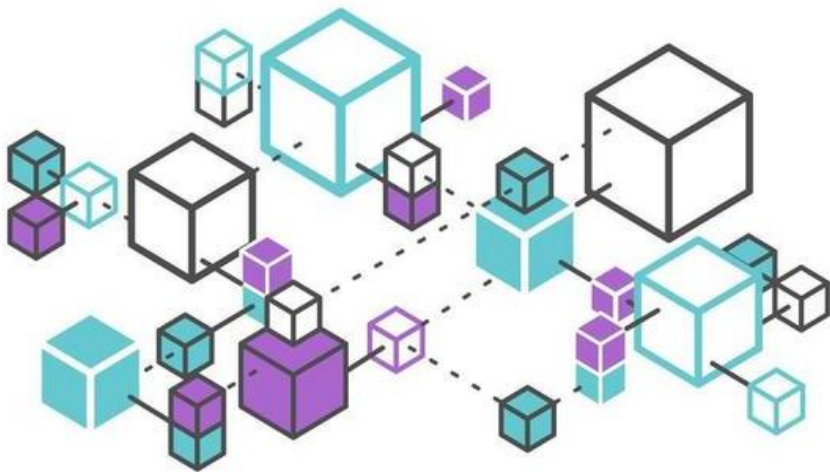




BLOKČEJN



Univerzitet u Beogradu
Saobraćajni fakultet

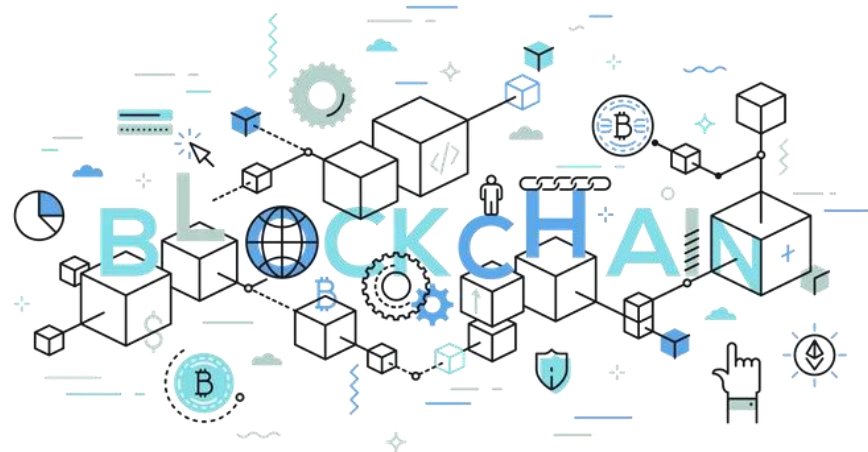
Prof. dr Gordana Radivojević
Prof. dr Dražen Popović

Copyright © 2025 Radivojević

Sva autorska prava su zaštićena i prezentacije se mogu koristiti samo za nastavu studenata odseka za logistiku, Saobraćajnog fakulteta Univerziteta u Beogradu u školskoj 2024/2025. Prezentacije i njihovi delovi se ne mogu koristiti za druge svrhe bez pismene saglasnosti autora.



- Blockchain (engl) – BC
- Blokčejn (srp)



Block Chain – Lanac blokova

Blokčejn tehnologija je distribuirana knjiga digitalnih zapisa
o svim transakcijama u poslovnoj mreži.

(ibm.com, 2025)

Blokčejn tehnologija je napredni mehanizam baze podataka koji omogućava
transparentno deljenje informacija u okviru poslovne mreže.

Blokčejn čuva podatke u blokovima koji su povezani u jedinstveni lanac.

(aws.amazon.com, 2025)



- Modeli računarskih i IT sistema su: centralizovan, decentralizovan i distribuiran.
- Centralizovan model podrazumeva da su svi učesnici i entiteti direktno povezani na centralnu jedinicu od koje dobijaju komande, podatke i informacije (npr. Internet usluge Facebook-a, Amazon-a ili Google-a).
- Decentralizovan model raspoređuje kontrolu na više čvorova u mreži povećavajući toleranciju na greške i skalabilnost.
- Distribuirani model raspoređuje kontrolu na pojedinačne čvorove koji su u koordinaciji i formiraju jedinstveni sistem za krajnjeg korisnika.
- Blokčejn tehnologija je decentralizovan sistem u kome postoji konsenzus između svih čvorova mreže.





- ▶ **Osnovni elementi BC**
- ▶ **Kako radi BC?**
- ▶ **BC arhitektura**
- ▶ **Vrste BC**
- ▶ **Karakteristike BC**
- ▶ **Prednosti i izazovi BC**
- ▶ **Primena BC**
- ▶ **BC u logistici i LS**





► Osnovni elementi BC

Osnovni elementi koji omogućavaju funkcionisanje BC tehnologije su:

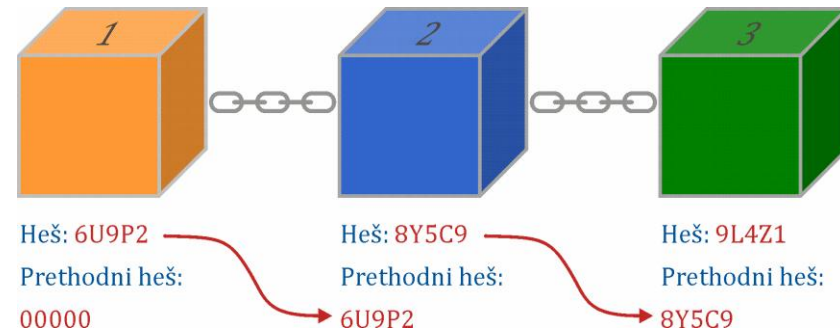
- Blokovi,
- Heš funkcija,
- Čvorovi,
- Mreža i
- Mehanizam konsenzusa.





Blokovi

- Blokovi su osnovna strukturna jedinica BC.
- Blok je rastuća lista transakcija koje su verifikovane od strane učesnika.
- Blok se sastoji od zaglavlja i tela. Zaglavlje predstavlja vezu sa prethodnim blokom a u telu se nalaze transakcije i brojač transakcija.
- Kada se dostigne maksimalni broj transakcija blok se zapečati i dodaje lancu.



Heš funkcija

- U opštem slučaju, heš (engl. Hash) funkcija je svaki algoritam koji podacima proizvoljne dužine dodeljuje podatke fiksne dužine.
- U BC se svakom bloku pri kreiranju dodaje heš prethodnog bloka.
- Zaglavlje bloka sadrži heš prethodnog bloka i heš svih transakcija u bloku.
- Blokovi se kreiraju hronološkim redom i heš svakog bloka omogućava njihovo povezivanje u lanac (block chain).

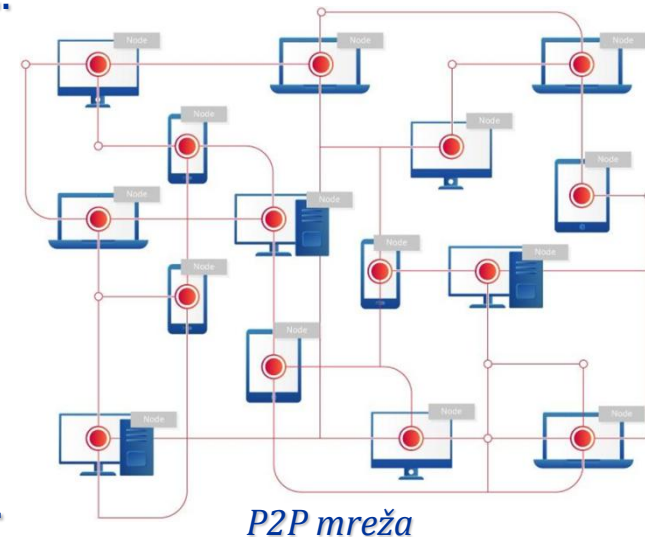


Čvorovi

- Čvorovi su računari i serveri koji čine infrastrukturu BC.
- Čvorovi su uređaji koji pokreću BC softver i na osnovu mrežnog protokola obezbeđuju interakciju sa drugim čvorovima.
- Osnovne funkcije čvorova su održavanje, validacija i pristupačnost.
- Čvorovi čuvaju kopije svih blokova (transakcija) u BC.

Mreža

- Mreža je rezultat integracije i kooperacije svih čvorova – partnera u BC.
- BC mreža je P2P mreža (engl. Peer-to-peer) koja je decentralizovana i u kojoj su svi čvorovi ravnopravni.
- Transakcije se primaju u čvorovima mreže i prosleđuju u sve druge čvorove.
- BC baza podataka je distribuirana u celoj P2P mreži.





Mehanizam konsenzusa

- Konsenzus je procedura u kojoj svi čvorovi BC mreže postižu dogovor o statusu podataka u mreži.
- Svaka transakcija se beleži u bloku i potrebno je uraditi verifikaciju transakcije pre dodavanja bloka u lanac.
- Mehanizam konsenzusa garantuje da su se svi učesnici složili o verifikaciji transakcije (bloka).
- Mehanizam konsenzusa definiše koja je transakcija važeća a koja nije.
- Ovime se BC mreža štiti od zlonamernih napada i grešaka.
- Postoji mnogo različitih mehanizama konsenzusa u zavisnosti vrste BC i oblasti primene.
- Mehanizmi konsenzusa se razlikuju po potrošnji energije, bezbednosti i skalabilnosti.
- Cilj konsenzusa je da se obezbede istiniti i poštteni zapisi.



(cripto.com, 2022)



► Kako radi BC?

Postupak rada BC se može opisati kroz sledeće korake:

1. Zahtev za transakcijom,
2. Transakcija se prosleđuje u P2P mrežu,
3. Validacija transakcije,
4. Verifikacija transakcije,
5. Transakcija se dodaje u blok,
6. Novi blok se dodaje u lanac i
7. Transakcija je kompletna.



(pwc.com, 2025)



- Korisnik (čvor) ima zahtev i pokreće transakciju koju potpisuje svojim ključem.
- Privatni ključ generiše jedinstveni digitalni potpis koji se ne može menjati.
- Transakcija se prosleđuje svim čvorovima P2P mreže.
- Čvorovi primenjuju mehanizme konsenzusa za proveru transakcije.
- Kada svi čvorovi postignu konsenzus tada je transakcija verifikovana.
- Verifikovana transakcija dobija kriptografski heš i javni ključ i upisuje se u blok.
- Heš je veza koja povezuje transakcije tako da se one ne mogu više menjati.
- Svaki novi blok pojačava verifikaciju prethodnog bloka i celog lanca.



(101blockchains.com, 2025)



Rudarstvo u BC

- Rudarstvo u BC je kritična komponenta mehanizma konsenzusa.
- Rudarstvo je proces koji uključuje validaciju transakcija i njihovo dodavanje u lanac blokova.
- Rudari su čvorovi P2P mreže koji pokušavaju da dodaju blok u lanac kako bi ga učinili trajnim.
- Za dodavanje bloka u lanac neophodno je generisanje kriptografskog broja (heš) koji je jednak ili manji od zadatog broja.
- Kriptografski broj – heš bloka je 64-cifreni heksadecimalni broj.
- Generisanje heš broja podrazumeva rešavanje složenih matematičkih problema korišćenjem računarske snage.
- Rudari se takmiče u rešavanju ovih problema i ko prvi pronade rešenje dobija pravo da doda blok i naknadu za obradu transakcija (kripto valuta).

*Ilustracija
heš funkcije*





► BC arhitektura

BC arhitektura obuhvata sve elemente i lejere koji zajedno čine BC sistem. Svaki lejer ima svoju specifičnu svrhu koja obezbeđuje realizaciju svih zadataka u sistemu.

BC arhitektura obuhvata pet lejera:

1. Lejer infrastrukture

Infrastruktura obuhvata sve fizičke resurse koji su neophodni za funkcionisanje BC. Infrastrukturne komponente su čvorovi, računari, serveri, oprema za rudarenje, virtuelne mašine.

2. Lejer podataka

Lejer podataka obuhvata sve podatke koji postoje u BC. Podaci su organizovani u blokove a svaki blok je povezan sa prethodnim formirajući lanac.

3. Mrežni lejer

Mreža je skup svih čvorova koji su povezani komunikacionim protokolima i uključeni u BC.

4. Lejer konsenzusa

Postoje različite vrste konsenzusa i protokola koji se primenjuju za formiranje i dodavanje bloka.

5. Aplikativni lejer

Aplikacije obuhvataju različite mogućnosti primene BC u poslovnim i organizacionim sistemima.



Aplikativni lejer



Lejer konsenzusa



Mrežni lejer



Lejer podataka



Lejer infrastrukture

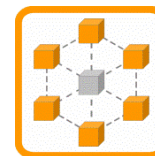
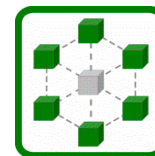
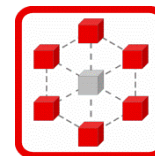
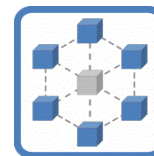


► Vrste BC

- BC obuhvata mrežu čvorova (računara) koji izvršavaju transakcije dodavanjem novih blokova u lanac.
- BC protokoli definišu način na koji se izvršavaju i dodaju nove transakcije.
- BC mreža može biti struktuirana na različite načine u zavisnosti od namene i svrhe primene.
- Različite varijante BC platforme imaju različite nivoe pristupa, brzinu obrade podataka, nivo bezbednosti i privatnost.

Vrste BC sistema su:

- ❖ Javni BC,
- ❖ Privatni BC,
- ❖ Hibridni BC i
- ❖ Konzorcijski BC.

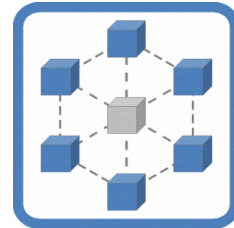


(crustlab.com, 2025)



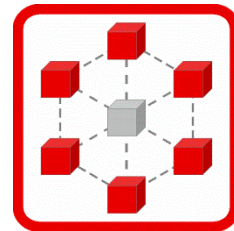
Javni BC

- Javni BC omogućavaju da svako može da se pridruži mreži.
- Svi članovi imaju jednaka prava da čitaju, uređuju i validiraju transakcije.
- Transakcije su javne a korisnici mogu ostati anonimni.
- Glavni nedostaci su visoki zahtevi za računarskom snagom, javnost transakcija i potencijalno slabija bezbednost.
- Primeri javnih BC su sistemi za rudarenje kriptovaluta Bitcoin, Eterijum i Lajtkoin.



Privatni BC

- Privatni BC su upravljani i kontrolisani od strane jedne organizacije koja određuje ko može da učestvuje u mreži.
- Privatni BC su zatvoreni sistemi koji imaju veći nivo poverenja između učesnika i veću bezbednost u mreži.
- Primer privatnog BC je Ripple mreža za digitalna plaćanja kriptovalutama između kompanija.

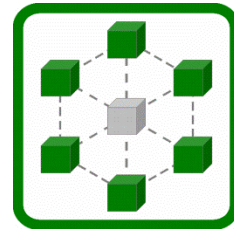


(solulab.com, 2025)



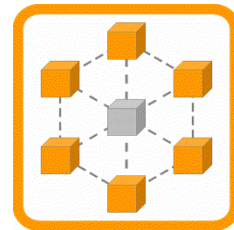
Hibridni BC

- Hibridni BC kombinuju elemente javnog i privatnog BC.
- Hibridni BC se mogu prilagoditi različitim nivoima pristupa i omogućavaju ravnotežu između javnih i privatnih BC.
- Ovi sistemi omogućavaju da neki podaci i transakcije budu javno dostupni a neki ostaju u privatnoj mreži.
- Hibridni BC se primenjuju u zdravstvu, prehrambenoj industriji, lancima snabdevanja itd.



Konzorcijumski BC

- Konzorcijumski BC su sistemi kojima upravlja skup – konzorcijum kompanija ili organizacija.
- Kompanije projektuju svoju mrežu kojoj ne može da pristupi ni jedan entitet van konzorcijuma.
- Konzorcijumski BC omogućava zaštitu poslovnih podataka i transakcija svih učesnika od spoljašnjeg pristupa.



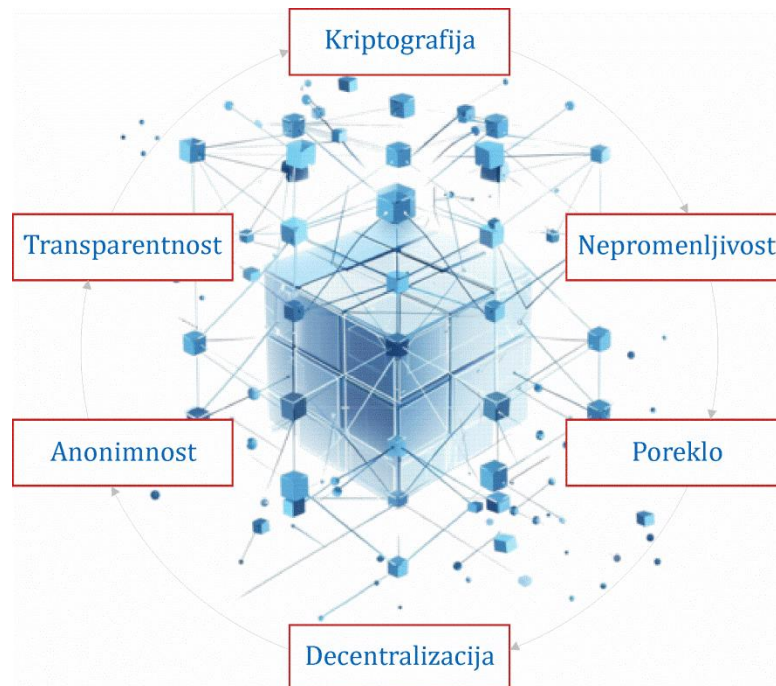
(aws.amazon.com, coinmarketcap.com, 2025)



► Karakteristike BC

Osnovne karakteristike BC su:

- Kriptografija,
- Nepromenljivost,
- Poreklo,
- Decentralizacija,
- Anonimnost i
- Transparentnost.



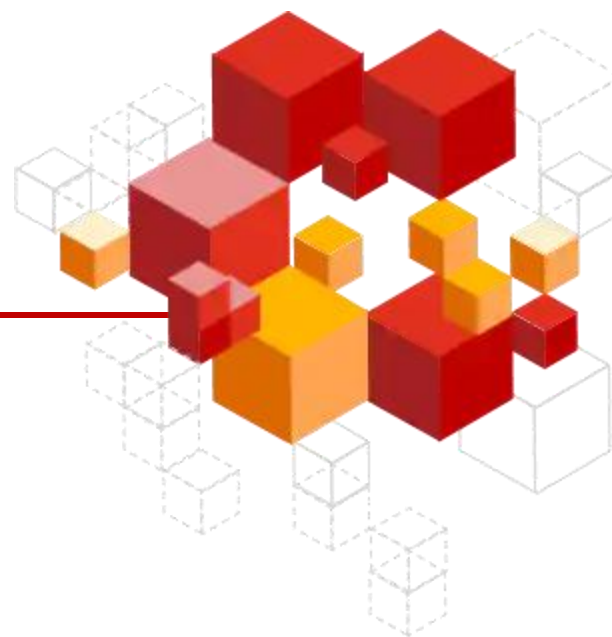
► Prednosti i izazovi BC

Prednosti AI

- ✓ Nepromenljivost i transparentnost,
- ✓ Kvalitet i bezbednost podataka,
- ✓ Dugovečnost i pouzdanost podataka,
- ✓ Sledljivost i mogućnost revizije,
- ✓ Novi poslovni poslovni modeli,
- ✓ Niži troškovi transakcija.

Izazovi AI

- ! Problem skalabilnosti,
- ! Visoka potrošnja energije,
- ! Pravni i regulatorni izazovi,
- ! Mogućnost zloupotrebe,
- ! Visoki troškovi implementacije i
- ! Tehnička složenost sistema.



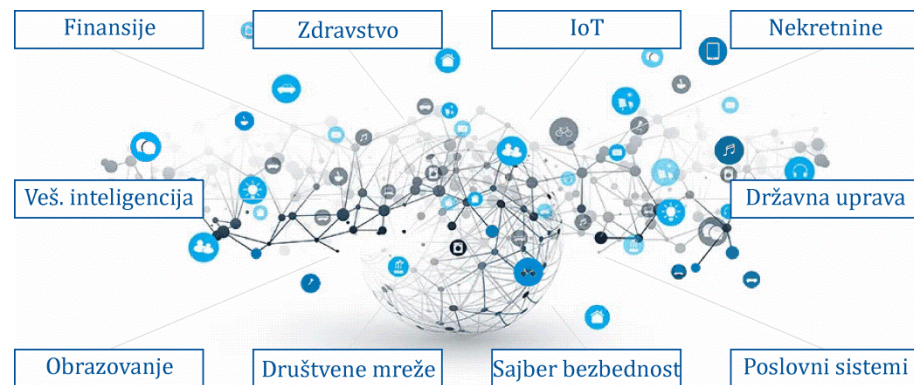
(www.financestrategists.com, 101blockchains.com, 2023)



► Primena BC

BC se primenjuje brojnim oblastima:

- ❖ Finansije,
- ❖ Zdravstvo,
- ❖ IoT,
- ❖ Nekretnine,
- ❖ Državna uprava,
- ❖ Poslovni i industrijski sistemi,
- ❖ Sajber bezbednost (bezbednost ličnog identiteta),
- ❖ Društvene mreže,
- ❖ Obrazovanje,
- ❖ Veštačka inteligencija, itd.





Primena BC u Industriji 4.0

- BC je ima značajnu ulogu u Industriji 4.0 i Logistici 4.0.
- BC unapređuje nivo digitalne revolucije i stvara nove vrednosti u Industriji 4.0.
- Transakcije je su brže, efikasnije i troškovno isplativije.
- BC omogućava kompletnu digitalizaciju poslovanja, bezbednost podataka i informacija, integraciju sistema i deljenje znanja između učesnika.

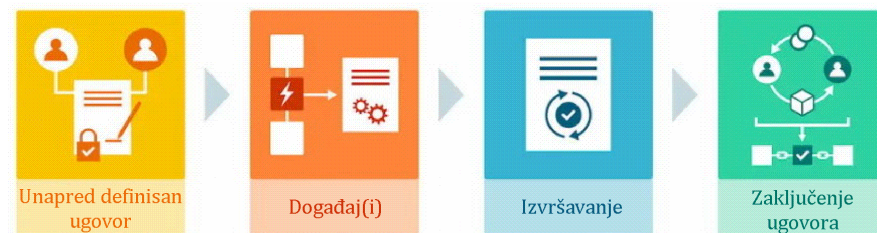
<i>Neke mogućnosti primene BC u Industriji 4.0</i>	
Finansije	Proizvodna oblast
Zaštita podataka o proizvodnji	Integracija sistema
Čuvanje podataka	Upravljanje
Bezbednost informacija	Poslovanje
Evidencija transakcija	Nadzor
Digitalni imenik	Identifikacija proizvoda i komponenti
Digitalna nabavka	Lanci snabdevanja

(Javaid et al., 2021)



Pametni ugovori

- Pametni ugovori (engl. Smart Contract) su računarski programi koji se izvršavaju kada su ispunjeni unapred definisani uslovi.
- Pametni ugovori su deo BC mreže i automatski se izvršavaju pomoću protokola za transakcije.
- Pametni ugovori ne zahtevaju centralizovan organ, pravni mehanizam i posrednike za realizaciju.
- Pametni ugovori su deterministički, nepromenljivi, autonomni, prilagodljivi, transparentni i bezbedni.
- Pametni ugovori mogu postojati na različitim BC platformama.
- Najviše korišćena platforma za pametne ugovore u 2025. godini je Eterijum.



(solulab.com, 2025)



► BC u logistici i LS

- BC ima velike mogućnosti primene u logistici i LS.
- BC se može primeniti za sve poslovne transakcije.
- Učesnici u logističkim procesima i LS postaju čvorovi BC mreže i imaju mogućnost pristupa podacima i informacijama.
- BC obezbeđuje tačnost, nepromenljivost i trajnost podataka.
- BC poboljšava transparentnost i efikasnost logističkih operacija.
- Primena pametnih ugovora ubrzava procese u LS, eliminiše greške u isporuci i posrednike između partnera.
- Primena BC u logističkim sistemima je još uvek u početnoj fazi razvoja.
- Procenjuje se da će rast BC u oblasti logistike biti 39.78% godišnje do 2027.
- BC će u velikoj meri transformisati poslovne modele u logistici i LC



(www.inboundlogistics.com, 2024, agilie.com, www.goodloading.com, 2025)



Neke prednosti primene BC u logistici i LS su:

- ✓ Ubrzavanje logističkih procesa,
- ✓ Nemogućnost falsifikovanja podataka,
- ✓ Transparentnost procesa,
- ✓ Integracija sa trećim licima,
- ✓ Zaštita od sajber prevara,
- ✓ Praćenje efikasnosti svih učesnika,
- ✓ Optimizacija ruta transportnih sredstava,
- ✓ Pametni ugovori,
- ✓ Poboľjšani sistemi plaćanja,
- ✓ Provera porekla robe,
- ✓ Povećanje efikasnosti,
- ✓ Smanjenje troškova itd.



(agilie.com, 2025)



Pitanja...

