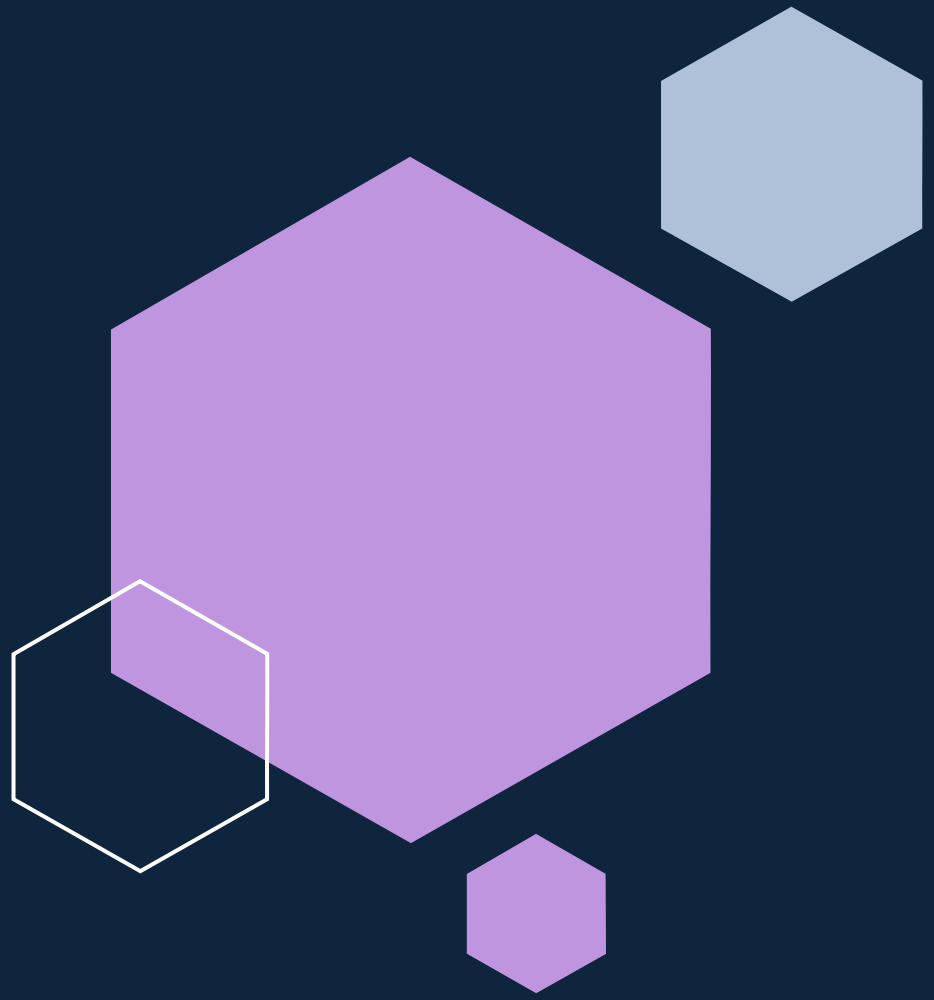
Konsenzus algoritmi

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.

Proof of burn

Sagorevanje kriptovalute

Etar adresa

Prednosti

- Niska potrošnja eksternih resursa
- Motiviše majnere da troše kriptovalutu

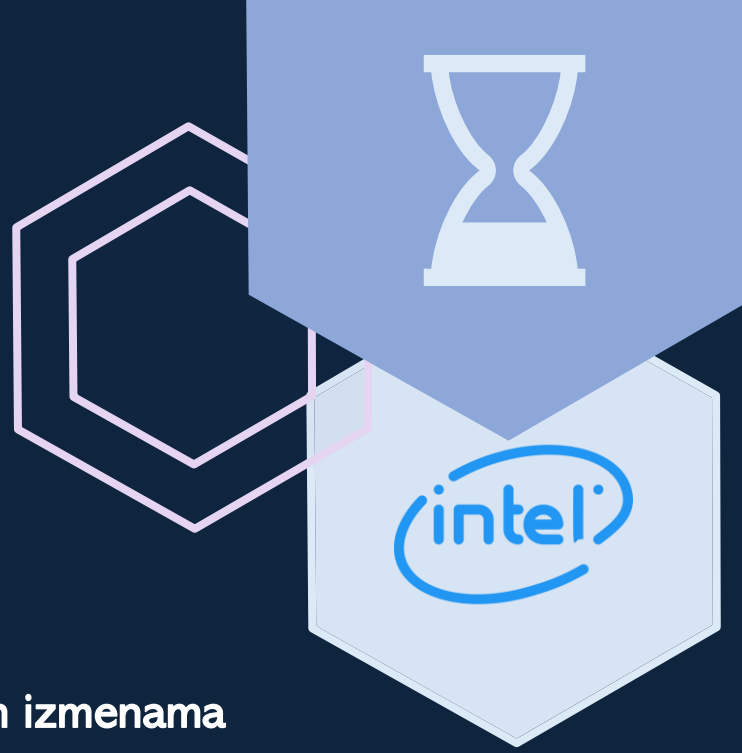
Nedostaci

- 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 izvšava 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)

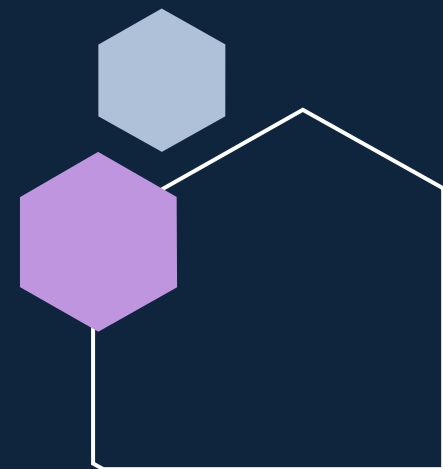
Nedostaci

- Još uvek jako mlad algoritam (nije dovoljno testiran)

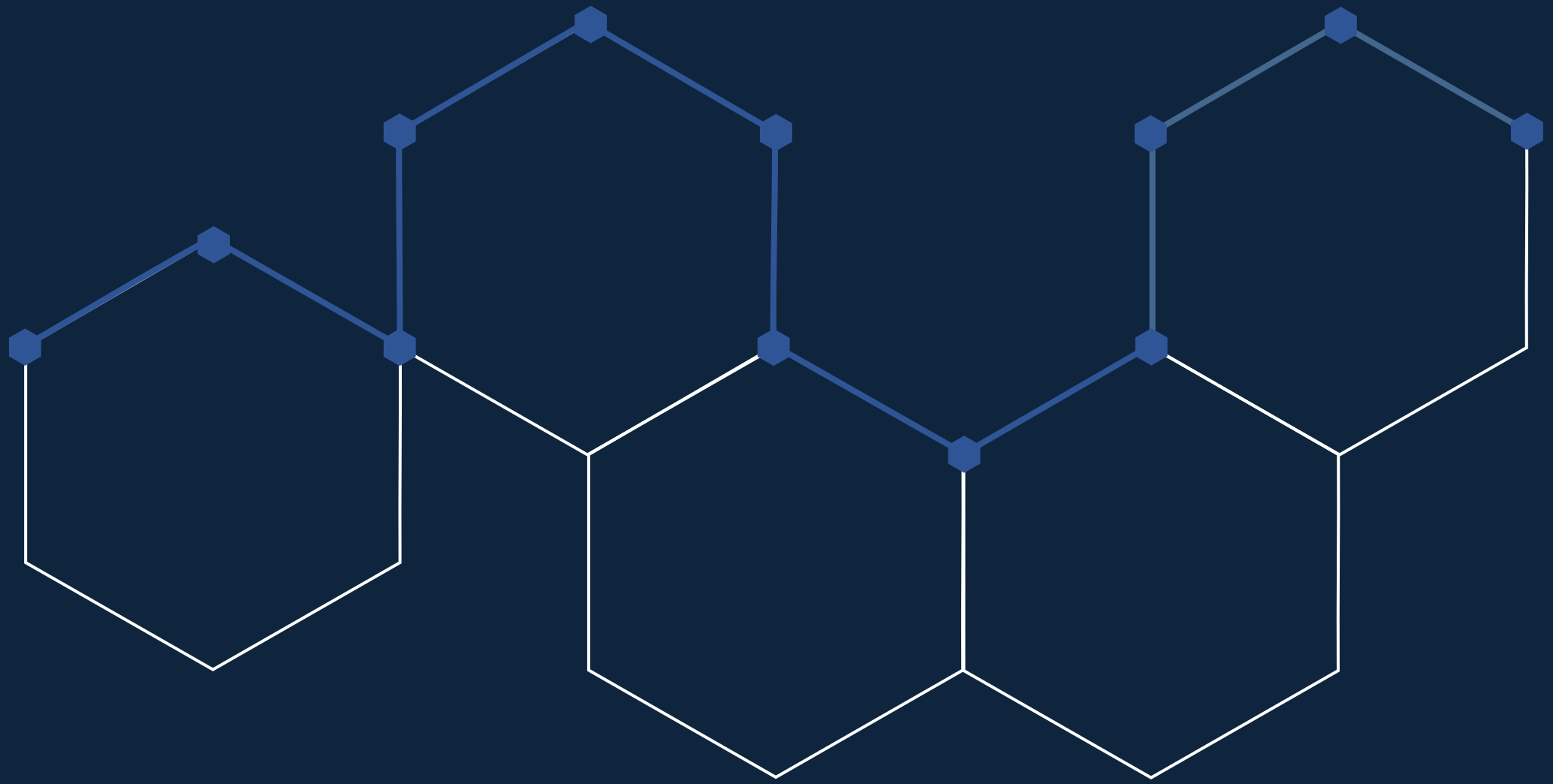
Implementacija

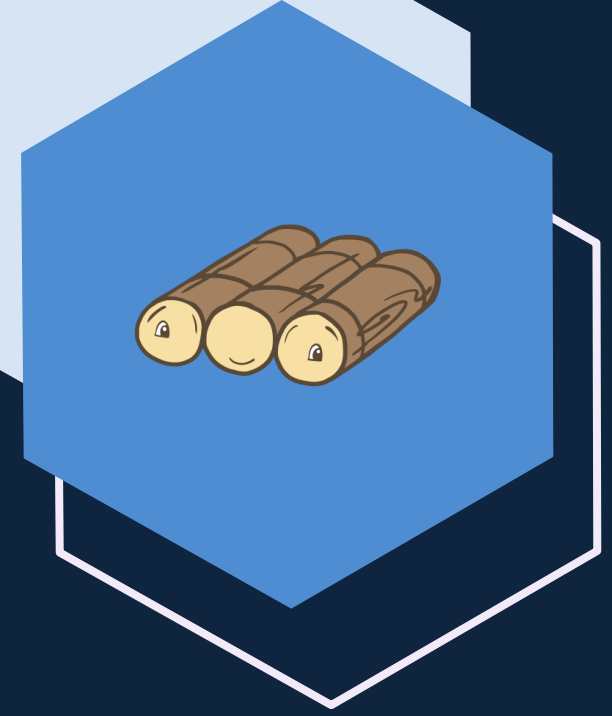
- Razvijen i korišćen od strane IOST (Internet of Service Token)

HotStuff



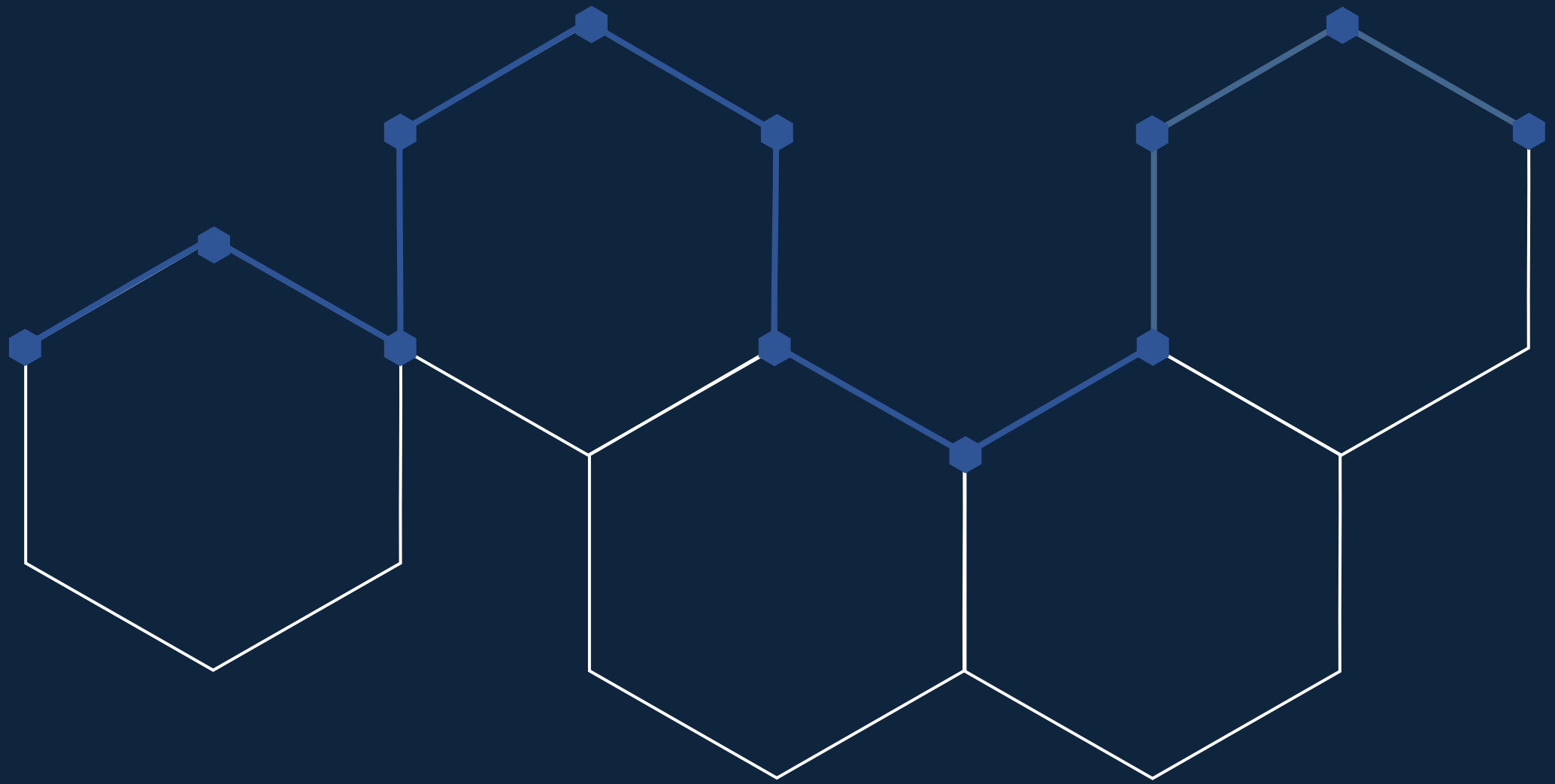
HotStuff - etape



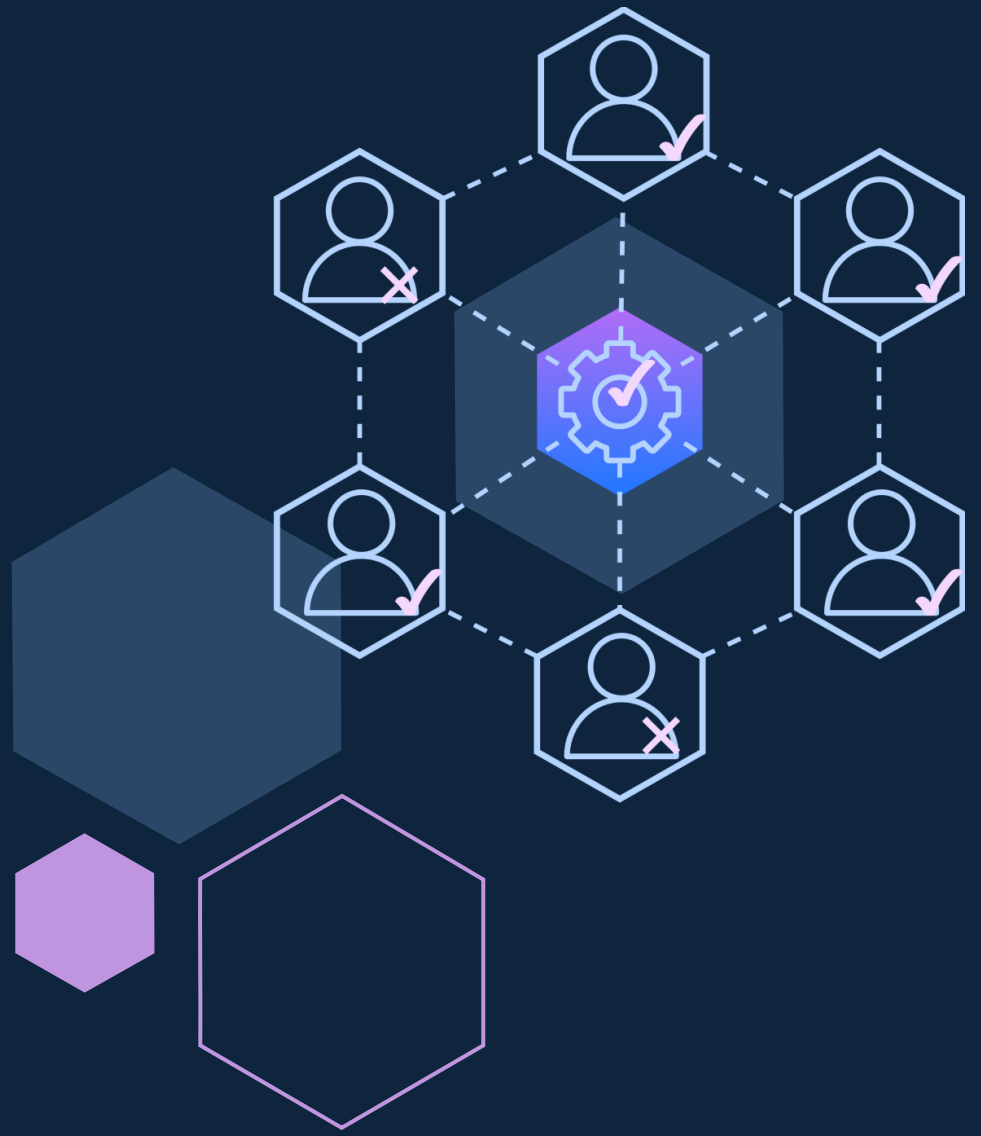


Raft

Raft - etape



Zaključak



Hvala na pažnji!