Tehničko i naučno pisanje

Kako i zašto funkcioniše blockchain?

Lazić Jovana, Nikić Ognjen, Nešković Ognjen, Sekešan Pavle

Matematički fakultet
Univerzitet u Beogradu

Beograd, 2022.

Literatura

- G. Woocakd et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1-2, 2014.
- S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.
- H. S. Shin, "Chapter V Cryptocurrencies: looking beyond the hype,"BIS 2018 Annual Economic Report, 2018.
- V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, 2014.

Pregled

Autentičnost dokumenata i konsenzus

- Kako da znamo da je neko zaista napravio neki dokument?
  - U stvarnosti: Potpisi, pečati, holografi, centralni autoriteti
  - U digitalnom svetu: Digitalni potpisi (pomoću asimetrične kriptografije)
- Kako postići konsenzus kada svi ne sarađuju ili se poruke mogu izgubiti ili izmeniti (problem vizantijskih generala)?
  - Algoritam za postizanje konsenzusa - na primer prihvatanje odluke koju donese 51%
  - U digitalnom svetu - kako obezbediti da svako dobije jedan glas?

Utvrđivanje hronologije

- Kako utvrditi hronologiju izmena ili objavljivanja podataka?
  - U stvarnosti: centralni autoritet u koji svi imaju poverenje
  - U digitalnom svetu: Ulančavanje kriptografskih heš funkcija
- Kada se ove ova tri problema reše moguće je napraviti javan, verodostojan skup podataka.

Kriptografske heš funkcije - osobine

- Heš vrednost poruke brzo je izračunljiva i značajno je kraća od same poruke
- Data poruka uvek ima istu heš vrednost
- Nemoguće je naći poruku na osnovu njene heš vrednosti
- Nemoguće je za datu poruku pronaći poruku sa istom heš vrednošću kao i uopšte pronaći dve poruke sa istom
- Male promene u poruci rezultiraju u velikim promenama u njenoj heš vrednosti

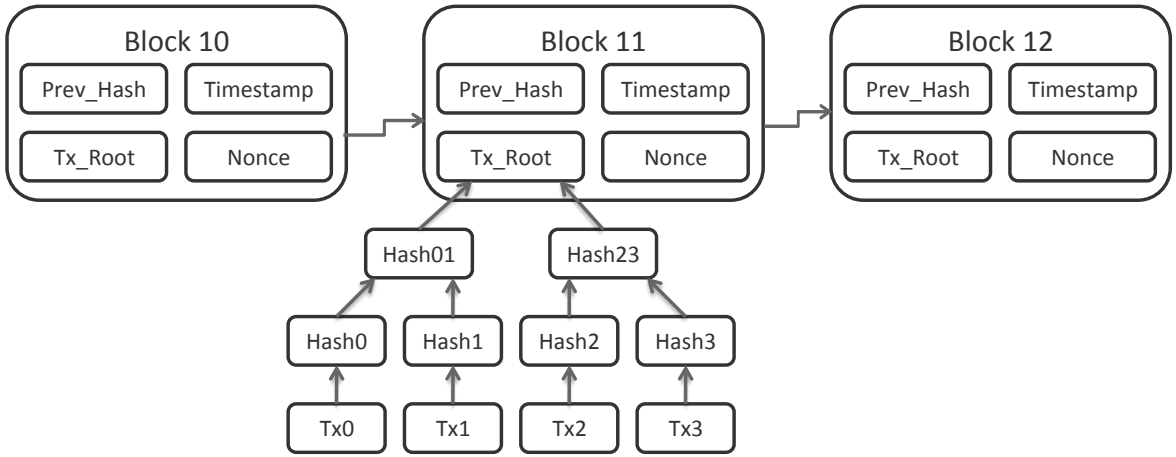
Kriptografske heš funkcije - algoritam

- Poruka podeljena u blokove (između 128 i 512 bitova)
- Za svaki blok ponavljamo računanje heš vrednosti sledećih delova fiksne dužine:
  - Deo poruke određen za taj blok
  - Heš vrednost prethodnog bloka
- Najpoznatije familije algoritama su MD i SHA, razlikuju se po broju i vrsti operacija u heš funkciji

Asimetrična kriptografija

- Javni ključ i privatni ključ
- Digitalni potpisi kao verifikacija identiteta
- RSA algoritam kao primer algoritma digitalnog potpisa

Struktura blokčejna



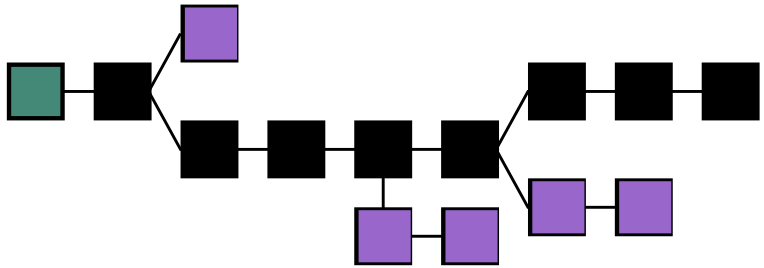
- Blokovi su manje grupe izmena na skupu podataka (npr. kod Bitkojna - transakcije)
- Blokovi su ulančani pomoću heš funkcija

Blokovi

- Uz svaki blok se čuva heš koji se dobija tako što se heširaju zajedno podaci iz trenutnog bloka i heš vrednost prethodnog bloka.
- Primetimo da je ovako nemoguće izmeniti neki blok bez toga da izmenimo sve blokove nakon njega.
- Ovako je utvrđena hronologija izmena

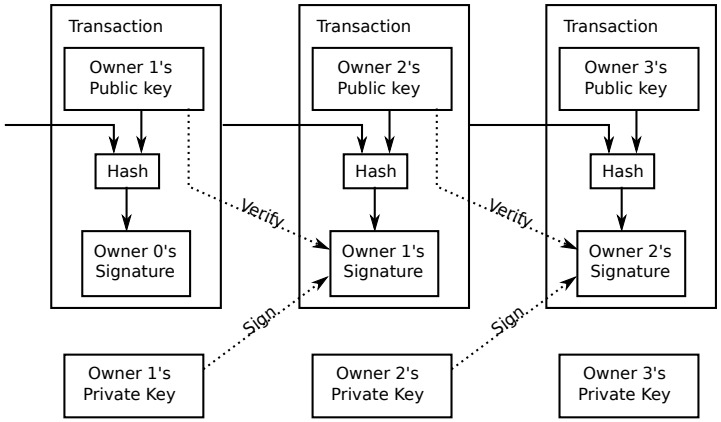
Decentralizacija

- Kako utvrditi koji lanac je ispravan?
  - Algoritam za postizanje konsenzusa, proof of work, proof of stake...
- Kako verifikovati da je neko odobrio neku izmenu?
  - Digitalni potpisi
- Ako se dva bloka kreiraju u različito vreme - fork:



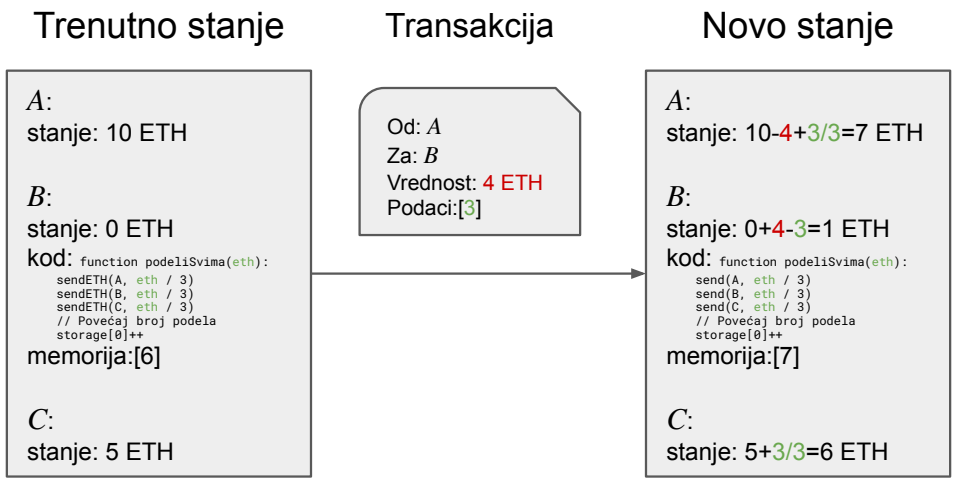
Kriptovalute

- Problem prihvatljivost decentralizovane valute
  - utvrđivanje vlasništva - **asimetrična kriptografija**
  - onemogućavanje da se isti novac potroši više puta (eng. double-spending problem) - **blokčejn**
- Prva kriptovaluta - **bitkoin**



Pametni ugovori

- Apstraktnije posmatranje bitkoin mreže - promena iz jednog u drugo stanje vlasništva
- Blokčejn opštije namene - **Ethereum**
- Pametni ugovori - javno dostupan kod koji se izvršava u okviru blokčejna



Zaključak

- Blokčejn - osnova kriptovaluta i pametnih ugovora
- Zašto su kriptovalute korisne?
  - eliminišu "double spending" problem
  - ne zasnivaju se na poverenju
  - nije im potreban centralni autoritet da bi održale vrednost
- Šta nam omogućavaju pametni ugovori?
  - automatsko izvršavanje dogovora
  - visoku bezbednost