# Unapređenje bezbednosti pametnog grada: pregled rešenja zasnovanih na blokčejn tehnologiji

*NIKOLA D. MATIJAŠEVIĆ,* Univerzitet u Beogradu,
Saobraćajni fakultet, Beograd
ORCID: 0000-0001-9157-2482
*MIRJANA D. STOJANOVIĆ*, Univerzitet u Beogradu,
Saobraćajni fakultet, Beograd
ORCID: 0000-0003-1073-5804

*Pregledni rad*
*UDC: 711.45:004.5*
*DOI: 10.5937/tehnika2504433M*

*Rad se bavi primenom blokčejn tehnologije za unapređenje bezbednosti i privatnosti u pametnim gradovima, sa posebnim fokusom na IoT sisteme. Pametni gradovi zavise od velikog broja uređaja i senzora koji prikupljaju i razmenjuju podatke u realnom vremenu, što stvara značajne izazove u pogledu bezbednosti i zaštite podataka. Centralizovani sistemi skladištenja podataka i veliki broj IoT uređaja izloženi su sajber napadima, zbog čega je blokčejn tehnologija predstavljena kao potencijalno rešenje. Kroz decentralizovanu arhitekturu i pametne ugovore, blokčejn omogućava bezbedno čuvanje i razmenu podataka, smanjujući rizik od jedinstvenih tačaka otkaza i neovlašćenog pristupa. Rad analizira primenu privatnih i javnih blokčejn platformi, ističući prednosti i mane svake od njih. Takođe se obrađuju izazovi poput skalabilnosti i energetske potrošnje, kao i mogućnosti daljeg razvoja ove tehnologije za unapređenje bezbednosti u pametnim gradovima. Zaključuje se da blokčejn nudi značajan potencijal, ali da su neophodna dalja istraživanja kako bi se prevazišli tehnički izazovi.*

**Ključne reči**: *blokčejn, pametni gradovi, IoT, bezbednost podataka, privatnost*

## 1. UVOD

Pametan grad (smart city) predstavlja novi talas u urbanističkom planiranju i razvoju, koji koristi tehnologije za poboljšanje kvaliteta života, održivosti i efikasnosti [1]. Digitalnu kičmu pametnih gradova predstavljaju mreže Internet of Things (IoT) i Industrial Internet of Things (IIoT). Ove mreže omogućavaju prikupljanje podataka i analizu u realnom vremenu u urbanim sistemima, poput saobraćaja, distribucije energije ili odlaganja otpada. Integracijom digitalnih mreža, pametni gradovi optimiziraju resurse, smanjuju troškove i odgovaraju na potrebe stanovnika, stvarajući povezaniju i inteligentniju urbanu budućnost [1].

Pametni gradovi se suočavaju sa izazovima bezbednosti i privatnosti zbog velike količine podataka i nebezbednih IoT uređaja, koji su često prvi na udaru sajber napada [2]. Takođe, centralizovano skladištenje podataka povećava rizik [3], dok složena integracija sistema povećava mogućnosti zlonamernih napada [4].

Pitanja privatnosti uključuju prikupljanje podataka i nadzor, uz izazove vlasništva i kontrole [5]. Pojavljuju se i ekološke i etičke dileme koje treba prevazići [6], [7].

Blokčejn tehnologija nudi decentralizovano i bezbedno upravljanje podacima u pametnim gradovima, rešavajući probleme centralizovanih sistema i jedinstvenih tačaka otkaza. Sa distribuiranim konsenzusom, nepromenljivošću i transparentnošću, blokčejn poboljšava bezbednost podataka, smanjujući opasnosti povezane sa centralizovanim sistemima i jedinstvenim tačkama otkaza [8].

Takođe, pametni ugovori u blokčejnu mogu automatski da sprovedu pravila privatnosti podataka čime regulišu pristup korisnika [9]. Privatne blokčejn platforme dodatno unapređuju privatnost zbog mehanizama koji ograničavaju ko može da vidi podatke i komunicira sa njima [10].

Motivacija ovog rada se ogleda u sledećem:

- Otklanjanje jedinstvenih tačaka otkaza u pametnim gradovima jer centralizovani sistemi zaostaju u pogledu bezbednosti.

Adresa autora: Nikola Matijašević, Univerzitet u Beogradu, Saobraćajni fakultet, Beograd, Vojvode Stepe 305
e-mail: nikola.matijasevic@sf.bg.ac.rs
Rad primljen: 20.09.2024.
Rad prihvaćen: 13.06.2025.

- Zabrinutost zbog privatnosti podataka, otpornosti infrastrukture i potencijala za poremećaje u pametnim gradovima.
- Neophodnost istraživanja inovativnih bezbednosnih rešenja za pametne gradove.

Ciljevi razmatranja primene blokčejn tehnologije u pametnim gradovima se svode na:

- Obezbeđivanje pregleda primene blokčejn tehnologije kao rešenja za bezbednosne izazove u pametnim gradovima.
- Ispitivanje različitih pristupa zasnovanih na blokčejnu radi prikaza njenog potencijala u poboljšanju bezbednosti, privatnosti i otpornosti infrastrukture pametnih gradova.
- Doprinos rastućem obimu znanja o ulozi blokčejna u jačanju bezbednosnog prostora u pametnim gradovima.
- Podsticanje budućeg razvoja u oblasti bezbednosti pametnih gradova kroz primenu blokčejn tehnologije.

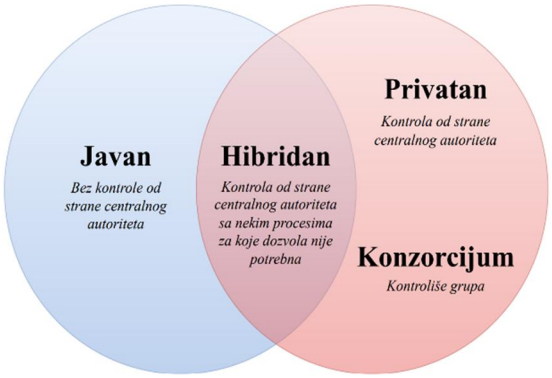
Ostatak rada je struktuiran na sledeći način. U drugom poglavlju dat je opis blokčejn tehnologije i njenih osobina. Treće poglavlje pruža metodologiju izbora relevantnih radova. Poglavlje 4 vrši evaluaciju rešenja, kao i njihova poređenja. Poslednje poglavlje daje zaključna razmatranja.

## 2. BLOKČEJN TEHNOLOGIJA

Blokčejn, prvobitno dizajniran za kriptovalute poput Bitkoina, postao je ključan za bezbednost i privatnost digitalnih transakcija. Njegova decentralizovana arhitektura pruža odbranu od sajber napada, ilegalnog pristupa i krađe podataka. Glavne osobine blokčejn tehnologije su [11]:

- Decentralizacija – Eliminiše jedinstvene tačke otkaza.
- Nepromenljivost – Podaci se ne mogu izmeniti ili obrisati.
- Integritet, autentičnost i neporicanje – Integritet podataka je očuvan, autentičnost je garantovana kroz kriptografske tehnike, a učesnici ne mogu poreći transakcije.
- Proverljivost – Zapis svih transakcija, unosi se mogu pratiti i pregledati.

Ove karakteristike čine blokčejn pogodnim za bezbednu, transparentnu i pouzdanu upotrebu u raznim industrijama. Moguće je praviti kompromise po karakteristikama u zavisnosti od svrhe korišćenja blokčejna (slika 1). Zbog toga, postoje različiti tipovi platformi poput javnih, privatnih, hibridnih i konzorcijumskih [12]. Ključna funkcionalnost ovih platformi jesu pametni ugovori. Oni predstavljaju izvršni kod koji se čuva i automatski izvršava na blokčejn mreži, deluju kao digitalni sporazumi između dve ili više strana bez posrednika [13].




*Slika 1 – Tipovi blokčejn platformi*

Integracija blokčejn tehnologije u pametne gradove poboljšava upravljanje gradskim sistemima, bezbednošću i privatnošću. Pametni gradovi se oslanjaju na mrežu povezanih uređaja koji donose bezbednosne i privatnosne izazove. Blokčejn nudi rešenje pružajući bezbednu i decentralizovanu platformu za upravljanje i skladištenje podataka IoT uređaja, ključnu za kritičnu infrastrukturu poput energetskih mreža i transportnih sistema [14]. Blokčejn omogućava bezbedno skladištenje i deljenje ličnih podataka sa ovlašćenim entitetima, povećavajući poverenje građana kroz transparentnost i nepromenljivost. Kombinacija bezbednosti i privatnosti čini blokčejn idealnim za stvaranje otpornijih, efikasnijih i pouzdanijih pametnih gradova [15].

Blokčejn se suočava i sa izazovima poput skalabilnosti, visoke potrošnje energije i regulatorne neizvesnosti [16]. Ovo se rešava kroz istraživanja i razvoj u oblastima kao što su sharding, rešenja za skaliranje na drugom sloju (layer-two scaling) i energetski efikasni konsenzusi, čime će se usvajanje blokčejna u pametnim gradovima ubrzati.

## 3. PRIMENJENA METODOLOGIJA

Početni skup radova je formiran pretragom *IEEE Xplore* baze podataka. Ključne reči koje su se koristile za pretragu su: „blockchain“, „IoT security“ i „smart city“. Pretraga je urađena u avgustu 2024. godine i razmatran je petogodišnji period od sredine 2019. do sredine 2024. godine. Pronađeno je 109 radova, gde je nakon ručne inspekcije i isključenja radova koji se ponavljaju, dobijeni skup od 45 radova. Ovaj broj je redukovan na osnovu naslova radova i njihovih rezimea, gde je fokus na one koji su imali originalan doprinos vezan za primenu blokčejn tehnologije u pametnim gradovima. Na kraju ovog koraka broj radova je 16. Nakon uvida u pune verzije, cilj je bio da se dobije skup jedinstvenih i uporedivih rešenja. Eliminisani su slični radovi istih autora i radovi različitih autora koji opisuju rezultate istih projekata, kao i radovi koji nisu koristili konkretne bezbednosne

napade za testiranje, predlog strategije za ublažavanje ili ih ne pominju kao brigu. Konačan broj radova je 9.

## 4. EVALUACIJA I POREĐENJE REŠENJA

Tabela 1 daje informacije o izabranim radovima poput primene u pametnim gradovima, ključnim izazovima, predloženom rešenju, tipu blokčejn platforme, konsenzus protokolu, funkcionalnosti pametnih ugovora i primenu dodatnih tehnologija. Rad [17] uvodi SecPrivPreserve okvir za poboljšanje bezbednosti podataka, dok rad [18] integriše blokčejn sa softverski definisanim mrežama (*Software Defined Networking*, SDN) radi unapređenja detekcije napada i bezbednost mreže. Rad [19] koristi blokčejn za bezbedno e-glasanje kroz transparentnost i sprečavanje manipulacije. Rad [20] uvodi DistB-Condo, koji kombinuje blokčejn, SDN i virtualizaciju mrežnih funkcija (*Network Function Virtualization*, NFV) za bezbedno upravljanje podacima u pametnim stambenim okruženjima. Fokus rada [21] je na bezbednosti i energetskoj efikasnosti u zelenim IoT implementacijama.

Radovi [22] i [23] ističu ulogu blokčejna u bezbednoj komunikaciji dronova i biometrijskoj bezbednosti za mreže vozila, respektivno. Fokus za [24] i [25] je skalabilnost: prvi predlaže skalabilnu blok graf platformu za IIoT aplikacije, dok drugi sistem potpisa bez sertifikata za efikasnu komunikaciju između IIoT uređaja.

Radovi zajedno demonstriraju svestranost blokčejna u poboljšanju integriteta podataka, bezbednosti, privatnosti i upravljanja resursima u različitim IoT aplikacijama, dok istovremeno prepoznaju stalnu potrebu za optimizacijom njegove primene u okruženjima sa ograničenim resursima.

*Tabela 1. Pregled izabranih radova: Opšte informacije*

| Rad | Primena u pametnim gradovima | Ključni izazovi | Predloženo rešenje | Tip blokčejn platforme | Konsenzus protokoli | Pametni ugovori | Dodatne tehnologije |
|---|---|---|---|---|---|---|---|
| [17] | Zdravstvo | Popuštanje privatnosti, računarska složenost, ograničenje resursa | SecPrivPreserve okvir sa višefaznom bezbednošću i minimizovanim kriptografskim operacijama | Privatan (*Hyperledger Fabric*) | Bezbednost korišćenjem HLF-a | Da | / |
| [18] | Generalno (mrežna infrastruktura) | Skalabilnost, bezbednosne pretnje, skladištenje i upravljanje podacima, jedinstvena tačka otkaza | Okvir koji kombinuje SDN i blokčejn za unapređenu bezbednost i prenos podataka | Javan (*Ethereum*) | Predložen protokol, PoW | Da | SDN |
| [19] | Elektronsko glasanje | Bezbednost IoT uređaja, propusti u privatnosti i bezbednosti u e-glasanju, identifikacija zlonamernih uređaja | Mehanizam za izračunavanje poverenja za IoT uređaje i sistem e-glasanja zasnovan na blokčejnu | Javan (*Ethereum*) | / | / | / |
| [20] | Stambene jedinice | Mrežna povezanost i bezbednost, skladištenje i prenos podataka, bezbednost i privatnost podataka, složenost implementacije blokčejna | DistB-Condo arhitektura sa integracijom SDN-a, blokčejna i NFV-a, pristup za selekciju klaster glava (čvora) radi energetske efikasnosti | Javan (*Ethereum*) | PoW, PoS | Da | SDN, Cloud |
| [21] | Generalno (ekologija) | Energetska ograničenja u decentralizaciji, visoka potrošnja energije u blokčejnu, računarska složenost kriptografskih tehnika | BENIGREEN sa energetski efikasnom selekcijom klaster glava (čvora), autentifikacijom koja čuva privatnost i skladištenje podataka na blokčejnu | / | / | / | Cloud |

| Rad | Primena u pametnim gradovima | Ključni izazovi | Predloženo rešenje | Tip blokčejn platforme | Konsenzus protokoli | Pametni ugovori | Dodatne tehnologije |
|---|---|---|---|---|---|---|---|
| [22] | Dronovi | Bezbednost mreže dronova, autentifikacija dronova, zabrinutost za privatnost | Decentralizovana arhitektura sa mrežom dron-kontrolera (DC) i autentifikacijom zasnovanom na blokčejnu | Javan (*Bitcoin*) | DDPOS, PoW, Network-based | / | AI |
| [23] | Inteligentni transportni sistemi | Bezbednost i privatnost u VANET mrežama, centralizovani bezbednosni sistemi, sledljivost zlonamernog ponašanja | Okvir za očuvanje privatnosti zasnovan na biometriji i blokčejnu | / | Kombinacija PoW-a i TOPSIS-a | Da | VANET |
| [24] | Generalno (raznovrsne usluge) | Ograničeni resursi IoT uređaja, skalabilnost, vreme odziva | Blok graf platforma sa hibridnim konsenzusom i specijalizovanim komitetima za upravljanje transakcijama | / | Integracija PoW i PoS, PBFT | / | / |
| [25] | Efikasan potpis bez sertifikata | Problem povratnog ključa u sertifikatima bez potpisa, ranjivost na napade, troškovi računanja operacija uparivanja | Poboljšan CLS sistem sa unapređenom bezbednošću protiv poznatih napada | Javan (*Ethereum*) | Bezbednost korišćenjem CLS-a | Da | CLS |

Tabela 2 opisuje korišćene alate, softverske i hardverske uslove i podešavanja parametara simulacije. Radovi [17] i [18] koriste Linux Ubuntu platformu, pri čemu [17] koristi Fabric SDK za simulaciju blokčejn mreže sa do 500 čvorova i do 5000 transakcija, dok [18] koristi Mininet emulator, Ryu controller i Pyethereum za simulaciju mrežne infrastrukture. Radovi [19] i [21] koriste MATLAB Simulator, ali se razlikuju po pristupima: [19] simulira komunikacione mreže sa 50 čvorova, dok [21] koristi stariju verziju MATLAB-a za simulaciju protoka podataka u specifičnim uslovima sa Intel i3 procesorom. Radovi [20], [22] i [23] se bave simulacijama velikih mreža koristeći različite alate: [20] koristi Cooja, Mininet i OpenFlow za simulacije IoT uređaja i SDN mreža, dok rad [22] koristi NS-3 i Bitcoin Simulator za simulaciju dronova u mrežama, a rad [23] koristi OMNeT++ i SUMO za simulaciju mreža vozila.

Radovi [24] i [25] se razlikuju u pristupima: [24] koristi Python model za simulaciju blokčejn grafova sa fokusom na kašnjenje mreže, dok [25] primenjuje MIRACLE za generisanje kriptografskih ključeva korišćenjem pametnih ugovora uz fokus na bezbednosti.

*Tabela 2. Informacije o simulaciji*

| Rad | Simulacioni alati | Operativni sistem | Hardverske specifikacije | Parametri simulacije |
|---|---|---|---|---|
| [17] | *Fabric SDK* | *Linux Ubuntu* | Intel i7 CPU, 16GB RAM | Broj čvorova: 100, 200, 300, 400, 500; Broj transakcija: 1000, 2000, 3000, 4000, 5000; Kanali: 1, 2, 3, 4, 5; Organizacije: 2; Čvorovi raspoređivanja: 4, 8, 12, 16, 20; Čvorovi potvrđivanja: 4, 8, 12, 16, 20; Čvorovi odobravanja: 4, 8, 12, 16, 20; Runde: 100; Veličina bloka: 2 MB, 4 MB |
| [18] | *Mininet emulator, Ryu controller, Pyethereum tester tool* | *Linux Ubuntu* | / | / |
| [19] | *MATLAB Simulator* | / | / | Broj čvorova: 50; Opseg komunikacije rutera: 120 m |

| Rad | Simulacioni alati | Operativni sistem | Hardverske specifikacije | Parametri simulacije |
|---|---|---|---|---|
| [20] | *Cooja, Mininet, OpenFlow, SDK APIs solidity, Wireshark* | *Linux Ubuntu* | Intel i5 CPU 2.20GHz, 6GB RAM, 1TB ROM | Broj IoT uređaja: 1-100; Vreme simulacije: 500 s; Površina simulacije: 2500 m x 2500 m; Brzina prenosa podataka: 10 Mbps; Veličina prenesenog paketa: 128-1024 bajta; Broj SDN kontrolera: 5; Broj *gateway*-a: 2 |
| [21] | *MATLAB Simulator 2017* | / | Intel i3-3217 CPU 1.80GHz, 4GB RAM | / |
| [22] | *NS-3, Bitcoin Simulator* | / | / | Broj dronova: 100; Brzina članova: 10 m/s; Broj zona: 10; Broj dron-kontrolera: 10; Tip saobraćaja: Konstantna brzina prenosa bitova; Vreme simulacije: 1800 s; Površina: 10 km x 10 km; Veličina paketa: 512 bajta; Veličina bloka: 0.1 MB do 1 MB; Zaglavlje bloka: 80 bajta; Broj rudara: 16 do 128 |
| [23] | *OMNeT++, Veins, SUMO* | / | / | Broj vozila: 100; Maksimalna brzina vozila: 50 m/s; Maksimalno ubrzanje vozila: 3 $m/s^2$; Maksimalno usporenje vozila: 5 $m/s^2$; Dužina vozila: 4 m; Širina vozila: 2.5 m; Broj jedinica pored puta: 15; Pokrivenost jedne jedinice pored puta: 2 km |
| [24] | *Custom block graph model (Python)* | / | / | Kašnjenje mreže: 0.01, 0.02, 0.05, 0.1, 0.2 s; Prosečno vreme između blokova: varijabilno; Period merenja za svaki eksperiment: 180 s |
| [25] | *Miracle library, Smart contract based key generation center* | / | Intel i7-4700 CPU, 8GB DDR4 3200MHz RAM | / |

Navedeni radovi se mogu grupisati u tri kategorije prema pristupu simulaciji i proceni blokčejn sistema. Radovi [23] i [25] koriste „specijalizovane mrežne simulatore“ OMNeT++, Veins, SUMO i MIRACLE za modeliranje i analizu blokčejna u složenim mrežnim okruženjima, što je korisno za velike aplikacije kao što su VANET mreže.

Nasuprot tome, radovi [17]-[22] koriste „jezike/-biblioteke opšte namene“ kao što su Fabric SDK, Python i MATLAB za fleksibilnu implementaciju i analizu specifičnih aspekata blokčejn sistema, fokusirajući se na evaluaciju efikasnosti i bezbednosti. Rad [24] koristi pristup „prilagođene implementacije“ tako što razvija jedinstveni model blok grafa u Python-u, istražujući alternativne pristupe za skalabilnost i efikasnost u IIoT okruženju. Ove informacije omogućavaju upoređivanje tehničkih postavki i performansi simulacionih modela.

U tabeli 3 prikazani su rezultati performansi koji su ostvareni u razmatranim radovima. Pored toga, navedene su i sve ključne metrike performansi koje su bile praćene, kao i prema kojim rezultatima različitih modela, algoritama, metoda i sl. je vršeno poređenje. Radovi [17], [19] i [25] istražuju bezbednost blokčejna, ali sa različitim pristupima. U [17] je fokus na autentifikaciji i zaštiti podataka, dok [19] naglašava otpornost na izmene poruka i DoS napade. Nasuprot tome, u [25] se optimizuju kriptografske operacije, smanjujući troškove generisanja potpisa i verifikacije, što ga čini efikasnim za sisteme sa ograničenim resursima. Sa druge strane, radovi [18], [20] i [23] se fokusiraju na mrežne performanse i raznolikost okruženja.

*Tabela 3. Rezultati i evaluacija performansi*

| Rad | Ključne metrike performansi | Dobijeni rezultati | Poređenje prema rezultatima |
|---|---|---|---|
| [17] | Vreme odziva; Vreme obrade; Kvalitet enkripcije; Vreme detekcije | 34 s; 94 s; 0.87 s; 0.82 s | Osnovni model 1 koji se fokusira na autentifikaciju i zaštitu podataka koristeći blokčejn; Osnovni model 2 koji se fokusira na validaciju podataka i kontrolu pristupa koristeći blokčejn |
| [18] | Propusni opseg; Vreme odziva; Iskorišćenost energije; Stopa gubitka paketa | Poboljšanja od 16.6% za 400 zahteva, 35.7% za 800 zahteva, 40% za 1200 zahteva, 10.3% za 1600 zahteva i 20.2% za 2000 zahteva; Poboljšanje od 0.001 za 400 zahteva i više; Poboljšanja su postignuta, ali nisu komentarisana; Poboljšanje od 37.5% za 40 čvorova i povećava se sa brojem čvorova | *Core* model; *DistArch-SCNet* model; *ClusterHead Selection* |

| | | | |
|---|---|---|---|
| [19] | Poverenje; Kašnjenje autentifikacije; Izmena poruka; Otpornost na DoS napade | Prenos poruka i autentifikacija čvorova imaju najveću težinu u određivanju legitimnosti čvora, što dovodi do poboljšanog uspostavljanja poverenja u odnosu na osnovnu metodu; Postignuta je brža autentifikacija nego kod osnovne metode; Poboljšana otpornost predloženog sistema na napade izmene poruka zahvaljujući distribuiranoj prirodi blokčejn sistema; Povećana otpornost na DoS napade kao rezultat sposobnosti blokčejna da identifikuje i ukloni zlonamerne čvorove | Osnovna metoda koja predstavlja blokčejn sistem za e-glasanje, dizajniran da očuva transparentnost, ograniči pretnje prilikom glasanja i kontroliše nepravilne operacije birača, koristi kriptografske mehanizme zasnovane na hešu i sertifikatima |
| [20] | Protok; Propusni opseg; Vreme odziva; Potrošnja gasa; Iskorišćenost CPU-a | Za 50 čvorova protok je bolji, dok za preko 50 čvorova pokazuje se značajno bolji protok; Stabilniji propusni opseg dok se stopa dolaska paketa povećava, sa padom od 11% pod DDoS napadom u poređenju sa padom od 81% kod drugih modela; Pokazuje 5% brže prosečno vreme odziva u odnosu na osnovni model prilikom prenosa datoteka različitih veličina; Povećava se linearno kako broj transakcija raste na *Ethereum*-u; Održava nižu prosečnu iskorišćenost CPU-a u poređenju sa osnovnim modelom tokom DDoS napada | *OpenFlow based SDN* model; Osnovni model koji se koristi samo za poređenje vremena odziva |
| [21] | Računarsko kašnjenje; Vreme operacije; Protok; Prosečna potrošnja energije | Povećava se za 0.02 s po bloku, u proseku 45.31% bolje; Nije najbolji rezultat, ali je u proseku 21.2% bolji; 31.21% bolje performanse; 39.07% manja potrošnja energije | Četiri predložena modela iz drugih radova |
| [22] | Protok; Kašnjenje od kraja do kraja; Stopa gubitka paketa; Kašnjenje autentifikacije; Verovatnoća detekcije napada | Ostvareno je 260 bps (bita po sekundi), što je bolje od dva druga rešenja (201.5 i 223.89 bps); Ostvareno je 0.0226 bps, što je bolje od dva druga rešenja (0.210 i 0.03985 bps); Niža stopa prikazana grafički u radu; Niže kašnjenje prikazano grafički u radu; Predložena arhitektura je detektovala 97.5% napada, u poređenju sa 55% za osnovni model. | *Secure Lightweight*; Osnovni model koji koristi uobičajenu tehniku autentifikacije dronova sa serverom za autentifikaciju treće strane; DPOS i POW modeli |
| [23] | Stopa isporuke paketa; Stopa gubitka paketa; Računarski trošak | Viša stopa isporuke paketa (0.99 bez DoS napada, 0.96 sa DoS napadom); Niža stopa gubitka paketa sa ili bez DoS napada; Niži računarski trošak (0.1 ms sa 20 vozila i 0.3 ms sa 100 vozila) | ASC algoritam; LAKAP algoritam; BC-VANET model |
| [24] | Protok transakcija; Odnos validnih blokova | Veći protok transakcija (252000) u poređenju sa tradicionalnim blokčejn platformama (kao što su *Bitcoin* (2520) i *Ethereum* (7200)) i drugim blokčejn platformama (*Blockclique* (180000)); Stabilan kada je vreme između blokova veće od 4 s | *Bitcoin*; *Ethereum*; *Blockclique* |
| [25] | Bezbednosne karakteristike; Trošak komunikacije; Trošak obrade | Poboljšana otpornost na različite bezbednosne napade; 480 bitova, uporedivo sa većinom drugih šema; Značajno smanjenje vremena generisanja potpisa (0.002 ms) i verifikacije (1.03 ms) | Pet predložena modela iz drugih radova |

U [18] dolazi do poboljšanja propusnog opsega i vremena odziva, dok [20] koristi OpenFlow za poboljšanje stabilnosti, protoka podataka i otpornost na DDoS napade. Iako se bavi mrežama vozila (VANET), [23] se fokusira na mrežne performanse, ali sa naglaskom na isporuku paketa i otpornosti na DoS napade. Radovi [21] i [22] kombinuju mrežne performanse i energetsku efikasnost. Prvi poboljšava računsku efikasnost i potrošnju energije, dok drugi postiže 97.5% uspešnosti u detekciji napada u mreži dronova. Ova dva rada ističu dugoročnu održivost mreža uzimajući u obzir energetske aspekte. Rad [24] uvodi prilagođeni blokčejn model fokusiran na povećanje broja transakcija i stabilnost sistema u složenim mrežnim okruženjima.

Za razliku od drugih radova, ovaj rad koristi specifičan blok graf u Python-u, dizajniran da reši izazove skalabilnosti u IoT okruženjima sa ograničenim resursima. U poređenju sa radovima poput [18] ili [25], koji koriste standardizovane modele i simulacione alate, [24] nudi inovativan pristup rešavanju problema specifičnih za IIoT. Radovi se mogu grupisati u dve kategorije. Radovi [1]-[4], [6] i [7] spadaju u kategoriju „detaljna komparativna analiza“ gde se vrši direktno poređenje svojih rešenja sa postojećim modelima, koristeći metrike poput vreme odziva, vreme obrade, propusni opseg, gubitak paketa i protok, kako bi kvantifikovali poboljšanja. Radovi [5], [8] i [9] pripadaju kategoriji „opšta evaluacija performansi“ gde se ističu ukupna poboljšanja bez direktnog poređenja sa specifičnim modelima, naglašavajući izvodljivost i potencijal pristupa. Ova podela ukazuje na različite metodologije i ciljeve u evaluaciji blokčejn tehnologije.

*Tabela 4. Razmatrani bezbednosni napadi*

| Bezbednosni napad | Rad [17] | Rad [18] | Rad [19] | Rad [20] | Rad [21] | Rad [22] | Rad [23] | Rad [24] | Rad [25] |
|---|---|---|---|---|---|---|---|---|---|
| DoS Attack | ✓ | ✓ | ✓ | X | X | ✓ | ✓ | X | X |
| DDoS Attack | ✓ | ✓ | ✓ | ✓ | X | ✓ | X | X | ✓ |
| Message Alteration | X | X | ✓ | X | ✓ | X | X | X | X |
| Brute Force/Cryptanalysis Attack | X | X | ✓ | X | X | X | X | X | X |
| Replay Attack | X | X | X | X | ✓ | X | ✓ | X | ✓ |
| MITM Attack | ✓ | ✓ | X | X | X | X | X | X | ✓ |
| 51% Attack | X | X | X | X | X | X | X | ✓ | ✓ |
| Sybil Attack | X | X | X | X | X | X | ✓ | ✓ | X |
| Authentication Attack | X | X | X | X | ✓ | ✓ | X | X | X |
| Privacy Attack | X | X | X | X | ✓ | X | X | X | X |
| Public Key Replace Attack | X | X | X | X | X | X | X | X | ✓ |
| Signature Forgery Attack | X | X | X | X | X | X | X | X | ✓ |
| KGC Compromised Attack | X | X | X | X | X | X | X | X | ✓ |
| Data poisoning | ✓ | X | X | ✓ | X | X | X | X | X |
| Ransomware | ✓ | X | X | X | X | X | X | X | X |

Svaki rad je razmatrao bar jedan bezbednosni napad kroz testiranje otpornosti, predlog strategije za njihovo ublažavanje ili kao brigu. Prema tome, u Tabeli 4 se može videti preciznije koji su se radovi bavili određenim bezbednosnim napadima. Radovi [17], [18] i [22] pokrivaju širok spektar napada uključujući DoS, DDoS i MITM napade, sa fokusom na mrežnu bezbednost i otpornost. Radovi [23] i [24] ciljaju napade koji su manje uobičajeni, ali značajni u specifičnim blokčejn kontekstima. Fokus u [23] je na Sybil napadu u decentralizovanim mrežama, dok [24] analizira 51% napad karakterističan za blokčejn konsenzus. Na drugoj strani spektra, radovi [21] i [25] se fokusiraju na sofisticirane kriptografske napade. Napadi na privatnost i autentifikaciju se razmatraju u [21], dok [25] analizira zamenu javnog ključa i falsifikovanje potpisa. Ova dva rada su jedinstvena po tome što se bave naprednijim pretnjama. Rad [19] se bavi naprednijim pretnjama, ali i DoS/DDoS napadima.

Po pitanju bezbednosti u blokčejnu i pametnim gradovima, ističu dva pristupa. Prvi pristup, kome pripadaju radovi [17]-[23], fokusira se na zaštitu specifičnih domena primene. poput pametnih gradova, SDN-IoT mreža, e-glasanja i komunikacije dronova, predlažući praktična rešenja za ranjivost. Rad [17] naglašava zaštitu podataka putem enkripcije, dok rad [23] predlaže biometrijsku bezbednost u mrežama vozila (VANET). Nasuprot tome, radovi [24] i [25] istražuju teorijske aspekte, fokusirajući se na ranjivost blokčejn arhitekture. Rad [24] analizira napade poput *Sybil* i 51%, dok rad [25] istražuje zaštitu potpisa bez sertifikata i robusno upravljanje ključevima. Ovaj dvostruki fokus naglašava ključan aspekt istraživanja bezbednosti blokčejna: potrebu da se adresiraju kako ranjivosti specifične za primenu, tako i druge slabosti koje bi mogle ugroziti integritet i pouzdanost blokčejn sistema.

Prema svim izabranim radovima i njihovom analizom, dolazi se do sledećih ključnih zapažanja:

- Različite metrike evaluacije: Radovi koriste širok spektar metrika, odražavajući višestruku primenu blokčejna u bezbednosti IoT-a u pametnim gradovima. Ova raznolikost čini poređenja izazovnim.
- Ograničeni kvantitativni podaci: Neki radovi se u velikoj meri oslanjaju na kvalitativne opise poboljšanja, dok drugi predstavljaju kvantitativne rezultate. Ova nedoslednost naglašava potrebu za standardizovanim okvirima evaluacije.
- Bezbednost kao primarni fokus: Mnogi radovi naglašavaju bezbednosne karakteristike i otpornost na napade, naglašavajući potencijal blokčejn thenologije u poboljšanju bezbednosti IoT-a u pametnim gradovima.

Takođe, pored ključnih zapažanja došlo se i do nekoliko opštih uvida koji su:

- Blokčejn tehnologija daje pozitivne naznake u rešavanju izazova bezbednosti i efikasnosti u različitim domenima IoT-a u pametnim gradovima.
- Specifične prednosti i poboljšanja performansi postignuta sa blokčejn tehnologijom variraju u za-

visnosti od primene, arhitekture i metoda evaluacije.

- Ovo polje bi imalo koristi od standardizovanijih pristupa evaluaciji kako bi se olakšala smislena poređenja i ubrzao razvoj robusnih IoT bezbednosnih rešenja zasnovanih na blokčejn tehnologiji.

## 5. ZAKLJUČAK

Rad istražuje primenu blokčejn tehnologije u pametnim gradovima, s posebnim naglaskom na poboljšanje bezbednosti, a delom i privatnosti u IoT ekosistemima. Pametni gradovi, sa svojim složenim mrežama uređaja i sistema, suočavaju se sa brojnim izazovima, uključujući ranjivost na sajber napade i narušavanje privatnosti podataka. Blokčejn tehnologija, sa svojom decentralizovanom i nepromenljivom arhitekturom, nudi robusna rešenja za te izazove, omogućavajući sigurnu razmenu podataka, otpornost na napade i bolju kontrolu nad privatnošću.

Jedan od značajnih doprinosa rada je analiza različitih pristupa primeni blokčejna u pametnim gradovima, koji pokazuju potencijal za poboljšanje bezbednosti, smanjenje rizika od centralizovanih tačaka otkaza i jačanje poverenja u digitalne transakcije. Iako blokčejn donosi značajne prednosti, poput veće transparentnosti i nepromenljivosti podataka, rad takođe ukazuje na izazove kao što su skalabilnost, energetska efikasnost, regulatorna neizvesnost i sl.

Zaključuje se da je blokčejn tehnologija ključan korak napred ka stvaranju sigurnijih i pouzdanijih pametnih gradova, ali da dalja istraživanja i optimizacije, naročito u pogledu performansi i skalabilnosti, ostaju neophodna kako bi se u potpunosti iskoristile njene mogućnosti u urbanim okruženjima budućnosti.

## LITERATURA


[1] Halegoua G. Smart Cities, The MIT Press, 2020.

[2] Rao P. M, Deebak B. D. Security and privacy issues in smart cities/industries: technologies, applications, and challenges, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, No. 8, str. 10517–10553, 2023.

[3] Panahi Rizi M. H, Hosseini Seno S. A. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city, *Elsevier B.V*, 2022.

[4] Ismagilova E, Hughes L, Rana N. P, Dwivedi Y. K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework, *Information Systems Frontiers*, Vol. 24, No. 2, str. 393–414, 2022.

[5] Rani S, *et al.*, Security and Privacy Challenges in the Deployment of Cyber-Physical Systems in Smart City Applications: State-of-Art Work, *Materials Today: Proceedings*, str. 4671–4676, 2022.

[6] Allahar, H. What are the Challenges of Building a Smart City?, Vol. 10, str. 38–48, 2020.

[7] Ahmad K, *et al.*, Developing future human-centered smart cities: Critical analysis of smart city security, *Data management, and Ethical challenges*, 2022.

[8] Wylde V, Rawindaran, N, *et al.*, Cybersecurity, Data Privacy and Blockchain: A Review, *SN Comput Sci*, Vol. 3, No. 2, 2022.

[9] Guo H, Yu X. A survey on blockchain technology and its security, *Blockchain: Research and Applications*, Vol. 3, No. 2, 2022.

[10] Peng L, *et al.*, Privacy preservation in permissionless blockchain: A survey, *Chongqing University of Posts and Telecommunications*, Vol. 7, 2021.

[11] Belotti M, Božić N, Pujolle G, Secci S. A Vademecum on Blockchain Technologies: When, Which, and How, *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 4, str. 3796–3838, 2019.

[12] Aithal P. K, Saavedra P. S, Ghosh R. Blockchain Technology and its Types-A Short Review, *International Journal of Applied Science and engineering*, Vol. 9, No. 2, 2021.

[13] Khan S. N, *et al.*, Blockchain smart contracts: Applications, challenges, and future trends, *Peer Peer Netw. Appl.*, Vol. 14, str. 2901–2925, 2021.

[14] Singh S, *et al.*, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, *Sustainable Cities and Society*, Vol. 63, 2020.

[15] Majdoubi D. E. L, El Bakkali H, Sadki S. Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment, *Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020*, str. 1–7, 2020.

[16] Islam M. R, *et al.*, A Review on Blockchain Security Issues and Challenges, *2021 IEEE 12th Control and System Graduate Research Colloquium, ICSGRC 2021–Proceedings*, str. 227–232, 2021.

[17] Padma A, Ramaiah M. Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities, *IEEE Access*, Vol. 12, str. 21985–22002, 2024.

[18] Rani S, *et al.*, Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain, *IEEE Internet Things Journal*, Vol. 10, No. 7, str. 6074–6081, 2023.

[19] Rathee G, Iqbal R, Waqar O, Bashir A. K. On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities, *IEEE Access*, Vol. 9, str. 34165–34176, 2021.

[20]Rahman A, *et al.*, DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium, *IEEE Access*, Vol. 8, str. 209594–209609, 2020.

[21]Goyat R, *et al*, BENIGREEN: Blockchain-Based Energy-Efficient Privacy-Preserving Scheme for Green IoT, *IEEE Internet Things Journal*, Vol. 10, str. 16480–16493, 2023.

[22]Yazdinejad A, *et al.*, Enabling Drones in the Internet of Things with Decentralized Blockchain-Based Security, *IEEE Internet Things Journal*, Vol. 8, str. 6406–6415, 2021.

[23]Alharthi A, Ni Q, Jiang R. A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET, *IEEE Access*, Vol. 9, str. 87299–87309, 2021.

[24]Yang C, Li X, Yu Y, Wang Z. Basing Diversified Services of Complex IIoT Applications on Scalable Block Graph Platform, *IEEE Access*, Vol. 7, 2019.

[25]Wang W, *et al*, Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices, *IEEE Transactions on Industrial Informatics*, Vol. 18, str. 7059–7067, 2022.

## SUMMARY

STRENGTHENING SMART CITY SECURITY: AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY-BASED SOLUTIONS

*The paper addresses the application of blockchain technology to enhance security and privacy in smart cities, with a particular focus on IoT systems. Smart cities rely on a large number of devices and sensors that collect and exchange data in real-time, which creates significant challenges regarding data security and protection. Centralized data storage systems and numerous IoT devices are vulnerable to cyberattacks, which is why blockchain technology is presented as a potential solution. Through decentralized architecture and smart contracts, blockchain enables secure data storage and exchange, reducing the risk of single points of failure and unauthorized access. The paper analyzes the use of private and public blockchain platforms, highlighting the advantages and disadvantages of each. It also discusses challenges such as scalability and energy consumption, as well as opportunities for further development of this technology to improve security in smart cities. The conclusion is that blockchain offers significant potential, but further research is necessary to overcome technical challenges.*

**Key Words**: *blockchain, smart cities, IoT, data security, privacy*