Kako blockchain deluje?

Jernej Vičič
FAMNIT in Inštitut Andrej Marušič, UP

Vsebina

- ponovimo,
- Kako deluje blockchain?
- Katere probleme rešuje blockchain?

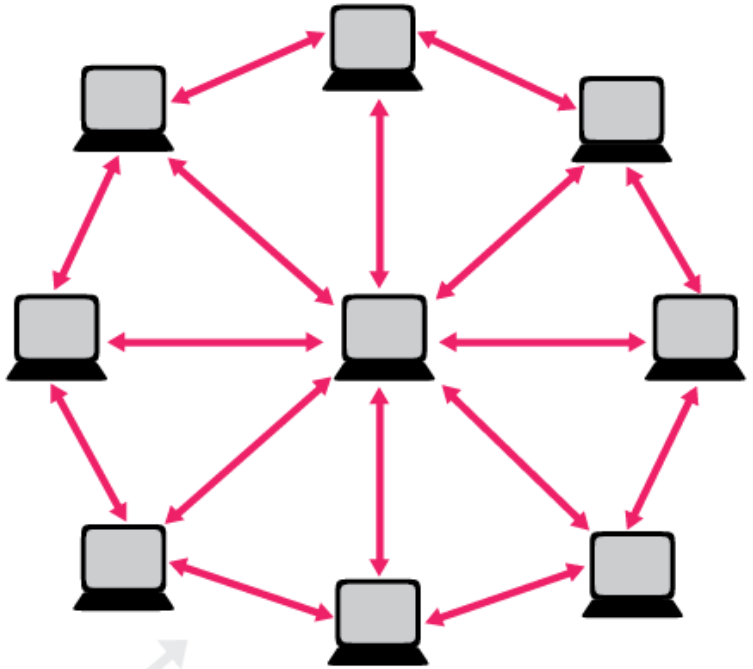
Ponovimo:

- transakcija,
- razpršitvena funkcija (hashing function),
- omrežje,
- blockchain,
- psevdo anonimnost,
- algoritem konsenza.

Ponovimo:

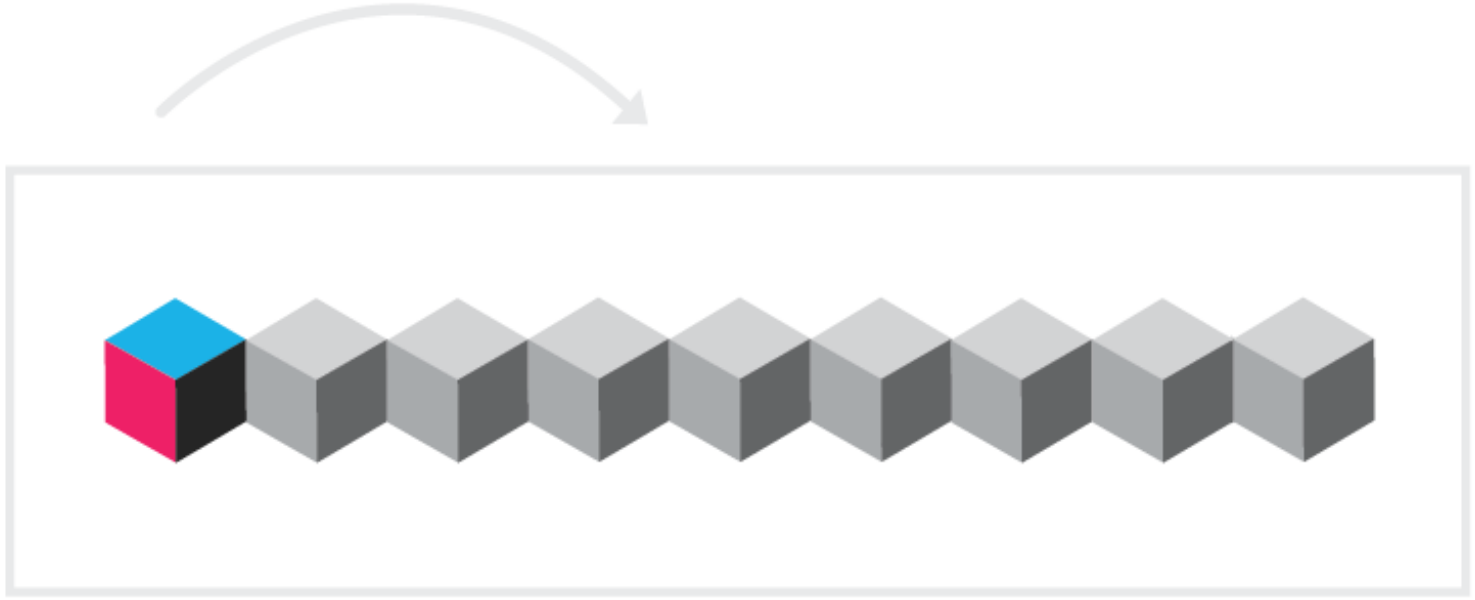
Blockchain je programska baza, ki nepokvarljivo hrani naraščajočo listo transakcij.

Nekdo zahteva **transakcijo**.



Transakcija je predana **omrežju**, ki ga sestavljajo računalniki.

Omrežje **potrdi** transakcijo in status uporabnikov s poznanim algoritmom.



Potrjena transakcija je skupaj z drugimi transakcijami združena v **blok** podatkov.

Novi blok je dodan že obstoječi verigi blokov, **blockchainu**, trajno in nespremeljivo.

Transakcija je **zaključena**.

Psevdo anonimnost

- vse transakcije so javne,
- vse denarnice so javne,
- zgodovina je nespremenljiva,
- nihče ne ve kdo je lastnik denarnice.

Public Address

SHARE

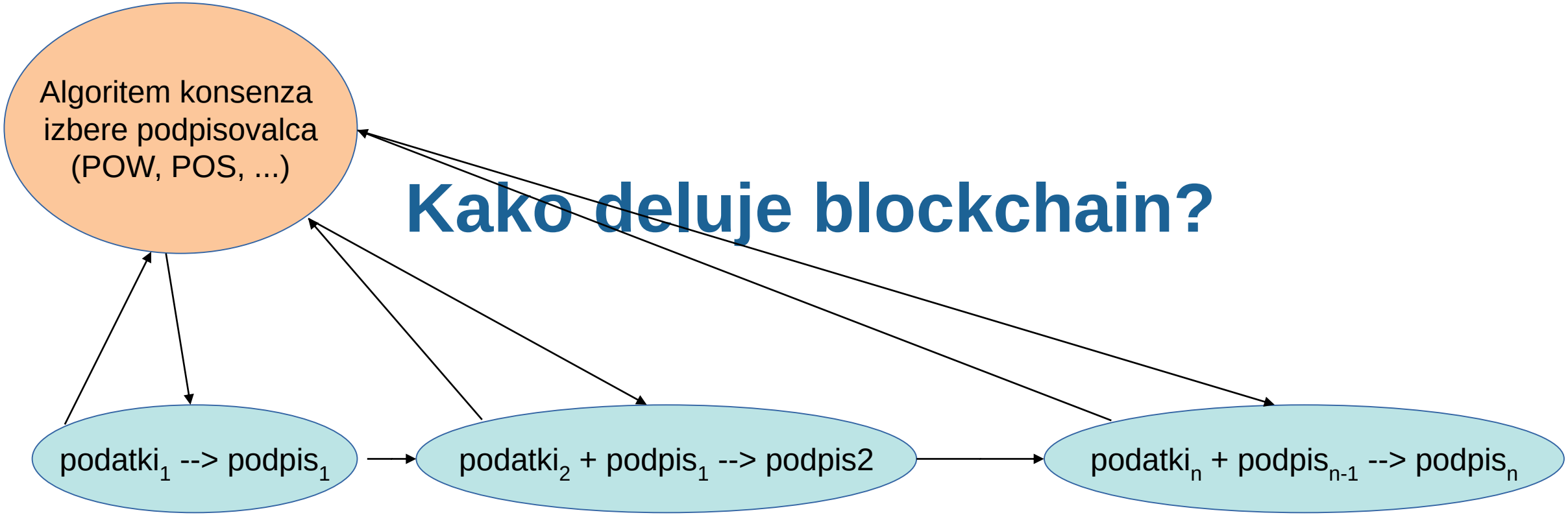
14gbLhYGErHgHMnE9QhsKm6DoErA1juDaU

Private Key (Wallet Import Format)

SECRET

5JQzarkhsado7ZPtyUTAZfjhfGVWdZmMoaa7wERhekFZqA2GCNX

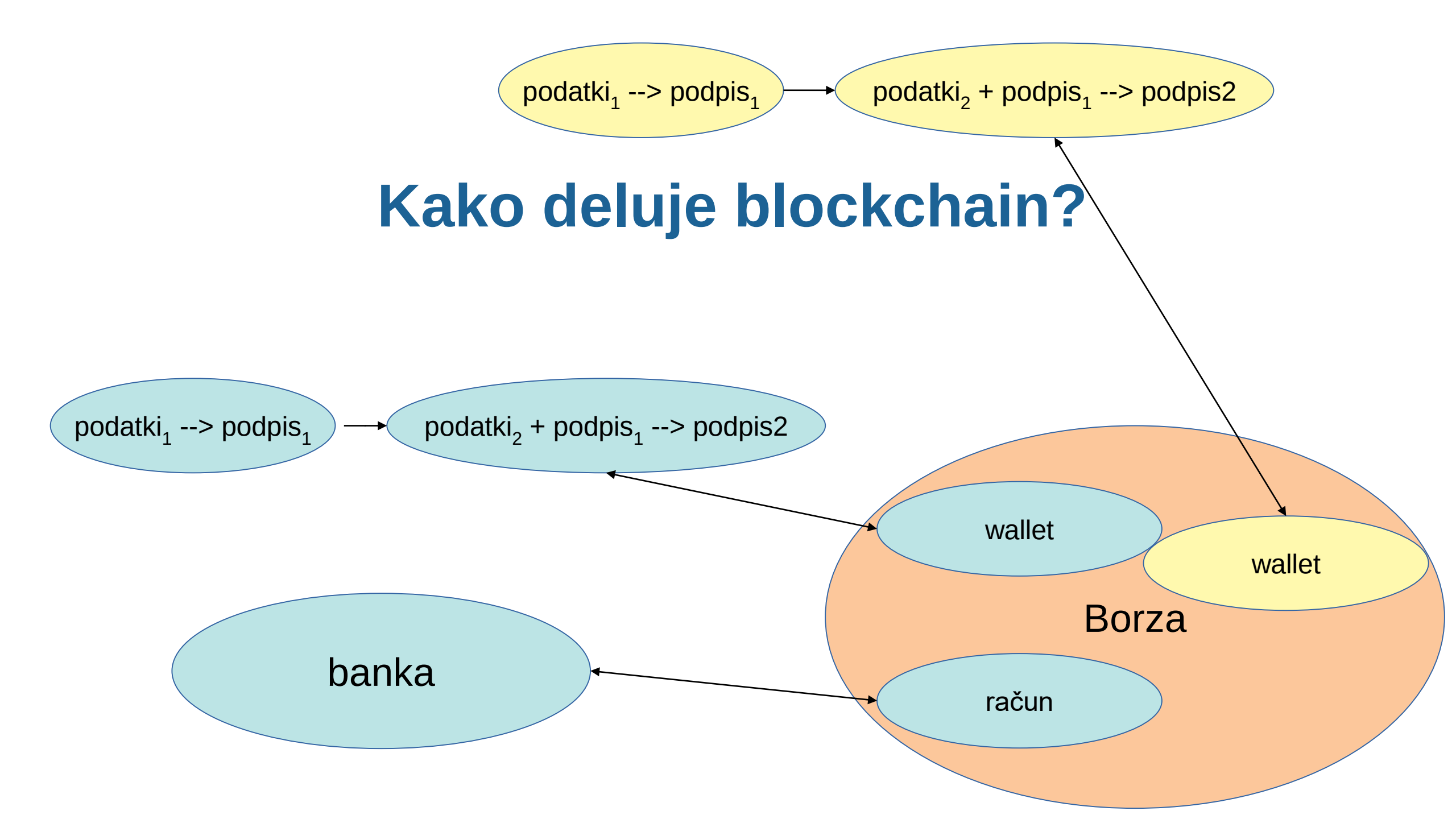
Kako deluje blockchain?



podatki

1

- Wallet dhse8r43jhfrevh nakazal 0.004 BTC na wallet 34jr7fdjdsjdfreerjfd8
- Ustvarjen now wallet: 734hef9dfj437fdj348
- ...


podatki1 --> podpis1
podatki2 + podpis1 --> podpis2
Kako deluje blockchain?
podatki1 --> podpis1
podatki2 + podpis1 --> podpis2
wallet
wallet
Borza
banka
račun

Algoritmi konsenza

- algoritem POW – Bitcoin,
  - rudarjenje (3 – 7 TPS - transactions per second),
  -
- konec 2017: All-time high: 4,7 TPS*,
- trenutno:
  - 5,2 je bilo 2.5.2019*,
  - 4,1 pa 20.5.2019*,
- VISA:
  - 2000 TPS**,
  - zmogljivost 24000 (56000)**.

*blockchain.co **news.bitcoin.co

Algoritmi konsenza

- bitcoin je počasen,
- transakcije so drage,
- obstajajo novejše kriptovalute:
  - hitre,
  - poceni,
  - 60000 TPS!
- Scalability Trilemma (Vitalik Buterin):

Algoritmi konsenza – scalability trilemma

- Sistemi na osnovi blockchaina lahko imajo največ dve izmed treh lastnosti:
  - **decentralizacija,**
  - **skalabilnost** (procesiranje dovolj velikega števila transakcij),
  - **varnost.**

Algoritmi konsenza

- Izbrati moramo »rudarja«, ki pripravi nov blok:
- Proof of Work – PoW,
  - rudarji poskušajo uganiti delno rešitev,
- Proof of Stake – PoS,
  - rudar – validator – je določen z vložkov v omrežje,
- Proof of Burn (PoB),
  - rudarji »uničijo« kovance: pošljejo na poseben naslov.

Proof of Work

- težki problemi (NP – polni problemi),
  - težko sestavimo dokaz (proof), enostavno preverimo pravilnost,
  - ugibamo in preverimo,
  - primer: kombinacija številske žabice,
  - problem: energetsko/računsko potratno,
- Bitcoin POW – ugibamo del niza,
- rudarji dobijo plačilo – vzdrževanje omrežja.

Proof of Work

- osnovno vodilo:
  - možnost validacije čimbolj razpršimo,
  - oprema že obstaja in ima druge namene,
- enostavno preverjanje,
- veliko preverjanj (ugibamo),
- vzporedna preverjanja,
- CPU ima več jeder
  - 2,4,6,8, … 32,
- GPU ima veliko več jeder,
  - 1000, … 3500.

Proof of Work

- posebna oprema,
- rešuje le en problem,
- zelo hitro rešuje ta problem,
- ASIC:
  - Application-Specific Integrated Circuit

Proof of Work

- nagrade za vsak blok,
  - nekaj minut,
- mining rig,
  - več GPU, večja verjetnost ...
- mining pool,
  - več ljudi prej najde rešitev,
  - delijo si zaslužek,
  - kopičenje moči – slabo.

Proof of Stake

- dokaz o lastništvu sredstev,
  - ponavadi denar,
- sredstva »zamrznemo« - stake,
  - dokaz je transparenten,
  - primer: 1% celotnih zamrznjenih sredstev,
- Primeri implementacije:
  - PureCoin, testno Loki.

Proof of Burn

- dokaz o uničenju sredstev,
  - ponavadi denar,
- nekoč bo »burner« nagrajen,
- sredstva »uničimo« - stake,
  - dokaz je transparenten,
  - ostalo na enak način kot PoS.

DPoS - Delegated Proof of Stake

- implementacija digitalne »demokracije«,
- izvoljeno določeno število delegatov - whitnesses,
  - za Ethereum je to 21 – 100,
  - določijo jih lastniki žetonov (stakeholders),
  - validirajo transakcije,
  - menjujejo se pri izdelavio blokov,
  - izključeni, če so »slabi«.

Private/public blockchains

- public – vse to kar smo do sedaj videli …
- private,
  - vse osnovne lastnosti blockchaina,
  - dodajamo različno funkcionalnost,
  - lokalno – ni potrebe po globalni podpori,
  - primer: Hyperledger fabric.

Hyperledger fabric

- privatno omrežje,
  - abstrakcija valute – asset – sredstvo,
  - sredstva vstopajo v omrežje,
  - sredstva premikamo,
  - premike ovrednotimo.

Privatne verige na Ethereum omrežju

- uporabljajo isti protokol,
- rešujejo lokalne potrebe,
- spore lahko rešujejo v globalnem omrežju.

Katere probleme rešuje blockchain?

- Blockchain ni samo Bitcoin,
- Blockchain niso samo kriptovalute,
- Kaj pa še omogoča?

Katere probleme rešuje blockchain?

- Javni sektor,
  - identifikacija
    - volitve,
    - potovanja,
    - upravne zadeve, ...

Katere probleme rešuje blockchain?

- Zavarovalništvo,
  - zahtevki, plačila in druga dokumentacija
  - zabeležijo se in shranijo na nespremenljiv način,
  - zagotovljena psevdo-anonimna sledljivost procesa,
  - zmožnost odkrivanja goljufij.

Katere probleme rešuje blockchain?

- Zdravstvo,
  - celotne kartoteke,
  - zagotovljena anonimnost,
  - zagotovljena varnost osebnih podatkov,
  - zagotovljena transparentnost dostopov,
  - ...

Katere probleme rešuje blockchain?

- Potovalna industrija,
  - identifikacija,
  - transparentnost prijave, checkin,
  - ...

Katere probleme rešuje blockchain?

- Odstranitev posrednika pri transakcijah,
  - transparentna hramba pogodb,
  - transparentno izvajanje pogodb,
  - ...

Katere probleme rešuje blockchain?

- Oskrbovalna veriga,
  - (transparentno) sledenje blaga od točke nakupa do dostave,
  - primer: lesna industrija, prehranjevalna industrija,
  - ...

Katere probleme rešuje blockchain?

- Omrežja senzorjev (sensor networks),
  - psevdo anonimnost:
    - omrežje se zaveda posameznika,
    - omrežje transparentno ponuja storitve,
      - smart contracts,
    - uporabniki omrežja ne morejo do osebnih podatkov,
    - omrežje loči posameznika, ki ostane anonimen.

Katerih problemov pa blockchain ne rešuje?

- nov, razvijajoč pojav,
- nizka likvidnost trgov,
  - možnost manipulacije trga,
- dotok denarja sumljivega izvora,
  - zasežena sredstva:
    - ZDA 200000 BTC, svet 453000 BTC,
- bad actors.

*www.theblockcrypto.com

Katerih problemov pa blockchain ne rešuje?

- rollback ni mogoč,
  - ko smo nakazali BTC na nek wallet,
  - in ko je ta transakcija spravljena na blockchainu,
- konec.

Katerih problemov pa blockchain ne rešuje?

- Binance hack,
  - preusmerili BTC v vrednosti 34 MIO $,
  - lastniki nadzirajo BTC wallet,
  - lahko prestavljajo na nove wallete,
    - sledljivost ostaja,
  - Monero,
    - avtomatsko blokiranje na borzi,
    - tainted BTX,
    - Blockchain Exchange Alliance.

Katerih problemov pa blockchain ne rešuje?

- bad actors:
  - Confido - 375.000 dolarjev brez lansiranja ICO,
  - Benebit - približno 2,7 milijona dolarjev,
  - Centra - 32 milijoni dolarjev,
  - Bitfinex – 120000 BTC,
  - ...

Praktični primeri