Decentralizirana Real-time komunikacija – dRTC

# UVOD

Korisnici su se udaljili od mobilnih I fiksnih poziva, te sve više prelaze na komunikaciju preko aplikacija za komunikaciju. Korisnici sve više preferiraju komunikaciju u stvarnom vremenu umjesto komunikacije preko npr. Emaila.

# RTC

RTC (Real-time communication) je tehnologija koja omogućuje izravnu i trenutnu razmjenu podataka, glasovnih poziva, videopoziva i drugih vrsta komunikacije putem interneta, bez značajnih odgoda.

## PREDNOSTI

Korištenjem RTC tehnologije podatci se prenose gotovo trenutno čim je omogućena interakcija u stvarnom vremenu. RTC ima nisku latenciju. Komunikacija je dvosmjerna, što znači da obje strane mogu istovremeno slati i primati informacije. RTC obuhvaća razmjenu glasovnih, video i tekstualnih podataka.

[„RTC rješenja su visoko skalabilna, prilagođavajući se rastućim potrebama poslovanja u razvoju. Štoviše, ove su tehnologije dizajnirane s integracijskim mogućnostima, omogućujući besprijekornu integraciju s postojećim poslovnim aplikacijama, CRM sustavima i alatima za upravljanje projektima.”](https://www.ecosmob.com/real-time-communications-rtc-a-detailed-guide/)

## [„Komunikacija u stvarnom vremenu dostupna je na webu (WebRTC) i mobilnim uređajima.”](https://getstream.io/glossary/real-time-communication/)

## KAKO RADI

[“Komunikacija u stvarnom vremenu nikada se ne pohranjuje u privremenom stanju bilo gdje između odašiljača i prijamnika.“](https://www.vonage.com/resources/articles/real-time-communications/)

Arhitektura koja se koristi je peer-to-peer.

## PRIMJERI

Primjeri RTC: glas preko fiksnih I mobilnih telefona, Internet relay chat, VoIP, razmjena trenutnih poruka(IM) (WhatsApp, Facebook Messenger), video i telekonferencije, streaming uživo.

Alati poput Zooma, Skypea i Google Meeta koriste RTc za prijenos zvuka i videa. Aplikacije poput WhatsAppa koriste RTC za glasovne i videopozive.

### Web komunikacija u stvarnom vremenu (WebRTC) – decentralizirana???

Okvir otvorenog koda. Omogućena audio, video i podatkovna komunikacija u stvarnom vremenu izravno u web pregledniku.  Izgrađena na JavaScript API-jima i HTML5. Omogućuje da se u web aplikacije izravno integriraju komunikacijske mogućnosti bez potrebe za dodacim ili softverima trećih strana.

[WebRTC koristi DTLS/SRTP kao svoj protokol za sigurnost, gdje je SRTP odgovoran za šifriranje različitih vrsta podataka, poput audio i video, koji se prenose putem WebRTC sesije. DTLS-SRTP je metoda koja se koristi za sigurnu razmjenu ključa za dešifriranje između uređaja uključenih u WebRTC komunikaciju.](https://hackernoon.com/decentralizing-real-time-communication-shaping-the-future-of-connectivity)

[Ključevi se generiraju lokalno na uređaju svakog korisnika; njima ne upravlja niti jedan centralizirani poslužitelj. Ovo sprječava trećim stranama pristup ključevima.](https://hackernoon.com/decentralizing-real-time-communication-shaping-the-future-of-connectivity)

WeRTC je peer-to-peer usluga, ali obično uključuje povezivanje putem web poslužitelja koji upravlja i olakšava lociranje i uspostavu veze između uključenih uređaja.

Dodatno:

<https://getstream.io/glossary/webrtc-protocol/>

<https://webrtc.org/>

### Voice over IP (VoIP)

VoIP tehnologija pretvara analogne audio signale u digitalne pakete podataka i prenosi ih preko IP mreža. Umjesto tradicionalnih telefonskih sustava koriste se VoIP rješenja kako bi se uštedilo kod međunarodnih poziva te olakšala međunarodna komunikacija.

## PODJELE

RTC sustavi se općenito dijele na Hard Real-Time (HRT) i Soft Real-Time (SRT).

Hard Real-Time (HRT) sustavi su oni sustavu kod kojih posljedice kvara mogu biti katastrofalne (npr. Sustavi upravljanja, automobilski kontroleri, medicinski uređaji i kritični sigurnosni sustavi). Soft Real-Time (SRT) sustavi su ne mogu izazvati katastrofalnu štetu nakon kvara (pr. WebRTC).

Half duplex – komunikacija se odvija u jednom kanalu u jednom smjeru u isto vrijeme. Pošiljatelj i primatelj mogu slati, ali ne i primati u isto vrijeme. (voki-toki)

Full duplex - pošiljatelj i primatelj mogu slati i primati poruke istovremeno u dva paralelna komunikacijska puta

## RTC PROTOKOLI?

Real-time Transport Protocol (RTP) i Session Initiation Protocol (SIP),

**XMPP (Extensible Messaging and Presence Protocol)**

**SRTP (Secure Real-Time Transport Protocol)**:

<https://www.dialogic.com/glossary/real-time-transport-protocol-rtp>

## RTC TEHNIKE

<https://www.linkedin.com/pulse/realtime-communication-techniques-you-must-know-gaurav-arora/>

## PROBLEMI RTC-A

Kod centraliziranih mreža postoji centralni poslužitelj koji upravlja podatcima. Korisnički podatci se pohranjuju na poslužitelju i potencijalno zloupotrebljavaju. Postoji problem privatnosti korisničke komunikacije.

* Prijetnja rudarenjem podataka, krsenje privatnosti korisnika
* Vecinom privatni
* Skloni hakiranju zbog pretjerane centralizacije I pojedinačnih točaka kvara
* Problem uskog grla kod iznenadnih skokova aktivnosti korisnika
* „ centralizirane platforme često su podložne državnom nadzoru i cenzuri,“
* Sve rade na cloudu I problema je sto se tamo mora pohranjivat Velika kol pod, sto je skupo, moraju puno paltit aws i slicno?

### IZVORI

<https://en.wikipedia.org/wiki/Real-time_communication>

<https://www.vonage.com/resources/articles/real-time-communications/>

<https://www.dialogic.com/glossary/real-time-communications-rtc>

<https://www.ecosmob.com/real-time-communications-rtc-a-detailed-guide/>

<https://www.tutorialspoint.com/real-time-communications-rtc>

<https://getstream.io/glossary/real-time-communication/>

# dRTC

Decentralizirane mreže imaju peer-to-peer arhitekturu odnosno svi korisnici su ravnopravni i ne oslanjaju se na centraliziranog poslužitelja. Podatci se ne pohranjuju na jednom poslužitelju već se distribuiraju kroz mrežu neovisnih čvorova i nitko između korisnika (npr. poslužitelj) nema pristup podatcima. Korisnici imaju potpuno vlasništvo nad svojim podatcima, time su smanjeni rizici povrede privatnosti i neovlaštenog pristupa. Decentralizirana mreža ima bolju skalabilnost jer može podnijet veću broj korisnika i veći podatkovni promet. Povećana je sigurnost i privatnost jer su eliminirane pojedinačne točke kvara. [Mrežnu infrastrukturu podržavaju sudionici koji upravljaju čvorovima.](https://medium.com/@sendinglabs/whos-really-building-secure-decentralized-communication-49badb1be593) [Centralizirane platforme često su podložne državnom nadzoru i cenzuri, što potkopava samu ideju privatne, sigurne komunikacije.](https://medium.com/@sendinglabs/whos-really-building-secure-decentralized-communication-49badb1be593)

Sva komunikacija je end-to-end enkriptirana i izravno usmjerena između korisnika. Općenito, dRTC nude bolju sigurnost od RTC-a.

* pravila se implementiraju ili modificiraju putem konsenzusa, a ne po želji i želji bilo kojeg centraliziranog entiteta
* secure **wallet-to-wallet** communications -> fokus na korisnika, ima potpunu kontroolu nad svojim podacima

### DECENTRALIZIRANI MESSENGERI

[Poruke prosljeđuju odabrani čvorovi nasumično, s novim skupom čvorova koji se koriste za svaku poruku.](https://trueconf.com/blog/reviews-comparisons/decentralized-messaging)

Problemi: mogu biti spori I ograničenog prostora za pohranu.

### KAKO SE USPOSTAVLJA VEZA?

Signalizacija ili uspostava veze se moze odvijat putem distribuiranih sustava poput:

- Matrix protokola: Koristi distribuiranu mrežu poslužitelja za razmjenu signalizacijskih poruka.

- Blockchaina: Autentifikacija i signalizacija mogu se odvijati putem pametnih ugovora ili distribuiranih baza podataka.

### DECENTRALIZIRANE TEHNOLOGIJE

DePIN - “poruke su šifrirane i prenose se izravno između korisnika bez prolaska kroz središnje tijelo“

Blockchain

- osigurava integritet podataka, transparentnost i zapise zaštićene od neovlaštenog mijenjanja. Također olakšava sigurnu komunikaciju i uklanja središnje točke kvara.

- Obicno prespor da bi komunikacija bila bas realtime

Streamr Network

- <https://streamr.network/>

* Aplikacije: TrueConf, Wickr, Signal, Session, Brirar

### PROTOKOLI

<https://www.linkedin.com/pulse/communication-protocols-distributed-systems-arthur-sergeyan/>

#### 1.MATRIX

* “besplatan i otvoren, siguran, decentralizirani protokol za komunikaciju u stvarnom vremenu”
* za razmjenu poruka i multimedijalnih podataka u decentraliziranoj mreži
* Podržava text poruke, grupni razgovore, audio/video pozive, botove.
* Matrix je poveziv s drugim protokolima i alatima.
* Koristi end-to-end enkripciju.
* Web aplikacija + desktop klijent + mobilne aplikacije dostupne
* Prepoznaje status prisutnosti
* “Svatko može postaviti samostalni kućni poslužitelj za sudjelovanje u globalnoj mreži Matrix i komunikaciju s drugima u sobama za čavrljanje”
* “Sadržaj sobe replicira se između svih poslužitelja koji sudjeluju, što znači da ne postoji jedinstvena točka kontrole ili kvara. Ali možete stvoriti lokalnu sobu dostupnu samo korisnicima poslužitelja.”
* BRIDGES – omogucuju da korisnici s razlicitih messengera komuniciraju u istoj sobi
* Sluzbeno podrzani mostovi = Slack, IRC, XMPP i Gitter
* WIDGETI - integraciju aplikacija trećih strana u sobe, npr zaj uredivanje dokumenata, kalendar, itd…
* ima izvrsnu funkcionalnost za izradu prilagođenih robota
* „Matrix is a rich ecosystem of clients, servers, bots and application services.“
* Element je messenger koji koristi Matrix protkol?

<https://trueconf.com/blog/reviews-comparisons/decentralized-messaging>

<https://matrix.org/>

#### 2.XMPP (Extensible Messaging and Presence Protocol)

- **Namjena**: Decentralizirani protokol za razmjenu poruka i praćenje prisutnosti.

- Podržava federaciju servera i end-to-end enkripciju

- Može se koristiti za RTC putem dodataka

#### 3. WebRTC (Web Real-Time Communication)

- **Namjena**: Omogućuje izravnu (peer-to-peer) razmjenu audio, video i podatkovnih tokova.

- **SRTP (Secure Real-Time Protocol)** za sigurnu razmjenu podataka.

**- ICE (Interactive Connectivity Establishment)** za uspostavu P2P veze kroz NAT/firewall.

**- DTLS (Datagram Transport Layer Security)** za enkripciju komunikacije.

#### 4. SIP (Session Initiation Protocol)

- Upravljanje i signalizacija za uspostavu glasovnih i video poziva.

- decentralizirana arhitektura

- end-to-end enkripcija

- koristi se kod VoIP aplikacija i decentraliziranih telefona

SIGNAL PROTOKOL

* Kriptografski protocol
* End-to-end ekripcija za glasovne I trenutne razgovore
* Koristi ga whatsapp

## IZVORI

<https://medium.com/@suryatamrakar395/how-media-nodes-work-in-a-drtc-network-decentralized-real-time-communication-74b766c3090b>

<https://medium.com/@sendinglabs/whos-really-building-secure-decentralized-communication-49badb1be593>

<https://trueconf.com/blog/reviews-comparisons/decentralized-messaging>

<https://hackernoon.com/decentralizing-real-time-communication-shaping-the-future-of-connectivity>

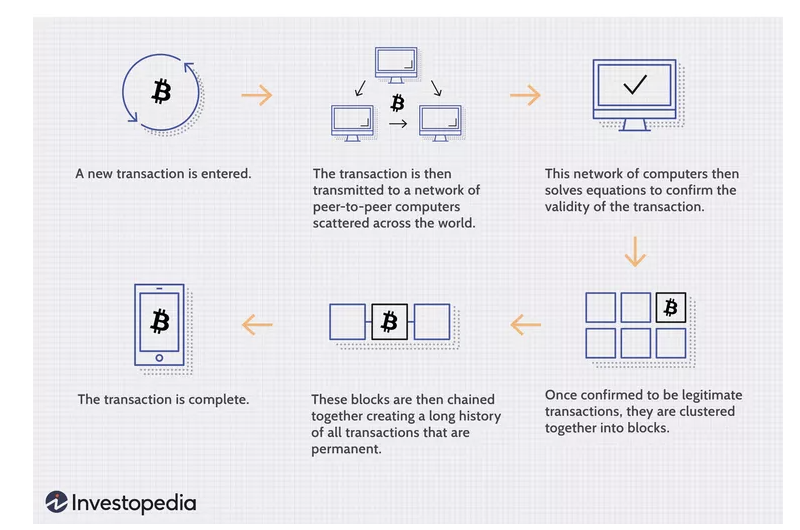
## BLOCKCHAIN

* osigurava integritet podataka, transparentnost i zapise zaštićene od neovlaštenog mijenjanja. Također olakšava sigurnu komunikaciju i uklanja središnje točke kvara.
* Obicno prespor da bi komunikacija bila bas realtime
* decentralizirana i distribuirana baza podataka, P2P
* lanac međusobno povezanih blokova koji sadrže podatke
* blok sadrzi: podatke(npr.transakcije), hash (kriptografski kod koji identificira blok), has prethodnog bloka
* promjena u jedno bloku mijenja sve blokove nakon njega -> sigurnost
* svako racunalo ima kopiju blockchaina
* transakcije se grupiraju u blokove i blokovi se dodaju na kraj lanca nakon validacije
* nema potrebe za third party validation
* jednom zapisani podaci se ne mogu mijenjat bez konsenzusa mreze -> nema potrebe za trecom stranom od povjerenja
* transparentnost – svi sudionici mreze mogu pregledati transakcije
* koristi metode poput Proof of Work (PoW) ili Proof of Stake (PoS**)** za postizanje dogovora o validaciji novih blokova.
* Moze biti javni (otvoren za sve), privatni (dostupan samo odredenim korisnicima), konzorcijski (kombinacija)
* Koristi se kod decentraliziranih apps (dapps)
* Kljucna uloga u sustavima kriptovaluta, sigurna i decentrlizirana evidencija transakcija
* Vrsta zajednicke baze podatka, drugacije pohranjuje podatke od tipicne BP,  lanci blokova pohranjuju podatke u blokove koji su međusobno povezani putem kriptografije

#### KAKO FUNCIONIRA BLOCKCHAIN?

BLOCKCHAIN = program od vise skripti koje obavljaju unos pristup spremanje podataka

* Kopije se spremaju na sva racunala u mrezi
* Podatci se unose u datoteku koja predstavlja blok
* Kad se blok napuni, podaci u bloku prolaze kroz kriptografsku hash funkciju, koja stvara heksadecimalni broj koji se naziva hash zaglavlja bloka
* Hash se unosi u zaglavlje sljedeceg bloka i enkripitira se s ostalim inforamacijama u tom bloku
* Time je napravljen lanac blokova



#### IZVORI

<https://en.wikipedia.org/wiki/Blockchain>

<https://www.investopedia.com/terms/b/blockchain.asp>

<https://www.ibm.com/topics/blockchain>

### YT VIDEI

<https://www.youtube.com/watch?v=A2RYrpmhV78&list=PLoSfx19fpj1hqtowHE4SJ8YPp0Hl61_MJ&index=2&pp=gAQBiAQB>

<https://www.youtube.com/watch?v=3AVsNqH_-9M&list=PLoSfx19fpj1hqtowHE4SJ8YPp0Hl61_MJ&index=5&pp=gAQBiAQB>

<https://www.youtube.com/watch?v=HHB2C_aG4SE&list=PLoSfx19fpj1hqtowHE4SJ8YPp0Hl61_MJ&index=7&pp=gAQBiAQB>

<https://www.youtube.com/watch?v=D7AKdVaCyHc>

<https://www.youtube.com/watch?v=3AVsNqH_-9M&t=443s>

<https://www.youtube.com/watch?v=vVsIHCTGjsE&t=301s>

<https://www.youtube.com/watch?v=1RJyzUxf0ME>

<https://www.youtube.com/watch?v=A2RYrpmhV78>

IDEJE ZA DALJE

SEMINAR 2

* istrazit kako napravti decentraliziranu aplikaciju za realtime komunikaciju
* odredit funkcionlanosti, protokole, tehnologije

ZAVRSNI PROJEKT

* Prva verzija aplikacije s osnovnim funkcionalnostima (npr. Samo razmjena poruka)

DIPLOMSKI

* Poboljsana verzija aplikacije sa vise funkcionalnosti, rijesena sigurnost, dobro sucelje