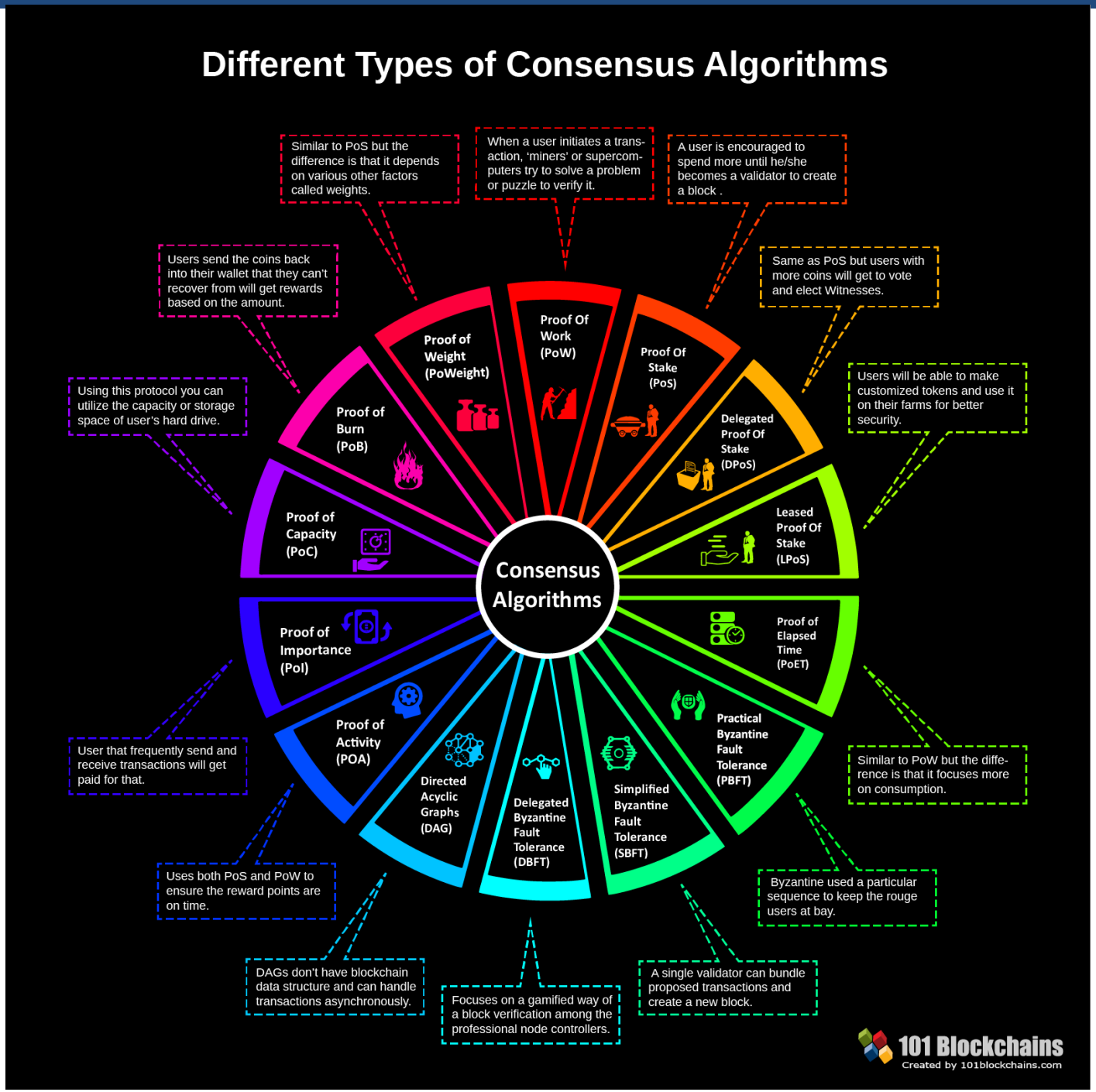
Prednosti blokčejna

- **Nepromenljiva** i **transparentna baza podataka** za **sve učesnike**
- **Nema posrednika** u realizaciji transakcija
- **Nema potrebe** za **poverenjem** u **centralni autoritet**
- **Otporan na maliciozne učesnike**
- **Nema jednu tačku otkaza** (SPoF), **unapređena bezbednost**

DLT i konsenzus algoritmi

Konsenzus algoritmi

- **Konsenzus** se odnosi na proces **postizanja dogovora** između učesnika u mreži o **ispravnom stanju podataka** u sistemu i dovodi do toga da svi čvorovi u mreži dele potpuno iste podatke
- **Konsenzus algoritam** osigurava da su **podaci upisani u glavnu knjigu isti za sve čvorove u mreži** i na taj način **sprečava maliciozne učesnike da manipulišu podacima**
- **Konsenzus algoritmi** zasnovani na **lutriji** (engl. *lottery* – npr. Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed time (PoET), …) i **glasanju** (engl. *voting* – npr. PBFT, SBFT)
- Dodatni materijali:
  - Consensus Algorithms: The Root of the Blockchain Technology: https://101blockchains.com/consensus-algorithms-blockchain/
  - ConsensusPedia: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f


Different Types of Consensus Algorithms
Consensus Algorithms
Proof of Work (PoW)
When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.
Proof Of Stake (PoS)
A user is encouraged to spend more until he/she becomes a validator to create a block .
Delegated Proof Of Stake (DPoS)
Same as PoS but users with more coins will get to vote and elect Witnesses.
Leased Proof Of Stake (LPoS)
Users will be able to make customized tokens and use it on their farms for better security.
Proof of Elapsed Time (PoET)
Similar to PoW but the difference is that it focuses more on consumption.
Practical Byzantine Fault Tolerance (PBFT)
Byzantine used a particular sequence to keep the rouge users at bay.
Simplified Byzantine Fault Tolerance (SBFT)
A single validator can bundle proposed transactions and create a new block.
Delegated Byzantine Fault Tolerance (DBFT)
Focuses on a gamified way of a block verification among the professional node controllers.
Directed Acyclic Graphs (DAG)
DAGs don't have blockchain data structure and can handle transactions asynchronously.
Proof of Activity (POA)
Uses both PoS and PoW to ensure the reward points are on time.
Proof of Importance (PoI)
User that frequently send and receive transactions will get paid for that.
Proof of Capacity (PoC)
Using this protocol you can utilize the capacity or storage space of user's hard drive.
Proof of Burn (PoB)
Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.
Proof of Weight (PoWeight)
Similar to PoS but the difference is that it depends on various other factors called weights.
101 Blockchains
Created by 101blockchains.com

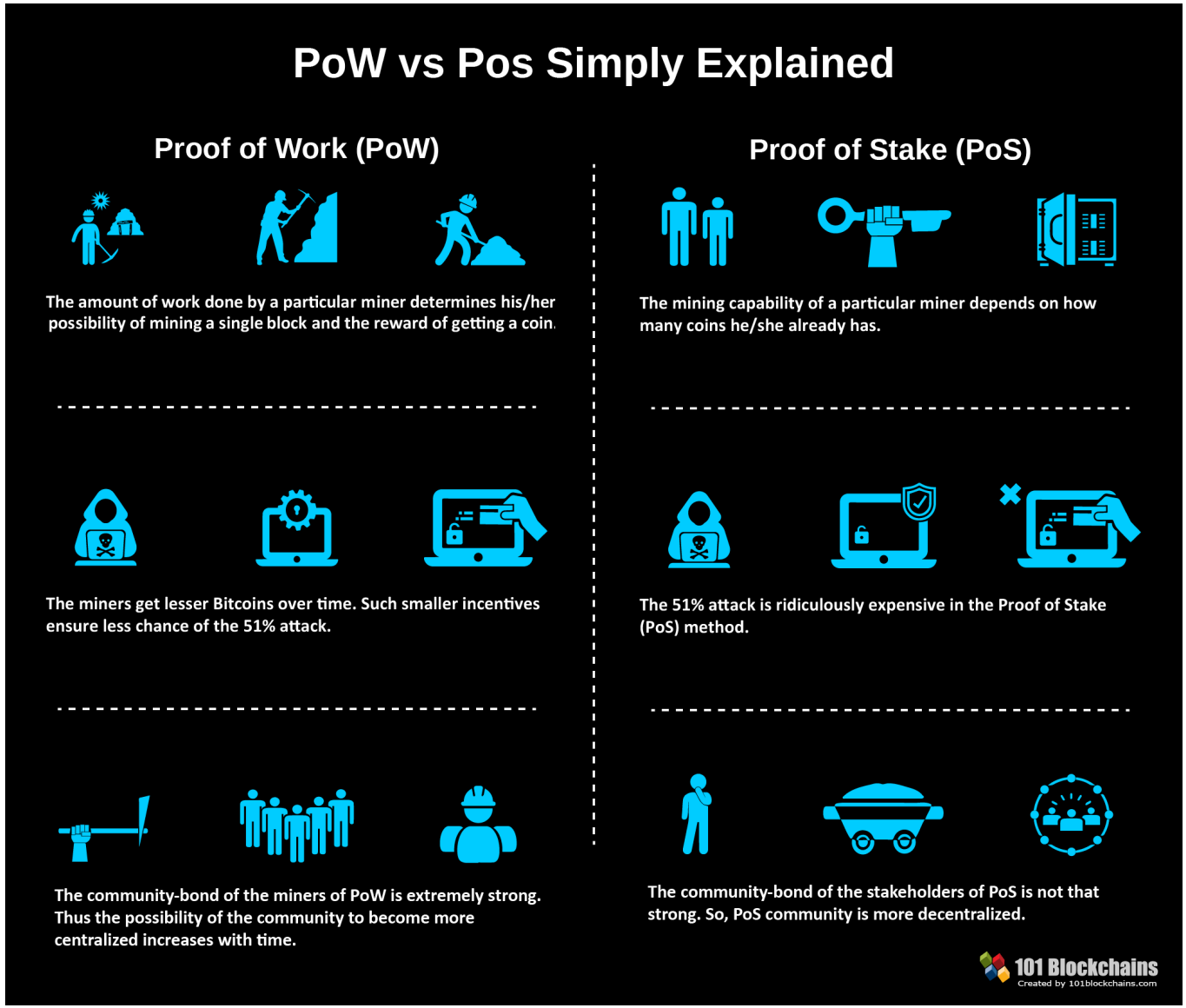
Konsenzus algoritmi: dokaz posla

- **Dokaz posla** (engl. *Proof of Work* – PoW) konsenzus algoritam podrazumeva **rešavanje zagonetke zahtevne za izračunavanje** kako bi se omogućilo kreiranje novih blokova u blokčejnu – zasnovan na **lutriji**
- Koncept – Cyntia Dwork i Moni Naor (http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps) 1993. kao ekonomska mera zaštite od slanja spam poruka
- **Hashcash** – Adam Back 1997. **PoW sistem** za limitiranje spama i sprečavanje denial-of-service (DoS) napada, koristi se i u **Bitcoinu** – jedini način da se pronađe zaglavlje sa željenim osobinama algoritmi grube sile (engl. *Brute force*), ali provera dokaza je laka
- Ključno svojstvo **asimetričnost** – posao mora biti umereno težak ali izvodljiv na strani zahtevaoca usluge, ali lako proveriv od strane pružaoca usluge
- Proces je kolokvijalno poznat kao **rudarenje** ili **majning** (engl. *mining*), a čvorovi u mreži uključeni u rudarenje kao **rudari** ili **majneri**. Podsticaj za rudarenje je ekonomski, zato što svaki novi blok donosi određeni iznos kriptovalute i provizije na transakcije uključene u blok

Konsenzus algoritmi: dokaz uloga

- **Dokaz uloga** (engl. *Proof of Stake* – PoS) konsenzus algoritam predstavlja generalizaciju PoW algoritma – takođe zasnovan na **lutriji**
- Kod PoS su čvorovi poznati kao **validatori** i, umesto rudarenja, oni validiraju transakcije kako bi zaradili proviziju od transakcije, nema rudarenja, svi novčići (engl. *coins*) postoje od prvog dana, koristi se kod **Ethereum**-a
- **Čvorovi** se **slučajno odabiraju za validatore** blokova, **verovatnoća** ove **slučajne selekcije** zavisi od **veličine uloga nekog čvora**
  - ako čvor X poseduje 2 novčića, a čvor Y 1 novčić, tada je verovatnoća da će X biti izabran za validatora dvostruko veća od Y
- **Ključno** je **uvođenje slučajnosti u proces odabira** kako bi se izbegao scenario u kome se **najbogatiji stalno biraju za validatore transakcija**, konstantno prikupljaju nagrade i postaju sve bogatiji
- **PoS algoritam** izbegava energetsku neefikasnost PoW algoritama

Konsenzus algoritmi: PoW vs PoS

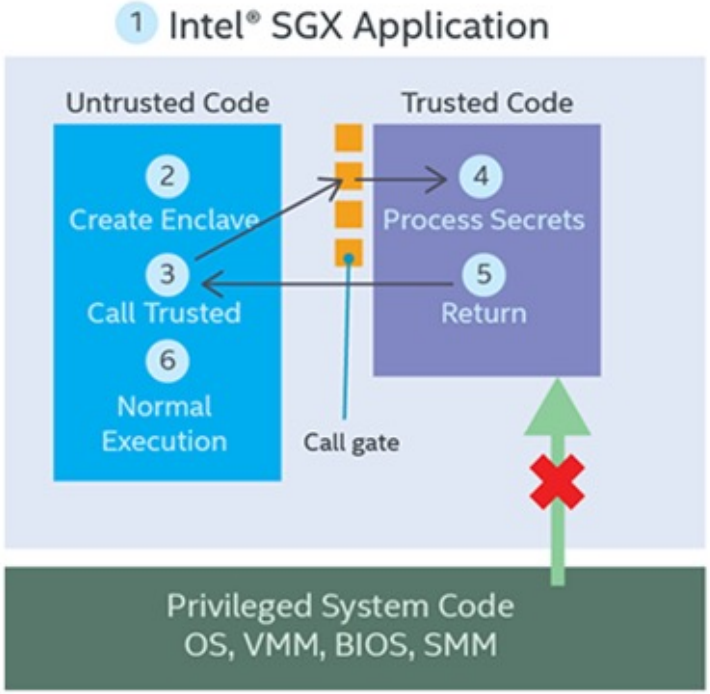


Konsenzus algoritmi: dokaz proteklog vremena

- **Dokaz proteklog vremena** (engl. *Proof of Elapsed Time* – PoET) je konsenzus algoritam koji rešava problem vizantijskih generala primenom **izvršavanja programa u okruženju sa poverenjem** (engl. trusted execution environment) – algoritam zasnovan na **lutriji**
- PoET **stohastički bira** pojedinačne **peer-ove** da **izvrše zahteve datom ciljanom brzinom**. Pojedinačni peer-ovi **uzorkuju slučajnu promenljivu sa eksponencijalnom distribucijom** i **čekaju onoliko vremena** koliko je **određeno uzorkom**. Varanje se sprečava primenom okruženja sa poverenjem, verifikacijom identiteta i stavljanjem na crnu listu putem asimetričnog kriptosistema i dodatnim skupom polisa za izbore (engl. election policies)
- Primer: Hyperledger Sawtooth – PoET u Intel SGX (Safe Guard Extension) okruženju (https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html)

Konsenzus algoritmi: dokaz proteklog vremena

- Primer: Hyperledger Sawtooth – PoET u Intel SGX:
  - **enklave** (funkcije u koje se veruje) dodeljuju vreme čekanja
  - **validator** sa najkraćim dodeljenim vremenom bira se za lidera
  - Funkcijama *CreateTimer* i *CheckTimer* kreira se i verifikuje tajmer za blok transakcija koji je garantovano kreirala enklava



1. App is built with trusted and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, and execution is transitioned to the enclave
4. Enclave sees all process data in the clear; external access to the enclave data is denied
5. Function returns; enclave data remains in trusted memory
6. Normal execution resumes

Izvor: https://software.intel.com/en-us/articles/intel-software-guard-extensions-tutorial-part-1-foundation

Konsenzus algoritmi: SBFT

- Konsenzus algoritam **pojednostavljene vizantijske tolerancije otkaza** (engl. *Simplified Byzantine Fault Tolerance*) implementira prilagođenu verziju PBFT – algoritam zasnovan na **glasanju**
- **Osnovna ideja** uključuje **jedinstvenog validatora** koji pakuje predložene transakcije i formira novi blok. Za razliku od Bitcoina, ovde je validator poznata strana pošto je algoritam namenjen glavnim knjigama sa kontrolom pristupa (engl. *permissioned*)
- **Konsenzus** se postiže tako što minimalni broj drugih čvorova u mreži potvrdi blok. Kako bi imao vizantijsku toleranciju, minimalni broj čvorova za konsenzus je $2f+1$ u sistemu sa $3f+1$ čvorova, gde je f broj otkaza u sistemu
- Primer: ByzCoin, unapređenje Bitcoin protokola u smislu skalabilnosti (https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b2a9148f950b7e4204bbbb8/1529516362810/ByzCoin.pdf)

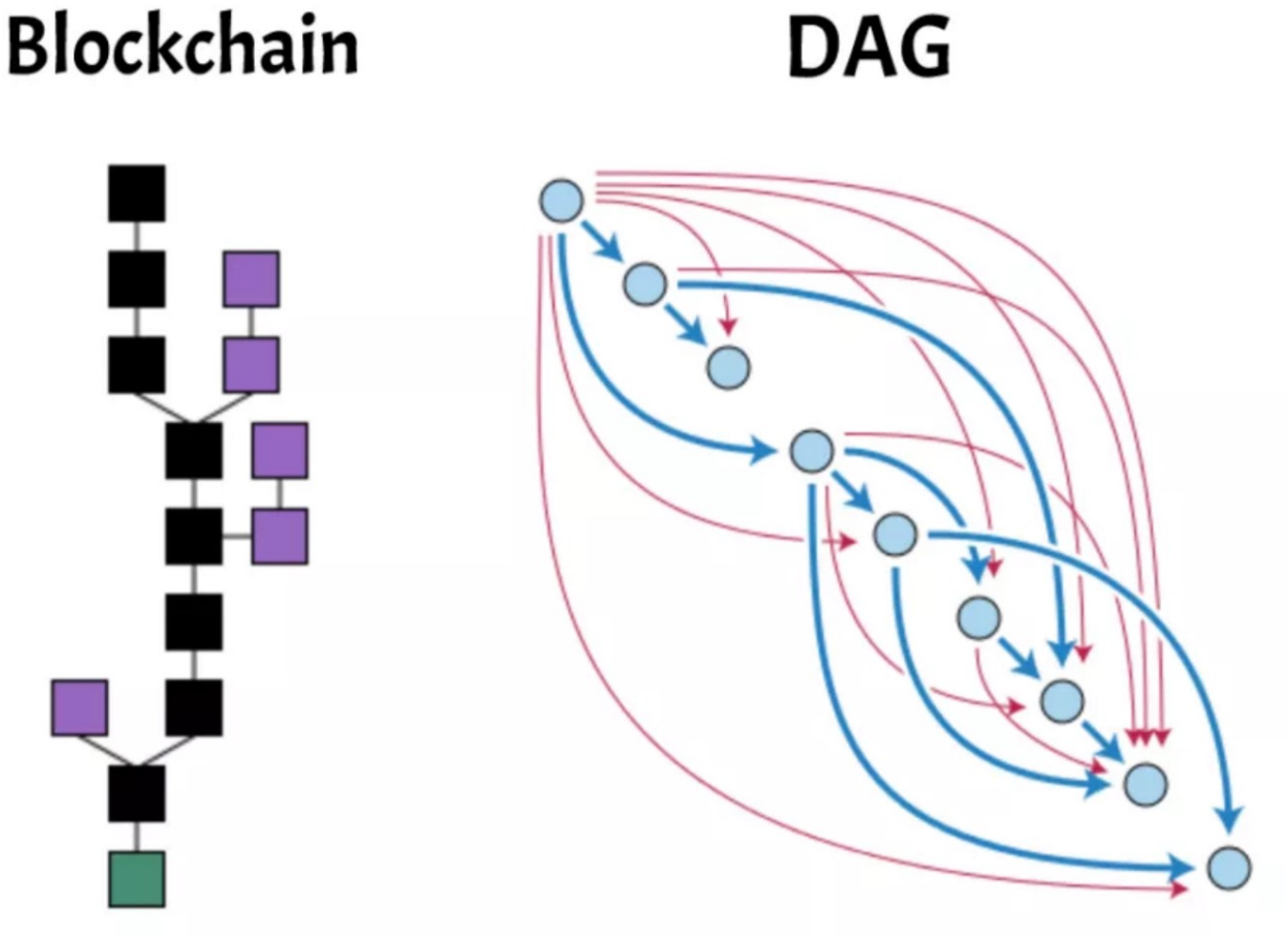
Konsenzus algoritmi: FBA

- Konsenzus algoritmi **federativnog vizantijskog dogovora** (engl. *Federated Byzantine Agreement* – FBA) se zasnivaju na opštoj ideji da je svaki vizantijski general odgovoran za svoj sopstveni lanac i uređuje dolazeće poruke kako bi utvrdio istinu (http://babel.ls.fi.upm.es/~agarcia/papers/fbqs/fbqs.pdf)
- FBA algoritmi pružaju **veliki propusni opseg**, **nisku cenu transakcija** i **visoku skalabilnost mreže**, tako da predstavljaju **jako dobro rešenje** za postizanje distribuiranog konsenzusa
- Kod **Ripple**-a (https://ripple.com) generali (tj. validatori) se unapred biraju od strane Ripple fondacije
- Kod **Stellar**-a (https://www.stellar.org) svako može biti validator, tako da učesnici biraju kojim validatorima će verovati

Konsenzus algoritmi: DAG

- **Usmereni aciklični grafovi** (engl. *Directed Acyclic Graphs* – DAGs) predstavljaju **generalniji oblik distribuirane strukture podataka** koji je interesantan zbog svoje **inherentne skalabilnosti**
- Klasični blokčejn sistemi zasnivaju se na **linearnoj strukturi** u koje se blokovi dodaju jedan po jedan u lanac što **sprečava paralelizaciju**
- Kod DAG se blokovi/transakcije mogu **dodavati paralelno**, pri čemu svaki blok/transakcija potvrđuje određeni broj prethodnih blokova što čini DAG inherentno skalabilnim
- Primeri DAG:
  - Constellation (https://constellationnetwork.io/)
  - Tangle (IOTA – https://www.iota.org)
  - Hedera Hashgraph (https://www.hedera.com/whitepaper) – asinhroni BFT
  - Block-Lattice (Nano) (https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf)
  - SPECTRE (https://medium.com/@avivzohar/the-spectre-protocol-7dbbebb707b5) – predloženo rešenje za skaliranje Bitcoina primenom PoW i DAG

Konsenzus algoritmi: DAG



Izvor: https://medium.com/coinmonks/dag-will-overcome-blockchain-problems-dag-vs-blockchain-9ca3026511 22