

ВЕЋУ ДЕПАРТМАНА ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ

Одлуком Већа Департмана за последипломске студије број 4 – 134/2024. од 31.10.2024. године као и на основу измене број. 4-188/2026 од 02.07.2026. године одређени смо за чланове Комисије за оцену и одбрану докторске дисертације кандидата Тасић Вукашина, под називом „*Унапређење дистрибуиране платформе за е-трговину на јавној blockchain мрежи у циљу минимизације рачунарског напора приликом извршавања трансакција*“ и на основу тога подносимо следећи о чему подносимо следећи

ИЗВЕШТАЈ

1. Основни подаци о кандидату и докторској дисертацији

Вукашин С. Тасић рођен је 16. августа 1996. године у Врању. Основне академске студије завршио је 2019. године на Високој школи академских студија „Доситеј“ у Београду, где је стекао звање дипломирани информатичар одбраном дипломског рада под називом „*Примена транспортног модела операционих истраживања у услужном сектору*“. На истој високошколској установи 2020. године завршио је мастер академске студије и стекао звање мастер информатичар, одбраном мастер рада „*Елементи заштите рачунарског система и рачунарске мреже у електронском пословању*“. Године 2025. дипломирао је на Математичком факултету Универзитета у Београду, стекавши додатно звање дипломирани математичар. Докторске академске студије уписао је 2021. године на Универзитету Сингидунум, на студијском програму **Напредни системи заштите**.

Професионалну каријеру започео је 2020. године као наставник математике и информатике у Средњој школи „Доситеј“ у Београду. Од априла 2022. до априла 2023. године био је запослен као програмер паметних уговора у компанији **AIN d.o.o.** у Београду, где је учествовао у развоју глобалне платформе за продају карата засноване на блокчејн технологијама, представљене на музичком фестивалу **EXIT**.

Од септембра 2024. године до априла 2026. године био је запослен као *Web3* програмер у компанији **CML Team** из Кингстона, Велика Британија. Ангажован је на развоју платформе за дигитализацију власништва над некретнинама засноване на приватном EVM блокчејн систему, у оквиру које обавља послове архитекте и програмера паметних уговора, са посебним фокусом на моделовање власничких односа применом фракционисаних незаменљивих токена.

Од марта 2025. године до фебруара 2026. године ангажован је као водећи блокчејн програмер у компанији **Tiksi** на развоју платформе за продају карата засноване на блокчејн инфраструктури *Telegram* екосистема. Пројекат је подржан средствима у износу од 300.000 евра у оквиру **Catapult Accelerator 2025** програма Светске банке.

Паралелно са индустријским ангажманом, од марта 2025. године сарађује и са **Web3 академијом** као предавач. У оквиру овог ангажовања реализује специјализоване обуке из области блокчејн технологија, паметних уговора и развоја децентрализованих апликација за полазнике академије и корпоративне клијенте, комбинујући теоријска знања са практичним примерима из индустрије. У оквиру ових активности одржао је и јавна предавања са радионицом.

Области његовог научноистраживачког рада и стручног интересовања обухватају блокчејн технологије, дистрибуиране информационе системе, паметне уговоре, криптографске протоколе, децентрализоване апликације, механизме консензуса, оптимизацију паметних уговора, незаменљиве токене (NFT), као и примену теорије графова, алгоритама и математичког моделирања у области информационих система.

Кандидат има следеће објављене радове:

Kategorija M2x:

1. **(M21) Tasic V. S.,** Veinovic M., Tasic I. (2024): "The Cost-Effective Management of Multiple E-Coupons on Public Ethereum-Based Chains Using NFT Standard With Implicit Ownership", IEEE Access, 12, 149889-149902, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2024.3476678
2. **(M21a) M. Malesevic, N. Stanisavljevic, D. Matijasevic, J. Curcic, V. Tasic, S. Tasic, M. Kojic.** (2023): "Metagenomic analysis of bacterial community and isolation of representative strains from Vranjska Banja hot spring, Serbia", Microbial Ecology, 86(4), 2344-2356, PMID: 37222803, DOI: 10.1007/s00248-023-02242-6

Kategorija M3x:

1. **(M33) Tasić, I., Đorđević, S., Tasić, V.** (2023): "Cad and Blockchain technology integration model for the purpose of data protection", XLII International scientific conference „The power of knowledge“, 60.3, 391-396, Proceedings, October, 05 – 08. 2023, Perea, Greece.
2. **(M33) Tasić, V., Tasić, I., Tasić, S.** (2021): Real-time water quality monitoring in a trout pond, VII International Congress "Engineering, Environment and Materials in Process Industry EEM2021", Electronic Book, Jahorina, March 17-19, 2021, p. 405-410 (ISBN 978- 99955-81-40-4, COBISS.RS-ID 133578241, Professional paper).
3. **(M33) Tasić, V., Tasić, I., Tasić, S.** (2021): Real-time water quality monitoring in a trout pond, Tasić, V., Veinović, M., Tasić, I. (2021): Computational methods application for finding the optimal transportation costs, SINTEZA International scientific conference on information technology and data related research, Belgrade, June 25, 2021, p. 34-38 (ISBN 978-7912-755-6, COBISS.SR-ID 42361609) <https://portal.sinteza.singidunum.ac.rs/Media/files/2021/Sinteza-2021.pdf>- страна 34d, VII International Congress "Engineering, Environment and Materials in Process Industry EEM2021", Electronic Book, Jahorina, March 17-19, 2021, p. 405-410 (ISBN 978- 99955-81-40-4, COBISS.RS-ID 133578241, Professional paper).

4. **(M33) Tasić, V., Tasić, I., Tasić, S. (2021):** Model energetske efikasnosti MHE “Prohor Pčinjski” u elektromreži Srbije, Peti naučno-stručni skup sa međunarodnim učešćem “Zaštita voda u zelenoj industrijskoj revoluciji”, Zbornik radova, 15. oktobar 2021, Beograd, Srbija, p. 401-411 (ISBN 978-86-81400-60-9, COBISS.SR-ID 53796873).
5. **(M33) Tasić, I., Tasić, S., Tasić, V. (2020):** Introduction of automated monitoring of wastewater quality in the plant for their biological treatment, 4th Scientific – Expert Conference with International Participation „Engineering Management in the Protection of Water Resources“, Proceedings, 16th October 2020, Belgrade, Serbia, (ISBN 978-86-81400- 25-8)
6. **(M33) Tasić, I., Tasić, S., Tasić, V. (2020):** Application of information technology in the introduction of automated real-time monitoring of drinking water quality in the Serbian sacred places of Kosovo and Metohija, Zbornik radova 2020, Akademija tehničko- vaspitačkih strukovnih studija Niš, p. 101-104 (ISBN 978-86-81912-00-3, COBISS.SR-ID 29176073) https://akademijanis.edu.rs/wp-content/uploads/2021/01/ZBORNİK-RADOVA-2020-ATVSSNIS-E_IZDANJE.pdf- страна 108
7. **(M31) Tasić, I., Kokanović, M., Tasić, S., Tasić, V. (2018):** Information Technologies in a Automated Monitoring of the Quality of Water Intended for Human Consumption in Real Time, 2th Scientific–Expert Conference with International Participation „Engineering Management in the Protection of Water Resources“, Proceedings, 16th October 2018, Belgrade, Serbia, p. 65 – 75 (ISBN 978-86-81088-17-3, COBISS.RS-ID 268727308) –Позивно писмо, број 317-3/18, од 02.10.2018. године.

Kategorija M5x:

1. **(M51) Tasić, V., Tasić, I., Tasić, S., Nikšić, M. (2021):** Real-time IT-monitoring of wastewater quality in the prevention of the Covid-19 pandemic, Scientific Journal Agricultural Engineering, No.2., 2021, p. 19-27 (ISSN 0554-5587, COBISS.SR-ID 16398594, Original Scientific paper) <https://scindeks-clanci.ceon.rs/data/pdf/0554-5587/2021/0554-55872102019T.pdf>

чиме је испуњен предуслов за одбрану докторске дисертације.

Докторска дисертација кандидата је урађена на укупно 157 страна, од чега 25 страна чине прилози и списак литературе. Списак литературе обухвата 269 референци које чине научни радови, књиге, зборници радова, законски прописи, корпоративна истраживања, као и електронски извори.

Докторска дисертација кандидата Вукашина Тасића је била подвргнута провери софтвером за установљавање преклапања/плагијаризма (iThenticate Plagiarism Detection Software). Укупан процентуални износ запажених преклапања износи 1% дисертације.

2. Образложење предложене тезе

Електронска трговина дефинише се као процес продаје или куповине робе и услуга реализован путем рачунарских мрежа коришћењем метода посебно пројектованих за пријем или издавање поруџбина. У основи сваког система електронске трговине налази се пословни модел који дефинише производе и услуге представљене јединственим идентификаторима, модел понашања купца који се бави комуникацијом између корисника и платформе, и инфраструктура неопходна за реализацију и подршку систему електронске трговине. Корисници представљају основни извор прихода система

електронске трговине и корисничко искуство директно зависи од перформанси информационе инфраструктуре на којој се систем заснива.

Савремени информациони системи, укључујући системе електронске трговине, доминантно су засновани на централизованом моделу у којем се поверење делегира трећој страни. Овакав приступ, иако функционалан, уводи одређена ограничења у облику асиметрије моћи између платформи и њихових корисника. Централизација подразумева да трећа страна управља подацима корисника и посредује у обради плаћања, чиме преузима кључну улогу у систему и одржава приватну књигу евиденције. Иако овакав приступ обезбеђује позитивно корисничко искуство, нарочито у домену плаћања, трошкови посредовања нису увек транспарентни крајњим корисницима. Поред тога, ослањање на централизоване ентитете може довести до проблема као што су злоупотреба података, нетранспарентност и системски ризици.

Појава *Bitcoin* (Биткоин) технологије представља значајан искорак у овом домену, јер уводи модел електронског плаћања заснован на криптографском доказу уместо поверења. На тај начин омогућава се директно извршавање трансакција између учесника, без потребе за централним посредницима. Систем се заснива на јавној доступности записа о свим трансакцијама извршеним на мрежи и њиховом редоследу кроз јавну дистрибуирану књигу евиденције коју одржава децентрализована мрежа чворова, чиме се обезбеђују транспарентност и верификабилност.

Елиминацијом централног посредника јавља се проблем координације и постизања консензуса о будућем стању система у отвореном окружењу јер може укључивати злонамерне актере. Овај проблем решава се Накамото консензусним механизмом, који уводи оскудан ресурс потребан за предлагање новог стања мреже. Тиме се успоставља асиметрија рачунарске сложености, јер проналажење решења једино је могуће значајним напором заснованим на методама грубе силе, док је верификација пронађеног решења брза и детерминистичка, чиме се обезбеђује сигурност система.

Приликом креирања трансакције корисник доказује право располагања средствима у складу са условима дефинисаним у самој трансакцији, при чему се улази трансакције у потпуности троше, чиме се решава проблем двоструке потрошње. Ово се остварује путем уграђеног скриптног језика, који представља саставни део трансакционе структуре и омогућава дефинисање једноставних, детерминистичких услова извршавања без потребе за поузданим посредницима. Овакав приступ концептуално је близак идеји самостално извршавајућих уговорних услова, коју је још 1994. године формално дефинисао *Nick Szabo*.

Даљи развој блокчејн технологија довео је до појаве платформе *Ethereum* (Етеријум), која интегрише концепт дистрибуиране књиге и паметних уговора, уводећи Тјуринг-комплетну глобалну дистрибуирану рачунарску платформу. Паметни уговори представљају програме на блокчејну у облику низа бајтних инструкција распоређених на одређеној адреси, чијим се извршавањем омогућава развој децентрализованих апликација, које омогућавају аутоматизацију пословне логике и директну интеракцију међу корисницима.

Примена децентрализованих апликација на јавним блокчејн мрежама задовољава пословни модел електронске трговине и представља значајан потенцијал у овом домену. Овакви системи обезбеђују висок ниво транспарентности, интегритета, доступности, аутентичности и непорецивости. Додатно, омогућена су директна плаћања између учесника система без потребе за

посредницима, чиме се смањују трошкови посредовања и поједностављује реализација пословних процеса. Паметни уговори представљају аутономне програме који се извршавају у дистрибуираном окружењу и омогућавају формализацију и аутоматизацију правила система.

3. Предмет истраживања

Предмет овог истраживања обухвата анализу блокчејн система као специфичне класе дистрибуираних система, са циљем утврђивања да ли они могу да задовоље оперативна својства савремених информационих система. Посебан фокус ставља се на испитивање утицаја децентрализације, као проширења социотехничке перспективе информационих система, на сложеност система и потребу за новим механизмима координације који омогућавају поуздано управљање заједничким стањем без централног ауторитета.

У раду се разматра генеза блокчејн технологије, као и класификација блокчејн система према различитим критеријумима, укључујући модел репликације, отвореност система, контролу приступа, консензусни механизам, модел управљања стањем, степен синхронизације извршавања и модел управљања системом, што има значајан утицај на дизајн платформе. Посебна пажња посвећена је анализи основних својстава, као што су децентрализација, сигурност и перформансе, која представљају кључне критеријуме и ограничења за евалуацију јавних блокчејн система.

Етеријум блокчејн користи се као репрезентативан случај за анализу и имплементацију предложеног решења пословне логике платформе за е-трговину, будући да представља један од најразвијенијих блокчејн система за развој децентрализованих апликација. С обзиром на то да ова мрежа стандардизује репрезентовање ентитета путем идентификатора и дефинисање основних операција над њима у оквиру јединственог паметног уговора, овакав приступ је посебно релевантан за системе електронске трговине, где сваки производ или услуга мора поседовати јединствену идентификацију.

Један од централних аспеката експерименталног истраживања односи се на трошковни модел јавних блокчејн система, који уводе експлицитне трансакционе накнаде. У том контексту анализирају се предвидиви трошкови повезани са репрезентацијом ентитета и извршавањем основних операција над њима, као и непредвидиви трошкови који произлазе из додатних функционалности и сложености дефинисаних пословним захтевима.

Фокус истраживања усмерен је на ентитете са јединственим идентификаторима, који представљају најопштији модел објеката са идентитетом, власништвом и атрибутима, при чему се истражују могућности оптимизације складиштења мапе власништва у постојећим стандардима за незаменљиве токене, ради ефикасније репрезентације података.

Анализа обухвата евалуацију различитих приступа енкодирању атрибута, где купони представљају репрезентативан студијски случај, као и ограничења у погледу губитка информација код таквих енкодирања. Посебна пажња посвећена је анализи основних операција над ентитетима, као што су креирање, пренос и уништавање, уз поређење трошкова извршавања у различитим сценаријима, са циљем унапређења ефикасности система.

Пословни захтеви система електронске трговине могу се формализовати кроз различите функционалне захтеве, чија се трошкова процена не може унапред у потпуности одредити због њихове сложености и бројности. Имајући у виду да је Етеријум виртуелна машина Тјуринг-комплетна, у раду се анализирају проширења паметних уговора за подршку функционалностима електронске трговине, као и примена модуларног дизајна који омогућава надоградњу постојеће платформе и проширење функционалности.

На крају, разматра се примена *IPFS* мреже као слоја за садржајно адресирано и дугорочно складиштење података, као и децентрализованог презентационог слоја који посредује у комуникацији између корисника и паметних уговора платформе, уз очување суверенитета корисника над криптографским идентитетом, чиме се употпуњује архитектура децентрализоване апликације.

4. Проблем истраживања

Упркос наведеним предностима, примена јавних блокчејн мрежа у електронској трговини суочава се са значајним ограничењима. Кључни проблем огледа се у чињеници да трошкови система, који су у традиционалним моделима имплицитно укључени кроз коришћење посредничких сервиса, у овом случају постају експлицитни кроз трансакционе накнаде које сnose корисници приликом извршавања операција на блокчејну, што уводи додатну сложеност из перспективе корисника и негативно утиче на укупни квалитет корисничког искуства.

Како се блокчејн посматра као систем заснован на односу понуде и потражње, где понуду чини расположива количина рачунарских ресурса мреже, док потражња одговара укупном захтеву за њиховим коришћењем, трошкови извршавања трансакција зависе од нивоа оптерећења мреже. То представља значајно ограничење за примену блокчејн технологија у електронској трговини, будући да корисници нису навикли на експлицитно плаћање накнада за коришћење услуга. Додатно, неоптимизован бајткод паметних уговора доводи до повећане потрошње гаса, услед чега корисници плаћају веће накнаде за извршавање функционално идентичних операција, нарочито у условима високе искоришћености мреже.

Посебно значајан фактор у овом контексту представља трајно складиштење података, будући да сваки податак уписан у складиште мора бити локално сачуван од стране свих чворова мреже, чиме се повећава укупна количина података коју систем мора да одржава. Додатно, операције приступа складишту захтевају улазно-излазне операције, што уводи додатно режијско оптерећење и чини операције читања и писања међу најскупљим операцијама у погледу потрошње гаса.

У контексту репрезентације производа и услуга електронске трговине коришћењем стандарда за незаменљиве токене, могуће је у мапи власништва искористити неискоришћен простор за енкодирање додатних атрибута. Међутим, овај приступ је ограничен карактеристикама виртуелне машине, пре свега величином складишних јединица. Ограничен број расположивих битова намеће потребу за компромисом између количине и прецизности информација које се енкодирају, што може довести до губитка информација или немогућности репрезентације сложенијих структура података.

Додатно, примена стандарда за незаменљиве токене који користе модел имплицитног власништва уводи специфичне трошковне карактеристике. У овим моделима, власништво се не чува

експлицитно за сваки појединачни ентитет, већ се разрешава током операција преноса и уништавања токена, што доводи до динамичке природе трошкова извршавања у зависности од улазних параметара. Додатно, модел заснован на имплицитном власништву намеће ограничење да ентитети креирани у оквиру исте секвенце деле заједничке атрибуте, што смањује флексибилност у моделовању произвољних објеката.

Приликом проширења функционалности паметних уговора за е-трговину кроз модуларни дизајн уводе се нови изазови, при чему свака додатна функционалност повећава сложеност система и трошкове постављања паметних уговора за компаније и предузећа. Такође, увођење нових функционалности често захтева додатне провере и приступ складишту, као и повећање броја извршних инструкција, што директно утиче на повећање трошкова у односу на модел из експерименталног дела и отежава прецизну процену укупних трошкова унапред.

С обзиром на то да блокчејн системи функционишу као затворена и детерминистичка извршна окружења, неопходно је увести додатне механизме за интеграцију са спољашњим изворима података. Ове информације могу бити јавне или приватне и често су неопходне за извршавање сложенијих пословних процеса, укључујући валидацију екстерних догађаја или генерисање насумичних вредности. Међутим, ослањање на спољашње изворе уводи додатне безбедносне ризике, јер компромитован или непоуздан извор може негативно утицати на извршавање паметних уговора.

Један од фундаменталних изазова блокчејн система представља компромис између децентрализације, сигурности и скалабилности, познат као блокчејн трилема, који неминовно утиче на платформу за е-трговину чија се пословна логика налази на блокчејну. Јавне блокчејн мреже дају приоритет децентрализацији и сигурности, што доводи до ограничења у погледу скалабилности. Овај проблем постаје посебно изражен у сценаријима масовне примене, због чега је неопходно анализирати постојеће приступе његовом решавању и правце даљег развоја.

На крају, додатни изазов представља динамичан развој блокчејн технологија, који отежава дугорочно предвиђање праваца развоја. Ипак, могуће је дефинисати општи оквир за интеграцију блокчејн технологија у системе електронске трговине на основу тренутно доступних технолошких решења и сазнања.

Из наведеног произлази да основни проблем истраживања представља идентификацију модела електронске трговине заснованог на блокчејн технологији који омогућава ефикасно управљање трошковима, уз очување функционалности, сигурности и прихватљивог корисничког искуства.

5. Циљеви истраживања

Општи циљ овог истраживања јесте развој модела и дизајна дистрибуиране платформе за електронску трговину засноване на јавној блокчејн мрежи, која омогућава ефикасно управљање трошковима извршавања уз очување функционалних захтева, сигурности система и прихватљивог корисничког искуства.

Ток и садржај рада непосредно су условљени дефинисаним циљевима истраживања, при чему се општи циљ разлаже на следеће специфичне циљеве:

1. Формализација референтног модела електронске трговине кроз идентификацију кључних елемената система, ради омогућавања анализе дизајна система електронске трговине.
2. Анализа савремених информационих система електронске трговине, са циљем идентификације њихових ограничења и имплицитних претпоставки у погледу поверења и управљања подацима корисника.
3. Увођење и формализација појма децентрализације као проширења класичне социотехничке парадигме информационих система.
4. Дефинисање аналитичког оквира за евалуацију информационих система, који укључује метрике за процену техничких атрибута инфраструктуре, перформанси и оперативних својстава система.
5. Анализа јавних блокчејн система као посебне класе дистрибуираних информационих система, у оквиру претходно дефинисаног аналитичког оквира, са посебним освртом на утицај децентрализације на сложеност система и ограничења која из тога произлазе.
6. Испитивање децентрализације, сигурности и перформанси Етеријум платформе, као и формализација појма гаса као основне јединице трошковног модела за утрошени рачунарски напор кроз анализу консензусног и извршног слоја.
7. Анализа трошковног модела складиштења података на Етеријум блокчејну.
8. Анализа енкодиране репрезентације ентитета максималне величине једне складишне јединице унутар јединственог идентификатора мапе власништва у оквиру стандарда за незаменљиве токене.
9. Компаративна анализа стандарда *ERC-721*, *ERC-721A* и *ERC-721Psi* модификованих за рад са е-купонима као репрезентативним студијским случајем, са фокусом на трошкове складишних операција над ентитетима приликом извршавања основних функција, укључујући креирање, пренос и уништавање.
10. Анализа механизма разрешавања имплицитног власништва у стандардима *ERC-721A* и *ERC-721Psi*, који настаје током операција преноса и уништавања токена, уз извођење формуле за одређивање трошка његовог разрешавања у зависности од првог токена у групи.
11. Експериментална евалуација перформанси овако дефинисаних е-купона, уз мерење трошкова извршавања основних операција у различитим стандардима и сценаријима параметара.
12. Испитивање проширења функционалности стандарда за незаменљиве токене, укључујући модуларни дизајн паметних уговора и интеграцију са спољашњим изворима података, у циљу пројектовања потпуно децентрализоване пословне логике система електронске трговине на јавној блокчејн мрежи.
13. Испитивање *IPFS* мреже као децентрализованог слоја за складиштење података и презентационог слоја ради остваривања потпуне децентрализације апликације.

Овако дефинисани циљеви омогућавају пројектовање архитектонског модела дистрибуиране платформе за електронску трговину засноване на јавној блокчејн мрежи, са посебним фокусом на оптимизацију трансакционих накнада корисника приликом извршавања основних операција над ентитетима са јединственим идентификаторима, укључујући њихово креирање, пренос и уништавање.

Аналитички и експериментални оквир успостављен кроз овако дефинисане циљеве представља основу за систематску евалуацију перформанси и трошкова предложеног решења, као и за његову примену и даља унапређења на другим блокчејн платформама.

6. Хипотезе истраживања

У оквиру овог истраживања постављена је општа хипотеза која гласи:

Могуће је дизајнирати дистрибуирану платформу електронске трговине засновану на јавној блокчејн мрежи, која применом оптимизованих модела складиштења и обраде података у паметним уговорима омогућава значајно смањење трансакционих трошкова корисника, уз очување функционалних и безбедносних својстава система.

Из овако дефинисане опште хипотезе произлазе посебне хипотезе које детаљније разрађују појединачне аспекте посматраног проблема, кроз формализацију кључних својстава блокчејн система, њихових ограничења и могућности примене у електронској трговини:

1. Јавни блокчејн системи са подршком паметних уговора могу формално задовољити референтни модел електронске трговине.
2. Децентрализација информационих система уводи додатну сложеност и захтева специфичне механизме координације.
3. Трошковни модел заснован на гасу омогућава квантификацију рачунарског напора приликом извршавања операција е-трговине.
4. Оптимизација репрезентације ентитета применом стандарда за незаменљиве токене значајно смањује трошкове гаса.
5. Модел имплицитног власништва уводи променљиве трошкове у зависности од начина разрешавања власништва.
6. Проширење функционалности паметних уговора повећава трошкове на нелинеаран и тешко предвидив начин.
7. Применом *IPFS* мреже могуће је реализовати децентрализован слој за складиштење података и презентациони слој платформе за електронску трговину, уз очување функционалности и децентрализованости система.

Појединачне хипотезе које су даље разматране у дисертацији односе се на квантитативну анализу трошкова извршавања основних операција модификованих стандарда за незаменљиве токене за рад са репрезентованим ентитетима у оквиру једне складишне јединице:

1. Трошак операције групног креирања у стандардима са имплицитним власништвом је знатно мањи него у стандарду *ERC-721*.
2. Трошак разрешавања имплицитног власништва зависи од удаљености од првог експлицитно дефинисаног токена у групи.
3. Трошкови операција преноса и уништавања у стандардима са имплицитним власништвом су знатно већи него у стандарду *ERC-721* због експлицитног разрешавања власништва.
4. Трошак операције преноса у стандарду *ERC-721Psi* постаје мањи од трошка исте операције у стандарду *ERC-721A* након одређеног растојања између првог токена у групи и посматраног токена.

5. Трошак операција уништавања само једног токена у трансакцији у стандарду *ERC-721* остаје константан и најмањи је јер једини омогућава експлицитан повраћај гаса услед ослобађања складишне јединице.
6. Трошак уништавања више токена у једној трансакцији у стандарду *ERC-721Psi* почевши од одређеног броја уништених купона постаје трошковно најповољнији од свих стандарда.
7. Трошак разрешавања имплицитног власништва у стандарду *ERC-721A* тежи вредности приближно 256 пута већој од одговарајућег трошка у стандарду *ERC-721Psi* када број купона креираних у једној трансакцији тежи бесконачности.
8. Трошак постављања паметног уговора који имплементира *ERC-721Psi* стандард је највећи у односу на остале посматране стандарде.

7. Методолошки приступ

Методологија истраживања заснива се на комбинацији теоријско-аналитичког, конструктивног и експерименталног приступа, са циљем систематске евалуације могућности примене блокчејн технологија у развоју платформи електронске трговине.

Валидација постављених хипотеза спроводи се у складу са њиховом природом. Посебне хипотезе које се односе на формална својства система и концептуалне моделе валидирају се теоријско-аналитичким приступом. Хипотезе које подразумевају дизајн и имплементацију система валидирају се конструктивно, кроз демонстрацију изводљивости предложених решења. Појединачне хипотезе, које се односе на квантитативне аспекте трошкова извршавања, валидирају се експериментално, на основу мерења потрошње гаса и компаративне анализе добијених резултата.

Теоријско-аналитички приступ обухвата формализацију референтног модела електронске трговине, као и аналитички оквир за евалуацију информатичких система.

У том контексту анализирају се основна својства јавних блокчејн система као специфичне класе дистрибуираних система, који омогућавају коришћење већ успостављене мрежне и безбедносне инфраструктуре. Анализа обухвата кључне аспекте као што су децентрализација, сигурност и перформансе, уз посебан осврт на утицај ових својстава на сложеност система и механизме координације.

Фокус истраживања, као основе за примену конструктивног приступа репрезентацији ентитета и операција над њима, усмерен је на анализу кључних аспеката Етеријум мреже кроз њен консензусни и извршни слој.

Додатно, анализирају се могућности примене садржајно адресираних мрежа за децентрализовано складиштење података и реализацију презентационог слоја децентрализованих апликација. У том контексту разматра се *IPFS* као репрезентативан пример инфраструктуре која омогућава дугорочну доступност података, очување суверенитета корисника над криптографским идентитетом и верификабилну интеракцију са системом.

Конструктивни приступ користи се за пројектовање архитектонског модела дистрибуиране платформе електронске трговине.

Развија се модел репрезентације ентитета заснован на стандардима за незаменљиве токене у оквиру ограничења Етеријум мреже, при чему електронски купони представљају репрезентативан студијски случај.

Развија се модел репрезентације ентитета заснован на стандардима за незаменљиве токене у оквиру ограничења Етеријум мреже, при чему електронски купони представљају репрезентативан студијски случај.

Експериментални приступ примењује се у циљу квантитативне евалуације трансакционих трошкова корисника приликом извршавања основних операција над ентитетима са јединственим идентификаторима, кроз анализу трошковног модела заснованог на гасу у оквиру Етеријум платформе.

У оквиру експерименталне анализе имплементирана је енкодирана репрезентација ентитета електронске трговине унутар једне складишне јединице у оквиру стандарда за незаменљиве токене, укључујући стандарде *ERC-721*, *ERC-721A* и *ERC-721Psi*, при чему се врши поређење трошкова операција креирања, преноса и уништавања токена у контролисаним условима, са посебним нагласком на број и тип приступа складишту као доминантном фактору трошкова приликом извршавања ових операција, који представља примарни предмет оптимизације.

Преостале инструкције које се извршавају у оквиру ових основних операција имају знатно мањи утицај на укупну потрошњу гаса и у даљој анализи биће апроксимативно моделоване ради поједностављења формалног записа.

Код стандарда који користе имплицитни модел власништва, посебна пажња посвећена је анализи алгоритама за његово разрешавање. Ови алгоритми се формално моделују, а њихова сложеност и трошак изражавају се кроз апроксимативне функције у зависности од растојања између посматраног токена и првог токена у групном креирању.

Експерименти су спроведени у контролисаном окружењу, уз коришћење истих улазних параметара и услова извршавања за све посматране стандарде, како би се обезбедила упоредивост резултата.

На овај начин успоставља се интегрисан методолошки оквир који омогућава свеобухватну евалуацију предложеног модела кроз комбинацију формалне анализе, дизајна система и емпиријских резултата.

Предложени методолошки оквир може се интегрисати у шире студије које се баве осталим доменама примене информационих система. Код њих у случајевима када је потребно користити више складишних јединица за запис сложенијих структура података, представљени шематски модел омогућава релативно једноставно проширење анализе и квантификацију ефикасности таквог приступа.

Додатно, иако је анализа спроведена над јавним блокчејн системима, концепт оптималног паковања података није ограничен искључиво на њих. Приступ је применљив и у дозволама ограниченим блокчејн мрежама, јер се заснива на општем принципу рационалног коришћења складишног простора. Овај приступ доприноси смањењу укупне количине података коју чувају

чворови мреже, смањењу величине блокова и повећању економске одрживости целокупног екосистема.

8. Експериментални метод

Експериментални метод заснива се на квантитативној анализи потрошње гаса током извршавања кључних операција над ентитетима електронске трговине. За мерење потрошње гаса коришћен је развојни оквир *Foundry*, који представља широко прихваћен алат за развој и тестирање паметних уговора, чиме је обезбеђена детерминистичност и поновљивост резултата. Овај развојни оквир обухвата алате:

1. Алат *forge* (v0.2.0), који се користи за изградњу, тестирање и имплементацију паметних уговора, као и за извршавање основних операција и читавање вредности потрошеног гаса по трансакцији.
2. Алат *anvil* (v0.2.0), који обезбеђује локални чвор Етеријум тестне мреже и користи се за спровођење експеримената, чиме је елиминисан утицај спољашњих фактора.

У оквиру овог окружења имплементирани су паметни уговори енкодиране репрезентације електронских купона за све посматране стандарде, при чему је мерена потрошња гаса за извршавање операција над електронским купонима.

У циљу прецизног поређења ефикасности имплементација, анализирана је искључиво потрошња гаса посматраних операција над купонима, без укључивања основног трошка трансакције од 21.000 јединица гаса, који је константан и независан од имплементације стандарда. У свим модификованим стандардима пре спровођења експеримената извршена је иницијализација свих релевантних интерних променљивих стања, укључујући променљиву за идентификацију наредног токена за креирање, променљиву за праћење укупно уништених токена код *ERC-721A* стандарда, као и обе битмапе код *ERC-721Psi* стандарда.

У експерименталном делу анализирана је зависност потрошње гаса од броја купона креираних у једној трансакцији. Тестови су спроведени позивањем функције за креирање са различитим вредностима параметра $n \in \{1, 2, 3, 5, 10, 20\}$, при чему је за сваку вредност измерена укупна потрошња гаса. Важно је напоменути да је број креираних купона једини параметар који утиче на потрошњу гаса ове операције, док остали параметри имају константан утицај.

Аналогно томе, за анализу операција преноса и уништавања коришћен је идентификатор купона облика $n+1$, који представља растојање између првог токена у групи и посматраног токена. На овај начин симулиран је најгори случај одређивања имплицитног власништва у оквиру групе. У случају анализе уништавања више купона у једној трансакцији, функција уништавања позивана је узастопно за различите идентификаторе купона, чиме је обезбеђено да се у сваком позиву обрађује различит купон.

Свако мерење извршено је више пута, а приказане вредности представљају аритметичке средине добијених резултата. Добијени резултати упоређени су између наведених стандарда, при

чему је референтна тачка била имплементација заснована на *ERC-721* моделу. На основу ове компаративне анализе изведени су закључци о ефикасности предложених приступа оптимизацији.

Ради обезбеђивања доследности и упоредивости резултата, сви паметни уговори компајлирани су коришћењем компајлера *solc* v0.8.22, са онемогућеном оптимизацијом. За имплементацију *ERC-721* стандарда коришћена је референтна имплементација библиотеке *OpenZeppelin* v4.9.0, док су за стандарде *ERC-721A* и *ERC-721Psi* коришћене имплементације v4.2.3, односно v0.7.0.

За сваки од посматраних стандарда имплементирани су основне функције за креирање, пренос и уништавање токена, након чега је извршено систематско мерење потрошње гаса при различитим вредностима улазних параметара. Посебно су анализирани:

1. Потрошња гаса наведених *NFT* стандарда приликом вишеструког креирања купона у једној трансакцији.
2. Потрошња гаса наведених *NFT* стандарда приликом преноса купона у зависности од удаљености од почетног елемента групе.
3. Потрошња гаса наведених *NFT* стандарда приликом уништавања купона у зависности од удаљености од почетног елемента групе.
4. Потрошња гаса наведених *NFT* стандарда приликом вишеструког уништавања купона у једној трансакцији.
5. Компаративна анализа потрошње гаса стандарда *ERC-721A* и *ERC-721Psi* приликом великих групних операција.
6. Потрошња гаса приликом постављања паметних уговора за наведене *NFT* стандарде.

9. Ограничења предложене методологије

У оквиру предложене методологије, за репрезентацију производа или услуга са јединственим идентификатором на јавним *EVM*-компатибилним блокчејн мрежама коришћени су постојећи стандарди за незаменљиве токене, модификовани за потребе овог истраживања, док стандарди за заменљиве токене који представљају групне идентификаторе нису разматрани.

Када је реч о методологији репрезентације ентитета у оквиру стандарда за незаменљиве токене, оптимизација је остварена искоришћавањем неискоришћених битова унутар мапирања власништва, чиме је омогућено паковање додатних атрибута производа или услуге у оквиру једне складишне јединице. На тај начин смањен је број операција читања и уписа у складиште, што директно утиче на смањење потрошње гаса. Међутим, ефикасност предложеног приступа директно зависи од тренутног модела обрачуна гаса, посебно односа између *SLOAD*, *SSTORE* и аритметичких операција. Промене у протоколу наплате складишних операција могу смањити релативну предност ове оптимизације.

Приликом паковања више променљивих у једну складишну јединицу полази се од претпоставке да је величина адресе у *EVM* окружењу 160 бита. С обзиром на динамичан развој блокчејн технологије, не постоји гаранција да ће ова величина остати непромењена. Евентуална промена могла би смањити расположиви простор унутар складишног слота, чиме би било неопходно

прилагодити предложени модел оптимизације, при чему би основни концепт методологије остао непромењен.

Употреба имплицитног власништва уводи ограничења у контексту групног креирања *NFT*-ова. Када се више токена креира у оквиру исте трансакције, подаци се експлицитно чувају само за први токен, док остали имплицитно наслеђују исте вредности. Овакав приступ је ефикасан у случају идентичних инстанци, али постаје ограничавајући у сценаријима који захтевају већу разноврсност атрибута унутар једне серије.

Анализа је фокусирана на статичке моделе производа и услуга, код којих се атрибути не мењају често или не захтевају сложене динамичке интеракције. Пословни модели са израженом динамиком података нису обухваћени овом анализом, а њихова подршка би захтевала додатне механизме ажурирања и потенцијално другачију структуру складиштења.

Пре дизајна система за електронску трговину неопходно је пажљиво проценити степен потребне надоградивости и модуларности, као и њихов однос према сложености имплементације и безбедносним ризицима. Свака од наведених архитектонских одлука има директан утицај на потрошњу гаса, величину бајткода и укупне трошкове постављања и одржавања платформе, као и на трошкове извршавања трансакција крајњих корисника, што није експлицитно анализирано у оквиру предложене методологије због сложености система.

Додатно, у оквиру предложене методологије није детаљно анализирана безбедност интеграције блокчејн система са спољашњим изворима података, нити је детаљно анализиран утицај предложених решења на перформансе система. За предложени слој складиштења података и презентациони слој није реализована потпуна имплементација нити експериментална евалуација, будући да је фокус дисертације усмерен на реализацију и извршавање корисничких трансакција платформе за електронску трговину. Такође, нису спроведена експериментална мерења перформанси приступа садржају и времена одзива, иако ови параметри имају значајан утицај на употребљивост платформе из перспективе крајњих корисника.

Представљени концепт може се применити и на друге, не-*EVM* блокчејн системе, уз ограничење да се разматрају блокчејн архитектуре засноване на линеарном низу блокова повезаних у строго хронолошки ланац, док парадигме засноване на усмереним ацикличним графовима нису обухваћене овим истраживањем.

У овом случају додатно ограничење представља претпоставка да изабрани блокчејн систем подржава постојање мале власништва у оквиру једног паметног уговора, као што је случај са Етеријум блокчејном. Овакав модел подразумева могућност складиштења свих токена унутар једног уговора са практично неограниченим складишним капацитетом, чиме се омогућава примена идентичне *NFT* логике.

Супротан пример представља архитектура каква је примењена на асинхроној блокчејн мрежи *Telegram Open Network*, где се сваки *NFT* имплементира као засебан паметни уговор, са ограниченим складишним капацитетом и условљеном асинхроном комуникацијом. У таквом моделу није могуће применити модел имплицитног власништва на начин коришћен у анализираним *NFT* стандардима.

10. Научни допринос

Научни допринос ове дисертације огледа се у систематском повезивању теоријских, конструктивних и експерименталних аспеката примене блокчејн технологија у домену електронске трговине, кроз развој интегрисаног модела који омогућава квантитативно и квалитативно сагледавање ограничења и могућности оваквих система. На основу спроведеног истраживања и добијених резултата, издвајају се следећи научни доприноси:

1. Дефинисање референтног модела електронске трговине у контексту јавних блокчејн система, чиме се успоставља јасан теоријски оквир за анализу и поређење различитих архитектонских приступа.
2. Дефинисање аналитичког оквира за евалуацију блокчејн система као посебне класе дистрибуираних информационих система, којим се омогућава структурисано разматрање односа између децентрализације, сигурности и перформанси, као и њиховог утицаја на сложеност и оперативна својства система.
3. Формализација оптимизованог модела репрезентације ентитета електронске трговине са јединственим идентификаторима унутар једне складишне јединице, заснованог на стандардима за незаменљиве токене, чиме се смањује број приступа складишту као доминантног фактора трошкова.
4. Формална анализа и моделовање механизма имплицитног власништва у стандардима за незаменљиве токене, укључујући извођење апроксимативних функција трошка експлицитног разрешавања власништва у зависности од удаљености од почетног елемента групе.
5. Компаративна анализа трошковне ефикасности основних операција стандарда *ERC-721*, *ERC-721A* и *ERC-721Psi* у различитим оперативним сценаријима, заснована на експерименталним мерењима потрошње гаса.
6. Предлог архитектонског модела децентрализоване платформе за електронску трговину засноване на јавној блокчејн мрежи и *IPFS* мрежи, који интегрише оптимизоване моделе складиштења података, модуларни дизајн паметних уговора, као и слој за складиштење података и презентациони слој засновани на садржајном адресирању, уз очување суверенитета корисника над криптографским идентитетом.

11. Структура дисертације

Рад је структуриран кроз више међусобно повезаних целина које прате логички ток од теоријских основа, преко аналитичког и методолошког оквира, до конструктивне реализације и експерименталне евалуације предложеног решења, при чему се у уводном поглављу систематски дефинишу предмет, циљеви, хипотезе и методолошки приступ истраживања.

У другој глави успоставља се концептуални оквир за анализу савремених информационих система. Најпре се разматра однос радних и информационих система, као и формална изражајност пословних захтева које такви системи треба да подрже. Затим се уводи информациони систем електронске трговине као репрезентативан пример савременог пословног информационог система, кроз анализу његових основних карактеристика, референтног модела и технолошких захтева. Даље се анализирају основни архитектонски обрасци организације информационих система, уз нагласак да већина савремених решења задржава централизован модел управљања, независно од тога да ли

су имплементирана на једном или више рачунарских чворова, као и ограничења таквог приступа. У том контексту уводи се појам децентрализације кроз различите димензије, као кључни теоријски оквир за разумевање потенцијала унапређења аутономије корисника и расподеле контроле над системом.

Трећа глава успоставља аналитички оквир за евалуацију информационих система кроз њихова техничка својства и компромис између перформанси, скалабилности, доступности и безбедности. Анализа обухвата фундаменталне принципе и ограничења дистрибуираних система, укључујући *CAP* теорему, скалабилност, загушење, режијско оптерећење, координацију, пропагацију, репликацију, консензус и контролу конкурентног приступа, као и њихове последице по перформансе и оперативну стабилност система. Посебна пажња посвећена је оперативним својствима информационих система кроз безбедносне моделе, криптографске механизме, аутентикацију, ауторизацију и евиденцију, чиме се показује да техничка архитектура система истовремено одређује и његове могућности и његова ограничења.

Четврта глава рада разматра блокчејн као инфраструктурни слој дистрибуираних система. Полазећи од теоријских основа, укључујући криптографско временско обележавање, доказ уложеног рада и ране моделе електронског новца, уводи се контекст настанка савремених блокчејн мрежа. Посебно се анализира Биткоин као први практично реализован систем, који кроз јавно доступну евиденцију трансакција и Накамото консензус омогућава постизање сагласности у окружењу без међусобног поверења. Даље се разматрају кључне архитектонске компоненте блокчејн система, укључујући структуру блокова и трансакција, моделе управљања стањем и контроле приступа, паметне уговоре, апстракцију налога и међуланчану комуникацију. Посебна пажња посвећена је блокчејн трилеми између децентрализованости, сигурности и скалабилности, укорењеној у самим теоријским основама блокчејн система.

Пета глава пружа преглед архитектуре Етеријум блокчејна кроз анализу консензусног и извршног слоја. Детаљно се разматрају механизми засновани на доказу улога, укључујући расподелу валидатора, процес гласања, као и алгоритме избора канонске гране и финализације, чиме се омогућава анализа безбедносних механизма, економских модела и потенцијалних претњи стабилности мреже. У наставку се обрађују унутрашња структура извршног слоја система, модел глобалног стања, рад Етеријум виртуелне машине (*EVM*) и процес обраде трансакција, чиме се пружа интегрисан и целовит приказ функционисања Етеријума као децентрализованог рачунарског система.

Шеста глава рада посвећена је методолошкој оптимизацији паметних уговора за потребе електронске трговине, са циљем смањења потрошње гаса и унапређења корисничког искуства. У претходном раду разматрано је моделовање електронских купона као специфичне инстанце дигиталних ентитета, што представља репрезентативан студијски случај за ширу примену незаменљивих токена у електронској трговини. Анализа је усмерена на операције приступа трајном складишту као кључни фактор оптимизације, будући да оне доминантно одређују укупну цену извршавања на блокчејн системима, уз предлог компактног паковања више информација у једну складишну јединицу и коришћења постојећих *NFT* стандарда. Имајући у виду широку примену Етеријум виртуелне машине, разматрају се стандарди *ERC-721*, *ERC-721A* и *ERC-721Psi* кроз детаљну анализу трошкова операција креирања, преноса и уништавања. Предложени приступи

евалуирани су експерименталним мерењима потрошње гаса, чиме се омогућава објективно поређење њихове ефикасности и практичне применљивости.

Седма глава посвећена је архитектури *IPFS* мреже и њеној улози у децентрализованим апликацијама. Анализирани су модели садржајног адресирања, организације и верификације података, механизми дистрибуираног проналажења и размене садржаја, као и могућности приступа садржају путем *IPFS* приступника. Размотрен је проблем дугорочне доступности података и приказано је решење засновано на децентрализованим економским подстицајима. На крају су анализирани механизми приступа децентрализованим апликацијама путем криптографских новчаника и *ENS* система за именовање.

Осма глава посвећена је дискусији о могућностима проширења, унапређења и практичне примене предложене архитектуре система електронске трговине засноване на блокчејн технологијама. Разматрани су регулаторни, безбедносни и технички аспекти имплементације децентрализованих система, као и напредне функционалности *NFT* стандарда и обрасци модуларног дизајна паметних уговора. Додатно су анализирани механизми повезивања блокчејн система са спољашњим изворима података применом децентрализованих мрежа пророчишта и *zkTLS* приступа, као и специфичности децентрализованог складиштења података заснованог на *IPFS* екосистему. Посебан акценат стављен је на изазове везане за перформансе, приватност, дугорочну доступност података и зависност од постојеће интернет инфраструктуре.

Девета глава представља завршни део дисертације у којем су обједињени резултати теоријске анализе, конструктивног моделовања и експерименталне евалуације. Разматра се допринос истраживања разумевању и пројектовању децентрализованих система електронске трговине, уз осврт на могућности даљег развоја и унапређења предложене архитектуре.

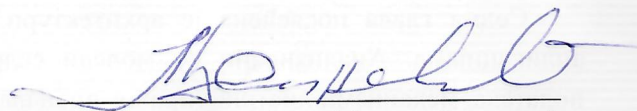
12. Мишљење и предлог Комисије о докторској дисертацији

На основу свега изложеног Комисија је мишљења да докторска дисертација кандидата Вукашина Тасића по својој теми, приступу, структури и садржају рада, квалитету и начину излагања, методологији истраживања, начину коришћења литературе, релевантности и квалитету спроведеног истраживања и донетим закључцима задовољава критеријуме захтеване за докторску дисертацију, те се може прихватити као подобна за јавну одбрану.

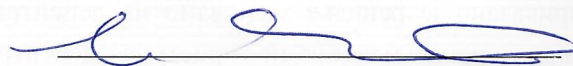
Сагледавајући укупну оцену докторске дисертације кандидата Владиомира Тасића под називом „Унапређење дистрибуиране платформе за е-трговину на јавној *blockchain* мрежи у циљу минимизације рачунарског напора приликом извршавања трансакција“ предлагемо Већу департмана за последипломске студије и Сенату Универзитета Сингидунум да прихвати напред наведену докторску дисертацију и одобри њену јавну одбрану.

Потврђујемо својим потписом, под пуном професионалном одговорношћу, да су подаци у Извештају веродостојни и у потпуности тачни, укључујући тачну категоризацију научноистраживачких резултата кандидата, а све у складу са Правилницима и актима Универзитета.

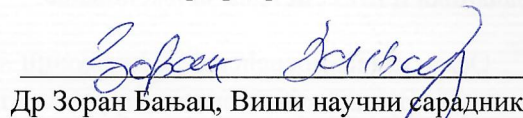
У Београду, 20.07.2026. године



Проф. др Младен Веиновић



Проф. др Милош Станковић



Др Зоран Бањац, Виши научни сарадник
Влатаком институт