https://doi.org/10.37528/FTTE/9788673954318/POSTEL.2020.019

MOGUĆNOSTI PRIMENE BLOCKCHAIN TEHNOLOGIJE ZA UNAPREĐENJE POUZDANOSTI U VANET-u

Branka Mikavica, Aleksandra Kostić-Ljubisavljević
Univerzitet u Beogradu - Saobraćajni fakultet,
b.mikavica@sf.bg.ac.rs, a.kostic@sf.bg.ac.rs

Rezime: *Vehicular Ad-Hoc Networks (VANET) omogućavaju deljenje poverljivih podataka u realnom vremenu između susednih vozila, kao i između vozila i infrastrukture, a sve u cilju prevencije saobraćajnih nezgoda i unapređenja komfora učesnika u saobraćaju. Međutim, čvorovi u VANET-u u nekim situacijama nisu kooperativni i ne poštuju pravila deljenja poverljivih podataka, čime narušavaju performanse saobraćajnih sistema i ugrožavaju bezbednost. Kako bi se sprečilo maliciozno delovanje čvorova u mreži, neophodno je stvoriti bezbedno okruženje za pouzdano deljenje poverljivih podataka. Imajući u vidu karakteristike VANET-a, obezbeđivanje pouzdanosti između učesnika predstavlja veliki izazov. Različiti mehanizmi za upravljanje pouzdanošću mogu se primeniti u cilju unapređenja bezbednosti bez uticaja na performanse mreže. Nedavno, blockchain tehnologija je prepoznata kao vitalni segment za obezbeđivanje pouzdanosti u saobraćajnom okruženju. U ovom radu su prikazane mogućnosti primene blockchain tehnologije u mehanizmima za upravljanje pouzdanošću u VANET okruženju. Osnovne karakteristike ovih mehanizama, kao i izazovi u njihovoj implementaciji takođe su analizirani.*

Ključne reči: *VANET, pouzdanost, blockchain*

1. Uvod

Unapređenje bezbednosti u saobraćaju je jedan od primarnih ciljeva VANET-a. U današnje vreme, vozila su opremljena brojnim senzorima, kao i računarskim i skladišnim kapacitetima koja omogućavaju prenos poverljivih informacija. Informacije za prevenciju nezgoda, nailazak na oštre krivine ili klizav kolovoz, mogu se deliti između vozila ili između vozila i infrastrukture. Prenos informacija mora biti takav da ne sme doći do bilo kakvih izmena u sadržaju. Zbog karakteristika komunikacije između čvorova u VANET-u, moguće je prenositi i saobraćaj od malicioznih čvorova. Uzimajući u obzir osetljivost informacija, kreiranje bezbednog i pouzdanog okruženja je od krucijalnog značaja. Istovremeno, ovo pitanje predstavlja veliki izazov. Nedavno je uvedeno upravljanje pouzdanošću kako bi se unapredila bezbednost bez uticaja na performanse mreže. Pouzdanost, u ovom kontekstu, predstavlja neophdno poverenje između vozila

kako bi se omogućio prenos informacija. Pouzdanost se može meriti na osnovu mišljenja susednih vozila, odnosno reputacije vozila u prethodnim interakcijama tokom komunikacije sa vozilima [1]. Usled velike mobilnosti vozila i ograničenog trajanja interakcija, evaluacija pouzdanosti je vrlo složena. Postoje različiti modeli za procenu pouzdanosti i autentičnosti prenetih poruka u VANET okruženju [2-5].

Blockchain tehnologija se sve više smatra obećavajućim rešenjem za brojne izazove koji se javljaju u VANET-u, a posebno za ona pitanja koja se tiču pouzdanosti. U osnovi, *blockchain* predstavlja distribuirani sistem koji obezbeđuje bezbednost, privatnost i pouzdanost u saobraćajnom okruženju. Najznačajnije prednosti *blockchain*-a su decentralizacija, pouzdanost, anonimnost, transparentnost i nepromenljivost [6]. Izgradnja pouzdanosti između čvorova u mreži ostvaruje se kroz mehanizam konsenzusa, bez potrebe za angažovanjem treće strane. Sve interakcije između učesnika u VANET-u zasnovanom na *blockchain*-u su javne, čime se obezbeđuje transparentnost. Za obezbeđivanje anonimnosti, koriste se pseudonimi. Jednom dodati segmenti *blockchain*-a, tzv. blokovi, vrlo teško se mogu naknadno menjati, čime se obezbeđuje nepromenljivost. Novi blokovi se dodaju u lanac u procesu rudarenja. Čvorovi koji imaju ulogu minera agregiraju validne transakcije u blokove. Nakon ostvarivanja konsenzusa, ti blokovi postaju sastavni deo *blockchain*-a. *Blockchain* se smatra tehnologijom sa mogućnošću široke primene. Do sada, *blockchain* je našao primenu u zdravstvenim sistemima, poslovanju, *Internet of Things* (IoT), a postoji i veliki potencijal za primenu u saobraćajnim i transportnim sistemima.

Ovaj rad je koncipiran na sledeći način. Nakon uvoda, u drugom delu rada opisana je osnovna klasifikacija mehanizama za upravljanje pouzdanošću u VANET-u. Osnovne karakteristike *blockchain* tehnologije predstavljene su u trećem delu rada. Nekoliko primera primene ove tehnologije za unapređenje pouzdanosti u saobraćajnom okruženju prikazane su u četvrtom delu rada. U petom delu rada analizirani su izazovi u pogledu primene *blockchain*-a. Zaključna razmatranja data su na kraju rada.

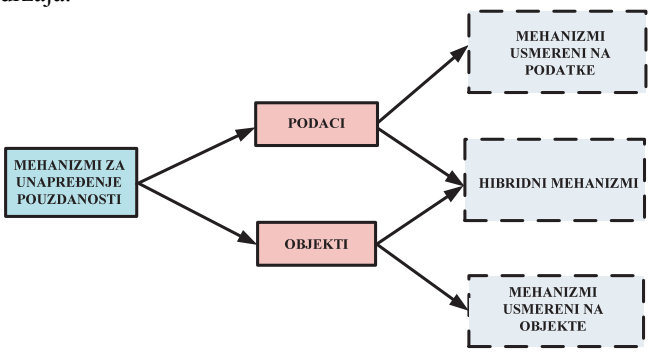
2. Mehanizmi za upravljanje pouzdanošću u VANET-u

Detekcija malicioznog delovanja čvorova i upravljanje poverenjem privlače sve veću pažnju istraživača. Termin maliciozno delovanje odnosi se na odstupanje od skupa dozvoljenih aktivnosti koje su predviđene za čvorove mreže. U literaturi se može pronaći nekoliko tipova nedozvoljenog delovanja čvorova: delovanje čvora sa delimičnim otkazom, delovanje čvora sa potpunim otkazom, sebični napad i maliciozni napad [7]. Sebični napad predstavlja tendenciozno pasivno delovanje. U tom slučaju, čvorovi selektivno učestvuju u prenosu podataka kako bi smanjili iskorišćenost sopstvenih resursa, kao što su računarski resursi, trajanje baterije itd. Maliciozni napadi se odnose na aktivna nedozvoljena delovanja, kada čvorovi namerno narušavaju operacije u mreži. Neki napadi su usmereni na podatke koji se dele između čvorova mreže. Stoga, važan zadatak svih pristupa za detekciju malicioznih delovanja jeste prevencija bilo kakvih modifikacija pri deljenju podataka.

Osnovna svrha upravljanja pouzdanošću je evaluacija različitih delovanja čvorova u VANET-u i određivanje reputacije svakog čvora u zavisnosti od procene delovanja. Reputacija se može koristiti za ocenu pouzadnosti čvorova, može pomoći u odlučivanju o uspostavljanju kooperacije sa pojedinim čvorovima i potencijalno, može

poslužiti za uspostavljanje sistema penala nepouzdanim čvorovima [7]. Mehanizmi za upravljanje pouzdanošću često primenjuju dve faze za evaluaciju delovanja čvorova. Prva faza se sprovodi od strane samih vozila u mreži. Rezultati istraživanja se mogu prikupljati pasivno ili aktivno. Pasivno prikupljanje informacija se vrši u slučaju kada čvor u mreži analizira akcije susednih vozila neselektivno. Definisanje reputacije čvorova može se zasnivati i na direktnim potvrdama o delovanju čvorova, kada se informacije prikupljaju aktivno. Druga faza se izvršava indirektno i to uglavnom nakon razmenjenih informacija iz prve faze. Osnovni nedostaci druge faze su povećani troškovi, netačno izveštavanje i kolizija podataka [7].

U zavisnosti od mete napada, mehanizmi za upravljanje pouzdanošću mogu se, u najširem smislu, klasifikovati u mehanizme usmerene na podatke, mehanizme usmerene na objekte i hibridne mehanizme, kao što je to prikazano na Slici 1. Ovi mehanizmi se najčešće integrišu u vozilima kako bi se ocenila pouzdanost podataka ili vozila primenom različitih tehnika. Primarni cilj je identifikacija malicioznih vozila i malicioznih sadržaja.



Slika 1. Mehanizmi za unapređenje pouzdanosti u saobraćajnom okruženju

Mehanizmi usmereni na podatke ocenjuju pouzdanost primljenih podataka. U te svrhe, neophodno je prikupiti informacije iz različitih izvora, kao što su susedna vozila ili infrastruktura kraj puta. Pouzdanost poruka može se ocenjivati na osnovu različitih faktora kao što su sličnost sadržaja, konflikti u sadržaju i sličnost putanja. Takođe, može se korisiti i sistem glasanja sa težinskim faktorima zasnovan na rastojanju od nekog događaja. U tom slučaju, veći težinski faktor biće dodeljen podacima koji potiču od vozila koje je na kraćem rastojanju od datog događaja. Nivo signala na prijemu može biti još jedan način merenja pouzdanosti, na osnovu određivanja rastojanja i pozicije vozila [8]. Evaluacija podataka može se izvršavati od strane centralizovanog sistema u infrastrukturi kraj puta. Pouzdanost podataka se tada određuje na osnovu povratnih informacija od infrastrukture. Vozila detektuju neki događaj i pokreću analizu zajedno sa procenom pouzdanosti na osnovu udaljenosti od događaja i broja ugrađenih senzora koji su detektovali događaj. Nakon toga, rezultati analize se dele sa infrastrukturom koja zatim ažurira listu događaja. Primenom različitih tehnika, jedinice infrastrukture evaluiraju pouzdanost i dele rezultate susednim vozilima. Ovaj pristup je adekvatniji za urbane zone, s obzirom na to da se u najvećoj meri oslanja na susednu infrastrukturu [1]. Mehanizam usmeren na podatke može se bazirati i na evaluaciju pouzdanosti svakog vozila. Na taj način, formira se skup vrlo pouzdanih vozila. Tabela pouzdanosti se

održava od strane svakog vozila. Kada se primi poruka od pouzdanog izvora, poverenje se uveća. Ovakav mehanizam podrazumeva samo direktna iskustva od vozila koja učestvuju u razmeni poruka, ali ne uključuje bilo kakve informacije koje se tiču pouzdanosti događaja [9].

Mehanizmi usmereni na objekte procenjuju pouzdanost vozila. Ovi mehanizmi primenjuju različite tehnike za uspostavljanje sistema reputacija ili pružaju podršku odlučivanju u skladu sa procenama susednih vozila. Višenivovski pristup može se primeniti u cilju detekcije izvora malicioznih podataka, kada se pouzdanost zasniva na ulozi, iskustvu, prioritetima i većini [8]. Infrastruktura kraj puta se takođe može koristiti za razlikovanje malicioznih ili sebičnih vozila u VANET-u. Reputacija svakog vozila može se definisati u skladu sa prethodnim iskustvima pri komunikaciji sa određenim vozilom, na osnovu preporuka od susednih vozila i na osnovu preporuka od centra za upravljanje. Usled velike mobilnosti vozila, teško je prikupiti dovoljno informacija i izračunati nivo reputacije. Takođe, neophodno je adekvatno analizirati i bezbednost sistema za određivanje reputacije vozila.

Hibridni mehanizmi su usmereni i na objekte i na podatke. Ovi mehenizmi analiziraju pouzdanost vozila i istovremeno procenjuju pouzdanost podataka. Time se obuhvataju prednosti, ali i nedostaci mehanizama usmerenih na podatke i mehnizama usmerenih na objekte. Pouzdanost vozila može se proceniti na osnovu funkcionalne pouzdanosti i pouzdanosti proistekle iz preporuka od ostalih učesnika. Pouzdanost vozila ukazuje na to da li posmatrano vozilo može ispuniti funkcionalna očekivanja i predstavlja nivo poverenja u informacije koje potiču od datog vozila. Pouzdanost podataka određuje se na osnovu podataka prikupljenih od više vozila. S obzirom na to da mnoge kontrolne poruke moraju biti obrađene u ograničenom vremenskom intervalu, hibridni mehanizmi zahtevaju i značajan dodatni *overhead*, što je najveći nedostatak ovih mehanizama.

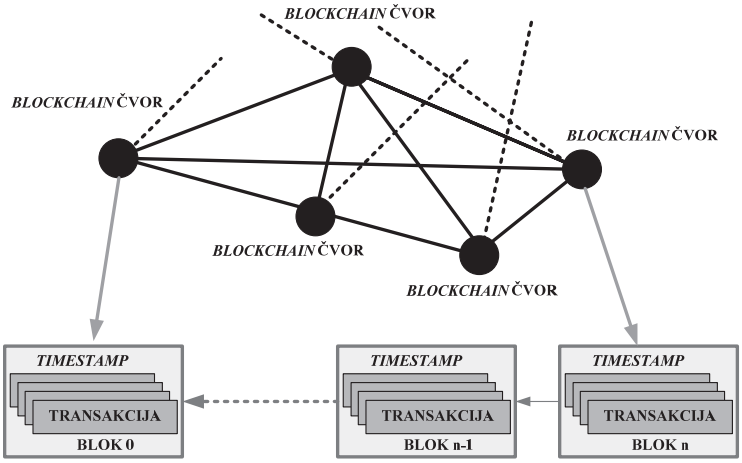
Vozila u telekomunikacionim mrežama prenose informacije od izuzetnog značaja za bezbednost u saobraćaju, kao što su upozorenja u raskrsnicama, upozorenja o vozilima hitnih službi u blizini, upozorenja o opasnostima na putu, nedozvoljenom smeru kretanja, ili upozorenja o mogućnosti nezgode [10]. Od krucijalnog značaja je kreirati bezbedno i pouzdano okruženje kako bi se omogućio prenos pouzdanih, autentičnih informacija. Obećavajuće rešenje za ove izazove jeste *blockchain*, tehnologija koja nudi brojne prednosti u poređenju sa ostalim konvencionalnim tehnologijama.

3. Osnovne karakteristike *blockchain*-a

Blockchain je bezbedna, distribuirana baza koja obezbeđuje skladištenje i praćenje resursa u *peer-to-peer* mreži. Sastoji se iz baze podataka i mreže čvorova, kao što je to prikazano na Slici 2.

Baza podataka u *blockchain*-u je deljena, bez grešaka, sa mogućnošću dodavanja bez izmena. Blokovi koji čine *blockchain* su povezani tako što svaki blok čuva *hash* vrednost svog prethodnika. *Hash* funkcija uzima ulaz proizvoljne dužine i generiše izlaz jedinstvene fiksne dužine. Ukoliko je jedna vrednost u ulazu modifikovana, izlaz se značajno menja. Svaki blok koji sadrži podatke ima svoju *hash* funkciju. Ukoliko dođe do nekih izmena, modifikovani blok ima potpuno drugačiju *hash* vrednost, kako bi svaki čvor u mreži imao uvid u izmene. Na taj način se postiže pouzdanost u podatke sačuvane u blokovima. Takođe, svaki blok sadrži *timestamp*, odnosno vremensku odrednicu

kreiranja bloka, kao i *nonce* vrednost za kriptografske operacije. *Nonce* vrednost ima 4 bajta koji počinju sa 0 i uvećavaju se svaki put kada se izvršava izračunavanje *hash* funkcije. Blokovi se ne mogu brisati ili modifikovati, što je najveća prednost *blockchain*-a. Komunikacija između čvorova u mreži odvija se bez učešća treće strane. Sve interakcije se čuvaju u bazi podataka, čime se zadovoljavaju zahtevi u pogledu bezbednosti. Korisnici šalju transakcije kroz *blockchain* mrežu u cilju interakcije sa ostalim korisnicima.



Slika 2. Blockchain mreža

Predefinisani čvorovi u mreži vrše proveru validnosti transakcija i kreiraju novi blok validnih transakcija. Ovaj proces se naziva rudarenje. Ukoliko je blok validan, dodaje se u bazu podataka. U suprotnom, blok se odbacuje. Nakon dodavanja bloka, naknadne izmene nisu moguće. U nekim aplikacijama zasnovanim na *blockchain*-u, čvorovi sa dozvolom rudarenja - mineri, koji prvi kreiraju blok bivaju nagrađeni. Pobednik u procesu rudarenja se određuje kroz mehanizam konsenzusa. Najčešće korišćeni mehanizmi konsensuza su *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS) i *Practical Byzantine Fault Tolerance* (PBFT) [11]. PoW postavlja složene matematičke probleme koji se često menjaju. Nakon što prvi čvor validira transakciju i reši matematički problem, blok biva kreiran. Kada drugi čvorovi sa ulogom minera validiraju blok, isti se dodaje u bazu *blockchain*-a. Pobednički miner biva nagrađen. Stoga, vrlo teško može doći do grešaka, imajući u vidu da je za to potrebno najmanje 50% kompromitovanih minera. U slučaju PoS, izbor minera se vrši na pseudo-slučajan način a u zavisnosti od uloga datog čvora. U osnovnoj verziji, pobednički miner se ne nagrađuje, međutim, novije verzije uključuju nagrade i penale u zavisnoti od performansi čvorova. U slučaju primene PBFT konsenzus mehanizma, čvorovi u mreži biraju lidera iz skupa čvorova. Čvor lider je zadužen za validaciju transakcija i kreiranje blokova. Blok se dodaje u bazu samo ako je dve trećine minera verifikovalo tačnost bloka. Čvor lider se periodično menja, čime se obezbeđuje decentralizacija.

Postoje tri generacije *blockchain* tehnologije koje podržavaju transakcije, resurse i pametne ugovore [11]. Prva generacija je ograničena na novčane transakcije i koristi *Bitcoin* kriptovalutu. Za razliku od prve, druga generacija dozvoljava razmenu

resursa. Tako, korisnici mogu razmenjivati bilo koju vrstu resursa, kao što su različita dobra, svojina, glasovi itd. Treća generacija *blockchain* tehnologije uvodi pametne ugovore. Pametni ugovor je programabilni ugovor proveren od strane svih čvorova u mreži koji se izvršava automatski po unapred definisanim pravilima.

Razvoj *blockchain* tehnologije omogućio je unapređenje raznih sistema. Decentralizacija, transparentnost, autonomnost, anonimnost i nepromenljivost su osnovne karakteristike *blockchian*-a. Decentralizacija omogućava izmeštanje funkcija i kontrole iz centralnog upravljačkog dela ka svim čvorovima u mreži. Svaki učesnik čuva kopiju svih transakcija, a blok se dodaje kroz validaciju transakcija. Na taj način ova *peer-to-peer* mreža funkcioniše u dencentralizovanom okruženju. Pored toga, *blockchain* podržava transparentnost i izvršava kontrolu kako bi se suzbile maliciozne radnje. Imajući u vidu to da je centralna kontrola izmeštena, pitanja pouzdanosti su delegirana na celu mrežu. Važno svojstvo *blockchain* tehnologije je anonimnost, koja je garantovana s obzirom na to da je potrebna samo *blockchain* adresa korisnika. Nakon skladištenja podataka u blok, naknadne izmene nisu moguće, čime se obezbeđuje nepromenljivost.

Neke od poznatijih *open-source* implementacija *blockchain*-a su *Bitcoin*, *Ethereum* i *HyperLedger*. *Bitcoin* je rasprostranjena platforma koja primenjuje PoW mehanizam konsenzusa. Osnovna prednost *Bitcoin*-a je skalabilnost, međutim, vrlo je zahtevan u pogledu računarskih resursa, kao i vremena izvršavanja. *Ethereum* je *blockchain* platforma koja primenjuje pametne ugovore i PoW ili PoS mehanizam konsenzusa. *HyperLedger* platforma primenjuje pametne ugovore i PBFT mehanizam konsenzusa. U poređenju sa drugim *blockchain* platformama, pokazuje bolje karakteristike u pogledu skalabilnosti.

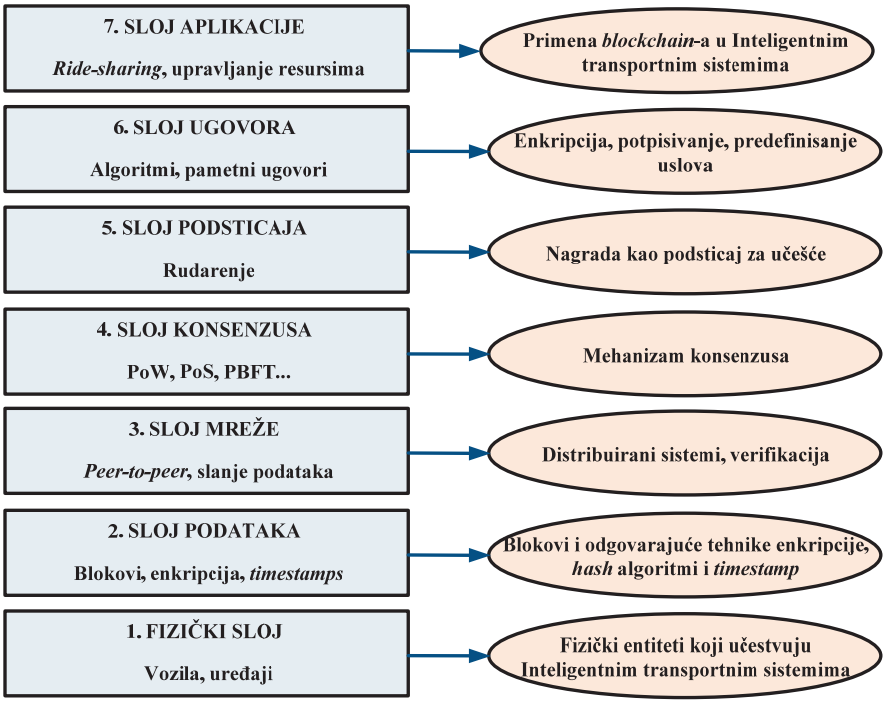
4. Primeri primene *blockchain*-a u pouzdanom saobraćajnom okruženju

Blockchain obezbeđuje prikupljanje podataka od vlasnika vozila, upravnika voznih parkova i proizvođača, kako bi se unapredila bezbednost u saobraćaju, efikasnost i komfor u toku vožnje. Do sada je izvršeno nekoliko implementacija *blockchain*-a u saobraćajnom okruženju. Jedna od implementacija podrazumeva formiranje bezbednog, pouzdanog i decentralizovanog saobraćajnog okruženja zasnovanog na *blockchain*-u kroz konceptualni model od sedam slojeva [12]. Drugi pristup zasnovan na *blockchain*-u kombinuje dve vrste aplikacija u vozilima, odnosno, neophodne aplikacije i opcione aplikacije [13]. Neophodne aplikacije obuhvataju regulisanje saobraćaja, osiguranje vozila, porez itd, dok opcione aplikacije aktiviraju upozorenja na zagušenja u saobraćaju ili vremenske uslove. Pored bezbednosti, neophodno je održati pouzdanost i privatnost. Rešenja zasnovana na *blockchain*-u podržavaju bezbedne, *peer-to-peer* komunikacione linkove između vozila bez otkrivanja privatnih informacija, čime se unapređuje pouzdanost. Zahvaljujući brojnim prednostima, sprega VANET-a i *blockchain*-a sve više privlači pažnju istraživača.

Tojotin istraživački institut, *Toyota Research Institute* (TRI), inicirao je tri *blockchain* projekta, deljenje podataka tokom vožnje, transakcije o deljenju vožnje i osiguranje zasnovano na korišćenju [14]. Vozila u VANET-u prikupljaju važne podatke pomoću senzora ugrađenih u vozilo, a zatim te podatke skladište na *cloud*. *Blockchain* tehnologija obezbeđuje centralizovanu platformu koja omogućava korisnicima deljenje i monetizaciju prikupljenih informacija iz saobraćajnog okruženja u bezbednom okruženju

sa garancijom očuvanja vlasništva nad podacima. Takođe, *blockchain* podstiče vlasnike vozila da monetizuju svoje resurse i dele vozilo, na primer, kroz deljenje vožnje ili deljenje prtljažnog prostora. Primenom *blockchain* pametnih ugovora, finansijske transakcije između korisnika izvršavaju se bez učešća treće strane. Ovaj sistem takođe može obezbediti daljinski pristup vozilu (zaključavanje/otključavanje, paljenje/gašenje motora). Skladištenje podataka u *blockchain*-u obezbeđuje korisnicima niže troškove osiguranja, s obzirom na to da se na osnovu prikupljenih podataka može evaluirati bezbednost i navike vozača.

Model od sedam slojeva u *blockchain*-u, predložen od strane Kineske akademije nauka, kreiran je po ugledu na poznati *Open Systems Interconnection* (OSI) referentni model [12]. Ovaj model predstavlja konceptualni okvir koji obezbeđuje uvid u kompleksne relacije između slojeva. Model obuhvata tipičnu arhitekturu, najveće komponente i pripadajuće tehnike *blockchain* sistema, kao što je to prikazano na Slici 3.



Slika 3. Slojevita struktura VANET mreže zasnovane na blockchain-u

U cilju unapređenja bezbednosti u VANET okruženju, predložena je i platforma ta autonomna vozila koja je zasnovana na *blockchain*-u [15]. S obzirom na to da se autonomna vozila u značajnoj meri oslanjaju na bežične tehnologije, rizik od pojave malicioznih napada je povećan. Osnovni cilj ovog koncepta je obezbediti alate za bezbedno ažuriranje softvera, izmene sadržaja i pružanja udaljene dijagnostike primenom *Ethereum blockchain* platforme. Predloženi sistem bazira se na tokenima i povezuje sve *blockchain* servise, uključujući deljenje podataka prikupljenih tokom vožnje, kao i osiguranja vozila. Na taj način, vlasnik vozila generiše podatke iz saobraćajnog okruženja koji se zatim čuvaju u *blockchain*-u, i za uzvrat dobija tokene. Korisnik koji

zahteva pristup tim podacima ulaže svoje tokene. Osiguravajuća društva i druge organizacije mogu obezbeđivati podatke takođe kroz upotrebu tokena. Na taj način, prodavci vozila, benzinske stanice, ili serviseri mogu ponuditi popuste pri nabavci vozila, održavanje vozila ili pogodnosti pri osiguranju vozila. Važno je naglasiti da ovakva platforma za autonomna vozila zasnovana na *blockchain*-u obezbeđuje pouzdano okruženje i štiti privatnost.

5. Izazovi u primeni *blockchain*-a u pouzdanom saobraćajnom okruženju

Blockchain tehnologija obezbeđuje značajna unapređenja u oblasti bezbednosti, podržavajući najviše nivoe privatnosti i pouzdanosti. Međutim, složenost tehnologije uzrokuje poteškoće u implementaciji u realnim scenarijima primene. Vozila u VANET-u suočavaju se sa raznim ograničenjima, kao što su ograničeni energetski i skladišni kapaciteti. Neophodno je najpre rešiti ove izazove, kako bi se postigla integracija *blockchain*-a i VANET-a.

Skalabilnost predstavlja jedan od najznačajnijih izazova u VANET okruženju. Odnosi se na mogućnost *blockchain*-a da podrži rastući obim distribuiranih baza podataka. U konvencionalnom *blockchain* sistemu, svaki čvor u mreži troši značajnu energiju u procesu rudarenja. Neophodan je server za trajno skladištenje podataka, čime implementacija *blockchain*-a u saobraćajnom okruženju postaje još složeniji izazov. Obećavajuće rešenje može biti periodično čuvanje podataka prikupljenih od strane vozila na eksterno skladište.

Brzina obrade transakcija i računarski kapaciteti su važni ograničavajući faktori u primeni *blockchain*-a. Mehanizmi konsenzusa u *blockchain*-u još uvek ne nude odgovarajuće rešenje za adekvatnu brzinu obrade transakcija. Na primer, vreme potrebno da se postigne konsenzus u kreiranju novog bloka pri primeni PoW iznosi 10 minuta za *Bitcoin*, dok primena PoS u *Ethereum*-u zahteva 17 sekundi. Takođe, prosečno vreme potvrde u *Bitcoin*-u je približno 250 minuta (najduže zabeleženo je 42 sata). Ovi rezultati su suviše spori za aplikacije u realnom vremenu, kakve se koriste u saobraćajnom okruženju. Čvorovi sa ulogom minera zahtevaju značajne energetske resurse. Stoga, potrošnja energije zahteva inovativne pristupe kako bi se prevazišla postojeća ograničenja.

Pouzdanost i transparentnost su često konfliktni ciljevi u VANET-u zasnovanom na *blockchain*-u. Mnoga regulatorna tela imaju različita gledišta po pitanju toga koje podatke treba čuvati u okviru distribuiranih sistema. U decentralizovanom modelu, svi učesnici dele informacije. U skladu s tim, privatni ugovorni podaci ne bi trebalo da se čuvaju u distribuiranoj bazi. Ove baze treba da sadrže minimum informacija, koje treba da budu dostupne samo korisnicima koji imaju mogućnost obaveštavanja, sinhronizacije i potvrde. S druge strane, poverljivi podaci se mogu čuvati u *blockchain*-u, s obzirom na to da *blockchain* garantuje bezbednost i nepromenljivost sačuvanih podataka.

U kontekstu očuvanja privatnosti podataka, razvijene su različite tehnike. Metode za očuvanje anonimnosti imaju za cilj zaštitu ličnih podataka. Međutim, pokazalo se da ove metode nisu efikasne u slučaju velikog obima podataka ili kada su neki delovi podataka otkriveni [16].

Lokalni karakter VANET-a i globalna sinhronizacija zahtevaju kompromisno rešenje. Integracija lokalnih mreža u saobraćajnom okruženju i globalno distribuirane

platforme uzrokuju određene probleme usled heterogenosti blokova u pogledu njihove zavisnosti od infrastrukture i softverskih komponenti. Većina zadataka u VANET-u su od značaja u lokalnom području. Nasuprot tome, *blockchain* predstavlja globalnu platformu. Nema potrebe za deljenjem lokalnih transakcija na globalnoj distribuiranoj platformi. Na taj način se može smanjiti obim podataka. Problem lokalnog značaja u saobraćajnom okruženju i globalnog karaktera *blockchain*-a može se rešiti detaljnijom analizom podataka u VANET-u.

4. Zaključak

VANET omogućava deljenje poruka između vozila u saobraćajnom okruženju, a koje se tiču uslova na putu, zagušenja u saobraćaju i slično. Ove poruke pružaju vozilima uvid u uslove u saobraćaju u realnom vremenu, čime se unapređuje bezbednost i efikasnost saobraćaja. Bezbedno, pouzdano okruženje koje ujedno štiti privatnost korisnika je neophodno za adekvatno deljenje poruka u VANET-u. Od presudnog je značaja izgraditi poverenje između vozila. Usled velike mobilnosti i heterogenosti u VANET okruženju, susedna vozila ne mogu imati potpuno međusobno poverenje. Složenost ovog problema raste u slučaju prisustva malicioznih vozila u mreži. Različiti mehanizmi su predloženi kako bi se unapredila bezbednost u VANET okruženju. U opštem slučaju, ti mehanizmi mogu se podeliti na mehanizme usmerene na podatke, mehanizme usmerene na objekte i hibridne mehanizme, u zavisnosti od mete napada u mreži. *Blockchain* tehnologija je prepoznata kao obećavajuće rešenje u VANET okruženju, obezbeđujući decentralizaciju, transparentnost, autonomnost, anonimnost i nepromenljivost. Moguće primene *blockchain* platformi u pouzdanom saobraćajnom okruženju prikazane su u radu. Uprkos brojnim prednostima, postoje izazovi koje je neophodno prevazići, kao što su skalabilnost, brzina obrade transakcija, potrošnja energije i transparentnost.

Literatura

[1]. F. Ahmad, A. Adnane, F. Kurugollu, R. Hussain, „A Comparative Analysis of Trust Models for Traffic Safety Applications in IoT-enabled Vehicular Networks“, *in Proceedings of the 2019 Wireless Days (WD),* Manchester, United Kingdom, 2019, pp. 1-8.

[2]. Z. Lu, G. Qu, Z. Liu, „A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy“, *IEEE Transactions on Intelligent Transportation Systems*, 20(2), pp. 760-776, 2019.

[3]. M. S. Sheikh, J. Liang, „A Comprehensive Survey on VANET Security Services in Traffic Management System“, *Wireless Communications and Mobile Computing*, 19, 2423915, 2019.

[4]. M. S. Sheikh, J. Liang, W. Wang, „A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)“, *Sensors*, 19(16), 3589, 2019.

[5]. M. Azees, P. Vijayakumar, L. J. Deborah, „Comprehensive Survey on Security Services in Vehicular Ad Hoc Networks“, *IET Intelligent Transport Systems*, 10(6), pp. 379-388, 2016.

[6]. M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, „A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond*“, IEEE Internet of Things Journa*l, 6(5), pp. 8114-8154, 2019.

[7]. W. Li, H. Song, „An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks*", IEEE Transactions on Intelligent Transportation Systems*, 17(4), pp. 960-969, 2016.
[8]. Z. Lu, G. Qu, Z. Liu, Z. „A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy*", IEEE Transactions on Intelligent Transportation Systems*, 20(2), pp. 760-776, 2019.
[9]. T. Gazdar, A. Belghith, H. Abutair, „An Enhanced Distributed Trust Computing Protocol for VANETs", *IEEE Access*, 6, pp. 380-392, 2017.
[10]. A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, S. A. Siddiqui, „A Hybrid Trust Management Heuristic for VANETs", *in Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* Kyoto, Japan, 2019, pp. 748-752.
[11]. T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, „Security Services Using Blockchains: A State-of-the-Art Survey*", IEEE Communications Surveys & Tutorials*, 21(1), pp. 858-880, 2019.
[12]. Y. Yuan, F. Wang, „Towards Blockchain-Based Intelligent Transportation Systems*", In Proceedings of the 2016 IEEE International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janerio, Brazil, 2016, pp. 2663–2668.
[13]. B. Leiding, P. Memarmoshrefi, D. Hogrefe, „Self-Managed and Blockchain-Based Vehicular Ad-Hoc Networks", *in Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing,* Heidelberg, Germany, 2016, pp. 137-140.
[14]. Toyota's Vision of How Blockchain Will Change the Auto Industry. (2017). Available at: http://www.thebanksreport.com/home-page/toyotas-vision-blockchain-will-change-auto-industry/
[15]. *Autonomous Car Network Security Platform Based on Blockchain*. CUBE White Paper, 2017.
[16]. G. Zyskind, O. Nathan, „Decentralizing Privacy: Using Blockchain to Protect Personal Data", *In Proceedings of the IEEE Security and Privacy Workshops*, San Jose, United States of America, 2015, pp. 180–184.

Abstract: *Vehicular Ad-Hoc Networks (VANET) enable vehicles to share sensistive information with neighbouring vehicles and with the infrastructure, with the aim to prevent traffic accidents and improve driving experience. However, network nodes in VANET may not be honest and cooperative, thus deteriorating traffic performances and safety. To mitigate misbehaving network nodes, a secure environment for reliable and trusted information dissemination among the network nodes is needed. Due to the characteristics of VANET, trust issues are highly challenging. Various trust management schemes can be used to enhance security without affecting network performance. Recently, blockchain technology appears as a vital segment in different approaches enabling trustworthy VANET environment. In this paper, the possibilities of blockchain implementation in trust management schemes in vehicular networks are addressed. Key characteristics of blockchain-based trust management approaches and challenges relevant to traffic safety improvement are also analysed.*

Keywords: *VANET, trust, blockchain*

POSSIBILITIES OF BLOCKCHAIN APPLICATION FOR IMPROVEMENT OF TRUST IN VANET

Branka Mikavica, Aleksandra Kostić-Ljubisavljević