

Konsenzus algoritmi

Stefan Aleksić

E2-42-2022



Agenda

Uvod

Proof of
Burn

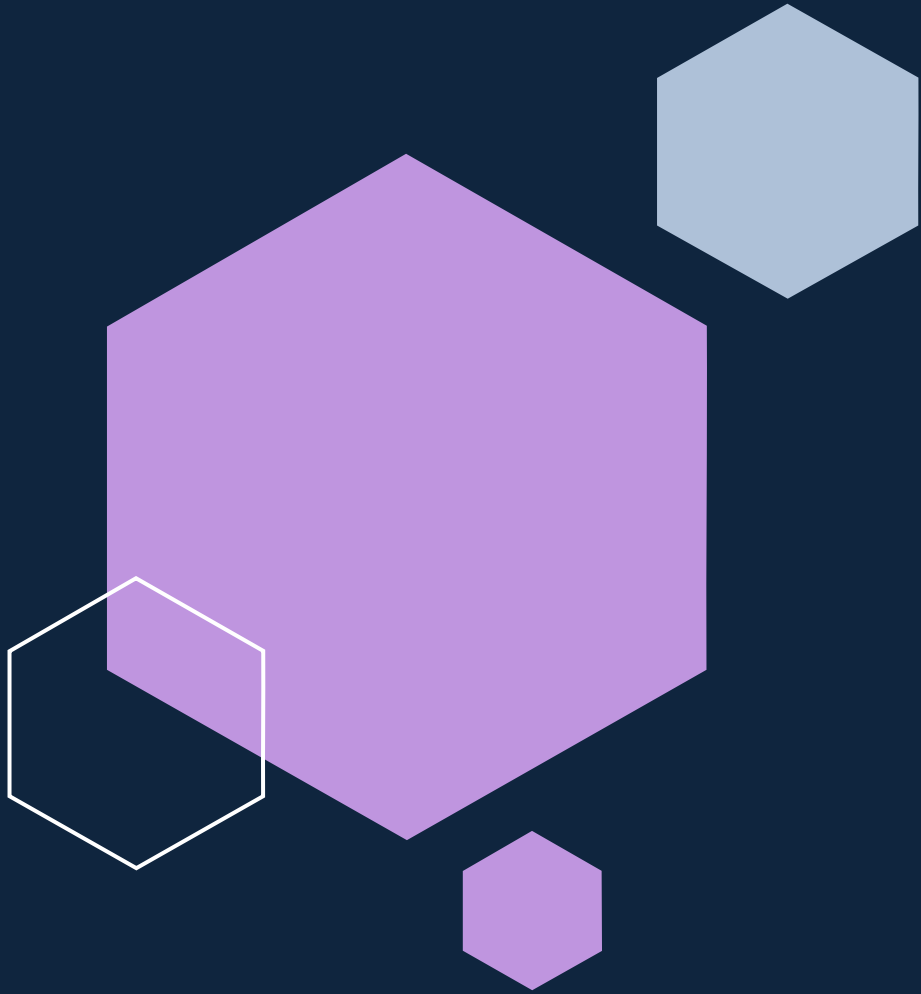
Proof of
Elapsed
Time

Proof of
Believility


HotStuff

Raft

Zaključak



Konsenzus algoritam je unapred definisan postupak za ostvarivanje konzistentnosti dupliciranih podataka u distribuiranom sistemu.



Svaki konsenzus algoritam se trudi da obezbedi:

1. Postizanje sporazuma
2. Učešće svih čvorova
3. Podjednak značaj čvorova
4. Sistem bez dvostruke potrošnje
5. Sistem otporan na greške
6. Jednaku aktivnost (opterećenje) čvorova

Proof of burn



Sagorevanje kriptovalute



Etar adresa



Prednosti

- Niska potrošnja eksternih resursa
- Motiviše majnere da troše kriptovalutu



Nedostaci

- Nestajanje valute tokom sagorevanja
- Potrošnja internih resursa



Implementacija

- Slimcoin (SLM), Counterparty (XCP), Factom (FCT)

Proof of elapsed time



Čekanje nasumično dodeljeno vreme



Prednosti

- Zahteva vrlo malo komputacione moći
- Kod se izvršava u bezbednom okruženju i nije podložan malicioznim izmenama



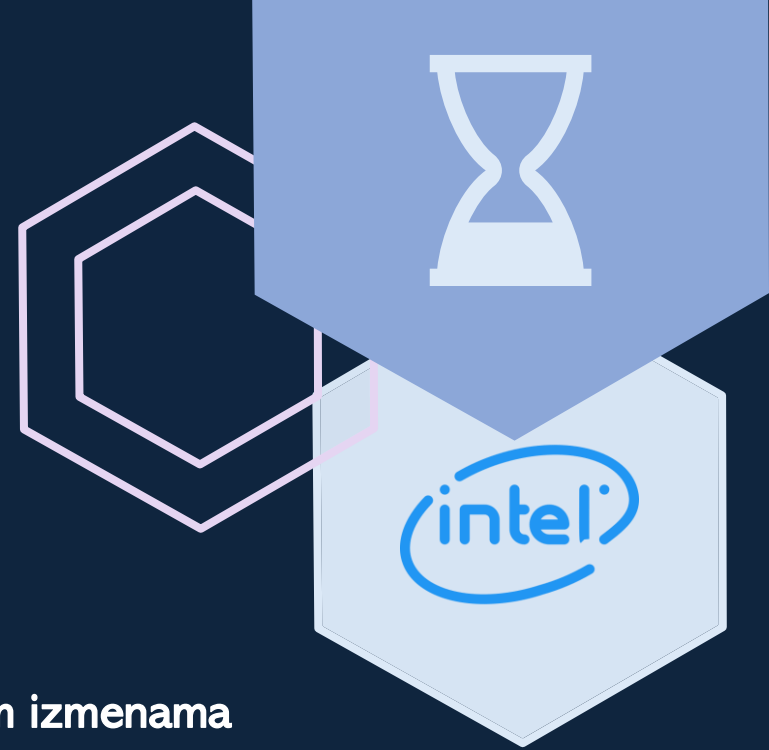
Nedostaci

- Potrebna je odgovarajuća arhitektura za izvršavanje, kao i dodaci (Intel Software Guard Extensions)
- Neophodna je dozvola pristupa mreži
- Latentnost u mrežnoj komunikaciji i nemogućnost vremenske sinhronizacije



Implementacija

Samo kroz Hyperledger Sawtooth (trenutno ne postoje valute koje koriste ovaj algoritam)



Proof of believability



Komitet (17 odabranih čvorova) odlučuje o stanju sistema



Servi nerazmenljivi pod-token kao valuta reputacije



Prednosti

- Skalabilnost, brzina, stabilnost
- Bias Resistant Distributed Randomness (BRDR)



Nedostaci

- Još uvek jako mlad algoritam (nije dovoljno testiran)



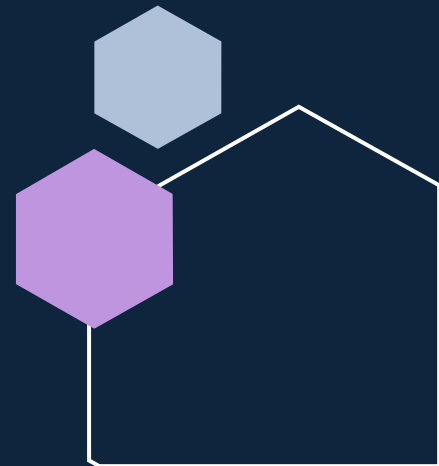
Implementacija

- Razvijen i korišćen od strane IOST (Internet of Service Token)

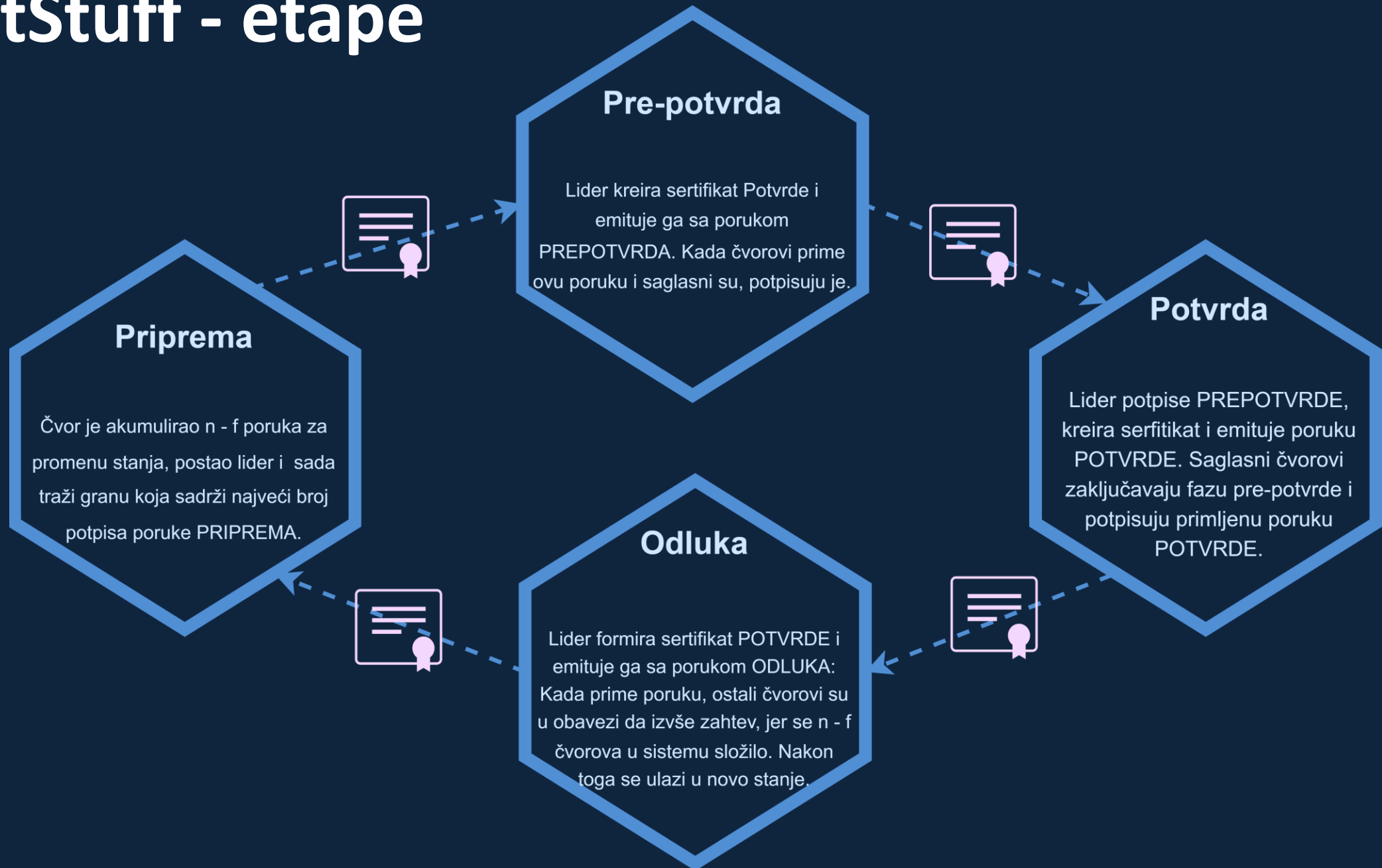


HotStuff

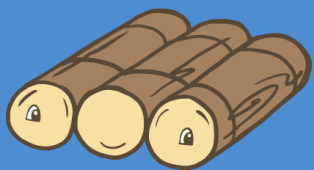
- ❖ Byzantine Fault Tolerance
- ❖ $n = 3 * f + 1$
- ❖ Delimično-sinhrona razmena poruka
- ❖ Sakrivena brava
- ❖ Učešće replika i topologija mreže
- ❖ Granični potpisi (TSS)
- ❖ Pejsmejker
- ❖ Leader based primary backup
- ❖ Kvalitet lanca
- ❖ Optimistični odziv
- ❖ Linearna promena stanja
- ❖ Sertifikat kvoruma



HotStuff - etape



Raft



**Replicated and fault tolerant
(Repliciran i otporan na defekte)**

Dnevnik evidentiranih događaja

- Rekonstrukcija stanja
- Kompresija u permanentnom skladištu

Faze algoritma

- Izbor lidera
- Replikacija dnevnika

RPC

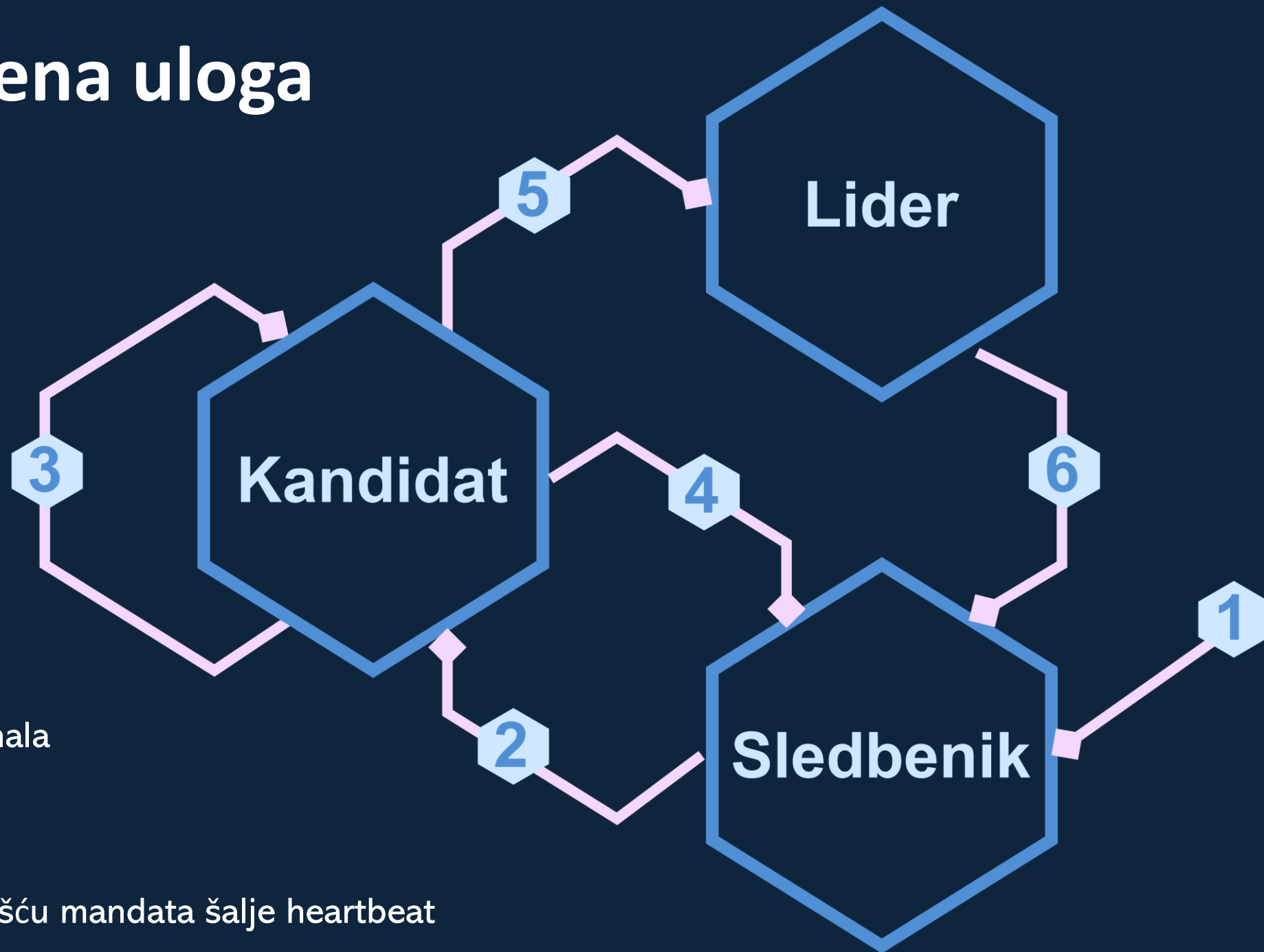
- AppendEntries(args)
- RequestVote(args)

Ograničenja

- Nema grešaka vizantijskog tipa.
- Nepouzdana mrežna komunikacija.
- Asinhrona komunikacija i procesori.
- Deterministički automat na svakom čvoru koji počinje u istom početnom stanju.
- Write-ahead logging skladišta podataka
- Klijent mora striktno da komunicira samo sa aktuelnim liderom.

Održavanje stanja automata konzistentnim

Raft – promena uloga



- 1 – Proces je pokrenut
- 2 – Timeout heartbeat signala
- 3 – Timeout izbora
- 4 – Heartbeat signal lidera
- 5 - Većina je izglasala
- 6 – Lider sa većom vrednošću mandata šalje heartbeat

Zaključak

Ne postoji konsezensni algoritam koji pokriva sve probleme.

Potrebno je analizirati sistem, potrebe, mogućnosti i na osnovu toga doneti zaključak koji iz širokog spektra algoritama izabрати.

Čak, s obzirom na fazu razvoja razmatranog distribuiranog sistema može se izmeniti trenutno implementiran i koristiti pogodniji.

Ono što je važno, to je poznavati karakteristike, prednosti i mane algoritama kako bi ih pravilno primenili.





Hvala na pažnji!