УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Горан М. Бјелобаба

МОДЕЛ КОЛАБОРАТИВНОГ УЧЕЊА И ЕВАЛУАЦИЈЕ СТУДЕНТСКИХ РАДОВА ЗАСНОВАН НА БЛОКЧЕЈН ТЕХНОЛОГИЈАМА

Докторска дисертација

Београд, 2024. године

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Goran M. Bjelobaba

A MODEL OF COLLABORATIVE LEARNING AND PEER ASSESSMENT OF STUDENTS' PAPERS BASED ON BLOCKCHAIN TECHNOLOGIES

Doctoral Dissertation

Belgrade, 2024

Ментор:

Др Зорица Богдановић,
редовни професор, Универзитет у Београду, Факултет организационих наука

Чланови комисије:

Др Маријана Деспотовић-Зракић,
редовни професор, Универзитет у Београду, Факултет организационих наука

Др Александра Лабус,
редовни професор, Универзитет у Београду, Факултет организационих наука

Др Вељко Јеремић,
редовни професор, Универзитет у Београду, Факултет организационих наука

Др Ивана Ковачевић,
ванредни професор, Универзитет у Београду, Факултет организационих наука

Др Марко Ђогатовић,
ванредни професор, Универзитет у Београду, Саобраћајни факултет

Датум одбране: 20.03.2024. године

Модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама

Апстракт:

Предмет истраживања ове докторске дисертације јесте развој модела колаборативног учења и евалуације студентских радова заснованог на блокчејн технологијама. У раду су приказане могућности примене блокчејн технологија ради обезбеђивања веродостојности и непорецивости података у колаборативном учењу и евалуацији студентских радова (енг. peer assessment). Циљ истраживања је дефинисање новог модела за унапређење наставног процеса у е-образовању који треба да применом метода колаборативног учења омогући релевантну, веродостојну, транспарентну и сигурну евалуацију студентских радова, нарочито у системима с великим бројем студената, попут масивних отворених онлајн курсева (енг. Massive online open courses – MOOC), или у системима е-учења с великим бројем студената. Приступ колаборативном учењу заснован је на учешћу студената у евалуацији студентских пројеката, а реализован је применом одабраних концепата из процеса рецензирања научноистраживачких радова, као и применом и прилагођавањем добрих пракса са сервиса као што су Публонс (енг. Publons) и Архив (енг. arXiv). Допринос овог рада је развој модела колаборативног учења и евалуације студентских радова у е-образовању заснованог на блокчејн технологијама, који ће омогућити квалитетнију евалуацију студентских радова и унапредити квалитет образовног процеса. Допринос рада састоји се и у примени и евалуацији тог модела над реалном популацијом студената и професора, као и на закључцима који су проистекли из спроведене анализе.

Кључне речи: *блокчејн технологије, евалуација, колаборативно учење, образовни процес, паметни уговори*

Научна област: *Информациони системи и технологије*

Ужа научна област: *Електронско пословање*

A model of collaborative learning and peer assessment of students' papers based on blockchain technologies

Abstract:

The research subject of this doctoral dissertation is the development of a model of peer to peer learning and evaluation of student papers based on blockchain technologies. The possibilities of applying blockchain technologies with the aim of ensuring data authenticity and non-repudiation in peer assessment and the evaluation of students' papers are demonstrated in the doctoral dissertation. The aim of the research is to define a new model for the improvement of the teaching process in e-education, which should enable relevant, credible, transparent and safe evaluation of student work by using the method of peer to peer learning, especially in systems with many students, such as MOOC (Massive online open courses) or e-learning systems with a large number of students. The approach to peer assessment is based on students' participation in the evaluation of students' projects and the same is implemented by applying the concepts selected from the scientific-research paper review process and by applying and adapting good practices from the services such as Publons and arXive. The contribution made by this doctoral dissertation reflects in the development of the blockchain-technologies-based peer assessment and students' papers evaluation model in e-education that will enable a more quality evaluation of students' papers and improve the quality of the education process. The contribution also includes the implementation and evaluation of the applied model over the real population of students and professors, as well as the conclusions derived from the conducted analysis.

Key words: *blockchain techmologies, peer assessment, collaborative learning, educational process, smart contracts*

Scientific field: *Information Systems and Technology*

Narrow scientific field: *E-business*

САДРЖАЈ

1 УВОД

1.1 Дефинисање предмета истраживања

Предмет истраживања ове докторске дисертације јесте развој и примена модела колаборативног учења и евалуације студентских радова заснованог на блокчејн технологијама. У докторској дисертацији истражене су и могућности примене блокчејн технологија ради обезбеђивања веродостојности и непорецивости података у колаборативном учењу и евалуацији студентских радова (енг. *peer assessment*).

У традиционалним приступима, на масовним предметима у високошколском образовању знање студената уобичајено се оцењује тестирањем, а исход је информација о томе да ли је студент положио тест. Међутим, често остаје непознаница који део градива је студент савладао и с коликом успешношћу, као и то да ли је студент оспособљен да научено градиво примени за решавање проблема у пракси. Овај сегмент се евалуира путем семинарских радова и пројеката, нарочито у инжењерским дисциплинама, где се као резултат учења очекује конкретан пројекат. Због тога је студентима неопходно обезбедити пројектно оријентисано учење, које треба да буде доминантније од репродуковања наученог [1]. За квалитетан образовни процес неопходно је да студенти раде практичне пројекте и истраживања, да развијају способности за решавање проблема, као и критичко размишљање [2][3][4][5][6], уз квалитетну евалуацију студентских радова [7][8][9].

Још од седамдесетих година прошлог века постоји идеја да студенти уче тако што ће евалуирати радове других студената са исте класе (са исте године студија или са истог предмета). Евалуацијом радова и пројеката својих колега студенти стичу нова знања, јер тај процес захтева разматрање постављених проблема, проверу добијених резултата, истраживање коришћене литературе и двосмерну комуникацију. Таквим начином колаборативног учења студент се интелектуално развија јер је мисаоно и функционално активан [10][11][12], учи методологију и развија критичко мишљење. С обзиром на природу процеса, студенти међусобно размењују знање. Колаборативно учење је тесно повезано с процесом обраде информација, па је погодно за окружења која су заснована на савременим технологијама са акцентом на доживљај учења. С развојем технологија е-образовања, а посебно у ситуацији масовног преласка на е-образовање, као на пример током пандемије вируса корона, трага се за новим приступима колаборативном учењу, оријентисаним ка практичном и пројектном раду.

Приступ колаборативном учењу који је заснован на учешћу студената у евалуацији студентских пројеката може се реализовати применом одабраних концепата из процеса рецензирања научноистраживачких радова и применом и прилагођавањем добрих пракса са сервиса као што су Публонс (енг. *Publons*) и Архив (енг. *arXiv*) [13]. Проблем обезбеђивања веродостојности и непорецивости података, који се у таквом приступу може јавити, може се решити применом блокчејн технологија.

Блокчејн представља децентрализовану и дистрибуирану базу података у којој се подаци не могу мењати или брисати и која омогућава верификацију трансакција [14]. Подаци о трансакцијама чувају се на различитим рачунарима у мрежи, повезаним коришћењем *peer-to-peer* протокола, где сваки чвор дели исту копију података, тј. дигитални регистар (енг. *Digital Ledger*). У блокчејну подаци се мењају по унапред дефинисаним правилима. Измене се прослеђују свим чворовима како би се ажурирала локална копија података. Након што је трансакција сачувана и након што су је потврдили сви чворови у мрежи, више није могуће променити податке те трансакције.

Процес потврђивања тих трансакција назива се рударење (енг. *mining*) и заснива се на неком од консензус алгоритама на основу којег се постиже договор између чворова при усвајању новог блока [14]. У блокчејну је обезбеђен висок ниво сигурности, јер су трансакције које се одвијају анонимне. Сваки дигитални догађај или трансакција који се реализују у оквиру блокчејн мрежа верификују се само уколико постоји консензус корисника који учествују у конкретном процесу, и то уз услов да они чине апсолутну већину [15].

Предности које пружа примена блокчејн технологија у различитим доменима јесу сигурност, децентрализација, транспарентност и непроменљивост [16]. Блокчејн технологија спречава злоупотребе у смислу фалсификовања и порицања садржаја јер чува потпуну евиденцију у блоковима података у низу с временским ознакама, где се стари и нови блокови података не могу избрисати, а криптографски алгоритам спречава неовлашћено подметање података и смањује могућност преваре [17]. Због тих особина, блокчејн технологија се користи у различитим секторима као што су финансије [18], пословање [19], здравство [20], туризам [21], енергетски сектор [22], јавни сектор [23] и образовање [24].

Иако се у образовању блокчејн технологије још увек недовољно примењују, актуелна истраживања указују на то да постоји велики потенцијал за њихову примену у образовном сектору [16]. Апликације засноване на блокчејну, иако у почетној фази, брзо се развијају у различитим областима образовања, укључујући: окружења за колаборативно учење с високим нивоом безбедности за све учеснике [25][26][27], управљање компетенцијама и исходима учења, управљање ауторским правима [28], системе за испитивање студената и полагање испита [29][30], оцењивање професионалних способности студената које компаније могу користити приликом запошљавања [30][31][32], целоживотно учење [33], онлајн образовање [17], издавање и верификација диплома, транскрипата и сертификата [34][35] који се могу делити између појединаца и организација ради верификације [36][37]. Пример овог приступа је платформа *EduCTX* за пренос евиденција акредитива међу партнерским високошколским установама елиминисањем посредника [38] и систем за управљање подацима у образовном систему [39]. Предности примене блокчејн технологија у образовању обухватају управљање и верификацију података без посредника, без угрожавања аутентичности, уз константну доступност и проверљивост с потпуном транспарентношћу.

У овој докторској дисертацији предлаже се модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама, који обухвата одабране концепте из модела евалуације резултата научноистраживачког рада. Евалуација студентских радова и пројеката биће унапређена путем колаборативног учења, слично поступку рецензирања научноистраживачких радова. Блокчејн технологије ће се у предложеном моделу користити за развој сигурне платформе за чување и размену података о студентским пројектима и радовима, студентима-евалуаторима, рецензентима из праксе и евалуацијама. Након што се подаци о евалуацији студентског рада забележе, ниједна страна их више не може поћи или променити.

Примена концепата отворене науке у образовном контексту омогућиће да радови студената буду квалитетнији, да цео процес буде транспарентнији, као и да постане део процеса развоја каријере. Учешћем у колаборативном учењу и евалуацији радова других студената студенти користе сличан начин размишљања и процедуре које се користе у поступку рецензирања научних радова [40][41][42][43][44][45][46], чиме стичу нова знања из домена учења и методологије, способност критичког и аналитичког размишљања, вештине комуникације и тимског рада, академско и

друштвено одговорно понашање. Учешћем у процесу евалуације радова студенти квалитетом свог рада граде кредибилитет и издвајају се они који то боље раде.

У приступу који је развијен у овој докторској дисертацији, учесници у колаборативном учењу и евалуацији студентских радова и пројеката су студенти који похађају исти предмет, студенти виших година студија или виших нивоа студија. Сваки семинарски рад и пројекат евалуирао је други студент, а информација о квалитету рада дата је квантитативно и описно тако да сви учесници у овом процесу могу да виде препоруку и евалуацију квалитета семинарског рада или пројекта. Учешће у процесу евалуације семинарских радова и пројеката других студената предлаже се као обавезни део процеса учења, тј. као једна од предиспитних обавеза. Примена блокчејн технологија омогућава и повезивање с партнерским високошколским установама, као и колаборативно учење између студената различитих факултета.

Такође, примена блокчејн технологија омогућава да учешће у евалуацији студентских радова постане део процеса развоја каријере. Евалуације и евалуирани пројекти доступни су заинтересованим послодавцима, тако да послодавац има информације о резултатима практичног рада студената, као и томе како су пројекат евалуирали други. Осим студената-евалуатора, за студентске радове и пројекте може бити обезбеђен и рецензент из праксе [47][17][48]. Да би се одабрао компетентни евалуатор, мапирају се компетенције евалуатора у односу на тему семинарског рада или пројекта преко кључних речи, при чему се чувају информације о квалитету рецензије за сваког рецензента.

- *Унапређење компетенција студената-учесника у колаборативном учењу*. Студенти имају обавезу да учествују у колаборативном учењу у оквиру образовног процеса, што подстиче стицање знања из области које се изучавају у оквиру предмета из кога је припреман и евалуиран семинарски рад или пројекат, боље повезивање усвојених знања из области које се изучавају у оквиру датог предмета, усвајање знања о коришћеним технологијама и структурама пројекта, аналитичке вештине, критичко размишљање, мотивацију за рад на пројектима;
- *Унапређење ефикасности и квалитета евалуације студентских радова*. Семинарске радове и пројекте евалуирали су други студенти. Студентима је омогућен приступ семинарским радовима и пројектима својих колега, као и датим евалуацијама. Давањем препоруке и оцене евалуације студентског рада студенти доприносе утврђивању квалитета евалуатора. На овај начин процес евалуације великог броја студентских радова постаје део процеса учења;
- *Унапређење сарадње високошколских институција и компанија*. Примена оваквог приступа компанијама омогућава бољу селекцију кадра „на извору".

С обзиром на то да послодавци немају приступ квалитетним студентима, обезбеђивање доступности таквим студентима од раних година школовања један је од интереса послодаваца да учествују у овом процесу. Послодавцима који учествују у блокчејн мрежи за колаборативно учење и евалуацију студентских радова омогућен је приступ будућем кадру и стицање бенефиција засновано на поенима, тј. на интерној криптовалути [17][18][19]. Поени се стичу учешћем у процесу евалуације студентских радова и верификацији трансакција, а троше се на додатне сервисе у оквиру система и повезивање с бољим студентима.

1.2 Циљеви истраживања

Циљ истраживања био је дефинисање новог модела за унапређење наставног процеса у електронском образовању који треба да применом метода колаборативног учења омогући релевантну, веродостојну, транспарентну и сигурну евалуацију студентских радова, [49] нарочито у системима са великим бројем студената, као што су MOOC - *Massive online open courses*, или системима е-учења са великим бројем студената [50][51][52].

1.3 Полазне хипотезе

Хипотетички оквир рада се састоји од једне основне и неколико посебних хипотеза. Основна хипотеза у раду гласи:

X_0. Увођењем колаборативног учења, заснованог на блокчејн технологијама у е-образовање омогућује се квалитетнија евалуација студентских радова, подстиче пројектно оријентисано учење и унапређује квалитет образовног процеса.

X_1. Колаборативним учењем и учешћем у евалуацији радова својих колега студенти стичу нова знања, вештине и компетенције.

X_2. Колаборативним учењем и учешћем у евалуацији радова својих колега студенти доприносе квалитетнијој евалуацији студентских радова и квалитету образовног процеса.

X_3. Могуће је применити одабране концепте из процеса рецензирања научних радова за унапређење евалуације студентских пројеката и радова.

X_4. Могуће је развити модел и применити систем колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама.

X_5. Примена блокчејн технологија омогућује сарадњу различитих интересних страна (стејкхолдера) у евалуацији студентских радова, укључујући студенте, професоре и потенцијалне послодавце.

X_6. Могуће је интегрисати развијени модел са системима за формално учење.

1.4 Методологија истраживања

Од општенаучних метода коришћене су методе анализе и синтезе постојећих научних резултата, моделирање, аналитичко-дедуктивна и статистичка метода. Методама анализе и синтезе дефинисане су и анализиране теоријске основе колаборативног учења, метода евалуације студентских радова применом колаборативног учења, концепти блокчејн технологија и могућности примене блокчејна као инфраструктуре за колаборативно учење [55][72]. Методе математичког моделовања и анализе друштвених мрежа (енг. *Social Network Analysis, SNA*) коришћене су за моделовање и анализу сарадње у колаборативном учењу [53][54][56]–[62][63]–[71]

Сваки појединац, у току образовања али и професионалног рада, похађа низ образовних програма и курсева, где стиче вештине и одговарајуће сертификате различитих образовних институција. Аутори [24] истичу нужност постојања евиденција ових сертификата, чију веродостојност послодавци могу проверити. У оквиру

истраживања разматрале су се предности дигитализације коришћењем блокчејн технологије и аутоматизације проверљивости података без посредника у сектору образовања. Слично, примену блокчејн система за једноставно дељење записа, односно информација о наградама и евиденцији студената, које су проверљиве, предложили су Шарплс и Доминге [73]. Аутори предлажу и неку врсту валуте повезане с репутацијом образовне институције.

Ради превазилажења „јаза" између академске заједнице и послодаваца, у раду [74] је приказан систем блокчејна у функцији потврђивања компетенција студената различитих образовних институција. Поред поузданије процене компетенција студената према потребама тржишта, односно послодаваца, модел може да пружи и ефикасан начин самопроцене наставе, а тиме и спремности образовних институција за брже прилагођавање својих образовних програма потребама тржишта.

У експерименталном делу рада урађена је евалуација развијеног модела. Експеримент је спроведен кроз апликацију за колаборативно учење, наменски развијену за потребе овог истраживања (доступну на *www.open-rev.com)*. Софтверски систем је развијен применом метода пројектовања софтвера и моделовања података. Развијени систем омогућава студентима да постављају своје радове и евалуирају семинарске радове и пројекте својих колега. Омогућено је и да стручњаци из праксе и будући послодавци евалуирају студентске радове. Резултати добијени експериментом потврдили су постављене хипотезе. Апликација је заснована на блокчејн технологијама у делу обезбеђивања веродостојности података о евалуацији студентских радова и података о студентима и рецензентима из праксе.

Статистичке метода су се користиле за анализу резултата добијених експериментом. Подаци су прикупљани путем примарног истраживања, и то: експлицитно: анкетирањем студената и других учесника у процесу, те имплицитно: сакупљањем података из развијеног информационог система.

Резултати истраживања су представљени текстуално, описивањем и графички у виду слика, дијаграма и табела са упоредним резултатима.

Истраживање је мултидисциплинарно и обухвата информатику, рачунарство, математику, педагогију и методологију.

2 КОЛАБОРАТИВНО УЧЕЊЕ

Колаборативно учење представља размену идеја, омогућава и побољшава интеракцију студент–студент за савладавање градива онлајн. Када замислимо појединце наизглед потпуно фокусиране на екране и тастатуре својих уређаја, чешће имамо предрасуду да они самостално користе те уређаје за учење. Пројекција такве форме индивидуалног учења, уз подршку електронских инструмената и алата, често није у могућности да сагледа реалност испод врха леденог брега, с обзиром на то да у стварности студенти неретко употребљавају личне рачунаре за интеракцију с другима, а често су то управо њихове колеге студенти [75][76][77][78].

Наведене идеје произлазе из технологије учења, која се у литератури среће под различитим именом – кооперативно учење или колаборативно учење. У наставку поглавља су представљене основне информације о колаборативном учењу, дефиниције, теорије у вези са оваквим видом учења и истраживања, принципи, могућности и значај примене у онлајн окружењима. У основи предложене идеје колаборативног учења у овој докторској дисертацији јесу модели засновани на блокчејн технологијама, а који се могу користити за промовисање сарадње међу студентима који раде у онлајн окружењима. Принципи колаборативног учења произлазе из добро утврђеног приступа образовању, имају специфично значење и примену у пракси [79][78].

2.1 Дефинисање појма колаборативног учења

Колаборативно учење представља образовни приступ употребе тимова за оптимизацију учења кроз заједнички рад. Тимови студената могу заједно да решавају одређене задатке, задате проблеме или сарађују у савладавању нових концепата. Овај приступ активно укључује студенте у анализу и синтезу информација и концепата, уместо да уче напамет и памте чињенице и бројке. Студентима је омогућена међусобна пројектна сарадња, при чему морају деловати као тим како би разумели предочене концепте. Бранећи своје ставове, преобликујући идеје, слушајући друга гледишта и артикулишући њихове тачке гледишта, студенти стичу потпуније разумевање као група него што би то постигли као појединци. Колаборативно учење може се дефинисати као „ситуација у којој два човека или више људи заједно уче или покушавају нешто научити” [75]. Ова широка дефиниција узима у обзир различите поставке учења, којима је заједничко то што се студентима не само презентују информације већ активно конструише знање у интеракцији с другим студентима. Колаборативно учење може се, на пример, одвијати у паровима (дијадама), на пример у реципрочној настави [80], у малим групама од по око четири студента [81] или с полазницима целог курса [82].

Често се у пракси појам колаборативног учења поистовећује с појмом кооперативног учења. Разлика између кооперативног учења и колаборативног учења огледа се у чињеници да у кооперативном учењу актери имају одговорност за конкретно дефинисан сегмент сопственог успеха и учења, а истовремено и за тим у целини. Актери овог процеса имају обавезу да своје знање и ресурсе употребљавају како би били сигурни да сваки члан тима схвата концепте које учи. Улоге и структура кооперативног учења дефинисане су унапред. Када је реч о колаборативном учењу, у смислу улога унутар организације, у развоју софтвера, група млађих програмера има задатак да научи нови оквир, а затим да развије део програма док га користи. Сваки од програмера поседује лични део кода за развој, али њихов рад ће се реализовати као успешан само уколико сви науче и исправно изведу свој део кода. Иако сваки

појединац има јединствену улогу у раду, цео тим бележи удео и у успеху других. У процесу заједничког учења, појединачни актери такође морају прихватити одговорност за тимски успех и учење, али су њихове улоге, организација и ресурси препуштени њима самима. Сам тим мора да се усмерава самостално, јер не постоји организатор који би спровео правила ангажовања.

Колаборативно учење датира још из седамдесетих година прошлог века и налази потврду у многим теоријама учења, укључујући социокултурну теорију Лава Виготског [83], теорију друштвене међузависности [83], хуманистичку психологију Маслова [84], друштвени конструктивизам Пејлинксарове [80][85] и теорију вишеструких интелигенција Гарднера [40][79]. Поред тога, на пољу колаборативног учења, и на самом практичном моделу рађено је мноштво истраживања. Иако колаборативно учење покрива широк спектар актера, области и начина учења, за потребе ове докторске дисертације усмерење ће бити на онлајн учење. Уопштено, колаборативно учење доноси бројне позитивне ефекте на когнитивне и афективне варијабле учесника [76]. Значајну пажњу стручне јавности данас завређују истраживања колаборативног учења које се односе на онлајн учење, што се може видети из интернет база података Међународне асоцијације за проучавање сарадње у образовању (*IASCE*) [79].

Колаборативно учење може се дефинисати као принципи и технике за помоћ студентима у сарадњи с колегама и другима [77]. Кроз праксу је развијено на стотине различитих модела колаборативног учења, од којих велики број њих пружа наставницима и студентима мноштво идеја за предузимање даљих корака за повећање вероватноће да ће интеракција студент–студент остварити свој потенцијал. Постоји оптимизам да ће студенти током целог живота имати користи од колаборативних ставова и вештина које развијају процесом интеракције са својим колегама, и у процесу целоживотног учења, и у било ком контексту у којем се нађу.

2.2 Модели и методе колаборативног учења

Постоји више модела колаборативног учења који се заснивају на принципима као што су хетерогено груписање, подучавање колаборативним вештинама, групна аутономија, максимална студентска интеракција, једнаке могућности за учешће, индивидуална одговорност, позитивна међузависност и сарадња као вредност. Бројни су заговорници тезе да је колаборативно учење тесно повезано са афективним и когнитивним исходима [83][79][86][87].

Хетерогено груписање укључује студенте који формирају групе за колаборативно учење са студентима с мањим предзнањем, који су различити од њих самих. Студенти се могу категоризовати на основу пола, припадности друштвеној класи, претходних постигнућа, националне или етничке припадности, религије, марљивости и др. Многи експерти у области колаборативног учења залажу се за хетерогене групе, јер је већа вероватноћа да ће се студенти укључити у подучавање колега када уче у групама које су хетерогене у погледу досадашњег успеха, јер они с вишим досадашњим успехом могу помоћи онима који су, бар привремено, слабије успешни. Такве интеракције носе користи обема странама [86]. Хетерогено груписање реализовано према другим социјалним варијаблама и варијаблама личности пружа студентима подршку у сагледавању различитих перспектива и учењу да раде с људима који се разликују од њих самих, утемељујући тако градњу складнијег социјалног окружења [79][83]. Мање сложен облик субвенција хетерогених група јесте када груписање студената врше професори. У систему који је више фокусиран на студента, професори могу са

студентима разговарати о значењу хетерогеног груписања и његовим потенцијалним користима, па се студенти могу охрабрити да формирају сопствене групе [79].

Подучавање сарадничких вештина као принцип колаборативног учења значи посветити време часа студентима да науче и размисле о употреби вештина сарадње. Постоје многе листе вештина сарадње [87][79]. Вештине важне за колаборативно учење укључују поређење разумевања, тражење помоћи, давање предлога и повратних информација, продуктивно одговарање на сугестије и повратне информације, тражење разлога, навођење разлога, љубазно неслагање, пружање посебних похвала и захвалности, и присуство групном функционисању. Када студенти користе колаборативне вештине, њихове групе ће вероватно боље функционисати, што доводи до више учења и више уживања у учењу [86].

Џонсон, Џонсон и Холубек [83] представљају процедуру од шест корака за подучавање сарадничким вештинама. Прво, неопходност да студенти схвате значај вештине сарадње и друго – шта та вештина укључује што се тиче вербалних и невербалних елемената. Треће, студенти вежбају вештину, односно раде само на вештини, на пример, кроз игру или игру улога, не обраћајући пажњу на тему часа. Четврто, студенти употребу вештине укрштају са учењем садржаја часа. Пето, води се расправа о томе колико добро, појединачно и као група, употребљавају вештину и како се могу побољшати. Шесто, пошто је често потребно време за обављање задатка како би студенти достигли ниво да спонтано употребљавају вештину сарадње, студенти истрајавају у увежбавању вештине. Подучавање колаборативне вештине може бити посебно важно у онлајн окружењима, као што су плоче за дискусије, електронска пошта и друштвене мреже, јер ова окружења представљају нове изазове, који захтевају варијације од вештина одговарајућих у окружењима лицем у лице [83].

Значајан принцип је аутономија групе која охрабрује студенте да прво од колега у групи затраже помоћ или повратну информацију. Често су студенти веома зависни од својих професора, стављајући у други план своје способности и способности својих колега. Како би студенти усвојили концепт целоживотног учења, неопходно је да преузму неку од улога за које се пре сматрало да су искључиви домен наставника, попут пружања помоћи и повратних информација. Такође, када студенти у оквиру својих могућности помажу једни другима, наставници могу пружити помоћ када она превазилази тренутне способности студената [83].

Литература колаборативног учења нуди многе идеје за промовисање групне аутономије, јер она може бити посебно важна у ИТ окружењима, чак и више него у учионицама, јер је мања вероватноћа да ће наставници бити одмах доступни да пруже помоћ.

Принцип колаборативног учења, максималне интеракције међу студентима, односи се на максимизирање двају аспеката међусобних интеракција. Прво, увећава се квантитет студентских интеракција приликом употребе групних активности, посебно када је број чланова у свакој групи мали. Друго, корисност студентских интеракција повећава се када студенти користе вештине размишљања вишег реда [88]. Заиста, срж колаборативног учења лежи у квалитету студентских интеракција, које промовишу више учења, већу дубину обраде и већи ангажман [89][90]. Дакле, што је већа количина ове квалитетне студентске интеракције, то је боље [91].

Информационе технологије пружају многе нове и ефикасне алате за интеракцију с колегама. Нажалост, пречеста употреба информационих технологија у образовању за последицу може имати то да наставници дају инструкције електронским путем, а не лицем у лице. То би се могло променити уколико би, док студенти слушају предавања онлајн или читају текстове на интернету, при чему треба укључити време и задатке за

интеракцију, задаци били такви да захтевају размишљање. Неопходно је да ти задаци за размишљање буду у оквиру тренутних способности студената. Овде наставници имају важну улогу у пружању подршке, која је потребна студентима како би задаци који захтевају интерактивно размишљање били изводљиви. Када су групе хетерогене у погледу досадашњег успеха, они с нижим степеном успеха могу затражити помоћ од колега у групи, уместо да лутају или одустану када се суоче са задацима који им се чине сувише тешким.

Могућност да сви студенти учествују подједнако од великог је значаја. Понекад један члан групе или више њих покушавају да доминирају групом, ускраћујући другима прилику да ступе у интеракцију и са задатком и с колегама у групи. Једнака могућност учешћа је принцип колаборативног учења, који се посебно односи на такве ситуације. На пример, ако се искључе чланови групе који су мање вешти у решавању задатка који група преузима, остали чланови групе пропуштају могућност студентског подучавања, које би имали да су сви укључени.

Технике колаборативног учења, заједно с различитим софтвером, нуде алате који свим члановима групе пружају једнаке могућности за учешће. На пример, за разлику од дискусија лицем у лице, у којима неки чланови групе могу имати потешкоћа да буду саслушани, асинхрона мрежна комуникација омогућава студентима да размене своје идеје без потребе да се такмиче да добију реч. Друге идеје које промовишу једнаке могућности за учешће укључују кодирање у боји како би се допринос сваке особе приказао на графици, табели или тексту или чланова групе који су насумично изабрани да поделе идеје своје групе.

Појединачна одговорност се манифестује у околностима где постоји једнака могућност за учешће, што значи да сви чланови групе имају прилику да одиграју важну улоге у групи. Принцип индивидуалне одговорности врши притисак на чланове да остваре правичан удео у групи [90]. Сваки студент треба да искористи понуђену могућност да допринесе групи у складу са својим способностима. Ако се студенти не осећају индивидуално одговорним, ако се неки студенти понашају као слободњаци, морал групе може трпети, а студенти могу изгубити веру у коришћење група за учење због присуства ових слободњака. Бесплатно учитавање отежава процењивање, јер наставници можда нису у могућности да процене доприносе чланова својим групама [90]. Колаборативно учење и ИТ алати нуде идеје за промовисање индивидуалне одговорности. Поред тога, исти софтвер који промовише једнаке могућности за праћење учешћа сваког члана групе може обавестити колеге у групи и наставнике и о томе ко не испуњава своја задужења у групи.

Два су начина да се потешкоће ове врсте превазиђу, а које предавачи постављају ради оцењивања: а) укључивање колега у оцењивање, јер су колеге у бољем положају да надгледају доприносе сваког члана и б) заједничко учење студената, али да се оцењују сами, на пример, након што студенти заједно раде на решавању скупа онлајн проблема, они сами раде још један скуп сличних проблема.

Позитивна међузависност је принцип колаборативног учења који охрабрује дељење међу студентима, јер када се студенти осећају позитивно међузависни од својих колега у тиму, група осећа да су њихови исходи позитивно повезани. Другим речима, тимови усвајају принцип „сви за једног, један за све”. Док индивидуална одговорност ствара притисак на чланове да допринесу тиму, позитивна међузависност пружа подршку, јер уколико су студенти суочени с потешкоћама, њихове колеге из групе нуде неку врсту помоћи. Позитивна међузависност такође може подстаћи мотивацију за учење, јер студенти не уче само за себе већ и за добробит својих тимова. Развијене су бројне идеје да мотивишу студенте да се осећају позитивно међузависно од својих вршњака у тиму. Још један начин промовисања позитивне међузависности јесте да сваки студент има

различите ресурсе. На пример, сваки члан групе могао би да на интернету истражи другу подтему основне теме групе, а затим да са својим колегама из групе подели оно што је научио [92].

Сарадња као вредност гради се на позитивној међузависности и настоји да тај осећај мале групе прошири до читаве генерације, целе образовне установе, читавог града, нације и света, проширујући се и на друге врсте. Сјајан пример су представници Факултета организационих наука који учествују на светским такмичењима *CASE STUDY* – осим што се боре за себе, представљају своју генерацију, факултет, Универзитет у Београду, али и своју земљу. Иако је неопходно да студенти знају на који начин да се такмиче и раде самостално, постоји тенденција да се путем принципа сарадње дође до спознаје да је управо сарадња жељена опција. Мноштво је средстава за унапређење сарадње као вредности [93], између осталог да увиде многе предности сарадње. На пример, студенти могу да науче о ИТ изумима, ИТ компанијама и ИТ мрежама којима је била потребна велика сарадња да би се остварила и расла. На основу тога, могу да схвате да њихова сарадња у малим групама представља основу за њихово касније ефикасно учешће у великим тимовима [93].

2.3 Колаборативно учење у е-образовању

С обзиром на природу процеса, реализује се трансфер знања између студената. Колаборативно учење је тесно повезано с процесом обраде информација, па је погодно за окружења која су заснована на савременој технологији, где фокус није ни хардверски ни софтверски, већ на самом доживљају учења. Технологије функционишу као главни алати у људском учењу. У процесу развоја технологија е-образовања, а посебно у ситуацији масовног преласка на е-образовање током пандемије вируса корона, трага се за новим приступима колаборативном учењу, оријентисаним ка практичном и пројектном раду.

Увођењем колаборативног учења у е-образовање омогућује се квалитетнија евалуација студентских радова, подстиче пројектно оријентисано учење и унапређује квалитет образовног процеса. Колаборативним учењем и учешћем у евалуацији радова својих колега студенти стичу нова знања, вештине и компетенције и доприносе квалитетнијој евалуација студентских радова и квалитету образовног процеса.

Технологије које су доступне групама у онлајн окружењу такође утичу на интеракцију. Компјутерски подржано окружење за учење олакшава различите аспекте сарадње, захваљујући приступу комуникационим каналима [94]. Сваки комуникацијски медиј повезан је са специфичним ограничењима и на тај начин одређује у којој мери студенти могу једно другом дати непосредну повратну информацију, колико се друштвених знакова (на пример израза лица) преноси кроз богатство медија и колико лако студенти могу развити заједничко разумевање и заједничко становиште. На пример, знатно је теже нешто објаснити путем електронске поште него усмено, путем видео-конференције. С друге стране, електронска пошта омогућава преглед порука и касније и приморава студенте да јасно опишу своје идеје, па студенти лакше могу уочити недостатке у објашњењу [95].

Примена колаборативног учења на мрежи састоји се од три главна концепта: заједничко учење, учење на мрежи и учење у заједници. Заједничко учење односи се на ванвременску стратегију, која се претежно користила у академском окружењу за побољшање учења студената заједничким радом [96]. У литератури се као општи израз користи групно учење [97]. Осим тога, Смит и Мекгрегор дају дефиницију да је

„заједничко учење кровни израз за различите образовне приступе који укључују заједничке интелектуалне напоре студената, или студената и наставника заједно" [98]. У већини ситуација заједничког учења студенти раде у групама од по двоје или више њих, узајамно тражећи разумевање, решења или значења или стварају производ. Што се тиче учења на мрежи, Минс, Бејки и Марфи дефинисали су учење на мрежи као интеракцију студената са садржајем и/или људима путем интернета у сврху учења [98]. Учење може бити део формалног курса или програма или једноставно нешто што студенти траже ради својих интереса. То је једна од прихваћених наставних метода у учењу на даљину [98].

Учење у заједници односи се на одељења која су повезана или груписана током академског рока, често око интердисциплинарне теме, и окупљају групу студената, за чију се изградњу користе различити приступи, а сви имају за циљ реструктурирање студентског времена, кредита и искустава у учењу како би се изградила заједница међу студентима, међу студентима и њиховим наставницима, те међу наставницима и самим научним дисциплинама [97]. Једна од прихваћених наставних метода учења на даљину јесте и колаборативно учење. Овај вид учења на мрежи сличан је колаборативном учењу лицем у лице, осим што се састанци чланова групе одвијају путем интернета на синхрони или асинхрони начин, а сам процес заснован је на пет међусобно зависних компонената традиционалног колаборативног учења [99]:

1. позитивна међусобна зависност;
2. персонална одговорност;
3. заговарање интеракције;
4. социјалне вештине;
5. тимски процеси.

Када су у питању концепти онлајн колаборативног учења у било којој форми е-образовања, према тврдњи аутора, постоје три главна конструкта [97][100]: интерактивност, друштвени контекст и технологије за заједничко онлајн учење. Интерактивност се односи на концепте и дизајн који студенте ангажују да активно сарађују, друштвени контексти се односе на заједницу за учење усредсређену на студента, а технологије описују све алате и технике који подржавају и побољшавају развој знања и управљање знањем. Они су објашњени на следећи начин: интерактивност укључује заједничко и активно учење. До сарадње не долази ако се студентима не да овлашћење и активно се баве својим активностима.

Колаборативно учење у е-образовању користе мале групе студената у настави, које их охрабрује да максимизирају своје и међусобно учење. Колаборативно онлајн учење подстиче студенте да размењују знања, инспиришу једни друге, зависе једни од других и примењују активну друштвену интеракцију у малој групи [100]. Стога такво онлајн учење зависи од уметности друштвених интеракција међу студентима, а не од механичког процеса.

Са аспекта оперативности, у колаборативном учењу у е-образовању, и студенти и наставници су студенти који деле своје одговорности у мрежној заједници, те би им требало омогућити да одлучују о искуствима учења која ће стећи. Друштвени контекст наглашава карактеристике студента и окружење друштвеног учења усмерено на студента (заједница учења).

Ради пружања подршке професионалном развоју наставника, е-образовање диктира околности у којима је важно да се усредсреди на кључне факторе за развој наставничких перформанси у смислу организовања учења, методе подучавања и учења,

алате и ресурсе институционалних димензија. Заједничко учење интегрисано је са онлајн учењем. Заједно с њима пребацују се у „заједницу". Разлог за то је што осећање „заједнице" мора бити одрживо при заједничком онлајн учењу [99].

Увођење колаборативног учења у е-образовању технологијама пружа бројне могућности, јер је могуће интегрисати развијени модел са системима за формално учење. Такође, могуће је применити одабране концепте из процеса рецензирања научних радова за унапређење евалуације студентских пројеката и радова. Могуће је развити модел и применити систем колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама. Примена блокчејн технологија омогућује сарадњу различитих стејкхолдера у евалуацији студентских радова, укључујући студенте, професоре и потенцијалне послодавце.

Редмонд и Лок указали су на то да се с колаборативним учењем у е-образовању могу стећи глобална искуства учења у којима студенти раде као виртуелни чланови тима, имају приступ низу стручности и стварају знање заједно с људима с којима се можда никада неће лично упознати, већ само онлајн [101][102]. Даље, према Палофу и Прету, у недавним студијама онлајн окружења примећено је да је укључивање или „друштвено присуство", познатије као осећај заједнице и повезаности међу студентима, позитивно допринело исходима учења и задовољству студената онлајн курсева [103].

2.4 Пројектно оријентисано колаборативно учење

Пројектно оријентисано учење је својеврсна педагошка активност усмерена на студенте. Укључује динамичан приступ процесу учења, у којем се верује да студенти стичу дубље знање активним истраживањем изазова и проблема у стварном свету. Сходно том концепту, студенти уче о предмету радећи дуже време на истраживању и одговарању на сложено питање, изазов или проблем. То је стил активног учења и учења заснованог на истраживању.

Томас Маркам [104] описује пројектно оријентисано учење као „процес који интегрише знање и рад, јер осим стицања знања, студенти примењују оно што знају за решавање аутентичних проблема и постизање резултата који су важни [104]. Студенти у примени пројектно оријентисаног учења користите предности дигиталних алата за производњу висококвалитетних производа за сарадњу. На тај начин ова форма учења преусмерава образовање на студента као носиоца знања и вештина, а не на курикулум – помак који захтева глобални свет и који награђује нематеријална добра као што су нагон, страст, креативност, емпатија и отпорност не може се научити из уџбеника, већ се мора активирати кроз искуство." [104]

Блуменфилд и његови сарадници елаборирају даље овај процес: „Учење засновано на пројектима је свеобухватна перспектива фокусирана на наставу ангажовањем студената у истраживању. Унутар овог оквира, студенти траже решења за нетривијалне проблеме постављајући и усавршавајући питања, расправљајући о идејама, дајући предвиђања, израђујући планове и /или експерименте, прикупљања и анализе података, извођење закључака, преношење њихових идеја и налаза другима, постављање нових питања и стварање артефаката [85]." Основа пројектно оријентисаног учења лежи у аутентичности или стварној примени истраживања. Студенти који раде као тим добијају захтев на који могу одговорити или направити артефакт (или артефакте) како би представили своја стечена знања. Артефакти могу укључивати различите медије као што су записи, уметност, цртежи, тродимензионални прикази, видео-записи, фотографије или презентације засноване на технологији [85].

Заговорници пројектно оријентисаног учења наводе бројне предности примене његових стратегија у учионици, укључујући дубље разумевање концепата, ширу базу знања, побољшану комуникацију и међуљудске односно социјалне вештине, побољшане лидерске способности, повећану креативност и побољшано писање вештине [85]. Све ово указује на то да пројектно оријентисано учење укључује врсту наставе на којој студенти раде заједнички на решавању проблема из стварног света у својим школама и заједницама. Успешно решавање проблема често захтева од студената да извуку поуке из неколико дисциплина и примене их на практичан начин. Обећање да ће се видети стваран утицај постаје мотивација за учење. Када су студенти основних студија укључени у пројекат курса, дидактичка стратегија сарадње, попут учења усмереног на пројекте, они могу развити додатне вештине које су стечене током процеса учења. Пројектно оријентисаним учењем студенти самостално бирају радно оптерећење, те су одговорни за своје деловање, чиме се постижу циљеви тима [105]. То подразумева ефикасност при додељивању задатака међу собом. Како студенти често поседују различите нивое зрелости, такво ефикасно деловање и понашање унутар тимова не дешава се само по себи. Међуљудски односи и групна динамика, затим конфликти, својствени људском понашању, могу довести у питање успех пројекта. Тако су емоције препознате као важан играч у приказивању одговорног и зрелог понашања [105].

Свеобухватно учење засновано на пројектима [106]:

- организовано је око отвореног питања или изазова:
- ствара потребу за познавањем битних садржаја и вештина;
- захтева упит да би се научило или створило нешто ново;
- захтева критичко размишљање, решавање проблема, сарадњу и различите облике комуникације, често познате као вештине 21. века;
- пружа могућност студентског гласа и избора, у одређеној мери;
- подразумева повратне информације и ревизију;
- резултира јавно представљеним производом или перформансом.

Употреба концепта колаборативног учења осмишљена је тако да повећа вредност студентских интеракција реализованих коришћењем електронских уређаја и широког спектра софтверских алата. Као основа платформе за сарадњу препознаје се доступност веба и алата заснованих на облаку, попут *Google* докумената, *Popplet*-а и *Prezi*-ја, који омогућавају да више корисника креира, пише, уређује и коментарише дељене документе. Адекватан пример представља дељење *Google* документа међу групом студента зарад заједничког писања истраживачког рада. При започињању задатка, сваки студент бира да буде одговоран свом тиму тако што ће написати први нацрт одређеног дела извештаја. По завршетку појединачног истраживања, студенти достављају нацрт у заједнички *Google* документ. Како сваки студент дели и гледа исти документ, сваки од њих има једнаку прилику да коментарише или уређује како би побољшао почетне доприносе својих колега у извештају. Такво колективно залагање и труд да се разјасни, исправи и разради основни садржај може унапредити извештај. Током заједничког рада студената на извештају многоструко се промовише максимална студентска интеракција, на пример када су групе у години студија позване да критички прегледају завршни рад других група, чиме се стимулишу вештине размишљања вишег реда.

Приликом осмишљавања активности пројектно оријентисаног колаборативног учења, наставници морају да утврде шта се од студената очекује да науче из те активности [107]. То се назива пројектним циљем (на пример учење о одређеној теми или стицање вештина сарадње). Ради колективног деловања, али не и идентичним с њим, повезана је врста интеракције која је усмерена мерама подршке за остварење овог циља. На пример, циљ активности учења може бити стицање нових знања о садржају. Да би постигао тај циљ, наставник може укључити студенте у узајамну наставу, где се студенти смењују објашњавајући нешто свом колеги. Сходно томе, циљ наставне подршке јесте јединствена форма интеракције између студената. Иако само неколико наставних оквира разликује ове димензије, разматрање ових аспеката одвојено омогућава прецизнији дизајн наставе [108].

Процесом колективног писања или решавањем пројектних задатака по фазама, студенти препознају вредност сарадње, свесни да квалитет и успех њиховог извештаја зависе од доприноса и повратних информација сваког студента понаособ.

Активности попут постављања питања која подстичу размишљање захтевају од студената да вербализују своје мисли (размишљајући наглас). Ово омогућава осталим члановима групе да посматрају процесе закључивања и интернализују их имитацијом (моделирање спознаје). Размишљање наглас уме да изазове нове дискусије уколико чланови групе генеришу одређене идеје и поведу расправу о њој. Кроз процес аргументације студенти имају обавезу да појасне своје идеје и образложе их примерима за илустрацију концепата (разрада) и креирањем експлицитних веза између појмова (организација). У случају да своје идеје не могу да учине разумљивим другима, студенти могу да мапирају недостатке у свом знању. То може покренути колаборативне процесе учења, који су усмерени на исправљање ових недостатака. Током аргументације студенти такође морају помирити когнитивне разлике које произлазе из супротних гледишта о теми дискусије.

Често не постоји јасна информација о томе који део градива је студент савладао и с коликом успешношћу, нити да ли је студент оспособљен да примени научено градиво за решавање проблема у пракси. Овај сегмент се евалуира путем семинарских радова и пројеката, нарочито у инжењерским дисциплинама, где се као резултат учења очекује конкретан пројекат. Због тога је студентима неопходно обезбедити пројектно оријентисано учење, које треба да буде доминантније од репродуковања наученог [1]. За квалитетан образовни процес неопходно је да студенти раде практичне пројекте и истраживања, да развијају способности за решавање проблема и критичко размишљање [109]. Значајан напредак у савладавању градива доноси и квалитетна евалуација студентских радова, која, осим евалуације наставничког кадра, укључује и вршњачку евалуацију [9].

2.5 Примена колаборативног учења за евалуацију студентских радова

Модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама представља збирне могућности примене блокчејн технологија ради обезбеђивања веродостојности и непорецивости података у колаборативном учењу и евалуацији студентских радова (енг. *peer assessment*). Применом једног таквог модела унапређују се наставни и евалуацијски процеси у е-образовању. Конкретно, применом метода колаборативног учења остварује се релевантна, веродостојна, транспарентна и сигурна евалуација студентских радова [110]. Таква примена налази своје место нарочито у системима с великим бројем студената, као што су масивни отворени онлајн курсеви (енг. *Massive Open Online Course*), или системима

електронског учења с великим бројем студената [52]. У традиционалним приступима, на масовним предметима у високошколском образовању, знања студената углавном се евалуирају тестирањем, а исход о томе је сазнање да ли је студент положио тест.

Током седамдесетих година прошлог века проистекла је идеја да студенти уче учешћем у евалуацији радова других студената исте класе (са исте године студија или са истог предмета). Учешћем у евалуацији радова и пројеката својих колега студенти стичу нова знања разматрањем постављених проблема, провером добијених резултата, истраживањем коришћене литературе и двосмерном комуникацијом. Таквим начином колаборативног учења студент се интелектуално развија, јер је мисаоно и функционално активан, учи методологију и развија критичко мишљење [11].

За протеклих двадесет година, колико се интернет широко користи у образовању, појавило се на десетине, ако не и стотине, система вршњачког онлајн оцењивања. Наставни кадар их је осмислио за многе дисциплине, попут енглеског језика, информатике и рачунарства, дизајна, пројектовања итд. Топинг је истакао компјутерски подржано вршњачко оцењивање као важан педагошки приступ развоју компетенција вишег нивоа [111]. Већина тих система дизајнирана је од темеља – до сада постоји мало доказа да су се дизајнери и програмери једног система консултовали с другим системима како би видели које постојеће технике одговарају њиховом искуству и шта се може унапредити. Више аутора дало је преглед приступа вршњачке процене који су заступљени у пракси [112][111][113][114][115][116]. Ипак, досадашња истраживања нису резултирала предлогом систематског оквира за истраживање и уопштавање могућности и ограничења система вршњачке процене који омогућавају образовне технологије [117].

Истраживања о примени система вршњачких оцењивања реализована су у два доминантна смера. Први се односи на систематична истраживања домена технолошких могућности система вршњачких оцењивања и други на развијање спектра веб-услуга за разноврсност апликација у таквим системима [117].

Испитивања низа заступљених система укључила су познатије системе, као што су *Calibrated Peer Reviev* [118], *CritViz* [119], *CrovdGrader* [120], *Ekpertiza* [121], *Mobius SLIP* [122], *Peerceptiv* [123] и *peerScholar* [124]. Током тих истраживања усвојен је термин „систем вршњачке процене на мрежи” (*online peer assessment system*) да се опише широк спектар рачунарских апликација које су наменски осмишљене и развијене да подрже међусобну рецензију и оцењивање ученика. Конкретно, систем оцењивања на мрежи могуће је дефинисати као апликацију засновану на вебу која олакшава ток процеса процене колега, као што је прикупљање артефаката за слање, додељивање рецензената за критику и/или оцењивање означених артефаката који су достављени колегама, уз постављање рокова и усмеравање рецензената на формат квалитативне и квантитативне повратне информације. Овај термин покрива класу система који се у литератури описују као систем рачунарске стручне процене (технологија, ИТ, ИЦТ, ЦИТ, интернет, веб-мрежа, облак) (засновани, подржани, уз помоћ, омогућени, посредовани) (преглед, евалуација) – у било којој комбинацији [117]. Мрежни системи процењивања су подскуп опште класе друштвених рачунарских система који укључују рецензије (укључујући друштвене мреже и апликације на друштвеним медијима, попут викија, блогова и форума за дискусију), али се одликују посебним ограничењима тока рада и усмеравањем на одређене образовне циљеве.

Ранија пионирска истраживања Лакстон–Рејлија [125] и Сондергарда и Малдера [117] разматрала су могућности једног по једног система, а затим су их упоређивали. Каснији истраживачки приступи били су усмерени на функционалности система, а потом на описе на који начин поједини системи остварују те функционалности [126].

Приступ колаборативном учењу који је заснован на учешћу студената у евалуацији студентских пројеката реализован је применом одабраних концепата из процеса рецензирања научноистраживачких радова и применом и прилагођавањем добрих пракса са сервиса као што су Публонс (енг. *Publons*) и Архив (енг. *arXiv*) [13]. Проблем обезбеђивања веродостојности и непорецивности података, који се у оваквом приступу може јавити, може се решити применом блокчејн технологија.

Евалуација студентских радова реализује се кроз базу података.

Примена концепата отворене науке у образовном контексту омогућава да радови студената буду квалитетнији, да цео процес буде транспарентнији, као и да буде део процеса развоја каријере. Учешћем у колаборативном учењу и евалуацији радова других студената студенти користе сличан начин размишљања и процедуре које се користе у поступку рецензирања научних радова, чиме стичу нова знања из домена учења и методологије, способност критичког и аналитичког размишљања, вештине комуникације и тимског рада, академско и друштвено одговорно понашање [14]. Студенти квалитетом свог рада граде кредибилитет и издвајају се они који задовољавају одређене критеријуме квалитета евалуације.

Учесници у колаборативном учењу и евалуацији студентских радова и пројеката јесу студенти који похађају исти предмет, студенти виших година студија или виших нивоа студија. Сваки семинарски рад и пројекат евалуираће други студент, а информација о квалитету рада дата је квантитативно и описно тако да ће сви учесници у овом процесу моћи да виде препоруку и евалуацију квалитета семинарског рада или пројекта. Учешће у процесу евалуације семинарских радова и пројеката других студената предлаже се као обавезни део процеса учења, тј. као једна од предиспитних обавеза.

Предности примене развијеног приступа:

- *Унапређење компетенција студената-учесника у колаборативном учењу*. Студенти имају обавезу да учествују у колаборативном учењу у оквиру образовног процеса, што подстиче стицање знања из области које се изучавају у оквиру предмета из кога је припреман и евалуиран семинарски рад или пројекат, боље повезивање усвојених знања из области које се изучавају у оквиру датог предмета, усвајање знања о коришћеним технологијама и структурама пројекта, аналитичке вештине, критичко размишљање, мотивацију за рад на пројектима;
- *Унапређење ефикасности и квалитета евалуације студентских радова*. Семинарски радови и пројекти евалуираће други студенти. Студентима је омогућен приступ семинарским радовима и пројектима својих колега, као и датим евалуацијама. Давањем препорука и оцена евалуације студентског рада студенти доприносе утврђивању квалитета евалуатора. На тај начин процес евалуације великог броја студентских радова постаје део процеса учења;
- *Унапређење сарадње високошколских институција и компанија*. Примена оваквог приступа може компанијама омогућити бољу селекцију кадра „на извору". Будући да послодавци немају приступ квалитетним студентима, обезбеђивање доступности таквим студентима од раних година њиховог школовања биће један од интереса послодаваца да учествују у овом процесу.

Организовање успешног заједничког учења заснованог на моделу *peer-to-peer* (*P2P*) – досадашње дискусије и искуства показују да *P2P* апликације које се данас користе нису нарочито погодне за заједничко учење упркос сличности у концептуалној архитектури. Чини се да су значајан део колаборативног учења друштвени аспекти

сарадње и равноправно учешће свих ученика. Алати које *P2P* окружење може понудити данас не подржавају довољно процес друштвене комуникације, већ промовишу нежељено понашање као сегментацију задатка и конкуренцију међу ученицима. Евидентне су и потешкоће у давању подршке другим члановима групе како би се резултат у коме постоји допринос свих учесника осигурао. Колективни рад у *P2P* окружењу има склоност ка изолацији слабијих чланова тима и промовисању доминантно понашање јачих чланова, а тежња је да се то елиминише.

Иако окружење *P2P* нуди велике предности у групном раду, јер омогућава члановима да учествују асинхроно, када имају времена и могућности, то не уклања проблеме хетерогености и мотивације међу члановима групе. Неопходно је осигуравање хетерогености и мотивисаности док се планира заједничко учење засновано на *P2P*.

Окружење *P2P* такође нуди одличне могућности за дистрибуцију новијих верзија извештаја и материјала, који су пронађени и произведени за решавање задатог задатка, све док постоји добро дефинисана процедура како то учинити и како доставити потребне метаподатке. Детерминисање процедура које треба употребити за пројекат адекватно је одрађено. С обзиром на то да чланови групе делују независно од места и времена, распоред активности и одговорности чланова групе пажљиво је испланиран како би се осигурао допринос свих чланова групе коначном резултату групе. Значајна је улога наставника, који има обавезу да изради и контролише пројектне процедуре и шаблоне.

Развој функционалности *P2P* софтвера може побољшати понашање у колаборацији, те је он од изузетне важности. Међутим, будући да се пројектни задаци и студентски тимови веома разликују, не постоји генеричко решење за заједничко учење базирано на *P2P*. Чини се да је функционалност која побољшава комуникацију између чланова групе као што су електронска пошта, чет, аудио и видео конференције важан сет алата за развој. Други пакет алата за развој јесте онај који подржава процедуре пројекта и пројектно оријентисаног учења и заказивање активности с личним и групним календарима и системима личних информација. Важни су и алати који могу повећати мотивацију ученика. Није неопходно да алати предложени за *P2P* сарадњу буду интегрисани у исти софтверски пакет. Једноставан наменски софтвер показао се бољим од сложених вишенаменских пакета. Издвајање општих правила за организовање успешног *P2P* заједничког учења могу се свести на:

1. Адекватну припрему пројеката кроз садржај, целине, процедуре и мотивацију;
2. Дефинисање виших циљева и приказ шаблона и распореда за решење или резултат;
3. Формирање тимова студената сходно критеријумима везаним за различитости у знању, интересовању, вештинама и личности;
4. Осигурање, вођење и надгледање догађаја тимског рада и сарадње на почетку пројеката;
5. Предлог или набавка *P2P* алата за различите аспекте сарадње;
6. Дефинисање испитних критеријума за спречавање или умањивање ризика од злоупотреба.

С обзиром на ова правила, могуће је контролисати недостатке колаборативног учења и максимизирати резултати учења.

3 БЛОКЧЕЈН ТЕХНОЛОГИЈЕ У Е-ОБРАЗОВАЊУ

Блокчејн технологија, као база података отпорна на неовлашћену употребу и временски означена, омогућава појединцима, компанијама, јавним организацијама и другим учесницима да потврде трансакције и ажурирају записе на синхронизован, транспарентан и децентрализован начин. Поверење међу учесницима темељи се на правилима или консензусним механизмима, које учесници прате да би потврдили и додали трансакције блокчејну, уместо да почива на улози посредника.

Постоје различите блокчејн технологије с посебним функционалностима и архитектуром, тако да је потенцијална примена блокчејн технологије повезана с контекстом и специфичностима проблема, односно облашћу интересовања. Блокчејн поседује предиспозиције за трансформацију функционисања великог дела индустрија. Његове особине утичу на повећање, транспарентност и следљивост робе, података и финансијске имовине, чине лакшим приступ тржишту и утичу на квалитет и ефикасност трансакција. Због ових особина, блокчејн технологија се користи у различитим секторима као што су финансије [18], пословање [19], здравство [20], туризам [21], енергетски сектор [22], јавни сектор [23] и образовање [24]. У овом делу рада објашњен је концепт блокчејн технологије и могућност њене примене у високошколству у оквиру процеса колаборативног учења, евалуације и сертификације.

3.1 Концепти блокчејн технологије

Дистрибуирана технологија главне књиге (енг. *Distributed Ledger Technology – DLT*) специфична је форма базе података у којој се подаци евидентирају, синхронизују и деле у дистрибуираној мрежи рачунара или учесника. Блокчејн технологија је подскуп *DLT*-а, односно све врсте блокчејна су *DLT*. Разлика је у начину на који се подаци дистрибуирају, верификују и региструју. Блокчејн је комбинација већ постојећих технологија које заједно стварају мрежу која осигурава поверење међу учесницима, а који иначе немају разлога да верују једни другима. То значи да блокчејн употребљава *DLT* за чување криптографски верификованих података групе корисника, што је договорено унапред дефинисаним мрежним протоколом и често без контроле централног ауторитета за спровођење правила [127]. Уклањање централног ауторитета из структура базе података један је од важнијих и ефективних аспеката система блокчејна. Шифровање свих важних записа података у блокчејну врши се помоћу криптографских техника, које омогућавају конзистентан интегритет података и записа.

Блокчејн представља децентрализовану и дистрибуирану базу података у којој се подаци не могу мењати или брисати и која омогућава верификацију трансакција [14]. Чине га три основна дела: блок, ланац и мрежа.

Блок представља списак трансакција евидентираних у књигу/регистар током одређеног периода. Подаци о трансакцијама чувају се на различитим рачунарима у мрежи, који су повезани тако што користе *peer-to-peer* протокол. Овај регистар се може замислити као књига записа која евидентира и чува све трансакције између корисника по хронолошком редоследу и идентични примерак књиге имају сви корисници на мрежи, названи чворови. Такође, сваки чвор дели исту копију података, тј. дигитални регистар (енг. *Digital Ledger*). Мрежа се састоји од „пуних чворова" (енг. *full nodes*) [127]. Сваки чвор евидентира све икада забележене трансакције у том блокчејну. Поједини чворови имају улогу и да стално верификују аутентичност записа који се налазе у ланцу, те да одбаце блокове података уколико не прођу верификацију. По том

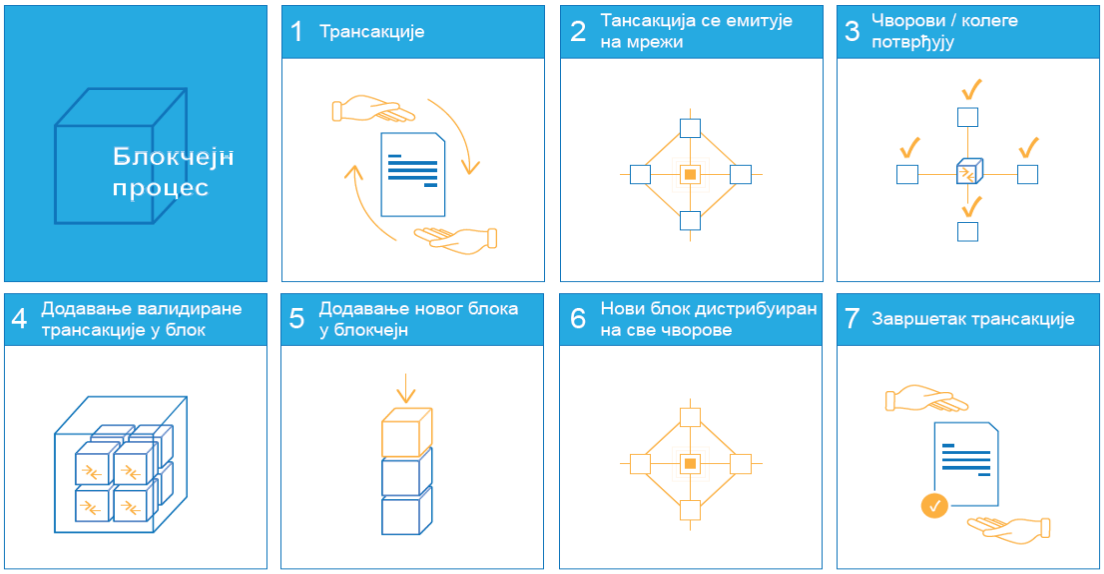
моделу, неопходно је да 51% мреже ради свој посао како мрежа не би била угрожена пласирањем лажних података. С друге стране, преузимање већег броја чворова у мрежи био би компликован и скуп подухват, па би напори за то далеко превазишли напоре потребне да се угрози било који централизован сервис. Стога се такав приступ за чување података сматра далеко безбеднијим у односу на централизоване базе података.

Рудари (енг. *miners*) јесу чворови мреже који поседују доста рачунарских ресурса за верификацију блокова. Они практично на основу претходних трансакција проверавају да ли пошиљалац поседује довољно средстава на рачуну. Како би се обезбедила демократичност у процесу валидације, односно могућност да баш сваки рудар добије прилику да његов чвор буде узет као валидан, они добијају и рачунарски интензиван задатак који морају да реше [128]. Управо на њега и троше већи део својих ресурса. Награду добија онај који први пошаље валидиран блок с решеним задатком. Такав приступ одабиру иницијално валидног блока трансакција назива се доказ посла (енг. *proof-of-work*) [129] и практично штити мрежу од злоупотреба [130]. Основни недостатак овог приступа јесте велика потрошња струје, као и брзина. Новије верзије ланаца користе и новије алгоритме, који омогућавају бржи и ефикаснији избор кандидата. На крају, валидиран блок добија своју јединствену временску ознаку (енг. *timestamp*) и потпис (енг. *hash*), те се као такав пропагира на остале чворове у мрежи. При додавању сваког наредног валидираног блока, инкрементира се бројач потврда за претходно уписане блокове, па се на тај начин даље смањује вероватноћа да су они лажни. С протоком времена расте поузданост записаних података.

У блокчејну подаци се мењају по унапред дефинисаним правилима. Измене се прослеђују свим чворовима како би се ажурирала локална копија података. Након што је трансакција сачувана и након што су је потврдили сви чворови у мрежи, више није могуће променити податке те трансакције или их је тешко променити. Процес потврђивања тих трансакција назива се рударење и заснива се на неком од консензус алгоритама на основу којег се постиже договор између чворова при усвајању новог блока [14]. Након потврде, следи повезивање с другим трансакцијама у нови блок, који се додаје у блокчејну. Читав процес осигурава да је сваки блок креиран на начин да се непобитно повезује претходни и следећи, чиме се формира ланац блокова или блокчејн [131].

Ланац је хеш који повезује један блок с другим, односно математички „уланчавање”. Хеш у блокчејну креира се на основу података који су били у претходном блоку. Хеш је могуће посматрати попут отиска прста података које закључава у блокове према параметрима времена и редоследа. Хеш формира једносмерну функцију (не постоји инверзна функција) која се не може дешифровати, док функција хеширања ствара математички алгоритам који мапира податке било које величине на низ бита фиксне величине. Више речи о хешу биће у наставку рада [129].

Блокчејн се састоји од три слоја: слој протокола, мрежни слој и апликациони или пословни слој (енг. *layers*). Сваки слој додаје различите компоненте блокчејну ради његовог развоја.



Слика 1: Блокчејн процес

3.1.1 Типови блокчејна

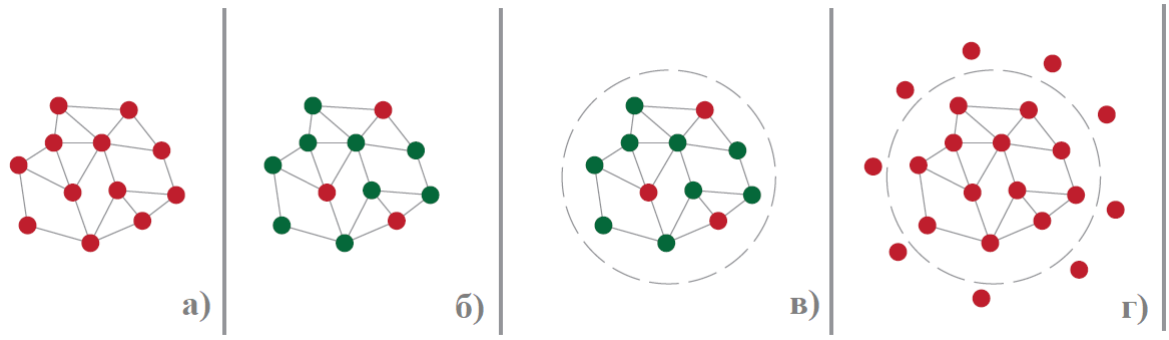
Постоји велики број блокчејн мрежа с различитом функционалношћу и архитектуром. Разликују се у зависности од тога ко може да чита, извршава и потврђује трансакције. Иако постоји низ различитих карактеристика, две важније су отвореност платформе (јавна или приватна) и ниво дозволе потребне за додавање информације у блокчејн (с дозволом или без дозволе). Јавна блокчејн мрежа (попут биткоина) [132] отворена је и свако може да приступи читавом блокчејну. У случају када само овлашћен ентитети има приступ, блокчејн мрежа је приватна или затворена. Слично, блокчејн мрежа с дозволом (енг. *permissioned*) дозвољава само одабраној групи корисника писање, тј. генерисање трансакција, и извршавање, тј. верификовање новог блока. Насупрот томе, блокчејн мрежа без дозволе омогућава свим корисницима да доприносе и додају податке у књигу [133].

У Табели 1 приказани су главни типови блокчејн мрежа сегментиране према моделу дозволе.

Табела 1: Главни типови блокчејн мрежа сегментираних према моделу дозволе

Тип		Објашњење	Пример
Отворен	Јавни без дозволе	Свако може да учествује у механизму консензуса. Сви корисници могу да врше трансакције и погледају цео дневник трансакција.	*Bitcoin*, *Litecoin*, *Ethereum* Слика 2 а)
	Јавни с дозволом	Корисници добијају дозволу за извршење и преглед трансакције, али само ограничени број чворова учествује у механизму консензуса.	*Ripple*, приватна верзија *Ethereum* Слика 2 б)
Затворен	Приватни с дозволом	Ограничење се односи на дозволе вршења и прегледа трансакције само на чворове који учествују у систему, док власник система одређује учеснике и чворове који могу да учествују у механизму консензуса.	*Rubix*, *Hyperledger* Слика 2 в)
	Приватни без дозволе	Ограничење се односи на дозволе вршења и прегледа трансакције, док је механизам консензуса отворен за све.	(*Partially*) *Exonum* Слика 2 г)

На следећој слици приказани су типови блокчејн мреже према моделу дозволе: јавни без дозволе, јавни с дозволом, приватни с дозволом, приватни без дозволе, а према претходној Табели 1.



Слика 2: Типови блокчејн мреже према моделу дозволе (а, б, в, г)

Црвене тачке на Слици 2 представљају чворове валидације, односно проверавају ваљаности трансакције у систему и учествују у процесу консензуса. Зелене тачке на Слици 2 означавају учеснике који могу да обављају трансакције, али не могу да учествују у процесу потврде, односно не учествују у процесу консензуса. Кружница на Слици 2 означава да само чворови унутар њега могу да виде историју трансакција. Илустрације без круга означава отворену мрежу, односно да сви корисници могу да виде историју трансакција.

Постоје и друге поделе блокчејн мрежа: на јавне, приватне и конзорцијум [129], где конзорцијум представља тип блокчејна где се процес консензуса контролише унапред изабраним скупом чворова. Аутори у [132][134] наводе и различите типове хибридних мрежа.

3.1.2 Кључне карактеристике блокчејна

Примена блокчејн технологија у различитим доменима пружа следеће кључне предности: сигурност, децентрализација, транспарентност, непроменљивост [16] и паметни уговори.

1. Децентрализација

Поверење између учесника остварује се на основу скупа правила за потврду и додавање трансакција блокчејну – процес консензуса. Чувени механизам консензуса *PoW* ослања се на рачунску или процесорску снагу чворова или рачунара (рудара) за решавање сложеног математичког проблема што је брже могуће. Чињеница да не постоји централни ентитет који контролише систем утиче на јаку флексибилност блокчејна. У систему не постоји централна тачка неуспеха и тешко га је напасти. Томе доприноси и постојање вишеструких и дистрибуираних чворова које је тешко напасти истовремено, односно срушити целу мрежу.

Међутим, у недавним истраживањима аутори [135][133] сугеришу да је мало блокова децентрализовано због високе концентрације или зависности у рударењу ограниченог броја учесника, као и базена великих размера где се спроводи рударење.

2. Отпорност на злоупотребу/непроменљивост

Још једна важна карактеристика блокчејна јесте та да је тешко променити или избрисати евиденцију о трансакцији (могуће путем „51% напада" или консензусом учесника). Свака модификација у блокчејну је видљива свима, па је готово немогуће неприметно извршити промену. Јавно-приватни кључеви или криптографски потписи такође осигуравају интегритет и потврду идентитета [136]. Систем трансакције у блокчејну базиран је на паровима јавних и приватних кључева који се генеришу око одређеног алгоритма за шифровање. Кључ додељује власништво оба пара кључева (јавни и приватни) ономе ко поседује приватни кључ. Блокчејн технологија спречава злоупотребе у смислу фалсификовања и порицања садржаја јер чува потпуну евиденцију у блоковима података у низу с временским ознакама, где се стари и нови блокови података не могу избрисати, а криптографски алгоритам онемогућује неовлашћено подметање података и смањује могућност преваре [17].

3. Транспарентност

Књига или блокчејн је доступан свим учесницима или унапред дефинисаном скупу учесника. У приватном или затвореном блокчејну, евиденција може бити ограничена на одређене учеснике, у јавном или отвореном блокчејну сви учесници имају иста права за приступ и/или ажурирање књиге према постојећем механизму консензуса. У овом последњем случају, све трансакције су транспарентне и видљиве. Ипак, транспарентни подаци у јавном блокчејну могу бити проблем када није требало да одређене информације буду јавно доступне или морају да буду измењене због грешака, нетачности или других проблема у уносу података [135]. Ово је тренутно једно од спорних питања – још увек нерешени компромис између транспарентности и приватности у јавним или отвореним блоковима.

4. Сигурност

У блокчејну је обезбеђен висок ниво сигурности, јер су трансакције које се одвијају анонимне. Свака трансакција или дигитални догађај који се одвија у блокчејн мрежи верификује се само ако је сагласан консензусом већине корисника који учествују у овом процесу [15].

Блокчејн технологија омогућава да се дигитална информација дистрибуира између свих чворова у систему. Тако сваки чвор одржава своју копију сваке релевантне информације и нема потребе за централним ауторитетом који контролише информације [135]. Контрола је такође дистрибуирана; помоћу механизама за валидацију сваки чвор може бити сигуран да је информација записана на блокчејну тачна. Ова технологија је настала за потребе дигиталне валуте биткоин, која је представљена 2008. године, а с радом је започела годину дана касније.

Количина поверљивих информација која се размењује је значајна, а начин на који се размењују и складиште није се много променио од деведесетих година прошлог века. Да би информације биле заштићене, систем за пренос и складиштење мора да поседује следеће карактеристике:

- информације се крећу кроз сигурну мрежу;
- информације се не смеју модификовати током ни након записивања;
- право коришћења дигиталних или материјалних добара везаних за информацију има само овлашћени корисник;
- брзина дељења информација мора бити што већа могућа;
- информације може једноставно прегледати било који заинтересовани корисник.

Блокчејн пружа максималну заштиту интегритета записа коришћењем криптографских метода. Записи су дистрибуирани, сваки чвор у систему поседује еквивалентне податке о томе шта је постигнуто алгоритмима за обезбеђење консензуса, од којих су познати *proof-of-work* и *proof-of-stake* алгоритам [137].

3.1.3 Процедуре и механизми консензуса

Блокчејн технологија омогућава да се очува стање успешности успостављања сервиса консензуса верификовањем и валидирањем одређене трансакције. Трансакције морају бити уписане у главну књигу по редоследу по којем се обављају, чак иако се извршавају између различитих учесника унутар мреже. У том случају, редослед трансакција мора бити успостављен, као и метода за одбијање „лоших" трансакција које се грешком чувају у главној књизи [138].

Механизми консензуса су пресудни у обезбеђењу валидности сваког блока, као и консензуса учесника у погледу сагласности с главном књигом и даљим одржавањем исте верзије главне књиге. Механизмима се уједно подстичу чворови да поступају искрено и стога су важније променљиве при дизајнирању блокчејна [137]. Једна од кључних карактеристика блокчејна јесу механизми консензуса који се користе за прикупљање сагласности. Договор између чворова у вези са „стањем" главне књиге од суштинске је важности за функцију књиге блокчејна. Тако, на пример, биткоин блокчејн користи консензус назван „доказ рада" (енг. *proof of work, PoW*), који захтева узајамно такмичење рудара у стварању и емитовању блокова ради добијања одобрења. Успех се награђује биткоинима [139]. Постоје и други механизми консензуса попут *Proof of Stake, Proof of Authority, Proof of Elapsed Time* и *Proof of Burn* – све су то

варијације средства помоћу којег се валидирају трансакције и осигурава мрежа, односно промене у главној књизи [140].

Постоје различити начини да се постигну и примене ови механизми, сваки са својим предностима и манама. На пример, *PBFT* (енг. *Practical Byzantine Fault Tolerance*) може обезбедити такав механизам да реплицирани фајлови могу комуницирати једни с другима, зарад одржавања константности сваке копије, чак и у случају корупције фајла. Алтернативно, одређивање редоследа у биткоин систему обавља се путем процеса назван „рударење", где се различити компјутери у мрежи „тркају" да први реше криптографске задатке који дефинишу редослед свих процеса [35].

На пример, *Hyperledger Fabric* је дизајниран тако да дозвољава креаторима мреже да одаберу механизам консензуса који ефикасније одражава везу која постоји између учесника. Постоји широк спектар потреба када се говори о приватности – од мрежа које су високо структуриране у смислу веза, до оних које су више *peer-to-peer*. Тренутни механизми консензуса *Hyperledger Fabric*-а јесу *SOLO* и *Kafka* [128].

У Табели 2 дата је упоредна анализа различитих консензус алгоритама.

Табела 2: Упоредна анализа различитих консензус алгоритама

Особине	***PoW***	***PoS***	***PBFT***	***DPOS***	***Ripple***	***Tendermint***
Управљање идентитетом чвора	отворен	отворен	контролисан	отворен	отворен	контролисан
Уштеда енергије	не	делимично	да	делимично	да	да
Толеранција	< 25% рачунарска снага	< 51% удео	< 33.3% неисправне реплике	< 51% валидатори	< 20% неисправни чворови у UNL	< 33.3% византијска гласачка снага
Пример	*Bitcoin*	*Peercoin*	*Hyperledger Fabric*	*Bitshares*	*Ripple*	*Tendermint*

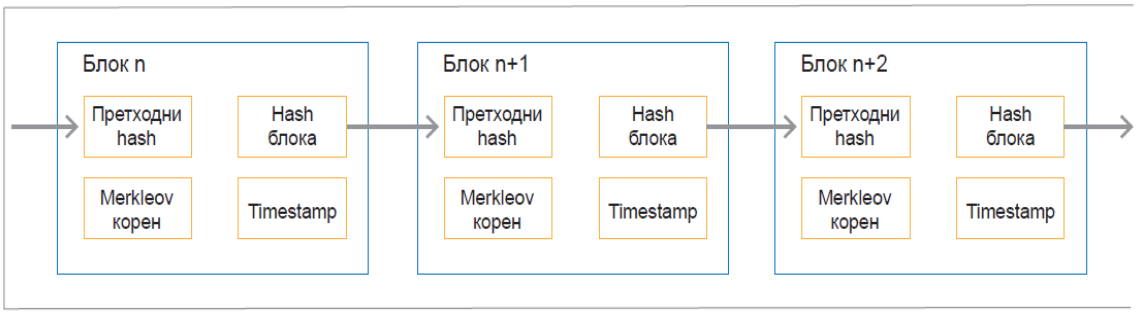
3.2 Структура блокчејна

Блокчејн технологија је настала за потребе дигиталне валуте биткоин, али су касније потенцијал те технологије препознале многе индустрије, нарочито финансијски сектор. Биткоин је коришћењем блокчејна и криптографских функција постигао сигурне трансакције дигиталног новца без централног ауторитета (банке). Овде блокчејн игра улогу главне књиге у којој је записана свака трансакција икад извршена у биткоин систему [141][134].

Основне карактеристике блокчејна су:

- Уобичајено је да је систем који користи блокчејн изграђен према моделу равноправних партнера (енг. *peer-to-peer*);
- Систем је у потпуности децентрализован, нема потребе за централним ауторитетом;
- Сваки нови запис је готово у реалном времену дистрибуиран између мноштва чворова;

- За идентификацију учесника у систему, потврду идентитета, доказивање аутентичности и у неким случајевима искоришћавање права за читање/писање користи се криптографија [135][131];
- Чворови система могу додавати податке у блокчејн;
- Чворови система могу читати податке из блокчејна;
- Блокчејн има развијен механизам који онемогућава промену на подацима који су једном уписани у блокчејн или у најмању руку омогућава лако откривање промена на подацима.



Слика 3: Структура блокчејна

Битна карактеристика блокчејна је и децентрализованост, што значи да су подаци сачувани преко *peer-to-peer* мреже. Такође, сваки чвор у децентрализованом систему садржи копију блокчејна. На тај начин се уклањају бројне опасности карактеристичне за централизован начин чувања података.

На следећој слици приказане су врсте блокчејн мреже.

Слика 4: Врсте блокчејн мреже

3.2.1 Структура блока

Блокчејн се, као што му само име говори, састоји од блокова. Блок је структура података у којој су записане дигиталне информације које се деле путем блокчејна. Један блок се састоји од заглавља у којем су уписани метаподаци те листе дигиталних информација варијабилне дужине (видети Табелу 3).

Табела 3: Структура блока

Величина	Назив	Опис
4 бајта	Величина блока	Величина блока у бајтовима
80 бајтова	Заглавље блока	Мета-подаци о блоку
1–9 бајтова	Бројач записа	Колико записа садржи блок
Варијабилно	Записи	Записи похрањени у блоку

3.2.2 Заглавље блока

Заглавље сваког блока састоји се од 80 бајтова података који служе као додатне техничке информације о блоку и повезивању блокова у ланац. Структура заглавља блока дата је у Табели 4.

Табела 4: Структура заглавља блока

Величина	Назив	Опис
4 бајта	Верзија	Верзија протокола у време настајања блока (специфично за биткоин)
32 бајта	Хеш претходног блока	Референца на претходни блок у ланцу који још називамо родитељ блока
32 бајта	Корен бинарног хеш стабла	Криптографски хеш који садржи информације о свим записима у блоку
4 бајта	Временска ознака	Време када је блок креиран и укључен у блокчејн
4 бајта	Тежинска ознака	Тежина алгоритма чије је решење потребно за укључивање блока у блокчејн
4 бајта	Nonce	Број помоћу којег је решен алгоритам за укључивање блока у блокчејн

3.2.3 Бинарно хеш стабло

Сваки блок у заглављу садржи поље под називом корен бинарног хеш стабла, који омогућава сажет приказ свих записа у блоку и једноставну проверу интегритета великог скупа података.

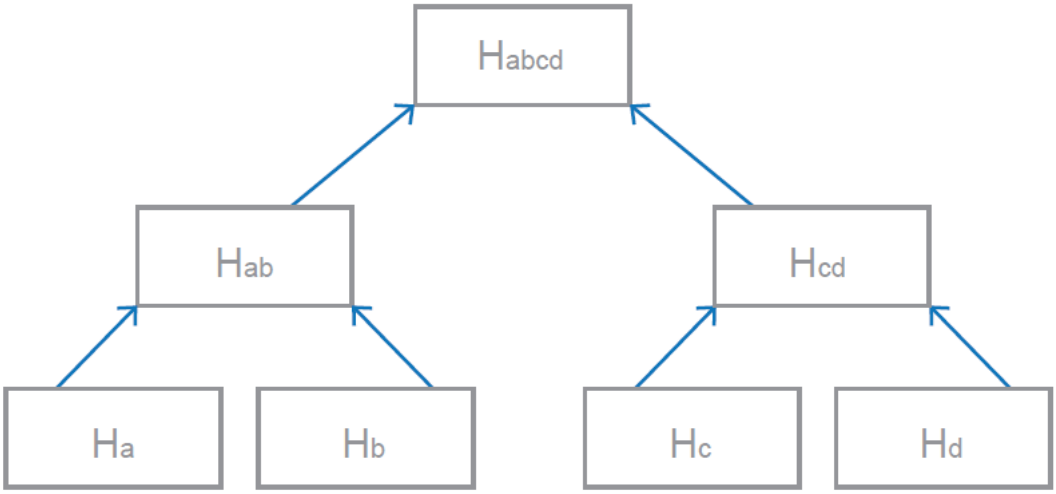
Бинарно стабло је коначан скуп података истог типа које зовемо чворови. При томе важи:

- Т је празан скуп (празно стабло) или
- постоји истакнути чвор р који зовемо корен од Т, а остали чворови граде уређени пар (ТЛ од *left*; ТР од *right*) дисјунктних бинарних стабала.

Бинарно хеш стабло је бинарно стабло у којем су листови, односно чворови без деце, хеш вредности неких података, а остали чворови су настали конкатенацијом хешева своје деце, те применом исте хеш функције на тај податак.

У биткоин систему листови бинарног хеш стабла су хешеви сваке поједине трансакције у блоку. Као хеш функција користи се *SHA-256* примењена два пута.

Меморисањем корена бинарног хеш стабла у заглавље блока добија се сажети приказ свих записа у блоку. Даље, ако се познаје тај сажети приказ, лако је одредити да ли неки запис припада блоку без увида у цели скуп записа [128][130].



Слика 5: Бинарно хеш стабло

Слика 5 приказује изградњу хеш стабла у случају да би у блоку биле записане четири трансакције, назовимо их *a*, *b*, *c* и *d*. Према структури бинарног хеш стабла, логично је да изградња тог стабла креће од дна према врху. Биткоин систем, као и сваки други систем који користи блокчејн технологију [135], има строго дефинисан формат података који се уписују у блокчејн, у овом случају трансакција. Међутим, у хеш стаблу нису записани ти подаци, већ хешеви тих података, па тако *Ha* добијамо на следећи начин:

$$Ha = SHA\text{-}256(SHA\text{-}256(a)).$$

Листове стабла *Hb*, *Hc* и *Hd* израчунавамо аналогно. Следећи корак је генерисање чворова родитеља листова:

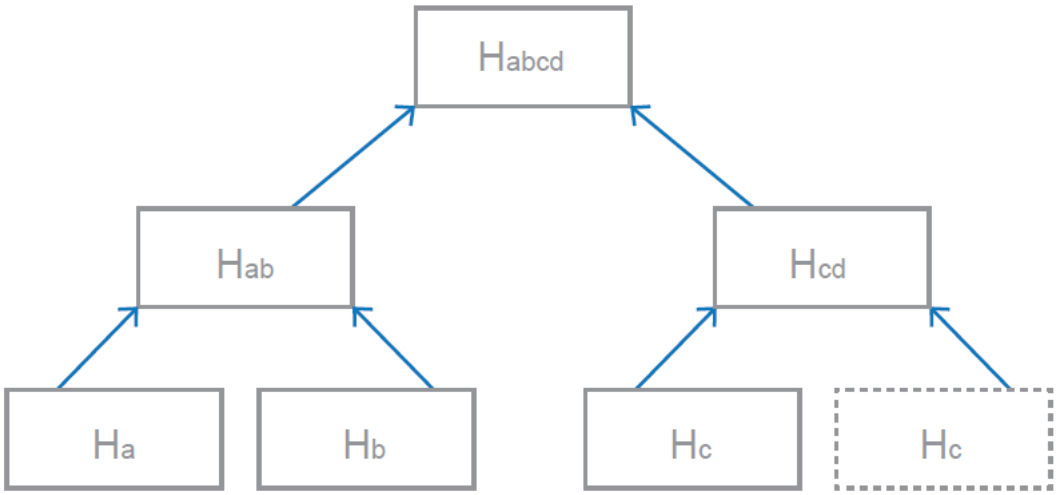
$Hab = SHA\text{-}256(SHA\text{-}256(Ha + Hb))$ i $Hcd = SHA\text{-}256(SHA\text{-}256(Hc + Hd))$, где оператор + представља конкатенацију стрингова.

Након тога можемо израчунати хеш који записујемо у корен стабла:

$$Habcd = SHA\text{-}256(SHA\text{-}256(Hab + Hcd)).$$

Идентичан алгоритам изградње бинарног хеш стабла користи се за било који парни број трансакција записаних у блоку. Ако је у блоку записан непаран број трансакција, тада једноставно удвостручујемо последњу трансакцију, као што Слика 6 приказује.

Напомињемо да је величина података записаних у корену стабла увек 32 бајта без обзира на број чворова.



Слика 6: Дуплирање трансакције у бинарно хеш стабло

Постоје чворови у систему који локално не меморишу читав блокчејн, већ само заглавља свих блокова. Хеширање и примена бинарних хеш стабала има двоструку улогу – омогућава проверу припадности записа блоку и лако утврђивање промене над подацима. Чвор који нема приступ целом блокчејну може одредити да ли одређени блок садржи неки запис познавањем само тог записа, односно његовог хеша и корена бинарног хеш стабла. То се одређује помоћу аутентификацијског пута у бинарном хеш стаблу. За сваки чвор бинарног стабла можемо одредити његов ниво [140]. Ниво се одређује из дефиниције која каже да је корен нивоа 1, а да су нивои деце неког чвора ниво *n* једнаке *n + 1*.

Аутентификацијски пут је коначан скуп А чворова бинарног хеш стабла *B*, за које важи [36][142]:

- за сваки ниво стабла *B*, осим за први, постоји тачно један чвор који припада скупу А;
- уз познавање још једног листа стабла *B* који не припада скупу *A* могуће је одредити корен бинарног хеш стабла *B*.

Бинарна хеш стабла наведеним чворовима омогућавају проверу интегритета података у блоку. Погледајмо хеш стабло са Слике 5 и замислимо да нападач на систем из неког разлога жели да промени трансакцију *b*. То би утицало на изглед хешева *Hb*, *Hab* и *Habcd*. Остали поуздани чворови који чувају копију блокчејна или само заглавља свих блокова могу лако утврдити да је дошло до промене над подацима у блокчејну.

3.2.4 Повезивање блокова

Блокове у ланцу можемо упоредити са страницама у овој докторској дисертацији. У заглављу сваке странице налази се име и број поглавља, а на дну број странице. Такви подаци из којих читамо додатне информације зову се метаподаци. Заглавље једног

блока у блокчејн структури садржи техничке информације о блоку, референцу на претходни блок и хеш свих података садржаних у блоку добијен коришћењем бинарног хеш стабла. Као и код докторске дисертације, тако и код блокчејна, ти подаци су важни за уређивање и организованост. Уколико би неко истргнуо све странице докторске дисертације, лако бисмо помоћу бројева страница закључили којим редоследом би требало да их читамо. Исто тако можемо одредити размештај блокова у ланцу помоћу референци на претходни блок [127][128].

Употребом хеш функција уместо временске ознаке или нумерисања добијамо и валидацију података. Свако ко има приступ подацима појединог блока или само заглављу тог блока може помоћу одређене криптографске функције одредити хеш тог блока. Тако, на пример, можемо два пута применити хеш функцију *SHA-256* на податке заглавља задњег доњег блока са Слике 7 и добијамо следећи хеш:

0000000000000000002046c0777217f1c155d834afe013e3c33acb8430117494a.

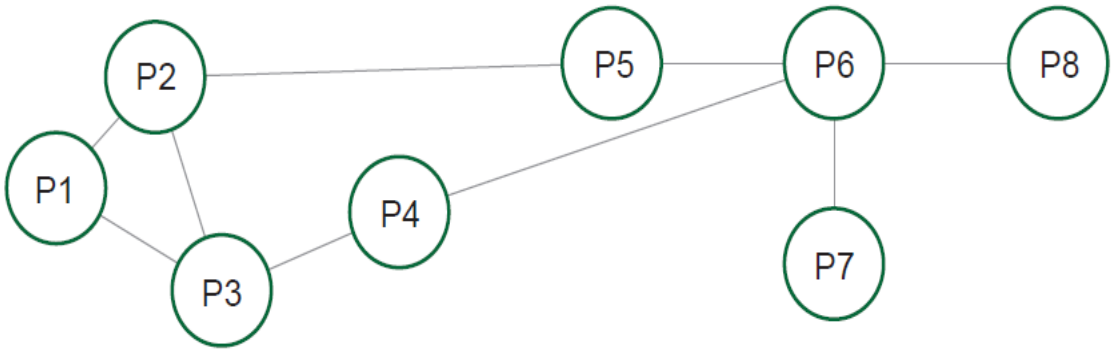
Блок који је касније настао похрањује хеш блока који је непосредно пре њега укључен у ланац. Ако хеш записан у блокчејну одговара хешу добијеном на поменути начин, сигурно је да су подаци у блоку конзистентни. Ако неко покуша измени податке, мора мењати и све хешеве од тог тренутка па надаље. Тиме би цели блокчејн изгледао потпуно другачије.

Слика 7: Повезивање блокова

Слика 7 приказује три блока у биткоин блокчејну под бројем 442226, 442227, 442228. Сви су настали у *биткоин* верзији 2, што није од велике важности за тему овог рада [143][127].

3.2.5 Централизовани систем равноправних партнера

Систем равноправних партнера, односно систем грађен према моделу равноправних партнера (енг. *peer-to-peer*), састоји се од великог броја истоврсних процеса, такозваних партнера (енг. *peer*). Партнери обављају задатке према потребама својих корисника. Ако је партнеру при обављању неког задатка потребна помоћ, он ступа у комуникацију са својим комшијама, а они са својим, па се тако комуникација одвија на нивоу целог система. Такви системи могу се, према структури, поделити на централизоване и децентрализоване. Централизовани системи су они код којих постоји сервер. Улога сервера је да повеже клијенте како би они могли да наставе међусобну комуникацију. Главна карактеристика децентрализованих система јесте та што не постоји истакнути сервер. Архитектуру децентрализованог система можемо видети на Слици 8 [127][130].



Слика 8: Архитектура система грађеног према моделу равноправних партнера

Системи који користе блокчејн технологију спадају у децентрализоване системе равноправних партнера. Тиме је омогућена размена података кроз рачунарску мрежу, при чему чворови преузимају информације једни од других, уместо с једног централног сервера.

Уопштено, систем равноправних партнера пружа високоефикасан и јефтин начин да велики број корисника дође до неке датотеке, а трошкови такве комуникације постају релативно мали и деле се међу корисницима.

У склопу блокчејн технологије, један партнер у принципу ради на рачунару једног корисника. Постоје четири задатка које партнер може обављати. То су: *новчаник* (енг. *wallet*), *мрежно усмеравање* (енг. *network routing*), *рударење* (енг. *mining*) и *одржавање блокчејна* (енг. *blockchain maintenance*).

На Слици 9 приказана је врста партнера у блокчејн систему на основу задатака које партнер обавља.

Слика 9: Врсте партнера у блокчејн систему

У приватном блокчејн систему, по правилу, сваки партнер обавља сва четири задатка, док у јавним блокчејн системима разликујемо партнере према задацима које обављају. То су следеће врсте партнера: *потпуни партнер*, *рудар, једноставни новчаник*, *блокчејн партнер* [130][127].

Као што је приказано на Слици 9, све врсте партнера обављају задатак мрежног усмеравања. Разлог томе је потреба сваког партнера за успостављањем и одржавањем веза с неким од осталих партнера у моделу равноправних партнера. Исто тако, сваки од партнера који учествује у систему задужен је за валидирање и дифузију (енг. *broadcast*) нових записа и нових блокова. У следећим потпоглављима објашњене су улоге блокчејн партнера, једноставног новчаника и рудара. Потпуни партнер може обављати све улоге осталих партнера.

3.2.6 Блокчејн партнер

Блокчејн партнер одржава блокчејн са свим записима, почев од првог блока који се назива генерички блок, на који се надовезују сви остали блокови, све до последње креираног. За разлику од једноставног новчаника, блокчејн партнер нема потребе да се ослони на остале партнере ради претраживања блокчејна или провере интегритета података. Ако је реч о запису трансакција у блокчејн, блокчејн партнер, ради валидације нове трансакције, има могућност да провери да ли средства која корисник жели да потроши у новој трансакцији заиста припадају том кориснику [28][144]. То ће урадити тако што ће повезати нову трансакцију са свим пређашњим трансакцијама тог корисника све до генеричког блока. Такав партнер ослања се на остатак мреже само

како би у реалном времену примио новокреиране блокове, које након тога верификује и надовезује на своју локалну копију блокчејна.

3.2.7 Блокчејн новчаник

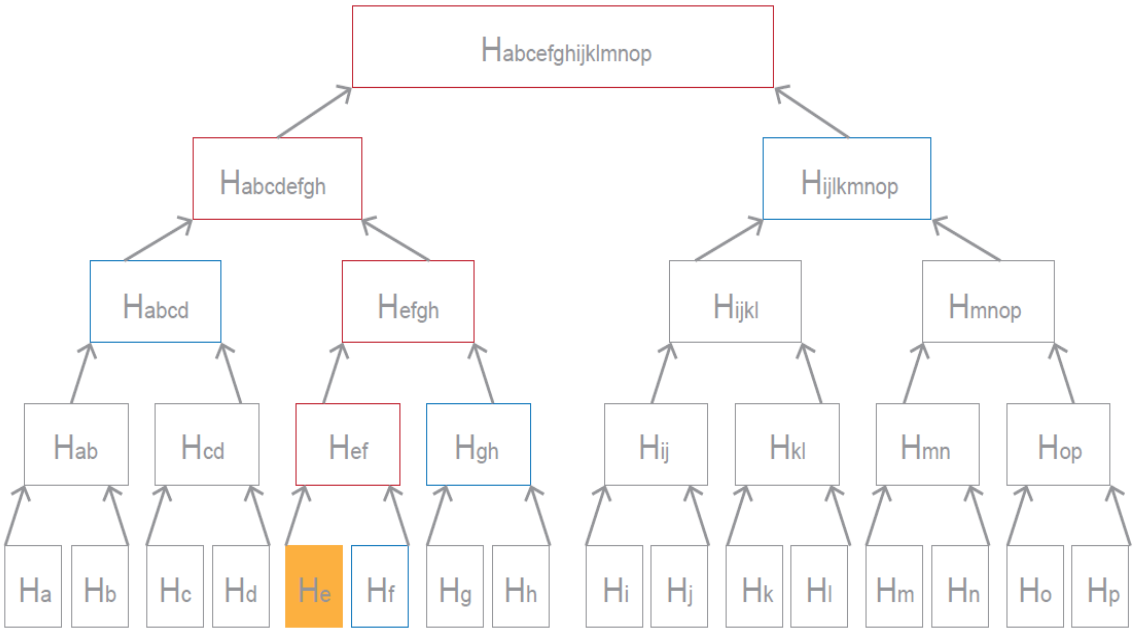
У јавним системима који користе блокчејн, због велике количине података, сваки корисник нема могућност да меморише цео блокчејн. Такав корисник тада у систему учествује као једноставан новчаник и на Слици 9 препознајемо га по томе што међу својим задацима нема црвени круг под називом одржавање блокчејна. Главни задатак једноставног новчаника јесте креирање нових записа у складу с протоколом који прописује систем. Ради потврде власништва над дигиталним новцем или неком другом дигиталном информацијом чији интегритет желимо заштити меморисањем на блокчејн, новчаници меморишу парове јавних и приватних криптографских кључева [145].

Из јавног кључа се генерише адреса која служи за примање новца од осталих корисника, аналогно броју банковног рачуна. Приватни кључеви су потребни за приступ адреси и новчаним средствима. Њих можемо упоредити с личним идентификационим бројем (енг. *pinom*) банковног рачуна и, за разлику од адреса, није препоручљиво делити их са остатком система. Како је већ речено, сви партнери у систему обављају валидацију и дифузију нових трансакција и блокова. Како једноставни новчаник сам не садржи запис о свим претходним трансакцијама, он спроводи такозвану поједностављену методу верификације [146][147].

Поједностављена метода верификације подразумева меморисање само заглавља блокова уместо целог блокчејна са свим записима. Будући да немају пуну слику трансакција које су се догодиле пре оне коју желе да валидирају, ослањају се на остале партнере који им на њихов захтев могу пружити увид у део блокчејна. Једноставни новчаници проверавају дубину трансакција. Блокчејн партнер који конструише ланац прећашњих трансакција враћа се временски у прошлост, што према структури и начину повезивања ланаца у блок подразумева да иде у висину [147].

Према поједностављеној методи верификације, једноставни новчаници верификују ланац свих блокова без трансакција, што могу да ураде с обзиром на то да имају локално меморисана заглавља блокова. Након тога, верификовани ланац повезује с трансакцијама. Како би се успоставила веза између трансакције и блока у којем је та трансакција записана, користи се пут у бинарном хеш стаблу. Када једноставни новчаник открије у којем се блоку налази трансакција коју жели да валидира, он чека да рудари обаве свој посао и додају још шест блокова у блокчејн како би био сигуран да је остатак мреже потврдио да се не ради о несигурној трансакцији [148][134][135].

Бинарно хеш стабло проверава партнерима новчаницима којем блоку припада одређена трансакција (Слика 10). У блок, чије је бинарно хеш стабло приказано на Слици 10, записано је 16 трансакција и једноставни новчаник жели да провери да ли трансакција *e* припада том блоку. Будући да познаје садржај трансакције *e*, партнер лако може да одреди припадни *хеш He*. Да би проверио припадност трансакције блоку, потребно је да прими од неког од својих суседних партнера који одржавају целу копију блокчејна хешеве *Hf, Hgh, Habcd* и *Hijklmnop*. Ти су хешеви на Слици 10 означени плавим правоугаоницима и називају се *аутентификацијски пут.* Након што једноставни новчаник добије аутентификацијски пут, може израчунати хешеве *Hef, Hefgh, Habcdefgh* и коначно корен бинарног хеш стабла *Habcdefghijklmnop* означене црвеним правоугаоницима на описани начин. Партнер тада упоређује израчунати корен стабла с кореном бинарног хеш стабла записаног у заглављу блока. Ако се ти подаци подударају, трансакција *e* припада блоку са Слике 10.



Слика 10: Пут у бинарном стаблу тражења у сврху потврде припадности трансакције блоку

Уочљиво је да у овом случају једноставни новчаник требало да израчуна само четири хеша за проверу припадности трансакције блоку у којем је записано 16 трансакција. Уопштено, ако је *N* број трансакција записаних у блок, тада је потребно *log2 N* хешева, од којих је сваки величине 32 бајта. У биткоин блокчејну сваки блок садржи неколико хиљада трансакција. Узмимо за пример неки блок који садржи 2048 трансакција. Величина тог блока тада је отприлике 512 килобајта. Провера припадности трансакције том блоку тада изискује log2 2048 = 11 хешева величине 32 бајта, дакле укупно 352 бајта. Из овог примера видимо да бинарна хеш стабла омогућавају велику просторну уштеду, уз могућност провере интегритета података.

3.2.8 Рудар

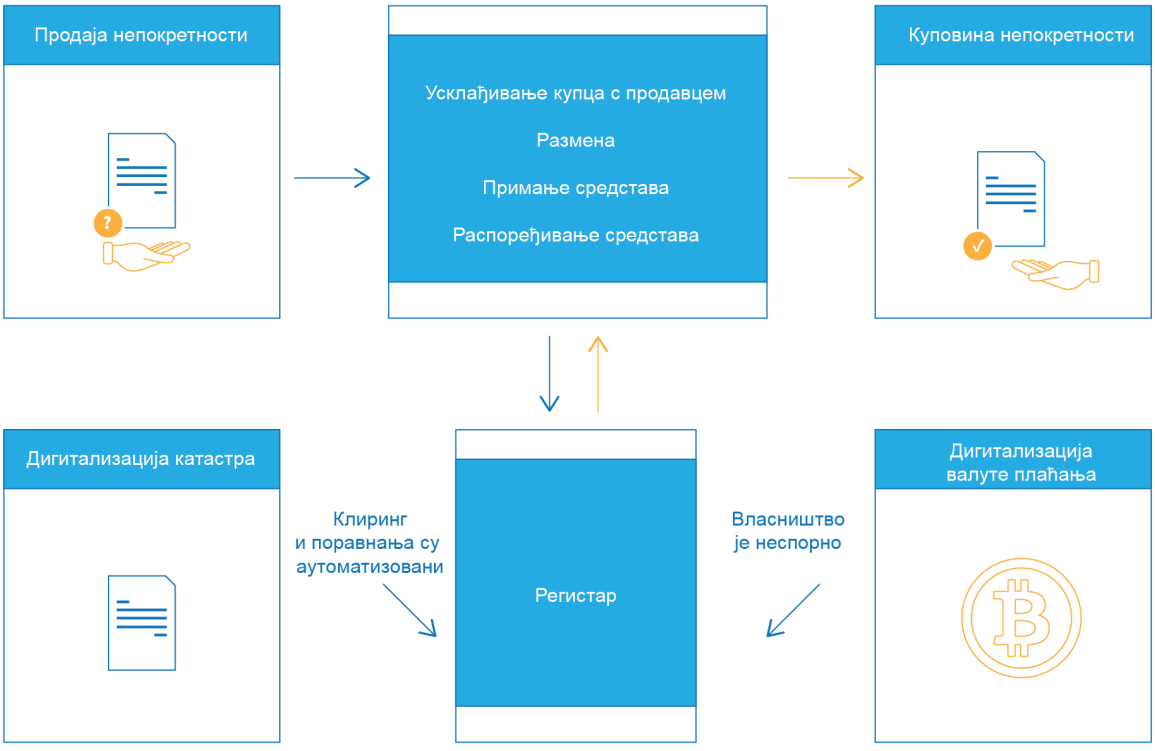
Партнери рудари преузимају нове записе које су креирали новчаници, формирају их у блокове и додају у блокчејн. У биткоин протоколу, додавање нових записа изискује коришћење рачунарских ресурса. Када рудар дода блок у блокчејн, решавајући алгоритам под називом *proof-of-work* и користећи своје рачунарске ресурсе, тада све трансакције у том блоку постају потврђене, а рудар за награду добија одређени број нових биткоина [134].

3.3 Паметни уговори

Паметни уговори су рачунарски програми који су способни да изврше услове из споразума између страна без потребе за људском координацијом или интервенцијом [149]. Ти споразуми могу бити забележени и потврђени у блокчејну, а затим уговори аутоматски извршени, обично према упутствима „ако – тада”. На тај начин, паметни уговор омогућава уговорним странама да изврше поуздану трансакцију без посредника. Услови паметних уговора више нису правно обавезујући, већ су обавезујући

алгоритмом. Аутори постављају питање погрешног назива за паметне уговоре, у смислу да паметни уговори нису ни „паметни", односно способни за превођење сложених правних споразума у софтвер, нити „уговори" јер немају законске основе [133]. Паметни уговори су изводљиви или применљиви под ограниченим и строгим условима. Проблем може настати у могућности креирања система правила, кроз паметне уговоре, као врсту аутоматизованих приватних регулаторних оквира, а који могу избећи правила одређених јурисдикција и деловати транснационално [150][151].

Паметни уговор представља кôд у неком програмском језику који олакшава размену новца, некретнина, деоница или било каквих вредности. Паметни уговори служе за регулисање неког пословног односа између странака међу којима не постоји узајамно поверење. Такав кôд се може записати на блокчејн и извршавати на било којем рачунару у дистрибуираној мрежи. Паметан уговор се аутоматски извршава када су задовољени специфични услови. Због чињенице да је кôд паметног уговора записан на блокчејну, извршавање се одвија без икакве могућности цензуре, преваре или уплитања треће стране. Можемо рећи да блокчејн на којем су паметни уговори представља дистрибуирани оперативни систем. Имовина или валута преноси се у програм. У тренутку извршавања програма он аутоматски препознаје стање у којем се систем налази [134][133]. Такође, када више особа затражи трајно или привремено власништво над тим вредностима, програм одређује коме треба оне да припадну. У случају да нико не задовољава услове, вредности се враћају почетном власнику. У међувремену, нека врста документа у којем је записана одлука програма смешта се у блокчејн, који му даје одређену сигурност и непроменљивост.



Слика 11: Паметни уговор

Слика 11 приказује процес креирања паметних уговора:

1. Могућа размена добара између два (или више) партнера записује се као програмски кôд и смешта се на блокчејн. Партнери остају анонимни, међутим садржај паметног уговора јавно је доступан свим партнерима у систему;

2. Варијабле попут датума или одређене количине новца подстичу извршавање уговора према правилима дефинисаним у коду;
3. Остали корисници система могу претражити блокчејн како би разумели активности дефинисане уговором или проверили резултат извршавања уговора.

Пример употребе паметног уговора може се илустровати у случају изнајмљивања апартмана. Претпоставља се да особа Б жели гостовати у апартману који изнајмљује особа А. Особа Б може трансакцијом уписаном у блокчејн платити своту потребну за изнајмљивање апартмана. Тако добија дигитални рачун који је садржан у виртуалном уговору између те две странке. Особа А тада шаље особи Б дигитални кључ, који ће особи Б бити на располагању од договореног датума. Ако особа Б не прими кључ на време, кôд који садржи паметни уговор аутоматски враћа уплаћена средства. Ако особа А прерано пошаље кључ, функција унутар програма га чува до датума када је договорено изнајмљивање. Заједно с кључем функција чува и накнаду у криптовалути коју исплаћује особи А када особа Б прими кључ. Кôд је записан у блокчејн који одржава на хиљаде партнера у систему и особа Б не мора бринути о томе да ће доћи до грешке или преваре. Такође, особа А може бити сигурна да ће јој услуга изнајмљивања бити плаћена ако пошаље кључ. Уговор се аутоматски искључује након договореног времена, а кôд не може променити нико од учесника без знања другога – сви ће учесници бити истовремено упозорени о променама [152][134][153].

На примеру изнајмљивања апартмана види се само једна могућност коришћења паметних уговора. Још неки случајеви у којима се користе или постоји могућност да ће се у будућности користити паметни уговори јесу:

- аутоматизација система гласања, где блокчејн технологија може помоћи при веродостојности целог система;
- клиничка истраживања која спроведене више институција, уз заштиту личних података испитаника;
- праћење удела власништва и инвестиција од стране компаније која ради на пројекту у који средства улажу страни улагачи;
- аутоматизација исплате и враћања кредита, као и праћење камата итд.

У комбинацији с другим технологијама добијамо још ширу примену паметних уговора. На пример, можемо аутоматизовати осигурање возила и омогућити готово тренутну исплату осигуравајуће куће оштећеном клијенту. У случају незгоде, исплата би се вршила на темељу података прикупљених од сензора који прате параметре стања возила у паметним аутомобилима.

Пример:

Chaincode може бити имплементиран у више програмских језика. Уговори у Солидити (енг. *Solidity*) слични су класама у објектно оријентисаним језицима. Сваки уговор може да садржи [154]:

1. Варијабле стања (енг. *State Variables*). Промењљиве чије се вредности трајно чувају у складишту уговора;

```
contract SimpleStorage {
   uint storedData;
}
```

2. Функције. Извршне јединице кода у оквиру уговора;

```
contract SimpleAuction {
    function bid() public payable {
    }
}
```

3. Модификатори функција (енг. *Function Modifiers*). Могу се користити за измену семантике функција на декларативни начин;

```
contract Purchase {
    address public seller;

    modifier onlySeller() { // Modifikator
        require(
            msg.sender == seller,
            "Only seller can call this."
        );
        _;
    }

    function abort() public view onlySeller { // Upotreba modifikatora
        // ...
    }
}
```

4. Догађаји (енг. *Events*). Наследни чланови уговора. Позивање узрокује да се аргументи чувају у евиденцији трансакције – посебној структури података у блокчејну;

```
contract SimpleAuction {
    event HighestBidIncreased (address bidder, uint amount); // Događaj

    function bid() public payable {
        // ...
        emit HighestBidIncreased(msg.sender, msg.value); // Pozivanje događaja
    }
}
```

5. Структурни типови (енг. *Struct Types*). Структуре су прилагођени типови који могу да групишу неколико променљивих;

```
contract Ballot {
    struct Voter { // Struct
        uint weight;
        bool voted;
        address delegate;
        uint vote;
    }
}
```

6. Енуми (енг. *Enum Types*). Енуми се могу користити за креирање прилагођених типова с коначним скупом „константних вредности”. Експлицитно су конвертибилни у све целобројне типове и из свих целобројних типова, али имплицитна конверзија није дозвољена.

```
contract Purchase {
   enum State { Created, Locked, Inactive } // Enum
}
```

Приватне функције и варијабле стања видљиве су само у уговору у коме су дефинисане, а не и у изведеним уговорима. Све што је унутар уговора видљиво је свим посматрачима изван блокчејна. Функција *private* спречава да други уговори читају или мењају информације, али и даље ће бити видљиви целом свету изван блокчејна [133].

Када се уговор креира, његов конструктор (функција декларисана кључном речи *constructor*) извршава се једном. Конструктор није обавезан, али је дозвољен само један конструктор. Након извршења конструктора, коначни кôд уговора распоређује се у блокчејн. Овај кôд укључује све јавне и екстерне функције и све функције до којих се одатле може доћи њиховим позивом. Постављени кôд не укључује кôд конструктора или интерне функције које се позивају само из конструктора.

Ако се уговором жели створити други уговор, креатор мора да зна изворни кôд (и бинарни облик) креираног уговора. То значи да су цикличне зависности немогуће. Могуће је уговор наследити из других уговора.

3.4 Консензус алгоритми

Усаглашавање око стања блокчејна спада у категорију проблема који је у рачунарству познат под називом проблем усаглашавања византијских генерала. У овом поглављу описан је тај проблем и познати алгоритам за постизање консензуса у синхроној мрежи. Такође, описана су два алгоритма помоћу којих системи који користе блокчејн могу решити наведени проблем.

3.4.1 Проблем усаглашавања византијских генерала

У дистрибуираним системима могу настати различите грешке у раду процеса. Те грешке можемо поделити у три групе:

- престанак рада процеса;
- пропуст у раду процеса;
- византијска грешка.

Византијска грешка представља тежи облик грешке. Процес греши тако што се понаша сасвим непредвидиво. Може да прекине рад, опет га настави, да пропушта слање или примање порука, погрешно рачуна, шаље корумпиране поруке. Познатији проблем постизања консензуса у дистрибуираном систему уз присуство византијских грешака јест проблем усаглашавања византијских генерала [133].

Следи неформални опис тог проблема. *N* војних јединица окружује један дворац у намери да га нападну. Сваку војну јединицу предводи по један генерал, а постоји и

један водећи генерал, односно краљ. Унутар дворца налази се непријатељска војска која брани дворац. Циљ је постизање договора између N генерала о времену напада на дворац. Будући да се овај сценарио одвија у доба када нема мобилних телефона и могућности да генерали позову једни друге, они договарају време напада слањем порука које преноси гласник на коњу. Неки од генерала су издајице и њихова војна јединица бори се на страни непријатељске војске. Постоји највише f од N генерала који су издајници. Остали генерали не знају који су генерали издајници и немају начин да то сазнају. Војне јединице лојалних генерала довољно су јаке да преузму дворац, али уз услов да су њихове акције координиране и да све јединице у исто време крећу у напад. Нека се, на пример, унутар дворца налази 300 војника и нека дворац окружује пет војних јединица са по 100 војника. Једино је генерал који води 3. војну јединицу издајник, назовимо га Г3. Према томе, генерали Г1, Г2, Г4 и Г5, односно вође 1, 2, 4. и 5. војне јединице лојални су краљу. Када би сви лојални генерали напали дворац у исто време, њихових 400 војника имало би шансе да поразе војску од 300 војника која брани дворац, чак и у случају да се одбрамбеној војсци придружи 100 војника генерала Г3. Циљ генерала Г3 је избећи исто време напада свих лојалних војних јединица, што може лако постићи. Размотрите следећи низ догађаја:

1. Г1 шаље поруку „Напад у 16 сати" према Г2;
2. Г2 шаље ту исту поруку „Напад у 16 сати" према Г3;
3. Г3 је издајица, он мења садржај поруке у „Напад у 15 сати" и шаље је према Г4;
4. Г4 шаље поруку „Напад у 15 сати" према Г5.

Након размене порука, генерали Г4 и Г5 нападају дворац са 200 војника у 15 сати, надајући се да ће им се остатак војске придружити. Будући да су генерали Г1 и Г2 уверени да ће се напад одржати у 16 сати, њихове војне јединице не прикључују се нападу у 15 сати. Војна јединица генерала издајника може се у било којем тренутку прикључити војсци бранилаца, тада укупно 400 војника брани дворац. Двеста војника генерала Г4 и Г5 у 15 сати нема шансе против војника који бране дворац и они губе битку. Такође, у 16 сати 200 војника из 1. и 2. војне јединице губе битку од бројчано моћније војске бранилаца.

Ако посматрамо систем који користи блокчејн технологију у терминима пре описаног проблема, партнери у дистрибуираном систему представљају генерале. Дигитални подаци које желимо уписати у блокчејн јесу поруке међу генералима [152][137]. Блокчејн има улогу меморисања договореног времена напада. Појединi партнер не зна број осталих партнера, као ни који су партнери издајници. Издајницима је у интересу да у блокчејн упишу податке који нису истинити. Алгоритми за постизање консензуса омогућава партнерима да у оваквим условима буду сигурни да су подаци који се уписују у нове блокове тачни, те да су подаци који су пре записани у блокчејн истинити и непромењени.

3.4.2 Лампоров алгоритам

Лампоров алгоритам је такође познати алгоритам за постизање консензуса у синхроној мрежи. У овом случају, ради једноставности, посматрамо ситуацију када се генерали договарају око одлуке о нападу или повлачењу. Тако је потребно постићи консензус око варијабле величине једног бита. Треба напоменути да се генерали договарају о времену напада, које се може приказати варијаблом типа *integer*, тада би било потребно постићи договор око сваког од 32 бита те варијабле. Проблем усаглашавања византијских генерала захтева да обликујемо алгоритам помоћу којег сви

лојални генерали бирају исту акцију. Генерале поистовећујемо с партнерима или чворовима у систему [137][143]. Лампортов алгоритам се састоји од $f + 1$ корака, од којих се сваки корак дели на три фазе. f је број генерала издајника, а N укупан број генерала. Овај алгоритам захтева да је $N > 4f$. Сваки партнер има свој предлог одлуке (0 или 1) који се може променити у сваком кораку, а иницијализован је неком улазном вредношћу. На крају алгоритма, сви лојални партнери имаће усаглашене предлоге одлуке. Алгоритам је заснован на ротирајућем координатору краљу. Током корака k, улогу краља игра партнер Pk. Фазе сваког корака су следеће:

1. Сваки партнер шаље свој предлог одлуке свим другим партнерима. Партнер свој предлог и примљене предлоге других партнера записује у локално поље $V[\ ]$, тако да $V[j]$ садржи предлог од Pj.
2. Краљ обликује свој краљевски предлог тако да пронађе већинску вредност у локалном пољу $V[\ ]$ или тако да уважи подразумевану ако нема већине. Краљ шаље свој предлог свим другим партнерима. Партнери чувају краљев предлог у локалним варијаблама *kingValue*.
3. Сваки партнер обликује свој нови предлог одлуке и спрема га у локалну варијаблу *myValue*. Нови предлог одлуке је или већинска вредност из локалног $V[\ ]$ или краљев предлог из *kingValue*. Партнер се одлучује за локалну вредност из $V[\ ]$ ако се она појављује у $V[\ ]$ на више од $N = 2 + f$ места, иначе се одлучује за *kingValue*. На крају треће фазе партнер уписује израчунати *myValue* на одговарајуће место у локално поље $V[\ ]$, тако да би послужио као иницијални предлог одлуке у идућем кораку.

Овим алгоритмом можемо постићи договор између генерала Г1, Г2, Г3, Г4 и Г5 из претходног примера, али само зато што је познато да је један генерал издајник, односно $f = 1$, док је $N = 5$ и важи $5 > 4 \cdot 1$.

3.4.3 *Proof-of-work*

Proof-of-work алгоритам настао је у склопу криптовалуте биткоин и своди се на решавање криптографског проблема у заглављу блока. Проблем решавају партнери рудари користећи рачунарске ресурсе у процесу који се назива рударење (енг. *mining*) и тиме укључују нови блок у блокчејн. Процес рударења подразумева тражење броја *nonce* помоћу којег ће рудар, заједно с осталим подацима из блока, израчунати хеш који задовољава одређене критеријуме. Рудари се међусобно такмиче у томе ко ће први израчунати такав хеш. Онај рудар који то успе шаље нови блок дифузијом кроз систем и бива награђен за свој рад. Критеријуми се могу мењати с обзиром на време које је било потребно да се претходни блокови укључе у ланац како би се постигао једнак размак између додавања нових блокова [138][146].

Поставља се питање која је улога *proof-of-work* алгоритма и коришћења рачунарских ресурса при додавању нових блокова. Када за додавање новог блока у ланац не би било потребно спроводити *proof-of-work* алгоритам, тада би најбржи рачунар у мрежи увек могао додати нови блок и послати га осталим партнерима. То би значило да цео процес више није децентрализован и да тачност података које записујемо у блок зависи од једног или неколико партнера из мреже. Израчунавање хешева с различитим вредностима броја *nonce* служи као доказ да рудар активно учествују у обради нових записа и проналажењу решења за блок у који се ти нови записи складиште [146][147].

Биткоин систем захтева да излазни хеш *proof-of-work* алгоритма буде мањи од броја или једнак броју који се назива циљ. Чињеницу да је хеш мањи од броја циљ можемо интерпретирати и тиме да хеш започиње одређеним бројем нула. Циљ се израчунава из тежинске ознаке записане у заглавље блока и аутоматски се прилагођава како би се осигурало да време потребно за прихватање блока буде отприлике десет минута. Тренутни циљ се добије као количник почетног или базног циља који износи

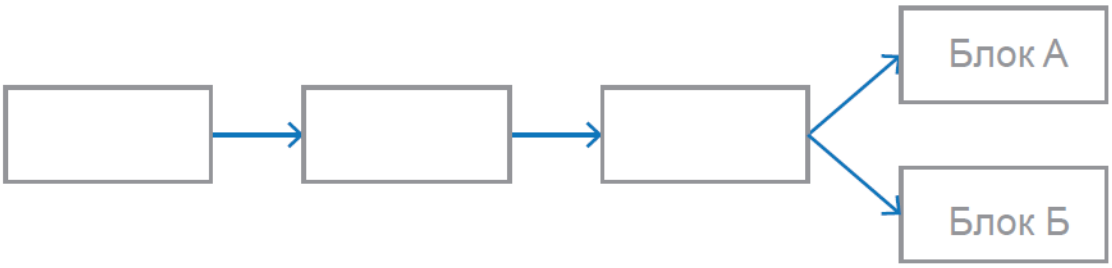
00000000FFFF0000000000000000000000000000000000000000000000000000 и тежине записане у заглављу блока.

Алгоритам *Proof-of-work* једноставно можемо описати следећим корацима:

1. Скупи нове трансакције и креирај нови блок;
2. Одабери број *nonce*;
3. Израчунај хеш заглавља новог блока и броја *nonce*;
4. Провери да ли је хеш из корака (3) мањи од тренутног броја циљ. Ако да, пошаљи нови блок осталим партнерима у систему. Ако не, врати се на корак (2).

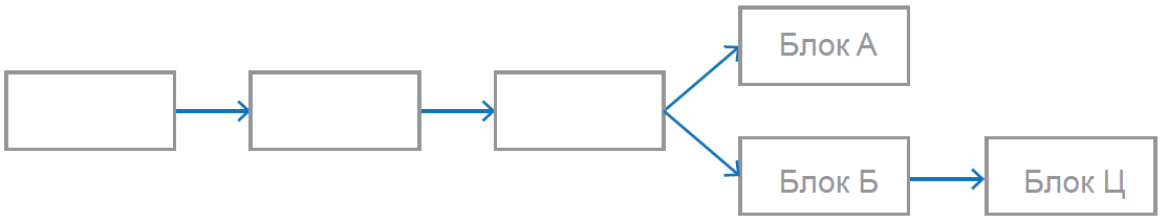
3.4.4 Рачвање у блокчејну

Замислимо ситуацију када два рудара, назовимо их Р1 и Р2, у релативно кратком периоду израчунају задовољавајући хеш. Нека је Р1 израчунао задовољавајући хеш за блок који ћемо назвати БлокА, а Р2 за БлокБ. Релативно кратко временско раздобље значи да рудар који је први нашао решење алгоритма *proof-of-work* није стигао да обавести остале партнере у систему да је ова рунда додавања блока готова и да други рудари могу почети да раде на додавању новог блока. Рудар Р1 тада шаље БлокА кроз мрежу, док рудар Р2 шаље БлокБ. Неки партнери ће прво добити нови блок рудара Р1, тј. БлокА, и додати га у своју локалну копију блокчејна, док ће други додати БлокБ, за који је решење алгоритма *proof-of-work* нашао рудар Р2. Након неког времена партнери у систему ће примити и блок другог рудара и тада долази до рачвања у блокчејну.



Слика 12: Рачвање у блокчејну

У таквој ситуацији сви партнери у систему прате оба ланца, будући да су оба блока добијена решењем алгоритма *proof-of-work* и оба су правилни блокови. Ти блокови у ланцу тада имају истог родитеља, као што је приказано на Слици 12, али рудари раде на оној грани блокчејна на којој се налази блок који су први прихватили. Тако отприлике пола партнера рудара покушава додати нови блок на БлокА, а друга половина на БлокБ. Претпоставимо да је рудар Р3 успео додати блок под називом БлокЦ на БлокБ као на Слици 13.



Слика 13: Додавање блока након рачвања

Сви партнери у систему придржавају се такозваног правила најдужег ланца. Дужина ланца зависи о тога колико је рада на алгоритму *proof-of-work* потрошено на креирање ланца, што се добије сумом тежинских ознака блокова који чине тај ланац. Присетимо се, тежинске ознаке блокова записане су у заглављу блока, па сваки партнер може израчунати дужине ланаца. Након што партнери приме вест о томе да је рудар Р3 додао нови блок, тада доњи ланац са Слике 13, односно ланац који садржи БлокБ и БлокЦ, постаје најдужи. Рудари који су досад радили на продужавању тог ланца то настављају чинити и даље. Остатак рудара због правила најдужег ланца мора одбацити БлокА и наставити на изградњи истог линеарног ланца. Записи на Блоку А игноришу се и не сматрају се делом блокчејна.

У биткоин систему, због рачвања и чињенице да неке трансакције могу бити записане на краћем ланцу и тиме одбачене након неког времена, постоји правило да је трансакција исправна ако су задовољена следећа два услова:

- Трансакција је записана на најдужем ланцу у блокчејну;
- Након блока у којем је записана трансакција додато је још пет блокова у блокчејн.

Могуће је да су трансакције које су биле записане у блоку који је одбачен већ уписане у блокчејн, у блок који је настао отприлике у исто време као и одбачени. Ако то није случај, биће записане након неког времена, јер су партнери рудари примили те трансакције и оне се налазе међу кандидатима за нови блок.

3.4.5 *Proof-of-stake*

Proof-of-stake је још један алгоритам за постизање консензуса, односно договора о тренутном стању блокчејна међу партнерима у дистрибуираном систему. Настао је од криптовалута које су конкуренција биткоину, нешто касније од алгоритма *proof-of-work*. Многи информатички стручњаци који се баве проучавањем криптовалута као велику замерку алгоритма *proof-of-work* наводе велику потрошњу рачунарске снаге и могућност рударења такозваних спољних партнера. Под тим се подразумева партнер који не учествује у стварању записа у блокчејну, већ само поседује довољно добар рачунар да би могао бити конкурентан у стварању нових блокова. Алгоритам *proof-of-stake* покушава да елиминише ту слабост сужавањем круга партнера који имају право генерисања нових блокова и мањом тежином алгоритма хеширања коју ти партнери морају задовољити кôд генерисања новог блока. Постоји више начина на који се одређује ко има право да укључује нови блок у блокчејн. Овде је описан начин који користи дигитална криптовалута пиркоин (енг. *Peercoin*). Док *proof-of-work* подразумева коришћење рачунарске снаге како би се додао нови блок у блокчејн *Proof-*

of-stake, алгоритам омогућава креирање новог блока оним корисницима који поседују одређену количину новца у систему. Као и у случају алгоритма *proof-of-work*, валидатори се такмиче ко ће први израчунати задовољавајући хеш. Генерисање новог блока укључује слање пиркоина самом себи како би се доказало да валидатор поседује одређени износ новца.

Важна величина која се користи у пиркоин систему јесте старост новца. Старост новца једноставно је дефинисана као резултат множења количине новца и дана који тај новац стоји у новчанику партнера непотрошен. Ако неки партнер у систему поседује 80 пиркоина које није потрошио у протеклих десет дана, тада је старост тог новца 800 дана. У тренутку када партнер уплати тај новац неком другом партнеру у систему (или сам себи), кажемо да је старост новца уништена, односно старост је једнака 0. Како би се лакше утврдила старост новца, свака трансакција у пиркоин систему мора садржавати време извршења.

Код алгоритма *proof-of-stake* партнери који имају могућност укључивања нових блокова у блокчејн називају се још и валидатори. Валидатори на неки начин дају свој новац као полог за обављање алгоритма *proof-of-stake*. Постоји минимални износ јединица криптовалуте који чвор треба поседовати како би постао кандидат за креирање новог блока односно валидатор. Тај минимални износ назива се циљ и у систему се прилагођава тако да време између додавања два нова блока буде отприлике једнако. Код алгоритма *proof-of-work* циљ је представљао број у хексадецималном запису помоћу којег се дефинисала тежина израчунавања задовољавајућег хеша.

Код алгоритма *proof-of-stake* број од којег задовољавајући хеш мора бити мањи мења се код сваког новог блока и за сваког партнера је другачији. Главну улогу у дефинисању тежине проналаска задовољавајућег хеша имају раније поменути циљ и старост новца према следећој формули: задовољавајући хеш < старост новца **x**циљ.

Старост новца из формуле је старост оног новца који партнер који се такмичи у генерисању новог блока уплаћује сам себи како би доказао да је он подобан валидатор. Погледајмо пример када се два валидатора B1 и B2 такмиче у креирању задовољавајућег хеша. Нека валидатор B1 у новонастали блок укључује трансакцију којом себи уплаћује 100 пиркоина старих десет дана, а валидатор B2 као доказ да поседује довољно новаца за рударење себи уплаћује 900 пиркоина старости седам дана. Будући да је циљ у датом тренутку једнак за све валидаторе, B1 мора произвести хеш мањи од броја 1000 **x**циљ, а B2 хеш мањи од 6300 **x**циљ. Наравно, B2 има пуно веће шансе за победу у овој рунди додавања блока, јер се такмичио с новцем веће старости. Ако валидатор B2 заиста победи и његов блок буде укључен у блокчејн, трансакција којом сам себи уплаћује 900 пиркоина такође постаје ваљана и тај новац сада има старост 0. Уништавање старости новца има за последицу то да валидатор B2 готово да нема шансе за победу при укључивању следећих неколико блокова. B2 мора препустити осталим партнерима креирање нових блокова док не прође довољно времена да старост његовог новца поново буде конкурентна.

Старост новца у пиркоин систему има још једну улогу. Ако дође до рачвања у блокчејну, укупна старост новца у целом ланцу одређује на коју грану треба наставити додавати блокове. Како свака трансакција у блоку садржи информацију о старости новца, сумирањем тих вредности лако је израчунати укупну старост новца по блоку и у целом ланцу. Партнери у систему бирају ланац с највећим укупним збиром као главни ланац.

3.4.6 Решење проблема византијских генерала

Претпоставимо да византијски генерали за договор о времену напада користе блокчејн и запис нових информација помоћу алгоритма *proof-of-work*. Сваки генерал када први пут прими поруку с временом напада за које још није чуо, покрене на свом рачунару израчунавање хеша који садржи информацију о том времену. Број циља од којег тај хеш мора бити мањи како би постао задовољавајући за уписивање записа у блокчејн прилагођен је тако да је потребно десет минута да један генерал нађе решење [135].

Када неки генерал нађе задовољавајући хеш, пошаље га дифузијском поруком осталима у мрежи како би га они уписали у локалну копију блокчејна. Остали генерали тада почињу да израчунавају нови хеш који у себи садржи претходно изгенерисани хеш. На тај начин генерали желе изградити што дужи ланац са истим временом напада и поштују правило да се у једној грани ланца налазе само хешеви који имају у себи записано једно време напада. Ако неки генерал-издајник жели уписати неко друго време напада, он мора започети рачвање у блокчејну. Међутим, будући да има више генерала оданих крају, према правилу најдужег ланца, грана генерала издајника ће након неког времена бити игнорисана. Након два сата, постоји ланац односно део блокчејна са 12 хешева са истим временом напада. Сваки генерал сада има доказ да се на изградњу тог ланца потрошила одређена количина рачунарске снаге и може веровати да су време напада записано у том ланцу договорили сви генерали.

Код алгоритма *proof-of-stake* имамо сличну ситуацију [147]. Разлика је у томе што ново време напада неће први објавити насумично одабрани генерал који је први израчунао задовољавајући хеш, већ онај којем крај највише верује или онај који има власништво над највише парцела у земљи. Такав генерал има највећи углед и хеш који он мора израчунати мора задовољити слабије критеријуме од хешева које морају израчунати остали генерали. Након њега, остали генерали крећу у израчунавање новог хеша који садржи исто време напада као и претходни. У томе највеће шансе за нови блок у ланцу има следећи генерал по угледу.

3.4.7 *Pure Proof-of-stake* (*PPoS*)

Pure Proof of Stake (*PPoS*) јесте механизам консензуса који користи блокчејн платформу за валидацију трансакција и креирање нових блокова у мрежи *Algorand*. Овај механизам консензуса дизајниран је тако да обезбеди већу сигурност и децентрализацију у поређењу с другим алгоритмима *Pure Proof-of-Stake* (*PPoS*) [155].

Једна од кључних карактеристика *PPoS*-а јесте да корисници не морају да бирају валидаторе или делегате, што је уобичајена пракса у другим *PoS* системима. Уместо тога, сваки корисник који има *Algorand* новчиће (*ALGO*) може учествовати у валидацији трансакција и креирању нових блокова. Сваки корисник има право да креира нови блок сразмерно броју *Algorand* новчића које поседује.

PPoS такође користи „одабирање случајних бројева” (енг. *random number selection*) како би се обезбедила непредвидивост у процесу избора корисника који ће учествовати у валидацији трансакција. Овај процес одабира корисника који ће учествовати у процесу валидације трансакције заснован је на случајном одабиру свих корисника који поседују *Algorand* новчиће.

Још једна карактеристика *PPoS*-а јесте да корисници који учествују у валидацији трансакција и креирању нових блокова не добијају никакве додатне награде осим накнада за трансакције. Овај приступ има за циљ смањење ризика од централизације и

избегавање ситуације у којој већи корисници могу да искористе своју моћ да креирају нове блокове и контролишу мрежу.

PPoS је механизам консензуса који се истиче по својој безбедности, брзини и скалабилности и одржава децентрализацију мреже.

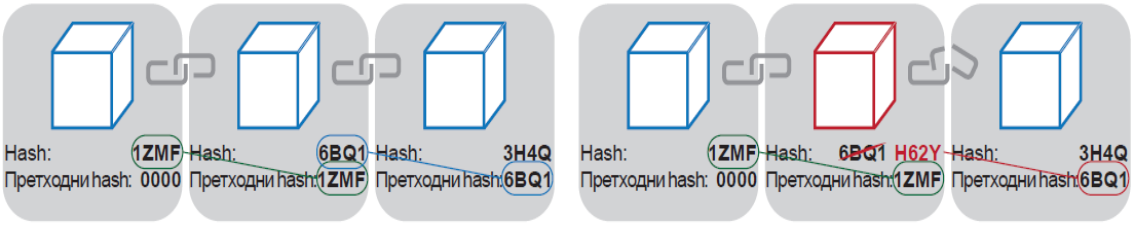
3.4.8 Криптографска хеш функција

Криптографска хеш функција је посебна класа хеш функције која има одређена својства која је чине прикладном за употребу у криптографији. Уопштено, хеш је функција која за улаз има податке произвољне величине, а као излаз враћа податке фиксне величине. Вредност хеш функције често се назива хеш вредност или кратко хеш, док се улазни податак назива порука. Криптографске хеш функције су једносмерне, односно немају инверзну функцију. Једини начин да се креирају улазни подаци криптографске хеш функције из излаза јесте да се покуша претраживање алгоритмом *brute-force*. Све могуће вредности улаза испробавају се како би се видело који од улаза одговара излазу који поседујемо.

Пожељно је да криптографска хеш функција задовољава следећих пет својстава:

- Детерминистичка је и вреди ако су два излаза добијена помоћу исте функције различити, тада су и улази били различити;
- Лако и брзо се може израчунати вредност функције за било који улаз.

Хеш функције као аргумент узимају податке варијабилне дужине, док је резултат увек фиксне дужине. Блокчејн технологија искоришћава важна својства хеш функције, односно вредности хеш функција. Није тешко произвести хеш из података, али је готово немогуће открити који су то подаци ако се гледа само хеш.



Слика 14: Хеш функција (прилагођено Savjee 2017)

Лако је произвести хеш из велике количине података, при чему је сваки хеш јединствен. Ако се промени само једно слово или бројка, хеш се комплетно мења. Узмимо текст: Ово је семинарски рад о блокчејн технологијама, на њега додајемо број *X*, где је *X* = 0, 1, 2, ... и рачунамо вредност *SHA-256* хеш функције.

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji0") =
4a8140c36617e405529468263582cd553b8ba949fff2a4ee4466eb769d054e21

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji1") =

a44d0a6b0c79f53827f9a99d1bc8d36474106f638d411cf4cf629d3e0754d94e

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji2") =

3758b36cd3f7113090decd8267914bf2a45166537601130a081d190e65f31717

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji3") =

16682e08d6c5fdc590acf40c49a9c24c351465d576c50951b69abe75038f96c5

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji4") =

ba891692b7642d087deF7f7267c9732487f73d7269e0caa6b58ed54496f06565d

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji5") =

b3e213fbc4b84d315c4e16fb64695c8dc087ffd1cfdeb522f73d4f56b7d31e17

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji20") =

9c3b4fa42488da75f47849c455e0bd7ca4d6416c65a4bb1e16d54dcfb3edcdce

SHA-256("Ovo je seminarski rad o blokčejn tehnologiji21") =

098bd24561e3491df483fd8b41db24b2362588ae558d1f943aaec8edaf11c21a

Желимо ли у наведеном примеру пронаћи хеш који започиње ознаком 0 или који је у нумеричком смислу мањи од хексадецималног броја

0x1000000000000000000000000000000000000000000000000000000000000000

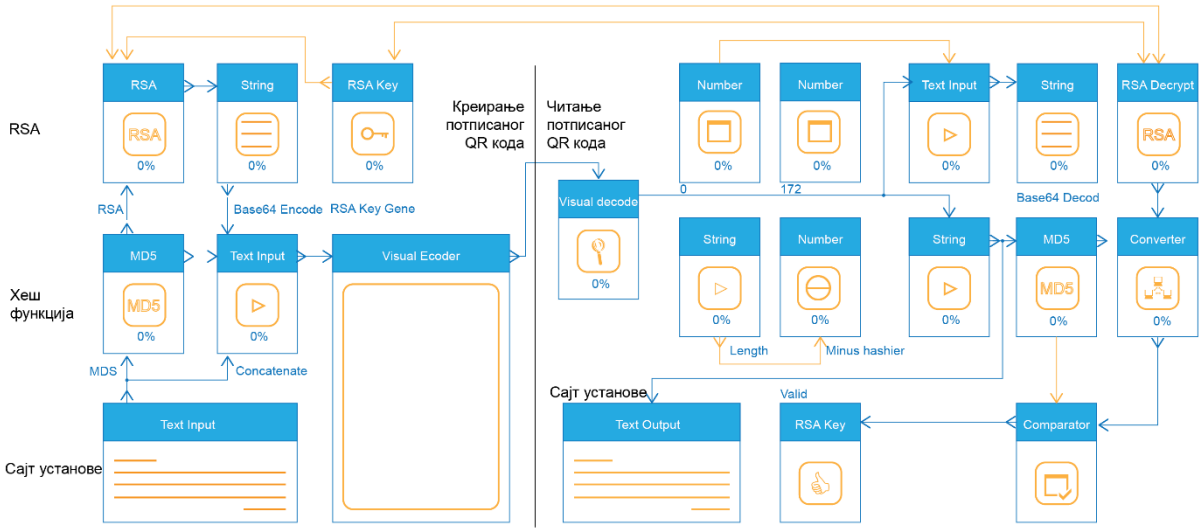
потребно је доћи до вредности $X = 21$. Да је тражени број 0 на почетку хеша био већи, требало би нам дуже време да пронађемо *X*, уз који би израчунати хеш био задовољавајући. Ако погледамо кораке алгоритма које смо пре навели, посао партнера рудара је сличан овом из претходног примера. Они прво прикупљају нове записе које треба уписати у блокчејн и конструишу нови блок. На податке из заглавља тог блока, које смо претходно описали, додају редом различите вредности броја *nonce*, па на тај податак два пута примењују функцију *SHA-256*, све док резултантни хеш не постане мањи од броја циља. Рудар који први пронађе задовољавајући хеш то јавља осталим партнерима у систему како би они престали да раде на укључењу тог блока у блокчејн.

3.4.9 RSA аутентификација

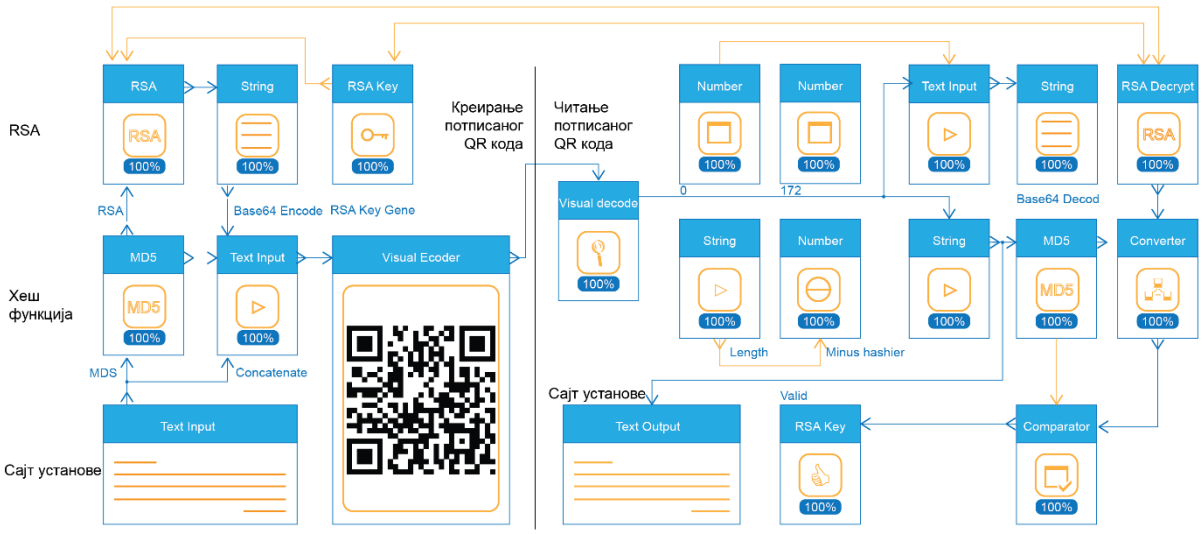
За улогу „предавача” у предложеном моделу колаборативног учења и евалуације студентских радова предвиђена је Ривест–Шамир–Едлманова (енг. *Rivest–Shamir–Adleman – RSA)* аутентификација *QR* кодираног записа који води ка линку установе у којој је предавач ангажован, као што је приказано на Слици 15.

Прво је одређена хеш вредност записа, применом неке од *SHA* (*Secure Hash Algorithms*) хеш функција, а затим је та вредност шифрована применом алгоритма *RSA*, при чему се користи приватни део кључа. Алгоритам *RSA* је заснован на сложености проблема факторизације производа два велика проста броја, чији је избор усклађен са захтевима за практичну примену криптографије јавног кључа [156].

RSA потписана порука затим се преводи у *QR* (*Quick Response*) кодирани запис, као што је приказано на Слици 16.



Слика 15: Модел система аутентификације применом RSA алгоритма



Слика 16: Генерисање QR кодираног записа, потписаног применом RSA

На страни пријема, која је приказана на десном делу слике жутом бојом, дешифрују се потписане хеш вредности записа применом јавног дела кључа, а у доњем прозору исписује се линк ка сајту установе, као што је приказано на Слици 16.

Криптографија с јавним кључем одабрана је зато што обезбеђује поверљивост, што је битно за пренос и складиштење података, аутентификацију и дигитални потпис, који гарантује интегритет и непорецивост (енг. *non-repudiation*), за разлику од криптографских система са симетричним кључем, који не нуде сервис непорецивости [157].

Дигитални потпис је сервис који треба да обезбеди интегритет поруке и непорецивост.

Под интегритетом поруке подразумева се да пријемна страна може да буде сигурна да порука на преносном путу није измењена или, уколико се то деси, да то може једнозначно да се детектује.

Непорецивост је сервис који пријемној страни може да буде необорив доказ да је порука примљена од тачно одређене особе.

Код *RSA* дигиталног потписа, употребом јавног дела кључа (*N, e*) и приватног дела кључа *d*, дигитални потпис *S* поруке *M* добија се као:

$$S = M^d \pmod N$$

За рачунање *S* је неопходно познавање приватног дела кључа *d*, што значи да су *RSA* дешифровање и *RSA* дигитално потписивање у суштини исте операције.

Потврда исправности дигиталног потписа на поруци *M* добија се на основу:

$$S^e \pmod N = (M^d)^e \pmod N = M$$

Ова операција је иста као и код *RSA* шифровања и у том смислу свако ко зна јавни део кључа (*N, e*) може да потврди исправност дигиталног потписа.

Основна идеја алгоритма *RSA* јесте проналажење функције $C = E(M, K_e)$ која мења поруку *M* (отворени текст) у шифрат *C*, при чему је потребно да функција $E(M, K_e)$ буде једносмерна.

Применом ове функције порука се шифрује пре процеса слања.

Потребно је да особа на страни пријема има могућност да, уз познавање тајне вредности K_d, примени инверзну функцију, $M = D(C, K_d)$, како би од шифрата *C* добио поруку *M*.

При томе, за свако *M* треба да важи:

$$M = D(E(M, K_e), K_d)$$

односно потребно је наћи неку једносмерну функцију са замком.

Примена алгоритма *RSA* полази од претпоставке да је релативно лако наћи два велика проста броја (*p* и *q*) и одредити њихов производ ($N = pq$), а да је тешко, односно практично немогуће, факторисати број *N*, који има стотине цифара, на чиниоце *p* и *q*.

Функција која задовољава изнете претпоставке има облик:

$$f(x) = x^e \pmod N$$

Уз одговарајући избор вредности *e* и *N*, ова функција је једносмерна, што подразумева да се уз познавање тајне вредности може наћи њена инверзна вредност, а да је то без познавања тајне вредности практично нерешив проблем.

Поступком шифровања од поруке *M* добија се шифрат *C*:

$$C = M^e \pmod N$$

док се поступком дешифровања на основу шифрата добија порука:

$$M = C^d \pmod N = (M^e)^d \pmod N = M^{ed} \pmod N$$

Обе стране у комуникацији знају вредности *N* и *e*, док само пријемна страна зна вредност *d*.

На основу тога формира се јавни део кључа: (*N, e*) и приватни део кључа: *d*, при чему је потребно да буду испуњени следећи захтеви:

- *e, d* и *N* треба да су такви да је $Med = M \pmod N$ за свако $M < N$;
- релативно је лако израчунати: Ме и С за $M < N$;
- практично је немогуће израчунати *d* за дато *e* и *N*, што је рачунски сигурно за довољно велико *e* и *N*.

Приликом генерисања кључа спроводе се следећи кораци:

- Изаберу се два велика проста броја p и q (који су приближно једнако велики);
- Формира се производ N = pq;
- Израчуна се φ(N) = (p – 1)(q – 1);
- Изабере се e такво да је узајамно просто са φ(N) и мање од φ(N);
- Одреди се d такво да је d = e – 1 (mod φ(N));
- или de = 1 (mod φ(N));
- Јавни део кључа одређен је са: (N, e);
- Приватни део кључа одређен је са: d.

У оквиру математичке основе алгоритма потребно је за дато $C = M^e \pmod N$ показати да важи:

$$M = C^d \pmod N = M^{ed} \pmod N$$

У том поступку користи се Ојлерова теорема:

Ако је x узајамно прост у односу на N, тада је $x\varphi(N) = 1 \pmod N$

Чињенице:

$ed = 1 \pmod{\varphi(N)} = 1 \pmod{(p-1)(q-1)}$

По дефиницији мода $ed = k(p-1)(q-1) + 1$

$\varphi(N) = (p-1)(q-1)$

Тада је $ed - 1 = k(p-1)(q-1) = k\,\varphi(N)$

$M^{ed} = M^{(ed-1)+1} = M \cdot M^{ed-1} = M \cdot M^{k\,\varphi(N)}$

$M \cdot (M^{\varphi(N)})^k \pmod N = M \cdot 1^k \pmod N = M \pmod N$

Ради одређивања N, потребно је пронаћи довољно велике просте бројеве p и q.

- $N = pq$, p и q су прости бројеви, N треба да је довољно велико:
- Простих бројева има бесконачно ⇒ постоји довољно великих простих бројева;
- Постоји више ефикасних алгоритама за проналажење простих бројева (на пример Рабин–Милеров тест, *APR* тест...).

Ради одређивања јавног дела кључа e, потребно је да буду испуњени следећи услови:

- e мора да буде узајамно прост са (p - 1)(q - 1), па се за e често бира прост број;
- Због брзине шифровања постоји захтев да e буде што мање, али то може нарушити снагу алгоритма;
- Многи корисници користе исти експонент e унутар јавних кључева:

  e=3 или $e = 65537 = 2^{16} + 1$

На овај начин се не компромитује шифарски систем, а омогућава се да процес шифровања буде много бржи од дешифровања.

Што се тиче одређивања (рачунања) тајног кључа *d*, потребно је решити једначину:

$$ed = 1 \pmod{\varphi(N)}$$

С обзиром на то да је *e* изабрано тако да је:

$$\gcd(e, \varphi(N)) = 1$$

та једначина увек може да се реши.

Ефикасно решавање ове једначине могуће је помоћу проширеног Еуклидовог алгоритма, при чему *gcd* (*the **g**reatest **c**ommon **d**ivisor*) представља највећи заједнички делилац.

Не постоји доказ да особа која жели ефикасно да реконструише поруку *M* на основу познавања *C*, *e* и *N* може то да учини, а да при томе не зна $\phi(N)$.

Верује се да не може, с обзиром на то да је доказано да је проблем проналажења $\phi(N)$ подједнако сложен као и факторизација броја *N*, а у данашњим условима сматра се, мада није доказано, да је проблем факторизације великих бројева практично нерешив.

Илустративни пример:

- Ако је N = 279978339112213278708294676387226016210704467869
  554285375600099293261284001076093456710529553608560618223519109513657
  886371059544820065767750985805576135790987349501441788631789462951872
  37869221823983

  ***N* је дужине: 200 декадних цифара или 663 бинарне цифре**

- Како одредити *p* и *q* (N = pq)?
- Предлог решења проблема (2005. године, тим са Универзитета у Бону)

  p = 353246193440277012127260497819846436867119740019 7
  625023649303468776121253679 42320005854795652808834 9

  q=792586995447833303334708584148005968773797585736421996
  0734330341455767872818 152135381409304740185467

Постоје и примењују се алгоритми факторизације целих бројева, као што су:

- Фермаова факторизација;
- Шоров алгоритам, назван по математичару Питеру Шору (*Peter Shor*), који је заправо квантни алгоритам (алгоритам који функционише на квантном рачунару), формулисан 1994. године;
- Факторизација помоћу верижних разломака;
- Факторизација помоћу елиптичких кривих;
- Сито у пољу бројева.

Повећање границе сигурности алгоритма *RSA* захтева повећање дужине кључа, с обзиром на то да се алгоритми за факторизацију броја стално унапређују. Пошто је време потребно за шифровање и дешифровање пропорционално трећем степену дужине кључа, алгоритам *RSA* постаје све спорији с повећањем захтева безбедности [156].

С обзиром на развој квантних рачунара, очекује се да ће одређивање тајног дела кључа алгоритма *RSA* бити решиво. Много боље могућности нуди примена блокчејн технологије у смислу сервиса непорецивости и следљивости података.

3.5 Блокчејн платформе

Блокчејн технологија пружа средства за сигурне и безбедне трансакције без потребе да верујете трећој страни. Овај концепт у блокчејну познат је као *trustlessness* – све док сваки учесник у трансакцији може да верује у тачност и интегритет главне књиге, не постоји додатни захтев за поверење између страна [158].

Употреба блокчејн технологија није више примарна у области криптовалута. Блокчејн платформе су нове платформе и у овом тренутку готово се не разликују у неким случајевима од основне блокчејн технологије. Користе се за општу дистрибуирану размену вредности, која се састоји од проширене листе криптографски потписаних неопозивих трансакционих записа које деле сви учесници у мрежи [159].

3.5.1 Врсте блокчејна

Избор блокчејн платформе за реализацију пројекта зависи од врсте блокчејна.

Јавно насупрот приватном (енг. *Public vs. Private*)

Јавни блокчејн (*public blockchains*) јесте блокчејн који је отворен за јавност и коме се свако може придружити без посебне дозволе. Сви који се придруже мрежи могу читати, писати и учествовати у овој мрежи коју нико не контролише [159]. Јавни блокчејнови омогућавају свим корисницима да додају податке у главну књигу. Јавни блокчејн је непроменљив и децентрализован. Приватни блокчејн (*private blockchain*) дозвољава приступ само на основу позивнице и свако ко жели да му приступи, мора затражити дозволу од управљачког тела блокчејна, а могућности за приступ су различите и одређују који корисници могу писати, читати и вршити ревизију блокчејна. У овом случају организације користе технологију дистрибуиране књиге, али не објављују своје податке, тј. нису јавно доступни – транспарентни. Приватни блокчејнови, за разлику од јавних, не нуде исти ниво децентрализоване безбедности, што значи да унос – трансакцију може променити његов власник. Приватни блокчејн захтева да сваки корисник има верификован идентитет, јер то дефинише ниво приступа који имају. Решење блокчејна које се користи за праћење рада непрофитне организације, тј. на који се начин користе добротворне донације, може бити пример приватног блокчејна. У таквом решењу само одређени службеници непрофитне организације треба да имају право управљања доделом и трошењем добротворних донација [159].

Најважнија разлика између наведених типова блокчејна јесте улога корисника на мрежи и начин на који се идентитетом управља. У приватном блокчејну, творац мреже од почетка зна ко су учесници. На јавној мрежи не можете изградити решење засновано на дозволама и корисници имају све гаранције анонимности [160].

Дозвољено насупрот без дозволе (енг. *Permissioned vs. Permissionless*)

Блокчејн без дозволе (енг. *permissionless blockchain*), као што име говори, представља врсту блокчејн мреже која омогућава било коме да постане део мреже и да

доприносе њеном одржавању [160]. Огромна већина криптовалута, укључујући биткоин, покрећу блокчејн мреже без дозволе. Кључне карактеристике блокчејна без дозволе јесу транспарентност, анонимност, децентрализованост и услужни или новчани жетони. Код блокчејна без дозволе лични подаци корисника нису видљиви на мрежи, јер се приликом приступа мрежи користи јавни кључ и корисници остају анонимни. Мреже без дозвола имају тенденцију да буду потпуно децентрализоване [160]. Овај модел блокчејна заснован је на „већинском" консензус протоколу, што значи да је за промену блокчејна потребан консензус више од 50% корисника. Дозвољени блокчејн (енг. *permissioned blockchain*) функционише другачије, те је неопходна дозвола власника да бисте постали део мреже [157]. Дозвољене блокчејн мреже карактеришу дефинисане структуре управљања, различити степени децентрализације и нетранспарентност. За разлику од блокчејн мрежа без дозволе, дозвољеним блокчејном се не управља протоколима заснованим на консензусу. Одлуке на централном, унапред дефинисаном нивоу доносе чланови мреже. Дозвољени блокчејн може имати различите степене децентрализације, тј. може бити делимично децентрализован или потпуно централизован. За разлику од блокчејна без дозволе, дозвољени блокчејн не мора да буде транспарентан. Блокчејнови без дозвола генерално су сигурнији, јер се смањује могућност договора малициозних актера унутар мреже, али су релативно спори јер могу аутентификовати тек ограничен број трансакција у конкретном времену. Насупрот томе, дозвољене блокчејн мреже имају тенденцију веће ефикасности и смањену безбедност. Безбедност дозвољене блокчејн мреже ослоњена је на интегритет својих чланова. Слично као и код традиционалних записа, дозвољени блокчејнови су такође подложни манипулацији. Висок ниво децентрализације на блокчејну без дозволе је по цени брзине и скалабилности [161].

3.5.2 Hyperledger

Hyperledger је пројекат отвореног кода (енг. *open source*) у склопу фондације *Linux* [162]. Иницијатива за унапређивање и развој блокчејн технологија и ширење могућности њихове примене у пословном свету заживела је крајем 2015, а њени чланови биле су водеће светске ИТ компаније, компаније у области финансија и банкарства, производње и дистрибуције производа (енг. *supply chain*) [162]. Пројекат *Hyperledger* је центар отвореног кода, који настоји да подржи развој индустријског блокчејна. Може се размишљати о томе као о пројекту покренутом ради убрзања развоја међуиндустријских блокчејн технологија.

Hyperledger интегрише независне отворене протоколе и стандарде за модуле прилагођене корисницима. Тим пројекта је јасно ставио до знања да неће израдити изворну криптовалуту за пројекат. Пројекат је почео да прихвата предлоге за инкубацију, као и друге технологије и кључне елементе 2016. године. Уместо да инсистирају на једном блокчејн стандарду, фондација *Linux* потенцира колаборативнији приступ за развој блокчејн технологија као део *Hyperledger*-а. *Hyperledger Fabric 2.0* је једноставан пројекат за креирање апликација блокчејн дистрибуираних записа. Као и друге блокчејн технологије, долази с главном књигом и користи паметне уговоре који му омогућавају да ради као систем у ком људи могу управљати трансакцијама. *Hyperledger Fabric* такође омогућава коришћење више различитих опција. На пример, дозвољава складиштење података главне књиге у различитим форматима. Креирање канала такође омогућава учесницима да креирају посебне књиге трансакција [163].

3.5.3 Multichain

MultiChain је генеричка платформа прилагођена за развој приватних блокчејнова унутар организације или између организација. Циљ му је да се превазиђу кључне препреке за примену блокчејн технологија у институцијама финансијског сектора, тако што обезбеђује потребну приватност и контролу. Ако је у питању приватни блокчејн, проблеми у вези с величином лако се решавају, јер учесници у ланцу могу контролисати максималну величину блока, док затворени систем, блокчејн, садржи само трансакције које су од интереса за те учеснике. Да бисмо разумели дозволе у *MultiChain*-у, потребно је знати да све криптовалуте управљају безбедношћу и идентитетом помоћу криптографије јавног кључа. Корисници насумично генеришу своје приватне кључеве и никада их не откривају другим учесницима. Осим контроле приступа средствима, ова врста криптографије омогућава кориснику да „потпише" билу коју поруку како би доказао да поседује приватни кључ који одговара одређеној адреси. *MultiChain* испољава особину ограничавања приступа блокчејн листи дозвољених корисника [164].

3.5.4 Ethereum

Замисао Виталика Бутерина је да *Ethereum* буде отворена софтверска апликација заснована на блокчејн технологијама која настоји да обезбеди оквир за програмере да осмисле децентрализоване апликације. *Ethereum* блокчејн садржи програмски кôд на којем се креирају децентрализоване апликације. Децентрализована апликација је посебна врста апликације која ради на *peer-to-peer* мрежи, а не на једном рачунару, као што је случај с многим апликацијама. Поред тога, оне су јединствен скуп софтверских апликација дизајнираних да постоје на интернету и да их не контролише један ентитет. *Ethereum* настоји да подстакне људе да дођу до сигурних дигиталних споразума, као и да имају потпуну контролу над својим новцем, користећи истовремено све предности криптографије. Требало би да блокчејн пројекти промене начин на који људи граде ствари у будућности, комуницирају и извршавају различите функције и задатке на мрежи. *Enterprise Ethereum* је још једна варијација ове платформе која се фокусира на решења предузећа [164].

Enterprise Ethereum је блокчејн платформа отвореног кода која се користи за примену паметних уговора на прилагођеној блокчејн мрежи. *Enterprise Ethereum* је познат по својој функционалности паметног уговарања, флексибилности и као такав може се користити на различите начине у индустрији и другим гранама привреде [165].

3.5.5 Corda

Corda представља платформу отвореног кода која се може користити за дизајнирање апликација посебно за финансијске организације, која ради на дозвољеној (*permissioned*) мрежи и стога се може користити за смањење трансакција и поједностављење пословања [165].

Компанија *R3*, која стоји иза развоја платформе *Corda*, има идеју да *Corda* буде водећа блокчејн платформа за примену у финансијском сектору. Надоградњом и еволуцијом платформе њене способности и функционалности постале су од великог значаја у различитим гранама привреде. Међутим, платформа и даље има доминантну улогу у финансијском сектору, и то захваљујући томе што користи предности блокчејна. *Corda* је углавном усмерена ка сложеним трансакцијама, иако ограничава приступ високоосетљивим подацима. У сваком случају, када говоримо о примени у

финансијској индустрији, *Corda* је заступљенија од других блокчејн платформи. Главни циљ платформе *Corda* јесте да пружи корисницима платформу са заједничким услугама, а истовремено да обезбеди компатабилност уграђених услуга са учесницима на мрежи. Платформа *Corda* настоји да искорени велики број проблема који успоравају трансакције између предузећа, омогућавајући им да обављају послове путем паметних уговора. Приликом њене употребе примењују се и највиши стандарди приватности и безбедности, што објашњава зашто се све више примењује у финансијској индустрији. У ери у којој је потреба за заштитом корисничких података велика, употреба блокчејн решења као што је *Corda* наставља перманентно да расте. Компанија *R3* представила је *Corda Enterprise*, комерцијалну дистрибутивну верзију *Corda*, која задовољава све захтеве савременог пословања када су у питању трансакције. Осим што олакшава предузећима да изврше трансакције, комерцијална дистрибутивна платформа нуди и јединствене функције, као што су корпоративни заштитни зидови (енг. *corporate firewalls*), као и функције за подршку која ради 24 сата дневно [163].

3.5.6 Algorand

Algorand је децентрализована блокчејн платформа која је развијена да обезбеди сигурност, брзину и скалабилност трансакција без губитка децентрализације. Брзина и скалабилност су кључне карактеристике. Процена је да може да обради хиљаду трансакција у секунди, што је брже од већине других блокчејн платформи. Платформа је скалабилна, што значи да се може прилагодити потребама све већег броја корисника и трансакција без губитка брзине или сигурности. Платформа користи сопствени механизам консензуса под називом *Pure Proof of Stake* (*PPoS*), који је дизајниран да спречи централизацију и смањи утицај већих корисника [166].

Поред брзине и скалабилности, платформа *Algorand* нуди и друге карактеристике које је чине атрактивном за кориснике и програмере. Платформа има уграђену подршку за паметне уговоре и омогућава изградњу децентрализованих апликација (*DApp*) на врху своје блокчејн мреже. Платформа нуди и алате за развој и примену апликација, као и подршку за интеракцију с другим блокчејн мрежама.

Као и код других блокчејн платформи, корисници платформе *Algorand* имају прилику да учествују у процесу валидације трансакција и креирања нових блокова. Корисници који учествују у овом процесу називају се валидатори, а награде за рад додељују се у виду новчића (*ALGO*). Платформа такође омогућава корисницима да прилагоде своје параметре консензуса и стекну већу контролу над својим трансакцијама и мрежом [167].

Algorand је једна од најпопуларнијих блокчејн платформи, са све већим бројем корисника и програмера. Његова брзина, скалабилност и сигурност чине га атрактивним за кориснике који желе брзе и безбедне трансакције, док карактеристике развоја и примене чине га привлачним програмерима који желе да граде децентрализоване апликације.

Платформа *Algorand* има потенцијал да се примени у образовању. Пошто је још увек у развоју, постоји могућност да се примени за развој будућих апликација у образовању.

Платформу *Algorand* могуће је повезати с *Moodle Learning Management System* (*LMS*) како би се пружиле додатне могућности за праћење и проверу активности студената, као и за проверу аутентичности њихових предатих радова и оцена.

Постоје различити начини на које се платформа *Algorand* може интегрисати са *Moodle Learning Management System*-ом, али један од најчешћих је преко *Algorand*

API-ја. *Algorand API*-ји су интерфејси за програмирање апликација (*API*) који омогућавају програмерима да приступе и користе различите функционалности блокчејн платформе *Algorand* путем програмског кода.

Примери неких опција интеграције између платформе *Algorand* и *Moodle Learning Management System*-а укључују:

- Аутентификација радова: платформа *Algorand* може се користити за креирање дигиталних потписа који ће бити повезани с радовима студената. На тај начин се може проверити да ли је рад оригиналан и да није мењан након што је послат;
- Верификација оцена: платформа *Algorand* може се користити за креирање паметних уговора који ће аутоматски додељивати оцене студентима на основу њихових резултата. На тај начин се могу смањити време и напор потребни за класично оцењивање [168];
- Праћење активности студената: платформа *Algorand* може се користити за креирање паметних уговора који ће аутоматски пратити и бележити активности студената у оквиру *Moodle Learning Management System*-а и пратити напредак студената.

3.6 Анализа примене блокчејн технологија у колаборативном учењу

Блокчејн представља децентрализовану и дистрибуирану базу података у којој се подаци не могу мењати или брисати и која омогућава верификацију трансакција [14]. Подаци о трансакцијама чувају се на различитим рачунарима у мрежи, повезаним коришћењем *peer-to-peer* протокола, где сваки чвор дели исту копију података, тј. дигитални регистар (енг. *Digital Ledger*). Измена података у блокчејну врши се по унапред дефинисаним правилима. Измене се прослеђују свим чворовима како би се ажурирала локална копија података. Након што је трансакција сачувана и након што су је потврдили сви чворови у мрежи, више није могуће променити податке те трансакције. Процес потврђивања тих трансакција назива се рударење (енг. *mining*) и заснива се на неком од консензус алгоритама на основу којег се постиже договор између чворова при усвајању новог блока. Применом блокчејн технологија обезбеђен је висок ниво сигурности, јер су трансакције које се одвијају анонимне. Свака трансакција или дигитални догађај који се одвија у блокчејн мрежи верификује се само ако је сагласан консензусом већинске стране корисника који учествују у овом процесу [15][14].

Предности примене блокчејн технологија у различитим доменима јесу висок ниво сигурности, децентрализација, транспарентност и непроменљивост. Блокчејн технологија превенира злоупотребе у смислу фалсификовања и порицања садржаја јер чува потпуну евиденцију у блоковима података у низу с временским ознакама, где се стари и нови блокови података не могу избрисати, а криптографски алгоритам спречава неовлашћено подметање података и смањује могућност преваре. Због ових особина блокчејн технологија се користи у различитим секторима као што су образовање, финансије, пословање, здравство, туризам енергетски сектор, јавни сектор.

Блокчејн технологије примењују се у неколико форми у колаборативном учењу у академским заједницама. Осим класичног колаборативног учења, и истраживачи у истраживачким центрима неретко користе блокове за решавање проблема у вези са академском заједницом. Примери апликација покривају читав животни циклус методологије истраживања, рецензија и истраживачких публикација за заштиту

интелектуалне својине. Прво, предложено је да се у експерименталној фази блокира и пусти систем за бележење података и његови резултати, уколико је потребно, како би се избегло да се немаром или намерним грешкама оштети експериментални интегритет, на пример ревизорски траг из података истраживања. У пракси је могуће употребити адаптивну кореографију засновану на ланцу блокова за колаборативне експерименте, који се могу репродуковати слично експериментима према робусним одговорним објашњеним (*RARE*) истраживањима и доступним интероперабилним резултатима за вишекратну употребу (*FAIR*) [169].

Осим тога, *папирна фаза* уводи платформу засновану на блоковима која складишти и мери доприносе аутора на основу промена које је направио аутор. Такође, систем блокчејна у фази рецензирања такође може стимулисати благовремен и одржив процес прегледа. Систем може дати испитивачима криптографску награду ако уредник прими проверу квалитета. Ова вредна валута касније се може користити за објављивање рецензентских радова у часописима, стварајући механизам подстицаја. Поред тога, овакав систем колаборативног учења заснован на блокчејну користи претходни рад технологије семантичког веба у фази објављивања како би аутору дао прилику да ради на еволуционој верзији научног истраживања која се може отворити за рецензије, конференције или часописе. То омогућава децентрализоване издавачке системе [169].

Блокчејн систем подржава непроменљиву евиденцију образовних процеса. Постоје предлози који бележе креативни рад или идеје за стицање научне репутације, воде дневник студентских активности у различитим организацијама за учење и омогућавају високошколским установама широм света да признају курсеве за студенте који су завршили излагање својих идеја [169].

Блокчејн има неколико карактеристика које га чине снажним инструментом, револуционарним, када је у питању примена у процесу колаборативног учења. Неке од најважнијих карактеристика у колаборативном учењу су следеће: то је децентрализован систем, ради на мрежи *peer-to-peer*, непроменљив је, заштићен је од неовлашћених приступа, осигурава приватност, али и транспарентност, заснива се на протоколу консензуса. Логично питање јесте на који начин се блокчејн технологија примењује у колаборативном учењу и које су добре или лоше стране те примене.

Блокчејн системи у образовању су децентрализовани системи. Због тога ниједан ентитет нема овлашћења над целокупном мрежом, те негује принцип колаборативности наспрам хијерархијских. Блокчејн се у потпуности множи на свим рачунарима у мрежи. Блокчејну у процесима колаборативног учења није потребна трећа поуздана страна, било интерна или екстерна, за ауторизацију његових активности [170]. Сваки корисник поседује своју копију трансакција и хешираних блокова, а информације о свакој новој трансакцији шире на целу мрежу. На овај начин, у колаборативном учењу нико не може да промени податке у блокчејну јер их не складишти појединачни ентитет, већ читава мрежа корисника чворова. Када се блок трансакција потврди и дода у блокчејн, сваки корисник ажурира своје локалне податке. Чак ни уз настојање да се измени локална књига, мрежа неће прихватити ниједан блок из измењеног блока блокова. Карактеристична непроменљивост је дата механизмом повезивања блокова у блокчејн помоћу криптографске хеш (енг. *hash*) функције. Због непроменљивости блокчејна, подаци ускладиштени у њему нису подложни хакерским нападима. Дакле, блокчејн у колаборативном учењу функционише као непроменљива књига. Са својством непроменљивости уграђеним у блокове постаје лакше открити неовлашћено мењање било којих података.

Алгоритам консензуса, својствен колаборативном учењу, јесте срж блокчејн архитектуре. Да би се задржала децентрализација мреже, сваки блокчејн мора имати алгоритам консензуса. У супротном, његова вредност се губи. Корисници морају да

постигну договор о ваљаности ланца пре него што додају још блокова, што управо и чини окосницу колаборативног учења. Сваки пут када чвор дода нови блок, сви корисници морају да потврде блок помоћу заједничког протокола. Консензус је одговоран за то да је мрежа неповерљива. Доказ о послу је механизам консензуса који од подносиоца захтева одређен рад, што обично значи време обраде рачунара. Заснован је на решавању сложене математичке загонетке која захтева велику рачунарску моћ за проверу ваљаности трансакција и стварање нових блокова. Чворови проверавају да ли нови блок испуњава захтеве њихове методе доказивања, укључујући проверу ваљаности за све трансакције унутар блока. Уколико је блок важећи, они га сматрају делом блокчејна и стално додају нове блокове [170].

Конструкција овог потписа заснована је на два кључа: приватном кључу пошиљаоца, који омогућава пошиљаоцу да врши трансакције, и јавном кључу примаоца, који примаоцу омогућава приступ трансакцијама. Сваки општи модел блокчејн операције у процесима колаборативног учења може имати одређене специфичности за сваки засебан блокчејн.

Иако су блокчејн технологије у образовању своју масовнију примену доживеле тек у неким азијским земљама, попут Кине и Јапана, и афирмацију у Сједињеним Америчким Државама, у остатку света се још увек недовољно примењују. Актуелна истраживања указују на то да постоји велики потенцијал за примену у образовном сектору.

Апликације засноване на блокчејну, иако још у пионирској фази, развијају се рапидно у различитим областима образовања, укључујући: окружења за колаборативно учење с високим нивоом безбедности за све учеснике, управљање компетенцијама и исходима учења, управљање ауторским правима, системе за испитивање студената и полагање испита и оцењивање професионалних способности студената, које компаније могу користити приликом запошљавања, целоживотно учење, онлајн образовање, издавање и верификација диплома, транскрипата и сертификата који се могу делити између појединаца и организација ради верификације. Пример овог приступа су платформа *EduCTX* за пренос евиденција акредитива међу партнерским високошколским установама елиминисањем посредника и систем за управљање подацима у образовном систему. Предности примене блокчејн технологија у образовању обухватају управљање и верификацију података без посредника, без угрожавања аутентичности, уз константну доступност и проверљивост с потпуном транспарентношћу.

Блокчејн технологија омогућава и повезивање с партнерским високошколским установама и колаборативно учење између студената различитих факултета.

Такође, примена блокчејн технологија омогућава да учешће у евалуацији студентских радова постане део процеса развоја каријере. Евалуације и евалуирани пројекти су доступни заинтересованим послодавцима. Послодавац има информације о резултатима практичног рада студената и како су пројекат евалуирали други. Осим студената-евалуатора, за студентске радове и пројекте може бити обезбеђен и рецензент из праксе. Ради одабира компетентног евалуатора, мапирају се компетенције евалуатора у односу на тему семинарског рада или пројекта преко кључних речи. Чувају се и информације о квалитету рецензије за сваког рецензента.

Вишеструке су користи које овај приступ доноси у пракси – раст колаборативних компетенција, раст ефикасности и квалитета процеса евалуације, мултиевалуативност, креирање мрежа универзитета, одсека, студената итд. Примена оваквог приступа омогућава и привредним субјектима као потенцијалним послодавцима бољу селекцију кадра „на извору”.

С обзиром на то да послодавци немају приступ квалитетним студентима, послодавци су, између осталог, заинтересовани да учествују у овом процесу како би им такви студенти били доступни од раних година њиховог школовања. Послодавцима који учествују у блокчејн мрежи за колаборативно учење и евалуацију студентских радова омогућен је приступ будућем кадру и стицање бенефиција засновано на поенима, тј. на интерној криптовалути. Поени се стичу учешћем у процесу евалуације студентских радова и верификације трансакција, а поени се троше на додатне сервисе у оквиру система и повезивање с бољим студентима.

4 РАЗВОЈ МОДЕЛА ЗА КОЛАБОРАТИВНО УЧЕЊЕ И ЕВАЛУАЦИЈУ СТУДЕНТСКИХ РАДОВА

Систематизација постојећих система за евалуацију студентских радова заснованих на блокчејн технологијама подразумева идентификацију, анализу и класификацију постојећих система за евалуацију радова који користе блокчејн технологију. Овај процес је коришћен за развијање система за евалуацију студентских радова *Open-Rev*.

Блокчејн технологија омогућава израду децентрализованих система за складиштење података, што значи да се подаци чувају на мрежи, а не на централном серверу. Такође, омогућава верификацију података путем криптографије, што значи да се подаци не могу изменити након што су унети у систем. Ово чини блокчејн технологију идеалном за системе за евалуацију студентских радова, јер обезбеђује транспарентност, верификацију и заштиту података.

Постојећи системи за евалуацију радова засновани на блокчејн технологијама могу се класификовати на основу различитих карактеристика: на основу врсте блокчејна који користе, типа података које чувају, врсте радова које евалуирају, начина евалуације, као и других фактора.

Међу постојећим системима за евалуацију радова заснованим на блокчејн технологијама налазе се *CryptoMnemosyne, ODEM, Blockcerts, Biblioteca* и други [171].

Сви ови системи пружају различите могућности за евалуацију радова и чување података на блокчејну.

Постојећи системи за евалуацију радова засновани на блокчејн технологијама, укључујући *CryptoMnemosyne, ODEM, Blockcerts, Biblioteca* и друге, представљају значајан напредак у области евалуације студентских радова јер пружају транспарентност, сигурност и објективност у процесу евалуације.

- *CryptoMnemosyne* је платформа за евалуацију радова која користи блокчејн технологију за верификацију података и спречавање плагијаризма. Ова платформа омогућава професорима да саставе тестове и задатке, а затим их додељују студентима на сигуран начин [172];
- *ODEM* је платформа за образовање која користи блокчејн технологију за верификацију диплома и сертификата. Ова платформа омогућава студентима да стекну дипломе и сертификате који су признати у целом свету, а да притом имају потпуну контролу над својим подацима;
- *Blockcerts* је систем за издавање дигиталних сертификата који користи блокчејн технологију за верификацију и чување података. Овај систем омогућава да се дигитални сертификати издају без потребе за посредницима, што смањује трошкове и повећава ефикасност процеса [173];
- *Biblioteca* је платформа за издавање дигиталних сертификата која користи блокчејн технологију за верификацију и чување података. Ова платформа омогућава да се дигитални сертификати издају на сигуран начин, а да притом имају потпуну контролу над својим подацима.

Постоје и други системи за евалуацију радова заснованих на блокчејн технологијама, који пружају различите функционалности и могућности. Међутим, сви ови системи имају заједничку карактеристику, а то је да користе блокчејн технологију

за гарантовање сигурности, транспарентности и објективности процеса евалуације радова.

Како се блокчејн технологија и даље развија, можемо очекивати да ће се појавити и нови системи за евалуацију радова који ће користити ове технологије. Међутим, иако постојећи системи представљају напредак у области евалуације радова, постоји потреба за даљим истраживањем и унапређењем ових система.

Један од изазова у вези с постојећим системима за евалуацију радова заснованим на блокчејн технологијама јесте њихова комплексност. Ови системи често захтевају од корисника да имају одређено техничко знање како би их ефикасно користили. Такође, примена ових система може бити скупа и захтевати велике инвестиције [174].

Поред тога, ови системи се углавном фокусирају на верификацију идентитета и спречавање плагијаризма, док остале аспекте евалуације, као што су оцењивање и додељивање бодова, остављају професорима, што за последицу може имати неједнак третман студената и субјективност у процесу евалуације [175].

При креирању система за евалуацију радова *Open-Rev* акценат је на једноставном коришћењу и примени, али и задржавању свих аспеката евалуације радова, укључујући оцењивање и додељивање бодова. У развој овог система укључена су и мишљења студената како би се осигурало да је прилагођен њиховим потребама и очекивањима [176].

4.1 Моделирање метода за колаборативно учење и евалуацију студентских радова

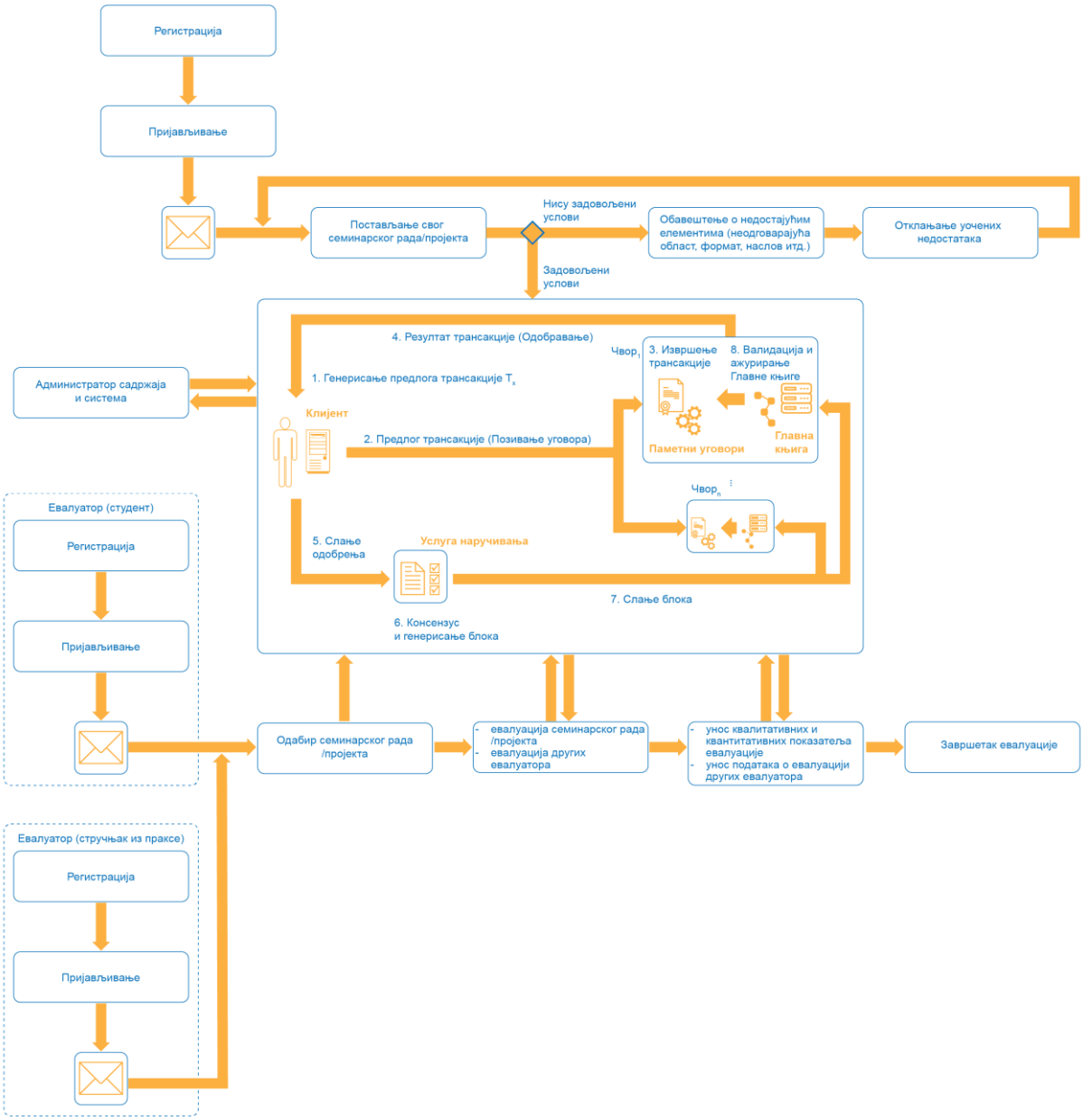
Модел колаборативног учења и евалуације студентских радова, заснован на блокчејн технологијама, обухвата одабране концепте из модела евалуације резултата научноистраживачког рада. Евалуација студентских радова и пројеката унапређена је колаборативним учењем, аналогно поступку рецензирања научноистраживачких радова [177]. Блокчејн технологије се у развијеном моделу користе за обезбеђивање сигурне платформе за чување и размену података о студентским пројектима и радовима, студентима-евалуаторима, рецензентима из праксе и евалуацијама [178]. Након што се подаци о евалуацији студентског рада забележе, ниједна страна их више не може поћи или променити.

4.2 Моделирање процеса колаборативног учења и евалуације студентских радова

У савременом образовном систему, колаборативно учење и евалуација студентских радова представљају кључне елементе у развијању критичког мишљења и стицању практичних вештина код студената. Међутим, постојећи процеси евалуације студентских радова често нису довољно транспарентни и поуздани, што доводи до проблема у мерењу успеха студената и установа у којима се образују.

Као потенцијално решење овог проблема, блокчејн технологије нуде транспарентност, следљивост, непорецивост и сигурност у процесу евалуације студентских радова [176]. У претходном делу докторске дисертације наведени су и укратко описани неки системи засновани на блокчејн технологијама. У наредном делу дат је приказ система у зависности од типа блокчејна који користе.

- *CryptoMnemosyne* је платформа заснована на блокчејн технологијама која омогућава издавање неотуђивих сертификата који потврђују успешно завршене курсеве и дипломе. Ова платформа користи *Ethereum* блокчејн како би осигурала да су сертификати аутентични и да не могу бити лажирани;
- *ODEM* је платформа која омогућава сигурно издавање сертификата и диплома путем блокчејна. Ова платформа користи паметне уговоре како би омогућила транспарентност и поузданост у процесу евалуације и издавања диплома;
- *Blockcerts* је платформа за издавање сертификата заснована на биткоин блокчејну. Ова платформа омогућава да се сертификати издају и проверавају путем блокчејн технологије, чиме се осигурава њихова аутентичност и непорецивост [179];
- *Biblioteca* је платформа заснована на *Ethereum* блокчејну која омогућава издавање и верификацију диплома и других образовних сертификата путем блокчејн технологије [180].



Слика 17: Процес рада (енг. workflow) предложеног модела

Ради моделирања процеса колаборативног учења и евалуације студентских радова заснованих на блокчејн технологијама, потребно је развити адекватне алгоритме и механизме за верификацију и аутентификацију радова путем блокчејн технологије. Такође, важно је осигурати да су сви учесници у процесу евалуације идентификовани и аутентификовани путем блокчејн технологије, чиме се смањује могућност манипулације и злоупотреба у процесу.

4.3 Моделирање података

Моделирање података представља процес дефинисања структуре података која се користи у одређеном систему или апликацији. Овај процес обухвата дефинисање ентитета, атрибута, веза између ентитета, као и ограничења и правила која се примењују на те ентитете и њихове атрибуте.

Моделирање података је кључно за развој ефикасних и поузданих информационих система. Коришћењем моделирања података, дизајнери система могу прецизно да дефинишу структуру података која ће се користити у систему, што омогућава брже и лакше развијање апликација, као и бољу скалабилност и одрживост система.

Постоје различити приступи моделирању података, а најчешће се користе релацијски модел и објектно оријентисани модел. Релацијски модел се користи за моделирање података који се складиште у бази података, док се објектно оријентисани модел користи за моделирање објеката у апликацији.

Када се моделирају подаци, важно је узети у обзир захтеве корисника и функционалности које ће систем обављати. Такође, треба водити рачуна о томе да се моделирање података изводи на начин који ће обезбедити висок ниво интегритета података и поузданост система [181].

Уз напредак технологије, моделирање података све се више користи у области вештачке интелигенције и машинског учења. Коришћењем моделирања података могу се креирати модели који могу да предвиде будуће догађаје и доносе одлуке на основу анализе великих количина података [182].

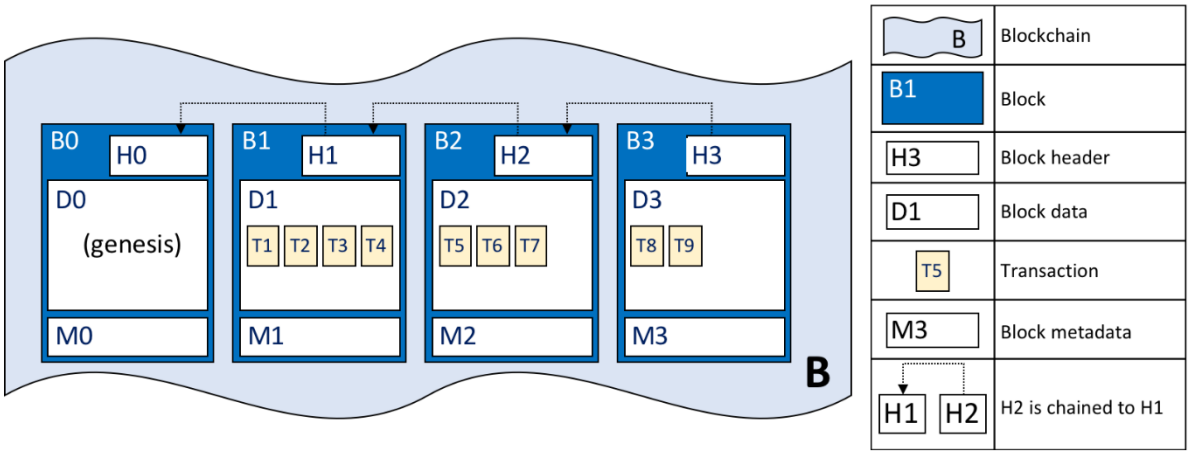
Моделирање података је кључни процес у развоју ефикасних и поузданих информационих система. Правилно моделирање података омогућава брже и лакше развијање апликација, као и бољу скалабилност и одрживост система.

Моделирање података је кључни корак у развоју система за колаборативно учење заснованог на блокчејн технологијама. Блокчејн технологија омогућава транспарентност, сигурност и следљивост у размени података и информација, што је кључно за систем за колаборативно учење. Правилно дефинисање ентитета, атрибута, веза и правила и ограничења у моделирању података може осигурати сигурност, поузданост и ефикасност система.

Приликом моделирања података за систем за колаборативно учење заснован на блокчејн технологијама треба размотрити различите ентитете, њихове атрибуте и везе између њих. Могући ентитети у таквом систему укључују кориснике, предмете, лекције, задатке, оцене и слично. Атрибути ових ентитета могу укључивати податке као што су име, презиме, идентификациони број, датум рођења, наслов задатка, опис задатка, оцена итд. Везе између ентитета могу се дефинисати као релације, где један ентитет има везу с другим ентитетом. На пример, корисник може бити повезан с лекцијом коју похађа или са задатком који је добио да реши.

Осим ентитета, атрибута и веза, моделирање података за систем за колаборативно учење заснован на блокчејн технологијама треба да укључи и дефинисање правила и ограничења која се примењују на ове ентитете и њихове атрибуте. Ова правила и ограничења могу се користити за обезбеђивање сигурности и поузданости система, као и за заштиту приватности корисника.

Важно је напоменути да се моделирање података у системима заснованим на блокчејн технологијама разликује од традиционалних система база података. У традиционалним системима база података, подаци се складиште у централизованој бази података, док се у блокчејн систему подаци складиште у децентрализованој мрежи [183]–[185]. Због тога је потребно узети у обзир ову децентрализовану природу система приликом моделирања података.



Слика 18: Континуиран низ блокова блокчејн ланца

4.4 Моделирање блокчејн мреже стејкхолдера

Моделирање блокчејн мреже стејкхолдера подразумева идентификацију и анализу важних учесника у блокчејн мрежи, њихових улога, циљева и интеракција унутар система.

У блокчејн мрежи, стејкхолдери су обично организације или појединци који имају интересе у мрежи и њеном функционисању. То могу бити берзе криптовалуте, рудари, програмери, корисници, регулаторне агенције и други [36].

Моделирање блокчејн мреже стејкхолдера почиње утврђивањем свих релевантних учесника у систему. Након тога, анализирају се њихове улоге, интереси и циљеви у мрежи. То укључује разумевање начина на који сваки стејкхолдер доприноси мрежи, као и начина на који се њихови интереси могу поклопити или разликовати.

Након утврђивања и анализе стејкхолдера следи развој модела који ће описати интеракцију између учесника у мрежи. Овај модел би требало да обухвати начине на које учесници деле информације, доносе одлуке, начине на које се трансакције обрађују и валидирају, као и начине на које се могу решавати проблеми у мрежи [184].

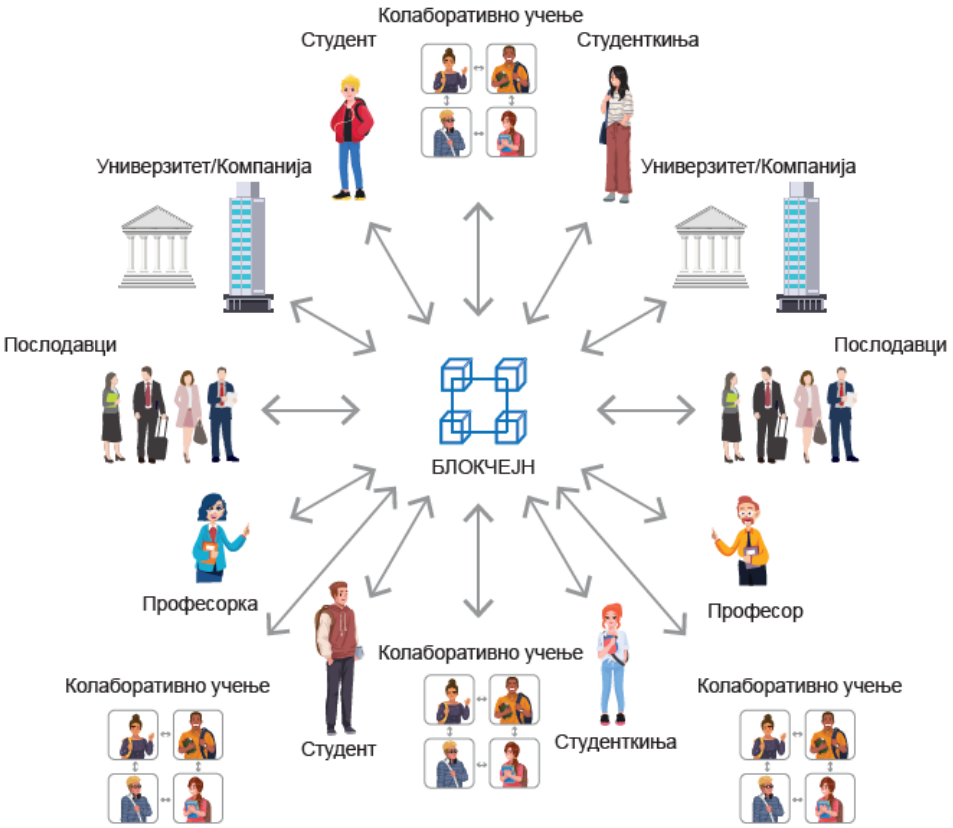
Један од важних елемената у моделирању блокчејн мреже стејкхолдера јесте утврђивање начина на који се учесници награђују за свој допринос у мрежи. То може укључивати рударске награде за потврду трансакција, накнаде за коришћење мреже или друге врсте награда за допринос [183].

Када се моделирање блокчејн мреже стејкхолдера заврши, следи имплементација система. Након тога, треба спровести тестирање и оптимизацију како би се осигурало да мрежа ради како треба и задовољава потребе свих учесника у мрежи.

На крају, успешно моделирање блокчејн мреже стејкхолдера кључно је за стварање ефикасног и одрживог система. То захтева добро разумевање свих учесника у мрежи и њихових интереса, као и пажљиво планирање и имплементацију система који ће задовољити потребе свих учесника у мрежи.

4.5 Развијени модел за колаборативно учење и евалуацију студентских радова

У раду је развијен модел колаборативног учења и евалуације студентских радова (енг. *collaborative learning and evaluation of student work model – CLESW model*). У развијеном моделу *CLESW* потребно је прво поменути све учеснике у мрежи, као што је илустровано на следећој слици. Предавачи из различитих високошколских институција додељују задатке, семинарске радове и пројекте студентима из својих предмета. Ради унапређења ефикасности и квалитета евалуације студентских радова, у приступу који је развијен у овом раду, учесници у колаборативном учењу и евалуацији студентских радова и пројеката јесу студенти који похађају исти предмет, студенти виших година студија или виших нивоа студија [177][178].



Слика 19: Учесници у мрежи модела CLESW

Сваки семинарски рад и пројекат евалуира други студент, а информација о квалитету рада даје се квантитативно и описно на прописаном обрасцу евалуације. На

тај начин сви учесници у овом процесу могу да виде препоруку и евалуацију квалитета семинарског рада или пројекта. Давањем препоруке и оцене евалуације студентског рада студенти доприносе утврђивању квалитета евалуатора. На тај начин процес евалуације великог броја студентских радова постаје део процеса учења. Учешће у процесу евалуације семинарских радова и пројеката других студената обавезан је део процеса учења, тј. једна од предиспитних обавеза [177].

Обавеза да учествују у колаборативном учењу у оквиру образовног процеса подстиче код студената стицање знања из области које се изучавају у оквиру предмета из кога је припреман и евалуиран семинарски рад или пројекат, боље повезивање усвојених знања из области које се изучавају у оквиру датог предмета, усвајање знања о коришћеним технологијама и структурама пројекта, аналитичке вештине, критичко размишљање, мотивацију за рад на пројектима. На тај начин унапређују се компетенције студената-учесника у колаборативном учењу. Студент-евалуатор мора континуирано показивати своју заинтересованост за процес евалуације, што позитивно утиче на његову репутацију у односу на наставника и учесника из праксе.

Репутација студената-евалуатора може се побољшати на неколико начина:

- на основу оцена професора или оцена предавача из праксе;
- на основу оцена студената који су евалуирани и који могу да дају повратну информацију о квалитету рецензије коју су добили;
- на основу оцена других студената који имају приступ пројекту и евалуацији;
- на основу оцене привредника као заинтересоване стране за одређени пројекат.

У развијеном моделу није кључна репутација студената као евалуатора, већ да студент као евалуатор усвоји нова знања. Знање се свакако оцењује на традиционалан начин, и то ради наставник. Репутација је значајна за додатне сервисе, тј. за повезивање с послодавцима. Такође, репутација је потребна и на нивоу препознавања кључних речи, што омогућава да се убудуће могу боље бирати евалуатори. Репутација утиче и на углед институције и наставника. Стога овај приступ пружа реалистичнију слику о стеченим знањима и вештинама студента, за разлику од само формалне провере знања. Поред тога, студент је заинтересован да његове компетенције односно репутацију препознају стручњаци из праксе [177][178].

Послодавац ће имати информације о резултатима практичног рада студената и како су пројекат евалуирали други. Осим студената-евалуатора, студентске радове и пројекте може евалуирати и рецензент из праксе [47][17][48]. Да би се одабрао компетентан евалуатор, мапираће се компетенција евалуатора у односу на тему семинарског рада или пројекта преко кључних речи. Чуваће се и информације о квалитету рецензије за сваког рецензента. На тај начин унапређена је сарадња високошколских институција и компанија. Примена оваквог приступа компанијама омогућава бољу селекцију кадра „на извору”.

4.6 Моделирање блокчејн мреже

Моделирање блокчејн мреже подразумева разумевање и описивање начина на који се управља блокчејн мрежом и доносе одлуке у њој. То укључује утврђивање учесника у мрежи и њихових улога, затим процесе доношења одлука и механизме управљања ризицима који се могу појавити у мрежи.

Кључни учесници у управљању блокчејн мрежом често су власници, програмери, корисници, рудари и регулаторне агенције. Утврђивање свих релевантних учесника у мрежи и њихових интереса и циљева најважнији је корак у моделирању управљања блокчејн мрежом.

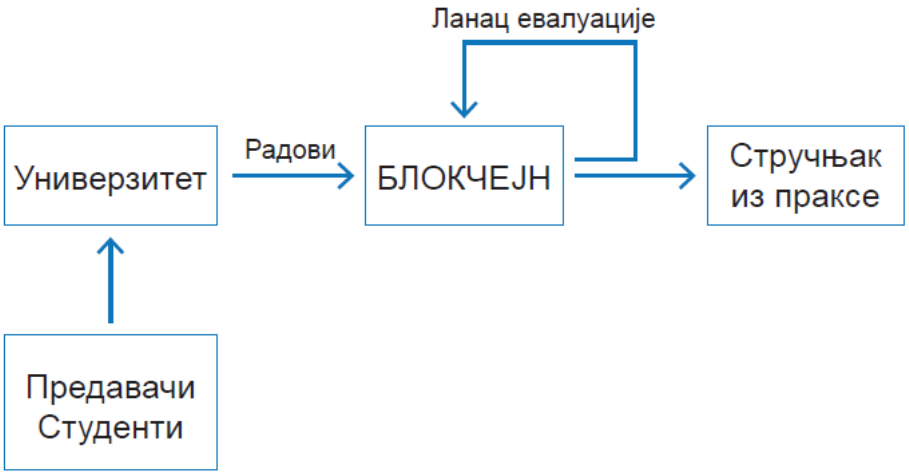
Процес доношења одлука у блокчејн мрежи често је заснован на консензусу, што значи да се одлуке доносе на основу споразума свих учесника у мрежи. Постоје различити механизми консензуса који се користе у блокчејн мрежама, као што су *Proof of Work, Proof of Stake, Delegated Proof of Stake, Pure Proof of stake* и други [175].

Важно је размотрити и ризике и изазове који се могу појавити у мрежи и развити механизме управљања ризицима како би се осигурало стабилно и сигурно управљање блокчејн мрежом. То може укључивати успостављање механизама заштите од напада, решавање проблема перформанси и скалабилности, као и решавање проблема са законском регулативом [182].

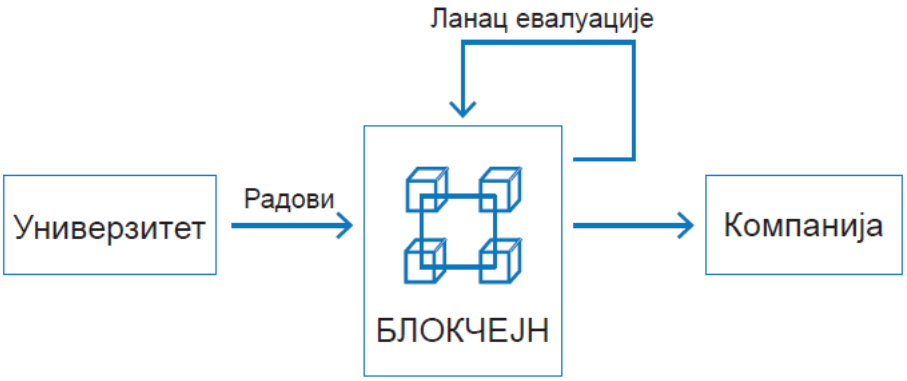
Моделирање блокчејн мреже може се спровести уз помоћ различитих алата и техника, као што су дијаграми тока, матрице одговорности и анализа ризика. Важно је нагласити да моделирање треба да буде флексибилно и да се може прилагодити потребама и променама у мрежи.

Успешно управљање блокчејн мрежом кључно је за стварање стабилне, сигурне и ефикасне мреже. То захтева разумевање свих учесника у мрежи и њихових интереса, као и пажљиво планирање и имплементацију система управљања који ће задовољити потребе свих учесника у мрежи.

Интеграцијом наведених идеја развијен је модел, као што је илустровано на наредној слици. Модел евалуације заснован на блокчејну затвореног је типа с дозволом, односно ограничење се односи на дозволе вршења и прегледа трансакције само на чворовима који учествују у систему, док власник система одређује учеснике и чворове који могу да учествују у механизму консензуса. Као што је приказано у Табели 1, *Hyperledger Fabric* као технолошка платформа може да подржи захтеве предложеног модела у неколико сегмената. Ова платформа испуњава услове потребне за мрежу учесника којима је неопходна дозвола, односно сваки учесник у систему претходно се конфигурише као валидан са одређене високошколске институције (или компаније) с потврђеним идентитетом. На тај начин је постигнут и услов за заштиту података.



Слика 20: Основна шема



Слика 21: Предложени модел

Пошто наставник зада задатке, следи део колаборативног учења са евалуацијом, односно попуњавање обрасца евалуације. На тај начин постиже се консензус и средства се ажурирају у главној књизи, што значи да је евалуација извршена и прихваћена и, коначно, одобрава се на паметан и аутоматски начин, чиме се смањује потреба за људском интеракцијом. Ово је од великог значаја за институције које имају велики број студената. Као битна функционалност *Hyperledger Fabric* истиче се то што нуди конфигурацију броја и врсте комбинације индосаната потребних да би се једна трансакција сматрала ваљаном [186].

Преко ове функционалности, односно дела алгоритма консензуса, наставник и студент имају своју копију главне књиге и постављених паметних уговора, тако да је поступак одобравања у ствари извршавање паметних уговора и слање резултата исхода даље у мрежи како би се проверила истинитост и постигао консензус [177].

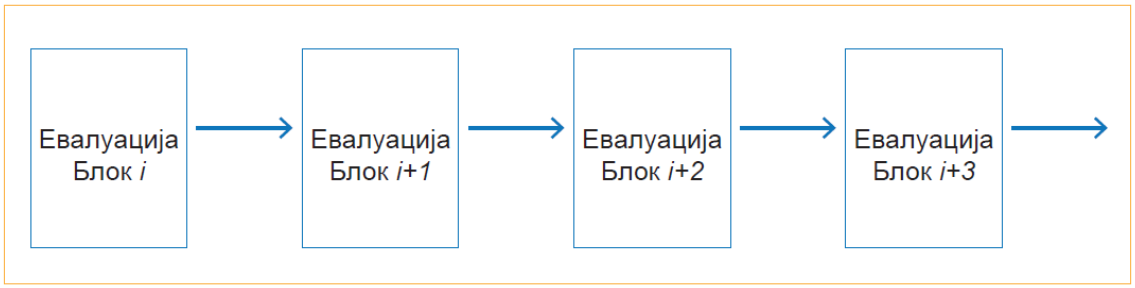
Трансакције система су похрањене у блокчејну, као централној тачки система, и сви учесници укључени у систем ступају у интеракцију с блокчејном. Важно је истаћи да први слој представља релациону базу и може се схватити као ниво управљања учесницима система. У оквиру овог дела одређени су приступи са улогама и привилегијама, али се одвија и колаборативно учење. Други слој садржи трансакције. Евалуација, односно упаривање евалуатора и предмета евалуације одвија се у бази података блокчејна. Процес почиње када студент добије одређени задатак од наставника.

У развијеном моделу студент мора показати знање у решавању задатка и евалуацији других радова. Задаци са евалуацијом сачувани су у бази података и одобрени од стране наставника. У интересу студента је да евалуација буде што боља. Ако нема консензуса, студент губи репутацију [177].

Евалуацијом базе података управља се аутономно и користи се дистрибуирани сервер с временском ознаком на *peer-to-peer* мрежи.

Ради поједностављења интероперабилности између стручњака из праксе (компанија) и евалуационог дела система заснованог на блокчејн решењу, овом делу могу да приступају директно кроз интеграциони слој, који је део система [177].

Блокчејн за евалуацију студентских радова дизајниран је на основу *DLT*-а. То је листа блокова, која је приказана на Слици 21. Блокчејн за евалуацију студентских радова представљен је као низ блокова евалуације уланчаних за сваки други блок секвенцијално. Приказ је дат на наредној слици.

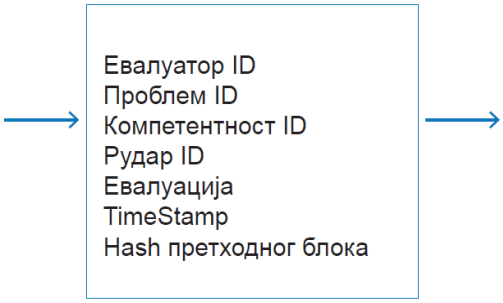


Слика 22: Блокчејн за евалуацију студентских радова

Први блок се зове блок генезе. Сваки блок садржи ИД евалуатора, евалуацију, потпис евалуатора, *TimeStamp* и хеш претходног блока, који је приказан на наредној слици и илустрован на следећи начин:

1. Евалуатор ИД је насумично додељен учеснику (предавач, студент, привредник);
2. Евалуација: на обрасцу евалуације оцењује се рад студента (семинарски рад, пројектни задатак и сл.);
3. Потпис евалуације: образац евалуације потписује евалуатор, при чему други учесници не могу да сазнају коме је дат глас, односно како је гласао учесник. Евалуатор користи свој приватни кључ за потпис обрасца, који се даље користи за евалуацију рада;
4. Временска ознака;
5. Хеш претходног блока: користимо алгоритам *SHA-256* за израчунавање хеш вредности претходног блока.

На овај начин постављена шема евалуације, заснована на блокчејну, отпорна је на модификацију података.



Слика 23: Блок евалуације

4.7 Моделирање метрика за оцену перформанси развијеног модела

Моделирање метрике за оцену перформанси развијеног модела кључни је корак у процени ефективности и успеха развијеног модела. Ове метрике се користе за процену квалитета предвиђања које је направио модел на основу доступних података и за одређивање колико добро модел ради у одређеном контексту [187].

Приликом моделирања метрике за оцену перформанси модела важно је узети у обзир различите аспекте и специфичности модела, као што су:

- тип проблема који модел решава (класификација, регресија, детекција аномалија итд.);
- врсте података који се користе за обуку и тестирање модела;
- карактеристике перформанси које су релевантне за конкретан проблем који се решава;
- различите методе евалуације доступне и погодне за одређени модел.

Неке од најчешће коришћених метрика за оцену перформанси модела јесу:

- тачност (енг. *accuracy*) – однос правилно класификованих узорака у односу на укупан број узорака у скупу података за тестирање;
- прецизност (енг. *precision*) – однос стварних позитивних класификација у односу на укупан број позитивних класификација [188][36];
- одговор (енг. *recall*) – однос стварних позитивних класификација у односу на укупан број позитивних узорака у скупу података теста [188];
- F1 мера – комбинација прецизности и одзива у једној метрици која обезбеђује равнотежу између прецизности и одзива;
- површина испод криве (енг. *area under the curve, AUC*) – мери квалитет класификације модела на основу површине испод *ROC* криве (енг. *receiver operating characteristic*) [189].

Избор метрике која ће се користити у процени перформанси модела зависи од конкретног проблема који се решава и од захтева пословних процеса [36][188]. Из тог разлога, моделирање метрике треба спровести темељно, при чему треба узети у обзир специфичност и контекст у коме се модел примењује.

Када се ради о систему за евалуацију студентских радова подржаних блокчејн технологијом, једна од метрика која би могла бити корисна за процену перформанси система јесте поузданост [190].

Поузданост се односи на степен стабилности и поузданости система у обављању његових функција. У овом случају, систем евалуације студентских радова мора бити у стању да осигура да су сви подаци о евалуацији и бодовању поуздани, конзистентни и недвосмислени [184]. С обзиром на то да се ради о систему подржаном блокчејн технологијом, веродостојност би могла бити кључни фактор за евалуацију радова студената на фер и транспарентан начин [184].

За мерење поузданости система за евалуацију студентских радова подржаног блокчејн технологијом могу се користити неке од следећих метода:

- Тестирање система: проверавање како систем функционише у стварном окружењу и како реагује на различите сценарије. Ово може укључивати тестирање система са стварним подацима о процени и бодовању [191];
- Анализа података: проучавање података које систем генерише како би се видело колико су поуздани и доследни. Такође, могу се користити неке од статистичких метода да би се проценила поузданост података;
- Коришћење вишеструких потврда да би се са сигурношћу потврдило да су све трансакције у систему верификоване више пута. Ово може укључивати потврде с више чворова у мрежи;
- Употреба криптографских алгоритама осигурава да су подаци за процену и бодовање сигурни и непроменљиви. Ово би могло да укључи употребу дигиталних потписа и хеш функција [192].

Комбинација наведених метода може помоћи у процени поузданости система евалуације студентских радова подржаног блокчејн технологијом [193].

С обзиром на то да се ради о пионирској примени модела колаборативног учења и евалуације студентских радова (модел *CLESW*) [178], било је потребно дефинисати параметре које систем треба да мери да би се користили за испитивање успешности развијеног приступа. Параметарски оквир чине:

- Оцена знања студента – студенти сматрају да је процена колега лакша за спровођење и тачнији одраз индивидуалног доприноса када је непрекидна током целог тимског рада (као више периодичних процена процеса), а не једнократна процена производа која се јавља на крају задатка;
- Укупна појединачна процена колега као укупан релативни допринос сваког члана тима плус индивидуални резултати;
- Тимска укупна процена колега као укупност бодова свих чланова тима;
- Просечна оцена тима подељена с бројем чланова тима;
- Фактор вишеструког скалирања за сваког студента;
- Квалитет студентских евалуација, као одраз квалитета тимског рада који се мери оценама, повећава се у задацима учења заснованим на проблемима и пројектима

када се континуирана провера међу колегама користи за процену појединачних доприноса пре других модела оцењивања, као што је процена појединачних доприноса само за наставнике или додељивање свим члановима тима исте оцене;

- Благовременост – посматрана кроз периодичну или кампањску активност евалуације студентских радова (у континуитету или непосредно пред испит);
- Продуктивност колаборативног учења – задаци тимског рада одражавају врсту вољне и продуктивне сарадње и завршени задатак може се оценити само као производ те сарадње, док се процена доприноса појединца пројекту мора фокусирати на процес стизања до тог производа. Будући да су ментори само део тог процеса, онда су сами студенти у најбољој позицији да прецизно оцене доприносе процесу;
- Студенти више преферирају индивидуалну процену својих доприноса него да сви чланови тима добију исту оцену.

4.8 Архитектура софтверског система

Архитектура софтверског система представља скуп важних одлука о организацији и дизајну софтверског система. Односи се на структуру система и начин на који су његове компоненте повезане и међусобно делују.

Архитектура система се обично развија на почетку пројекта, пре почетка спровођења, и састоји се од различитих аспеката као што су:

- Архитектонски стилови – шаблони који се користе за организовање система, као што су клијент-сервер, вишеслојна архитектура, архитектура заснована на услугама итд.;
- Компоненте система – делови система који обављају специфичне задатке. Они су организовани у модуле, библиотеке или услуге;
- Интеракције између компонената – начини на које се компоненте повезују једна с другом и размењују податке, као што су *API*-ји, протоколи и интерфејси;
- Системска дистрибуција – начин на који се компоненте система дистрибуирају на различитим машинама или серверима како би се осигурале ефикасност и скалабилност система.

Архитектура софтвера је важна јер може утицати на перформансе система, безбедност, могућност одржавања и скалабилност система. Добро дизајнирана архитектура може да обезбеди лакше одржавање система, лакше додавање нових функција и брже решавање проблема.

Развијени систем има класичну вишеслојну архитектуру, која се састоји од три главна слоја: презентационог слоја, логичког слоја и слоја података. Такав приступ омогућава да се функционалност система раздвоји на логички независне целине које се могу посебно развијати и тестирати, а затим интегрисати у целину.

Систем користи архитектонски стил *RESTful*. Презентациони слој је одвојен од логичког слоја преко *REST API*-ја, који омогућава комуникацију између различитих делова система преко *HTTP* протокола.

Систем користи микросервисну архитектуру. Ова архитектура омогућава раздвајање функционалности система на мање, независне сервисе, који се могу

развијати и тестирати засебно, а затим интегрисати у целину. Ово такође омогућава скалабилност система тако да се одређене компоненте система могу скалирати независно од других компонената.

Систем је заснован на инфраструктури облака (енг. *cloud infrastracture*). Ово омогућава скалабилност система тако да се системски ресурси могу повећати или смањити у складу с потребама система и захтевима корисника. Такође, омогућава већу доступност система, јер су системски ресурси доступни преко мреже.

Систем има сложену архитектуру, која се састоји од неколико слојева, користећи *RESTful* и микросервисну архитектуру, и засновану на инфраструктури облака. Ове карактеристике омогућавају одвајање функционалности, скалабилност и већу доступност система.

Слика 24 : Архитектура софтверског система

4.8.1 Протоколи и формати порука који се користе за комуникацију између компонената

За комуникацију између компонената користи се *REST API* и *HTTP* протокол. *REST API* користи *HTTP* методе (*GET*, *POST*, *PUT*, *DELETE*) за обављање операција над ресурсима и пружа различите формате порука, као што су *JSON*, *XML* и други.

Коришћена је платформа Кафка као средство за повезивање и комуникацију између различитих компонената у систему. Кафка користи сопствени формат бинарних порука, који се шаље преко *TCP* протокола. Поруке се могу конвертовати у различите формате, али се најчешће користи бинарни формат.

За комуникацију између микросервиса користи се протокол *gRPC*. Протокол *gRPC* је *RPC* (енг. *Remote Procedure Call*) систем високих перформанси који користи бинарни формат поруке заснован на *HTTP/2* протоколу.

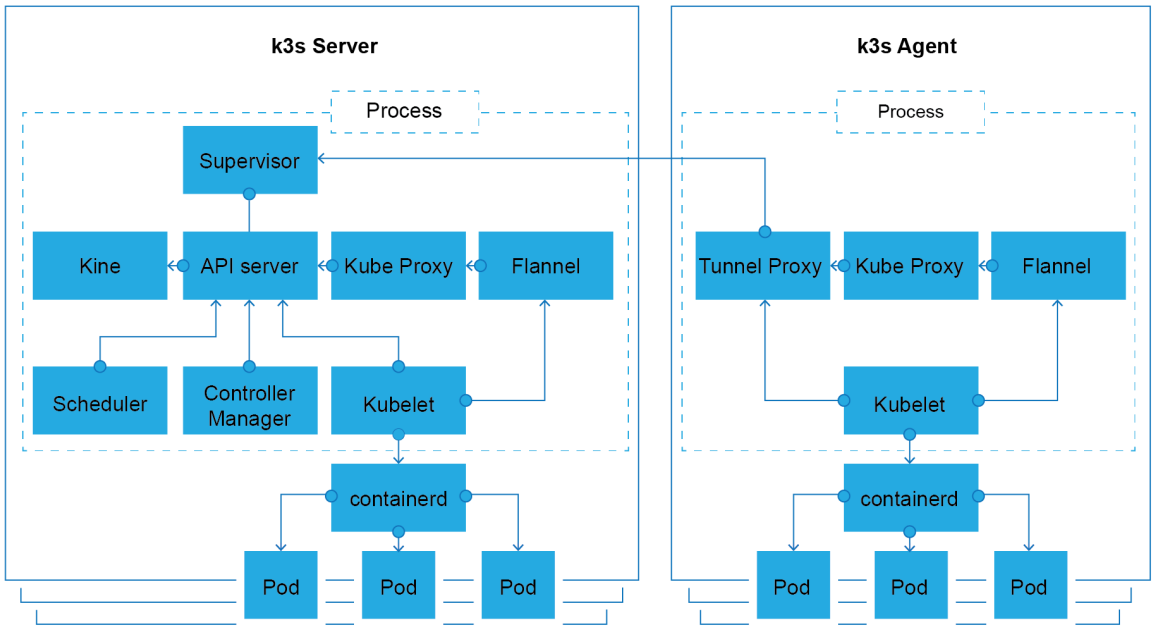
Систем користи различите протоколе и формате порука за комуникацију између компонената. Ово укључује *HTTP* протокол за *REST API*, платформу Кафка за бинарни формат порука преко *TCP* протокола и *gRPC* за бинарни формат поруке заснован на *HTTP/2* протоколу.

Компоненте су повезане преко различитих комуникационих механизама и протокола. У општем смислу, апликација користи микросервисну архитектуру, где се различити делови система извршавају у одвојеним процесима и комуницирају преко мреже. Систем се састоји од три главне компоненте: корисничког интерфејса, сервера апликација и базе података. Ове три компоненте су повезане преко *TCP/IP* протокола, а кориснички интерфејс комуницира са сервером апликација преко *HTTP* протокола. Сервер апликација користи *JDBC* протокол за комуникацију с базом података.

У оквиру апликације сервер користе се различити сервиси који комуницирају преко *RESTful API*-ја. Овај *API* користи формат *JSON* за размену података између услуга.

Што се тиче интеграције апликације са системима треће стране, комуникација са овим системима остварује се различитим протоколима и форматима порука, у зависности од специфичности сваког система.

Архитектура система је пројектована тако да се комуникација између компонената одвија на различитим нивоима и путем различитих протокола и формата порука, што омогућава да се различити делови система развијају и скалирају независно.



Слика 25 : Агент сервис архитектура

За бутстраповање *k8* кластера коришћен је Рančеров *K3s* алат.

4.8.2 Интеграција различитих технологија и алата у систему

Интеграција различитих технологија и алата у систему остварује се коришћењем одређених протокола и формата порука за комуникацију између компонената, као што је већ поменуто.

Конкретно, у првој компоненти је коришћена технологија за постављање веб-сервера *Python Flask*, док су у другој компоненти коришћене технологије *Node.js* и *React.js* за постављање веб-апликације која корисницима омогућава интеракцију са системом. У трећој компоненти коришћена је технологија *Apache Kafka* као платформа за дистрибуирану обраду и складиштење порука, а у четвртој компоненти технологија *Spark* коришћена је за дистрибуирану обраду података.

За интегрисање ових технологија и алата у јединствен систем *Apache Kafka* је коришћен као главни посредник у размени порука између компонената. Свакој компоненти је додељена посебна улога у систему, при чему су све компоненте интегрисане преко кластера *Apache Kafka*.

Интеграција различитих технологија и алата у један систем може бити изазовна и захтева детаљно планирање. У овом случају, архитектура система је дизајнирана тако да подржи флексибилност и скалабилност, што значи да се нове компоненте могу додати без већих проблема.

Интеграција се може извршити на различите начине, на пример, преко веб-сервиса, *REST API*-ја или неког другог протокола за размену података. Поред тога, за комуникацију између компонената могу се користити различити формати порука, као што су *JSON*, *XML* или неки други формат.

У свим компонентама су коришћени формати *JSON* порука за комуникацију међу њима, што је омогућило једноставну размену података између компонената, без обзира на коришћене технологије и алате.

На овај начин је интеграција различитих технологија и алата у систему омогућила ефикаснију и скалабилнију обраду података, као и бољу флексибилност система приликом додавања или уклањања нових компонената.

У процесу интеграције такође је важно размотрити на који начин ће се подаци чувати и обрађивати у систему. У овом случају, база података се користи као централно складиште података, што омогућава ефикасну размену података између различитих компонената у систему.

Ако се све наведено узме у обзир, интеграција различитих технологија и алата у један систем може бити сложен процес, али када је архитектура система таква да подржава скалабилност и флексибилност, то се може постићи уз минималне проблеме и без угрожавања читавог система.

4.8.3 Скалабилност система

У погледу скалабилности система, дат је увид у то како се систем може скалирати и проширити у складу с повећањем захтева.

Први део, који се односи на *backend*, користи архитектуру микросервиса која омогућава да се свака функција система изводи као посебна апликација, што олакшава скалирање система у складу с повећањем захтева. Употреба контејнера (енг. *Docker*) омогућава брзо постављање и управљање апликацијама.

Други део, који се односи на базу података, користи базу података *MongoDB, NoSQL*, која омогућава хоризонтално скалирање. То значи да се капацитет базе података може повећати додавањем нових чворова уместо проширења само једног сервера. Ово олакшава скалирање базе података у складу с растућим захтевима.

Трећи део, који се односи на *API*, користи *RESTful API*, који је веома скалабилан и може се прилагодити повећању броја захтева.

Четврти део, који се односи на клијентску страну, користи *ReactJS*, који има могућност лаког скалирања због своје модуларне структуре, као и могућност поновног коришћења компонената.

Све ове технологије и алати омогућавају хоризонтално скалирање система, односно повећање броја чворова који обављају задатке, уместо вертикалног скалирања, што подразумева повећање ресурса једног чвора. Ово олакшава прилагођавање система порасту захтева и побољшава перформансе система у целини.

4.8.4 Безбедност система

Безбедност система је кључна компонента сваког софтверског система, укључујући и овај. Да би се обезбедила безбедност система, потребно је анализирати све делове система у целини и препознати потенцијалне рањивости и начине смањења ризика.

Кључни аспекти безбедности система који се могу анализирати за сваки део система јесу:

1. Идентификација и аутентификација корисника: Како се аутентификују корисници у систему и како се верификује њихов идентитет? Да ли постоје механизми да се спречи преузимање идентитета других корисника?
2. Ауторизација: Како се утврђује која права приступа корисници имају у систему? Постоје ли механизми који спречавају неовлашћени приступ подацима?
3. Заштита података: Како се штите подаци у систему? Да ли су подаци шифровани или се користи неки други механизам заштите?
4. Безбедност комуникације: Како обезбедити безбедну комуникацију између различитих компонената система? Да ли се користи шифровање комуникације и како се потврђује идентитет комуникационих партнера?
5. Праћење и ревизија активности: Да ли се прате активности корисника и друге активности у систему и да ли се воде евиденције? Да ли постоји механизам упозорења за неуобичајене активности у систему?
6. Заштита од напада: Како спречити нападе на систем, као што су *DDoS* напади, *SQL* инјекције, *Cross-Site Scripting*? Да ли постоји механизам за откривање и спречавање ових врста напада?
7. Ажурирања система и безбедност софтвера: Како се одржава безбедност система ажурирањем софтвера и закрпа (енг. *patch*)? Да ли постоји механизам за редовно ажурирање софтвера и како се проверава безбедност нових верзија софтвера пре инсталације?

Све ове аспекте треба узети у обзир приликом анализе безбедности система у целини. Неопходно је примењивати најбоље праксе и редовно проверавати и ажурирати све делове система како би се смањили ризици од напада и неовлашћеног приступа.

Приликом пројектовања и постављања апликације веома се водило рачуна о безбедности система. Први део описује аутентификацију и ауторизацију корисника, што је основа за заштиту система од неовлашћеног приступа. У другом делу се наводи да коришћење *HTTPS* протокола обезбеђује енкрипцију комуникације између клијента и сервера, чиме се спречава прислушкивање података.

Трећи део говори о употреби технологија за спречавање напада на базу података, као што су *SQL injection* напади. Шифровање података користи се у бази података како би се спречило неовлашћено читање података у случају да је база података угрожена.

Четврти део описује употребу алата за праћење система и откривање инцидената, као и правилно конфигурисање система, како би се смањила изложеност потенцијалним нападима. Такође, наглашена је важност редовног ажурирања система и коришћења најновијих верзија софтвера и алата како би се смањио ризик од напада.

Безбедност система је била важан фактор током пројектовања и примене система и предузете су одређене мере заштите да би се смањио ризик од напада и неовлашћеног приступа. Ипак, безбедност система је континуиран процес и захтева стално праћење и ажурирање, па је важно да се ове мере и праксе редовно преиспитују и унапређују.

4.8.5 Одрживост архитектуре

Одрживост архитектуре односи се на способност система да одржи своју функционалност, да се лако одржава и надогради током времена. Да би се постигла одрживост архитектуре, потребно је приликом пројектовања система узети у обзир неколико кључних фактора, а то су флексибилност, проширивост и лакоћа одржавања.

У првом делу су коришћени микросервиси који су међусобно повезани преко *REST API*-ја. Такав приступ омогућава скалабилност система и лако додавање нових функционалности. Такође, употреба контејнера олакшава примену нових верзија система.

У другом делу, *Kafka* је коришћен као посредник између микросервиса, што омогућава лако додавање нових микросервиса и прилагођавање променама у системским захтевима.

У трећем делу је коришћена база података *Cassandra*, која је дизајнирана тако да буде високо скалабилна и доступна. То значи да је лако додати нове чворове у базу података како би се повећали капацитет и перформансе система.

У четвртом делу коришћени су алати за праћење и праћење перформанси система као што су *Prometheus* и *Grafana*. Ти алати омогућавају детаљно праћење и анализу перформанси система, што помаже у препознавању проблема и побољшању перформанси.

Све наведено указује на то да је архитектура система заснована на савременим технологијама које су флексибилне, проширive и једноставне за одржавање. Коришћењем микросервисне архитектуре, система *Kafka* и *Cassandra*, архитектура је дизајнирана тако да буде високо скалабилна и доступна. Поред тога, коришћење алата за праћење и праћење перформанси система помаже у одржавању система и пружању бољег корисничког искуства. Све ово заједно чини систем одрживим у архитектонском смислу.

4.8.6 Токеномички приступ

Циљ овог приступа јесте да формира инцентиве да они који евалуирају радове буду максимално добри у томе. То се реализује тако што се створи токен А који је трансферабилан у оквиру система у складу са одређеним паметним уговорима и токен Б који није. Токен А се периодично издаје као део нормалне операције једног или више универзитета који учествују у овом систему и даје се онима који рад предају (У1) аутоматски по почетку курса. Онима који рад предају (У1) треба токен зато што морају

да уз постављање рада на евалуацију направе улог деноминован у токену А. Постоји минимални улог, али се он може повећати, чиме се неки рад означава као нарочито вредан пажње.

Онима који радове прегледају (У2) потребан је токен А зато што њиме купују, на пример, право да први изаберу најквалитетније студенте којима ће понудити посао или други преферирани третман у оквиру система. (Ово је нешто што мора специфицирати универзитет, за токеномични приступ је једино битно да постоји неки разлог зашто они који радове прегледају (У2) желе токен.)

Они који радове прегледају „зарађују" токен А евалуацијом радова. Када се заврши евалуација рада, токени А који су улог уз њега поделе се између свих оних који су рад евалуирали на основу броја токена Б које има дати прегледач рада (У2). Токен Б представља комбинацију репутације и користи за систем неког индивидуалног прегледача рада (У2) и што више токена Б он има, то ће зарадити већи удео токена А.

Токен Б се може зарадити на основу понашања оног ко прегледа радове у неком периоду, који је у принципу произвољно подесив. На истеку тог периода њему се токен Б пенализује за ниску варијансу у датој оцени (спречавајући да се ико „обогати" стратегијом у којој увек гласа исто, у нади да ће један те исти глас (рецимо највећи) бити тачка система Шелинга посматраног кроз визуру теорије игара), а издаје у вредности која је пропорционална „тачности" евалуатора. Тачност евалуације је базирана на Хенсоновом футархичном принципу: од онога који прегледа рад тражи се да оцени не по личном нахођењу него да предвиди како ће други прегледач рада (У2) оценити рад. Они прегледачи радова чија су предвиђања најближа истини добијају највише токена Б. Они који су најдаље добијају најмање. Овај принцип подстиче оног који прегледа радове да оцену нити поклања, нити ускраћује из хира, будући да је мала вероватноћа да други прегледачи радова (У2) деле исту „великодушност".

4.8.7 Прикупљање информација и анализа постојећег стања и досадашњих резултата истраживања у развоју и имплементацији система за евалуацију студентских радова

Прикупљање информација и анализа постојећег стања кључни су кораци у развоју и имплементацији било ког система. Када је у питању развој и имплементација система за евалуацију студентских радова, ови кораци су од посебне важности јер нам помажу да боље разумемо тренутно стање система и препознамо проблеме који се могу појавити приликом његовог развоја и имплементације.

Један од начина за прикупљање информација о постојећем стању система за евалуацију студентских радова јесте интервјуисање професора и студената који користе овај систем. Овај процес нам помаже да разумемо њихове потребе и очекивања у погледу овог система, као и да препознамо било какве проблеме или недостатке у постојећем систему [194]. Други начин је анализа постојећих радова и оцена како би се утврдили трендови и обрасци у евалуацији [195].

Након прикупљања информација о постојећем стању система за евалуацију студентских радова, следи анализа досадашњих резултата истраживања у развоју и имплементацији система.

Ово укључује преглед литературе о сличним системима за евалуацију радова, као и анализу досадашњих истраживања која су се бавила овом темом. Овај корак нам помаже да стекнемо увид у најбоље праксе у развоју и имплементацији система за евалуацију студентских радова, као и у недостатке постојећих система [196].

На основу прикупљених информација и анализе досадашњих резултата истраживања, почиње се с развојем и имплементацијом система за евалуацију студентских радова. Овај систем би требало да буде дизајниран у складу с потребама и захтевима корисника, као и да буде заснован на најбољим праксама и резултатима истраживања [197].

Кључни елементи ефикасног система за евалуацију студентских радова јесу транспарентне и објективне оцене, доступност и ефикасност. Такав систем требало би да пружи студентима могућност да брзо и једноставно приступе информацијама о својим радовима и евалуацијама колега, као и да омогући наставницима да прегледају и оцене радове на бржи и ефикаснији начин.

С обзиром на значај прикупљања информација и анализе досадашњих резултата истраживања, као и развој система заснованог на потребама корисника и најбољим праксама, може се развити квалитетан и ефикасан систем за евалуацију студентских радова. Такав систем би могао бити од велике користи у високошколским установама, јер би омогућио ефикаснију и објективнију евалуацију студентских радова и олакшао процес учења и оцењивања.

4.9 Евалуација

Евалуација као оцењивање и вредновање рада у настави представља неизоставни сегмент поступка учења и образовног процеса. Процес оцењивања и вредновања рада студента у настави неопходно је да буде у функцији његовог индивидуалног напредовања, али и самог побољшања квалитета процеса наставе и самоучења. Приликом креирања плана наставе конкретног студијског програма треба планирати и дефинисати и сам поступак и план евалуације.

Вредновање или евалуација у мноштву дефиниција сматрају се синонимима (енг. *evaluation*). Евалуација подразумева одређивање релативне вредности нечега према усвојеном стандарду, а то је као суштинска одредница нешто што рефлектује његов сопствени значај. У дидактици и педагогији уопште евалуација се односи на процењивање развоја ученика према циљевима наставног програма [198]. Сходно томе, вредновање обухвата утврђивање и формулисање широког опсега важнијих циљева наставног процеса, њихово јасно дефинисање према понашању студената које треба да се оствари, затим избор и израду поузданих, добрих и практичних инструмената процењивања остварења.

Евалуација тако преставља шири појам од проверавања и оцењивања знања у настави. У суштини, то је осмишљен инструмент мерења, тј. процене „ефеката и резултата наставе и као такво не ограничава се само на ниво савладаности садржаја наставних програма, уже образовних, односно интелектуалних исхода наставе, него има задатак да обухвати шире промене личности студената, начине понашања, ставове, вредности, интересовања, социјабилност, однос према раду, дакле, шире промене личности изазване педагошким деловањем наставника” [199]. Евалуација обухвата промене личности студената, као исходе и постигнућа, изазване не само наставом него укупним образовним процесом, па се, сходно променама концепције наставног рада, разликује од традиционалног начина мерења образовног постигнућа тако што региструје више аспеката личности студента. Дакле, обухвата шире постављене циљеве и тако добија целовитију слику о студенту и степену и квалитету остварености пројектованих промена у личности студента.

Вишеструка је предност колаборативног учења и међусобног оцењивања:

- Сам предавач употребом података прикупљених евалуацијом коју студенти једни за друге спроводе у настави има могућност да вреднује наставни процес објективније, као и да евалуира квалитативно сопствени рад и саме услове реализације наставе;
- Студент има могућност да оцењивањем својих колега и евалуацијом њихових радова унапреди своје знање, допринесе конструктивно својим колегама и изгради критичко мишљење.

За конкретан случај, примене евалуације за колаборативно учење путем блокчејн образовне технологије, потребно је спровести двоструку евалуацију и извршити компаративну анализу добијених резултата.

Први ниво евалуације је међусобна евалуација студената унутар тимова, ограничена на чланове тима. Сви учесници и њихов допринос рада су познати.

Други ниво евалуације јесте групна евалуација међу тимовима студената који су заједнички радили на пројекту. Оптимално ограничење би било на пет радова, уз обавезу симетричне расподеле евалуација међу тимовима. При овој форми евалуације није познат допринос сваког студента понаособ, већ само заједнички допринос тима.

Трећи ниво подразумева евалуацију коју спроводе предметни наставници и сарадници у настави. Они такође оцењују тимски рад на пројекту, а не појединачне доприносе студената.

Тимови студената за семинарске и пројектне радове треба да имају од два до пет чланова.

Уз експерименталну групу потребно је поставити и контролну групу, у којој неће бити спроведена претходно дефинисана евалуација међу студентима, већ ће предавачи извршити класичну евалуацију и оцењивање.

Компаративна анализа резултата спроводи се на следећи начин:

- На првом нивоу: индивидуално постигнуће у односу на просечно постигнуће свих чланова тима;
- На другом нивоу:
    - Поређење просечног тимског постигнућа од стране чланова (добијеног на првом нивоу) и просечног тимског постигнућа међу тимовима (добијеног на другом нивоу);
    - Индивидуално постигнуће у односу на просечно постигнуће свих чланова тима добијено евалуацијом међу тимовима;
- На трећем нивоу: индивидуално постигнуће у односу на просечно постигнуће свих чланова тима добијеног на основу евалуације предметних предавача;
- Четврти ниво: упоређивање свих добијених резултата с постигнућем унутар контролне групе.

Задатак сваког студента је да:

- учествује у писању семинарског/пројектног рада са својим колегама;
- путем блокчејн платформе изврши евалуацију рада осталих чланова свог тима;

- путем блокчејн платформе изврши евалуацију пет семинарских/пројектних радова других тимова.

Задаци израде семинарског или пројектног рада прате план и програм наставног предмета у оквиру кога ће бити спроведено истраживање и не треба да одступају од досадашњих захтева који су стављани пред студенте као задатак.

Критеријуми евалуације се постављају кроз стандард и неопходно их је детаљно представити свим студентима који учествују у истраживачком подухвату пре почетка самог истраживања. Стандардном студентском скалом оцена треба оценити:

- индивидуални допринос појединца;
- квантитативни допринос појединца;
- вештине презентације;
- тимски рад (сарадња, конфликти, лидерство...);
- техничку обраду базирану на стандарду захтеваног академског писања (формат, цитирање, правопис...);
- комплексност извора (коришћена литература, практични примери);
- разумљивост написаног и презентованог;
- савременост и актуелност дела рада или пројекта;
- аналитичност, логичке процесе, закључивање.

Просечна оцена се изводи на основу средње вредности свих критеријума који се унапред усвоје и дефинишу у евалуацији.

Аналогно претходно наведеним критеријумима, оцењује се и тимски допринос.

Евалуација коју изводи тим предавача одвија се сходно претходно утемељеној пракси.

Целокупан процес евалуације је транспарентно доступан на блокчејн апликацији, али је сама евалуација анонимна.

Логичка последичност примене наведеног облика евалуације јесте својеврсно усмеравање ка учењу које тежи конкретним циљевима, а не само садржајима, али и подучавању прилагођеном сваком студенту, уместо подучавању при коме сви делују по истим задацима.

Осим евалуације процеса учења која представља формативну форму евалуације и евалуације постигнућа учења која представља сумативну форму евалуације, овај модел укључује и такозвано прогностичко вредновање које је усмерено према даљем развоју студента које се пројектује на различите фазе његовог учења и усавршавања.

Овако дефинисана евалуација, спроведена кроз блокчејн апликацију, доводи до тога да евалуативна функција оцењивања представља оптимални вишекритеријумски општи суд о успеху студената према унапред утврђеним стандардима или критеријумима оцењивања. Ова функција се односи на анализу и вредновање, сумирање свих доступних информација о унапређењу знања и вештина и успеху студената. Она долази до изражаја у одређеним периодима и карактерише је аутономни, интерперсонални и објективни стандард [200] [201].

Предности евалуације наспрам класичног оцењивања су многоструке. Њоме се превазилазе бројне негативне карактеристике функције оцењивања. У наредној табели дате су карактеристике функције оцењивања.

Табела 5: Карактеристике функције оцењивања

Карактеристике функције оцењивања
Оцењивање је најслабије решен проблем у образовању.
Упутства за оцењивање постоје, али су уопштена и већини професора непозната.
Велике су разлике у оцењивању у предметној настави.
Проблематика оцењивања покреће велики број проблема.
Професори су веома осетљиви кад се разговара о објективности њихове оцене.
Студенти су често незадовољни оцењивањем и није им дата могућност да изнесу примедбе на конкретне оцене.

На који начин блокчејн доприноси адекватнијој евалуацији и оцењивању студената? У наредној табели дати су принципи евалуације који се примењују у блокчејн технологијама.

Табела 6: Принципи евалуације у блокчејну

Принципи евалуације који се примењују у блокчејн технологијама
Објективност у евалуацији према утврђеним критеријумима.
Релевантност оцењивања на основу спроведене евалуације.
Коришћење разноврсних техника и метода евалуација.
Правичност у оцењивању на основу вишекритеријумске евалуације.
Редовност и благовременост у евалуацији.
Евалуација без дискриминације и издвајања по било ком основу и транспарентност.
Уважавање индивидуалних разлика, потреба, нивоа студија, претходних постигнућа студената и тренутних услова у којима се евалуација одвија.

4.9.1 Евалуација система

Да би се креирао модел системске евалуације, најпре треба дефинисати циљеве евалуације и критеријуме по којима ће се оцењивати систем. Ово укључује утврђивање кључних перформанси система, као и аспекте безбедности, скалабилности и могућности одржавања.

Након тога, потребно је прикупити податке о перформансама система у реалном окружењу како би се упоредили с дефинисаним циљевима. Ово укључује анализу оптерећења система, брзине извршења трансакције, времена одговора и других перформанси које су важне за функционалност система.

Важно је и тестирати безбедност система како би се препознали могући ризици и рањивости. Ово може укључивати тестирање пенетрације, тестирање отпорности на нападе и друге методе.

Након прикупљања података и тестирања система, потребно је анализирати и интерпретирати резултате евалуације и донети закључке о томе да ли систем испуњава

дефинисане циљеве и критеријуме. Ако постоје проблеми у перформансама или безбедности система, неопходно је препознати узроке и предузети кораке за побољшање система.

Да би се добили релевантнији подаци и прецизнији модел евалуације, препоручује се да се евалуација система спроводи у различитим окружењима и под различитим условима оптерећења и коришћења.

5 ПРИМЕНА И ЕВАЛУАЦИЈА РАЗВИЈЕНОГ СИСТЕМА

5.1 Анализа спремности наставника за примену блокчејн технологија у високошколском образовању

Ради анализе примене блокчејн технологије у образовању, спроведена је онлајн анкета међу наставницима високошколских институција.

5.1.1 Методолошки оквир истраживања анализе примене блокчејн технологија у образовању

Блокчејн представља релативно нов појам, који је широј јавности последњих неколико година постао познат захваљујући афирмацији валута као што је биткоин и применом у економији и пословању. Овај вид технологија своју примену проналази ефикасно и у многим други привредним гранама и у образовању.

5.1.2 Предмет истраживања

Предмет овог истраживања усмерен је на примену блокчејн технологија у образовању, односно посвећен је ставовима стручних лица о потенцијалној примени блокчејн технологија у образовању у Србији. С обзиром на то да је информисаност и познавање ових технологија и њихове примене у образовању очекивано ниска, предмет анализе били су ставови и мишљења предавача високошколских установа у Србији. Разлог за такав одабир приступа лежи у чињеници да ниска информисаност о овим технологијама и неискуство у њиховом коришћењу не пружа могућност емпиријског истраживања задовољства корисника, оцена ефикасности и слично, већ само вредновање потенцијалних користи.

5.1.3 Циљ и задаци истраживања

Циљ предметног истраживања јесте испитивање ставова наставног кадра који се тичу потенцијалне примене блокчејн технологија у образовању у Србији. Специфични циљеви односе се на мапирање користи које би потенцијална примена донела, одређивање крајњег корисника тих користи, али и детектовање проблема које би примена блокчејн технологија решила. На тај начин би се грубо могло закључити да ли постоји склоност ка увођењу ових технологија међу стручним кадром у образовању.

Неки од задатака истраживања су:

- утврдити степен упознатости с појмом блокчејн технологија;
- испитати степен познавања ставова о демократизацији, децентрализацији, транспарентности, мобилности и перманентности образовања утемељеног на блокчејн технологијама;
- испитати мишљења о утицају спречавања манипулације и злоупотреба образовних података и сертификата;
- испитати однос традиционалног и будућег облика наставе и учења утемељеног на блокчејн технологијама, начине њиховог реализовања, предности и недостатке који их прате;

- испитати ставове о временској извесности примене блокчејн технологија у образовању;
- утврдити користи које се препознају као доминантан разлог за прихватање блокчејн технологија.

5.1.4 Методе, технике и инструменти

Од истраживачких техника које су коришћене за ову врсту испитивања, прикладнија је била техника у виду анкете или анкетног упитника за прикупљање потребних података. Истраживачки инструмент је анкетни упитник намењен предавачима високошколских установа у Србији. Упитник је састављен од питања затвореног типа, на који су понуђени одговори у виду тростепене и петостепене скале, ради поузданог потврђивања или одбацивања ставова и мишљења испитаника.

Као инструменти прикупљања података коришћен је упитник, који су направили истраживачи за потребе овог истраживања. Узорак истраживања је случајан, а чини га наставни кадар у високошколским установама у Србији. Укупно је учествовало 130 испитаника. Овај онлајн упитник је анониман.

Истраживање је примењено јер има практичну усмереност на решавање проблема и импликације за потенцијалну примену блокчејн технологија у образовању. На основу прикупљених података, анализирани су подаци на квантитативном и квалитативном нивоу. У анализи истраживања је примењивана дескриптивна метода и метода теоријске анализе.

5.1.5 Узорак истраживања и организација

Узорком је обухваћено укупно 130 предавача у високошколским установама у Србији. Истраживање је спроведено јула 2021. године. Онлајн анкета постављена је на *Google* платформи, на линку који је циљно прослеђен испитаницима путем имејла и Viber апликације:
https://docs.google.com/forms/d/11Wx2kfpzE2SGiLjEv5pXB2FJOhNCBqP7q-eg8LdalsQ/edit#responses

Слика 26: Изглед онлајн анкете истраживања примене блокчејн технологија у образовању

5.1.6 Анализа и интерпретација добијених резултата

Прво питање из упитника: *Да ли сте се икада до сада сусрели с применом блокчејн технологија у образовању током своје досадашње радне праксе?* имало је циљ да утврди колико је овај појам познат наставом кадру. За потребе те индикације, ово питање није додатно појашњавано, као што је то случај с наредним питањима. Само 12,8% укупног броја испитаника одговорило је позитивно, што се може протумачити да је само тај део анкетираних имао јасну представу и знање о томе шта су то блокчејн технологије и да је имао некакво искуство када је реч њиховој примени. Готово половина (48,8% анкетираних) изјаснила се да се НИЈЕ сусрела с применом ових технологија током свог досадашњег рада, али не треба занемарити чињеницу да и међу њима може постојати мањи удео оних који знају шта су то блокчејн технологије, али да их нису користили. Трећу, не малу групу (38,4%), чине испитаници који са сигурношћу нису могли ни да потврде ни да оповргну лично искуство. Разлог тако високе стопе одговора лежи у чињеници да велики број испитаника није упознат са свакодневном применом овако утемељене технологије. У наредној табели приказане су структуре одговора.

Табела 7: Одговори на питање 1 из упитника

Одговори		Број	У %
●	Да	16	12,8
●	Не	61	48,8
●	Можда, нисам сигуран/сигурна	48	38,4

Друго питање има за циљ да испита отвореност према могућностима које блокчејн технологије носе: *Да ли бисте у процесу евалуације рада својих студената користили могућност блокчејн технологија, при којима су подаци о учењу студента, укључујући време учења, датотеке курсева и резултате тестова који се могу пратити, снимљени на блокчејну хронолошким редоследом и сваки запис података може бити означен*

временском ознаком (без могућности да се подаци избришу или мењају, па је тачност података заштићена и загарантована)? Више од половине испитаника (54,7%) изразило је спремност да користи могућност технологија ако би имали увид у време и начин учења студената при савладавању градива, што уз делимичну спремност од 26,6% представља значајну отвореност за ову могућност. За употребу овакве могућности није спремно 18,8% испитаника, што може бити последица веровања да време проведено у учењу не значи нужно савладавање градива.

Табела 8: Одговори на питање 2 из упитника

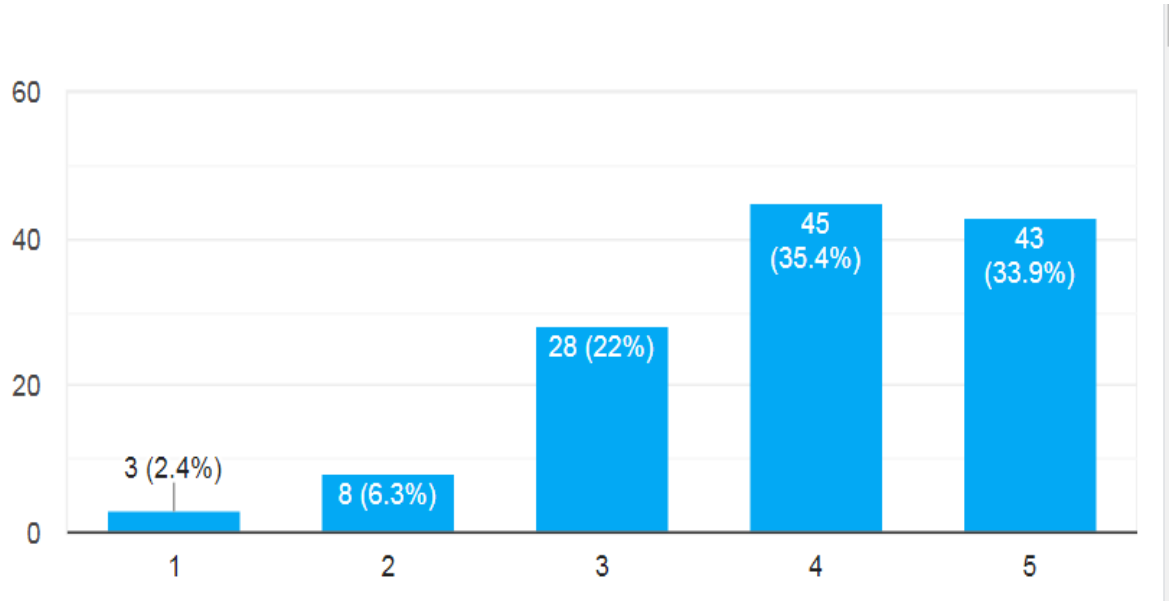
Одговори	Број	У %
Да	70	54,7
Не	24	18,8
Можда, нисам сигуран	34	26,6

Треће питање: *Да ли подржавате децентрализовано дељење образовних ресурса, на пример, да студенти у процесу учења и стицања завршних сертификата могу да користите ресурсе и курсеве и с других факултета?* можда више говори о последичном мењању тржишта образовања које би избрисало границе појединачних институција и прихватљивости да до тога дође. Генерално гледано, употреба других ресурса мимо обавезне литературе нешто је на шта се гледа благонаклоно, јер показује додатно залагање и отвореност студената за стицање додатних знања из конкретних предмета. Велика већина (82,8%) изразила је подршку оваквом виду деловања, док је неутралност задржало 10,9%. Негативан став поседује само 6,3% испитаника. Ограничавајући фактор јесте критичко валидирање прихватљивости података. У реду је уколико се студенти определе да користе ресурсе акредитованих високошколских установа у свету, али, насупрот томе, Википедија или било који извор ресурса без цензуре не може бити прихватљив.

Табела 9: Одговори на питање 3 из упитника

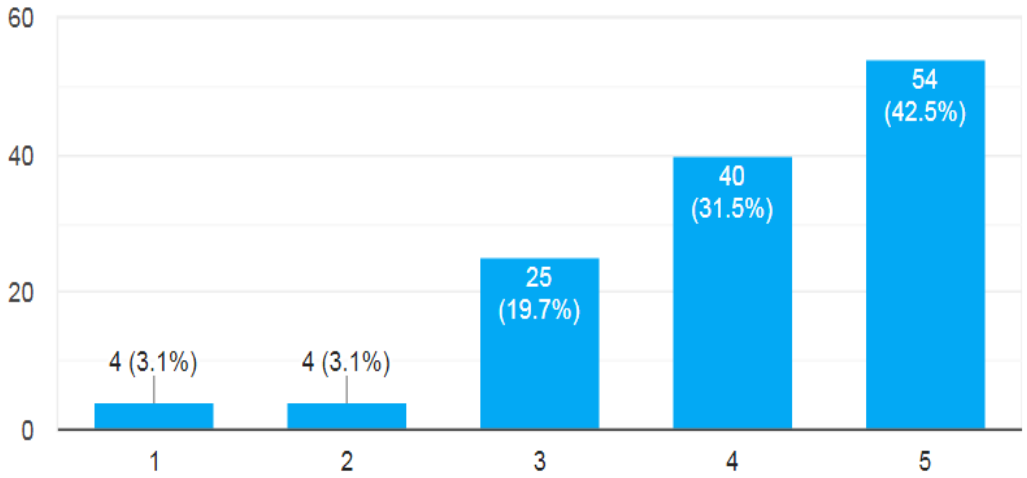
Одговори	Број	У %
Да	106	82,8
Не	8	6,3
Можда, нисам сигуран	14	10,9

Четврто питање: *Како бисте оценили потенцијал блокчејн технологија у образовању која резултира јединственим сертификационим системом?* изискивало је позиционирање на петостепеној скали, при чему је 1 најнижа а 5 највиша оцена. Иако је јединствена сертификација образовања једна од оспораванијих категорија блокчејн технологија, јер отвара мноштво правних питања, у предметном истраживању је високим оценама одговорио већински део испитаника, и то оценом 4 – 35,4%, а оценом 5 – 33,9%. Средњу оцену је доделило 22% испитаника, док је ниже оцене у укупном скору доделило мање од 9%.



Графикон 1: Графички приказ расподеле одговора на питање 4 из упитника

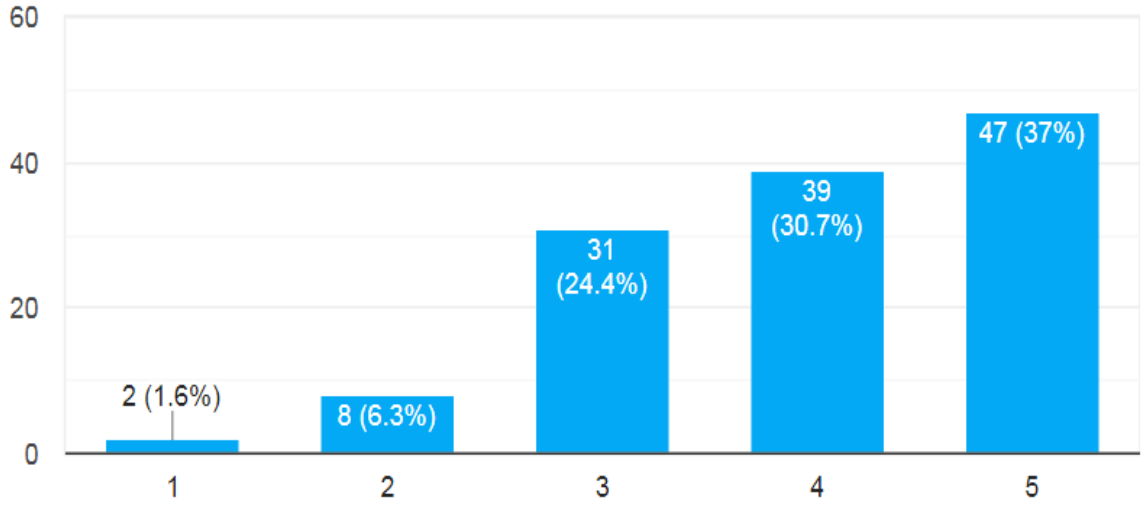
Питање под редним бројем 5 гласи: *Како бисте оценили потенцијал блокчејн технологија у образовању, при коме криптовањем усвојен топографски алгоритам спречава мењања података, додавање чињеница и нетачност података?* Ово питање такође је изискивало позиционирање на петостепеној скали, при чему је 1 најнижа а 5 највиша оцена. Могућност примене технологије која спречава мењање података, додавање чињеница и нетачност података највишом оценом оценило је 42,5% испитаника, а оценом 4 њих 31,5%. Овако висок скор указује и на то да испитаници препознају да су ови проблеми заступљени у образовним системима. Средњу оцену дало је близу петине испитаних и тек мали број њих определило се за ниске оцене.



Графикон 2: Графички приказ расподеле одговора на питање 5 из упитника

Наредно, шесто питање гласи: *Како бисте оценили потенцијал блокчејн технологија у образовању да трансформише вођење евиденције о сертификатима и акредитивима студената у институцијама за учење, њеном применом нема потребе за посредником у верификацији диплома, сертификата, диплома и других академских радова?* Ово питање изискивало је позиционирање на петостепеној скали, при чему је 1 најнижа а 5 највиша оцена. И ово питање однело је висок просек оцена, чија је средња вредност 3,95 на укупном броју испитаника, што потврђује став великог броја

анкетираних да би таква примена блокчејна умногоме олакшала и заштитила процес сертификације и акредитације постигнутих образовних резултата. Ову могућност највишом оценом оценило је 37% испитаника, оценом 4 њих 30,7 %, а скоро четвртина укупног броја испитаника оценом 3. Ниско вредновање забележено је код 6,3% испитаника (оцена 2), а само 1,6% испитаних доделило је најнижу оцену.



Графикон 3: Графички приказ расподеле одговора на питање 6 из упитника

Седмо питање: *Да ли мислите да би примена блокчејн технологија у образовању смањила случајеве злоупотреба у образовању?* односи се на спречавање манипулација, промене и брисање информација из образовних система, као и доделе незаслужених сертификата. Као највећи проблем у вези са овом темом у литератури препозната је додела незаслужених диплома, најчешће политичарима. Наиме, примена блокчејн технологија заиста се темељи на „принципима матичара" и не дозвољава мењање или фалсификовање података који су нужни за сертификацију. У пракси то значи да неко ко није присуствовао предавањима, извршавао задатке на вежбама, излазио на колоквијуме, испите, реализовао предиспитне обавезе, учио и савладао градиво – не може положити испит и коначно стећи диплому. У наставку је дат преглед добијених резултата, који носе високу сагласност, уз позитиван одговор код 61,4% испитаника.

Табела 10: Одговори на питање 7 из упитника

Одговори	Број	У %
Да	78	61,4
Не	15	11,8
Можда, нисам сигуран	34	26,8

Осмо питање: *Колико извесним оцењујете футуристички сценарио образовања заснован на блокчејн технологијама, кроз потпуну дигитализацију и децентрализацију образовања, и издавања образовних сертификата, и наступање концепта целоживотног учења?*

Табела 11: Одговори на питање 8 из упитника

	Одговори	Број	У %
●	Врло је извесно да ће се то ускоро догодити.	38	29,9
●	Делимично је сигурно да би се то могло догодити, али када у будућности.	46	36,2
●	Нисам сигуран да ће се такав подухват остварити.	30	23,6
●	Делимично је неизвесно да ли ће се то и када догодити.	9	7,1
●	Врло је неизвесно да ће се то догодити.	4	3,1

Посматрајући поларизацију ставова, уочавамо да готово две трећине испитаника верује да ће блокчејн имати своју примену у образовању, уз разлику да 29,9% њих верује да ће то бити веома брзо, а 36,2% није сигурно када ће се то догодити у будућности. Насупрот томе, једна трећина испитаника не оцењује овај подухват као известан – 23,6% изражава сумњу да ће се он остварити, 7,1% верује да је неизвесно да ће се то икада догодити и само 3,1% испитаника верује да се то никада неће догодити.

Девето питање: *Да ли слажете с констатацијом да недостатак поверења у технологију и недостатак знања о томе како искористити потенцијал решења blockchain-in-education могу довести до спорог усвајања таквих иновација на тржишту*? показало је да се 43% испитаника слаже у потпуности, 35,2% делимично се слаже, несигурност изражава 14,1%, делимично неслагање 3,9% и исто толико потпуно неслагање. При тумачењу такве дистрибуције одговора потребно је истаћи да отпор за усвајање нових технологија постоји увек, али је он обично интензивнији у друштвима ниже технолошке развијености, у која би се могла сврстати и Србија.

Табела 12: Одговори на питање 9 из упитника

	Одговори	Број	У %
●	Слажем се у потпуности	55	43
●	Делимично се слажем	45	35,2
●	Нисам сигуран/сигурна	18	14,1
●	Делимично се не слажем	5	3,9
●	Потпуно се не слажем	5	3,9

Десето питање: *Какве врсте блокчејн технологија у образовању са аспекта јавности треба да постоје?* понудило је три одговора: јавни, приватни и они ограниченог приступа. Занимљиво је да је 36,2% испитаника опредељење поклонило „јавном", што би у пракси значило да било ко, без обзира на старосну, националну или другу припадност, може глобално приступити било ком систему образовања. Тек петина, односно 20,5% испитаника, одговорила је да би требало да ови системи буду

приватни, што даје одређену могућност контроле и селекције у смислу ко им може приступити и под којим условима. Највећи број испитаника (43,3%) изнео је став да би требало да они буду ограниченог приступа, што се поклапа и са оптималним ставовима изнетим у теорији примене блокчејн технологија у образовању.

Табела 13: Одговори на питање 10 из упитника

Одговори		Број	У %
	Јавни	46	36,2
	Приватни	26	20,5
	Ограниченог приступа	55	43,3

Одговори на претпоследње питање: *Да ли би овакав систем образовања базиран на блокчејн технологијама – који може да складишти записе о учењу у поузданим базама, постави нови начин дистрибуције знања, обезбеди веродостојне дигиталне сертификате, реализује дељење ресурса за учење помоћу паметног уговора и заштитити интелектуалну својину шифровањем података – има више користи за студенте или за наставнике и образовне институције?* истичу да више предности могу имати студенти, према уверењу 57,1% испитаника, него наставници, према 42,9%.

Табела 14: Одговори на питање 11 из упитника

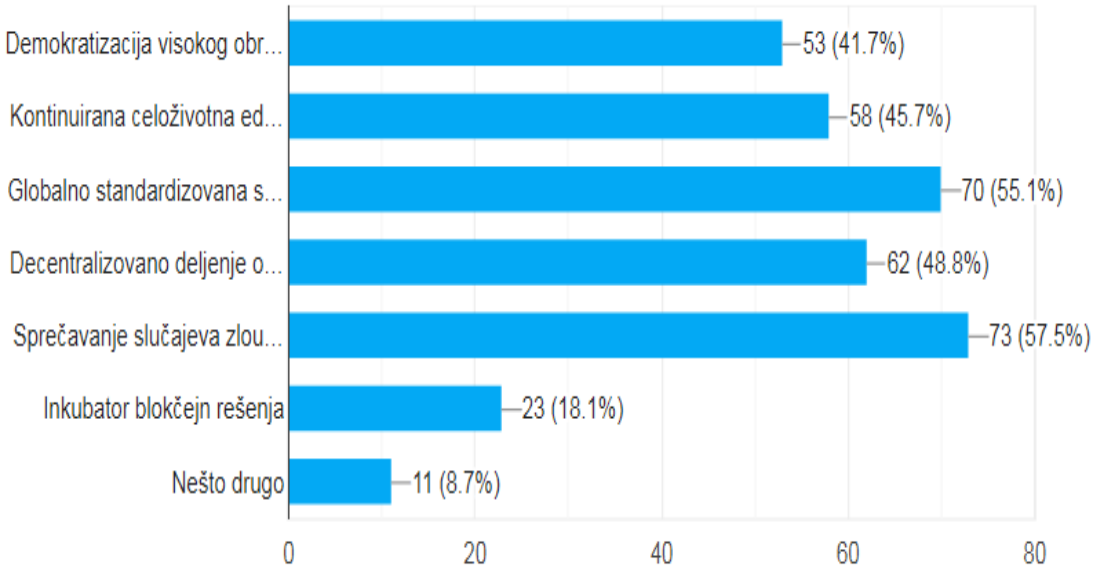
Одговори		Број	У %
	За студенте	72	57,1
	За наставнике и образовне институције	54	42,9

Последње питање: *Молимо вас да од понуђених подручје фокуса блокчејн технологија у образовању изаберете три које сматрате најзначајнијим доприносима квалитету образовања* пружало је избор између више понуђених, али не коначних опција, од којих су издвојене:

- демократизација високог образовања;
- континуирана целоживотна едукација;
- глобално стандардизована сертификација и акредитиви студената;
- децентрализовано дељење образовних ресурса;
- спречавање случајева злоупотреба и манипулација у образовању;
- инкубатор блокчејн решења;
- нешто друго.

На првом месту налази се следећа опција као подручје фокуса блокчејн технологија у образовању: „спречавање случајева злоупотреба и манипулација у образовању” са 57,5%, следи „глобално стандардизована сертификација и акредитиви студената” са 55,1% укупног броја гласова анкетираних. „Децентрализовано дељење образовних ресурса” однело је 48,8% гласова,

„целоживотна едукација” следи са 45,7%, а потом „демократизација високог образовања” са 41,7%. Знатно ниже проценте бележе „инкубатор блокчејн решења” са 18,1% и опција „нешто друго” са 8,7%.



Графикон 4: Графички приказ расподеле одговора на питање 12 из упитника

5.2 Пројектни захтеви

5.2.1 Спецификација захтева и случајеви коришћења

Развијена апликација је место на којем је могуће објавити семинарски рад, део пројекта који могу евалуирати други студенти или стручњаци из праксе, будући послодавци. Уведен је алгоритам који елиминише рецензије у случају примећене злоупотребе. Радови објављени преко апликације доступни су свима да би се пратили принципи отворене науке.

- Постоји база семинарских радова;
- Сваки семинарски рад има дефинисано:
  - ✓ наслов и *GUID*
  - ✓ аутор/аутори (*GUID*)
  - ✓ научна област и подобласти
  - ✓ апстракт
  - ✓ кључне речи
  - ✓ документ у ПДФ формату
  - ✓ листу референтних евалуација
  - ✓ изведену оцену на основу добијених евалуација
- Сваки корисник може без логовања да прегледа списак семинарских радова по областима, изабере рад, прочита га онлајн или преузме у ПДФ формату;
- Корисник који се региструје може да постави рад или уради евалуацију;
- Корисник има дефинисано:

- ✓ име, презиме и *GUID*
- ✓ списак семинарских радова
- ✓ оцену изведену из евалуације радова, која се прерачунава са сваком следећом евалуацијом
- ✓ списак евалуација
- ✓ оцену евалуатора

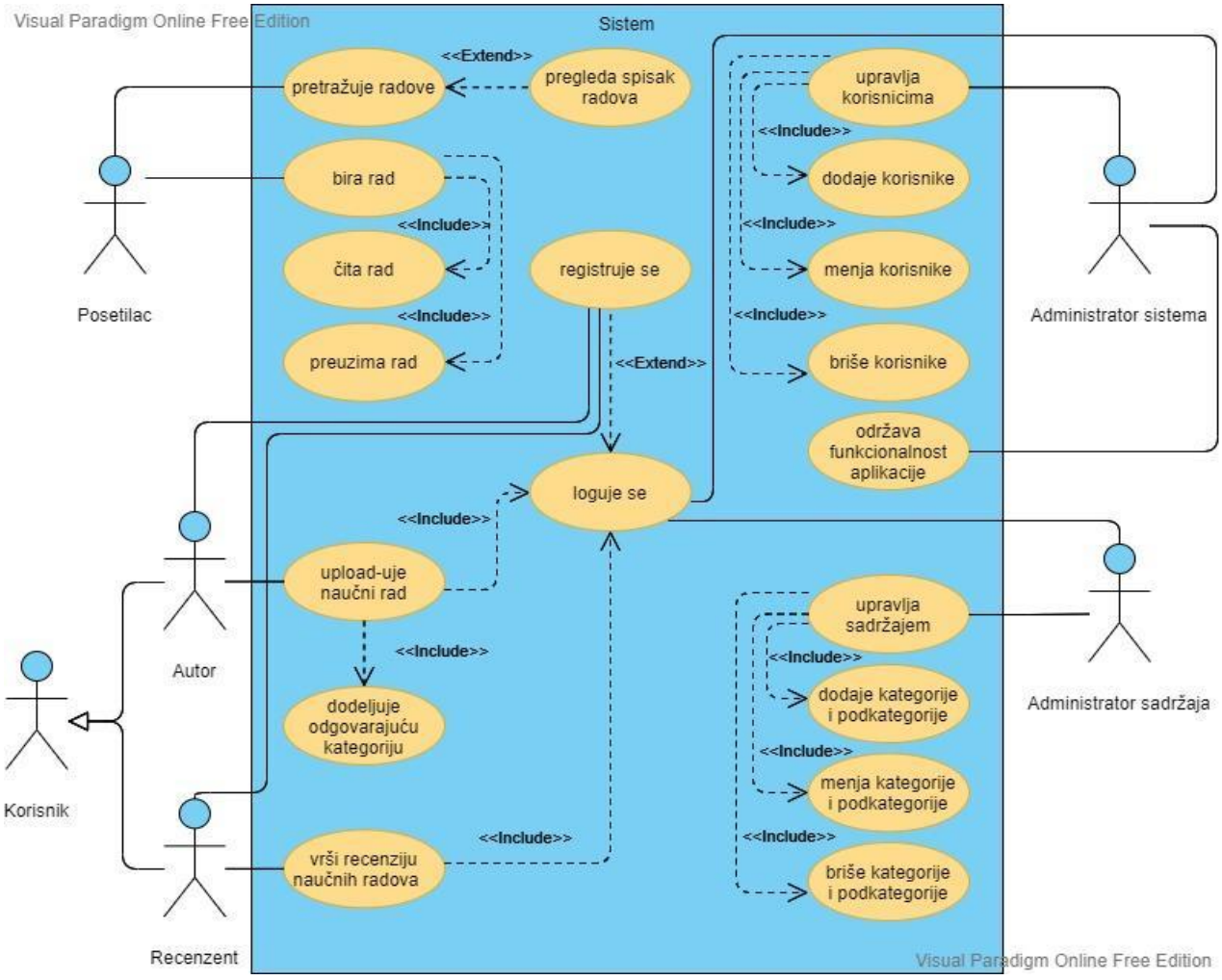
- Постоји могућност постављања семинарског рада који има дефинисано:
  - ✓ наслов семинарског рада и *GUID*
  - ✓ име аутора (*GUID*)
  - ✓ научну област и подобласти
  - ✓ кључне речи
- Постоји могућност претраживања базе семинарских радова по:
  - ✓ аутору
  - ✓ научној области (опционо)
  - ✓ наслову
  - ✓ кључним речима
  - ✓ висини рецензије са опцијом сортирања
- Постоји могућност постављања евалуације за семинарски рад која има дефинисано:
  - ✓ наслов семинарског рада и *GUID*
  - ✓ име аутора (*GUID*)
  - ✓ име евалуатора (*GUID*)
  - ✓ евалуација у облику: писана форма, оцена, препоручујем ДА/НЕ
- Постоји могућност оцењивања рецензента на основу постојећих рецензија. Оцена рецензента представља тежински фактор његове рецензије;
- Постоји могућност искључивања појединих рецензија уколико је препознатљив Фраудов модел;
- Постоји могућност приказа листе аутора по рангу уз наведену област у којој објављује рад, на првој страни: на пример: најбољи аутори (прва три или пет);
- Постоји могућност приказа листе рецензената по рангу, на првој страни: на пример: најбољи рецензенти (прва три или пет);
- Права регистрованих корисника:
  - ✓ Постоји улога „корисник”, која има право да постави семинарски рад на веб-апликацију и додели је одговарајућој категорији и да врши евалуацију семинарских радова и пројеката;
  - ✓ Постоји улога „администратор”, која може да управља корисницима и отклања проблеме на апликацији (у случају да неко поставља непримерени садржај, може да санкционише);
  - ✓ Постоји улога „администратор садржаја”, која има право да управља, додаје и брише области и подобласти.

5.3 Пројектовање и имплементација решења

5.3.1 Пројектовање система

Основни принцип дизајна апликације јесу једноставност изгледа корисничког интерфејса и кретања кроз апликацију.

На слици у наставку приказане су улоге и случајеви коришћења апликације за колаборативно учење која омогућава студентима да постављају своје и евалуирају семинарске радове и пројекте својих колега. Омогућено је и студентске радове да евалуирају стручњаци из праксе и будући послодавци. Корисник интегрише улоге аутора и рецензента, као и што администратор интегрише улоге администратора садржаја и система.



Слика 27: Улоге и случајеви коришћења

5.3.2 Улоге корисника

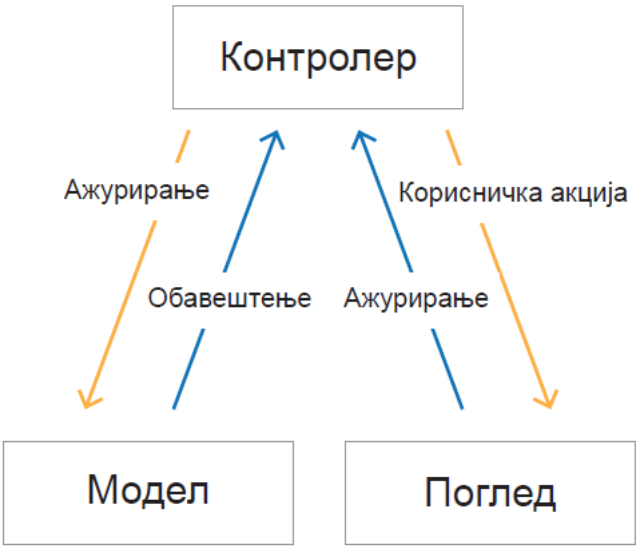
Корисник који није логован може да прегледа списак семинарских радова по областима, изабере рад, прочита га онлајн или га преузме у ПДФ формату.

Улога „корисник”: Успешном регистрацијом на апликацију аутоматски се додељује улога „корисник” новом члану. По завршеној регистрацији, корисник ће бити прослеђен аутоматски на страницу за логовање на апликацију, где уноси своје креденцијале. Као што је већ напоменуто, улога „корисник” омогућава објаву семинарског рада, као и давање рецензија другим објављеним семинарским радовима у апликацији.

Улога „администратор”: Администратору ће се по успешном логовању на апликацију приказати линк ка „администраторском панелу” у горњем десном углу сваког прозора у апликацији. Унутар панела, администратор има увид у све кориснике, семинарске радове, категорије и поткатегорије, као и у све дате рецензије. Напомена: У почетној фази су улоге „администратор” и „администратор садржаја” обједињене.

5.3.3 Архитектура система

При изради апликације коришћена је *MCV* (*Model-View-Controller*) архитектура. *MCV* архитектура подразумева постојање три врсте компонената (*Model-View-Controller*), које се међусобно налазе у посебно дефинисаном односу.



Слика 28: MCV архитектура

Model – садржи податке у облику погодном за конкретну примену. Садржи и логику апликације, дефинишући шта све можемо да урадимо с датим подацима и базом података.

View – приказује податке из модела у формату погодном за интеракцију.

Controller – координише моделе и *view*-ове, углавном на основу корисниковог уноса. Када се деси неки догађај, на пример клик на неко дугме, обавештава модел о томе.

5.3.4 База података

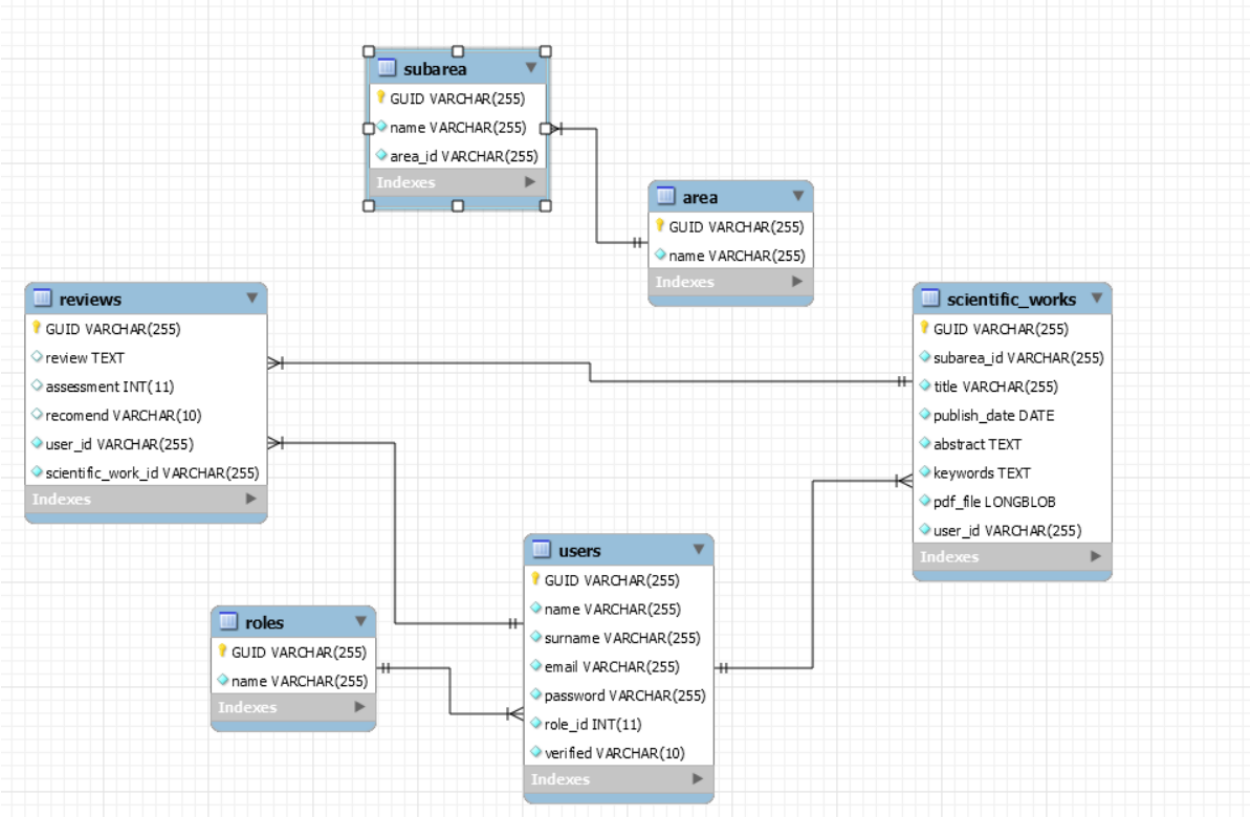
У првој фази примене модела, а у сврху тестирања предложеног модела, израђен је сајт с базом података која је рађена у *MySQL* језику и представља први слој задужен за

управљање учесницима система. Одређени су приступи са улогама и привилегијама, али се одвија и колаборативно учење. На доњој слици је приказ табела и колона у табелама.

Трансакције система су похрањене у блокчејну, као централној тачки система, и сви учесници укључени у систем у интеракцији су с блокчејном. Важно је истаћи да први слој представља релациону базу и може се схватити као ниво управљања учесницима система. У оквиру овог дела одређени су приступи са улогама и привилегијама, али се одвија и колаборативно учење. Други ниво садржи трансакције. Евалуација, односно упаривање евалуатора и предмета евалуације, одвија се у блокчејн бази података. Процес почиње када студент добије одређени задатак од наставника.

У развијеном моделу, студент мора показати знање у решавању задатка и евалуацији других радова. Задаци са евалуацијом сачувани су у бази података и потврђени су од стране наставника. У интересу студента је да евалуација буде што боља. Ако не постоји консензус, студент губи своју репутацију.

Базом података евалуација управља се аутономно и помоћу дистрибуираног сервера временске ознаке (енг. *timestamp*) на равноправној (енг. *peer to peer*) мрежи. Ради поједностављења интероперабилности између привредника (компанија) и евалуационог дела система заснованог на блокчејн решењу, омогућено је да приступају овом делу директно кроз интеграциони слој који је део система.



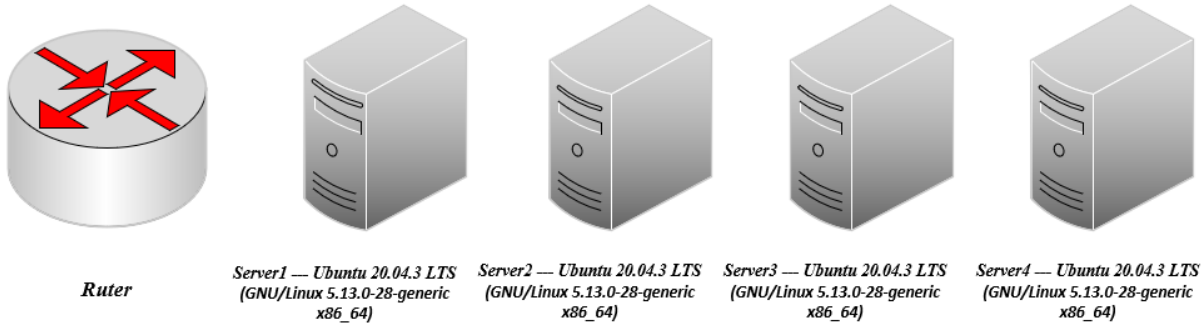
Слика 29: Шема базе података реализованог решења

5.3.5 Имплементација

Код апликације је постављен код хостинг провајдера *Unlimited* (*United Internet*). Инсталирани су потребни програмски пакети и код преко C-панела премештен је на

сервер. Код истог провајдера изнајмљен је и домен *open-rev.com*. Апликација је постављена на домен. Апликација је рађена у два програмска језика. За *backend* коришћен је *PHP + MySQL* база података. У фронтенд делу коришћена је *JavaScript „framework" React*.

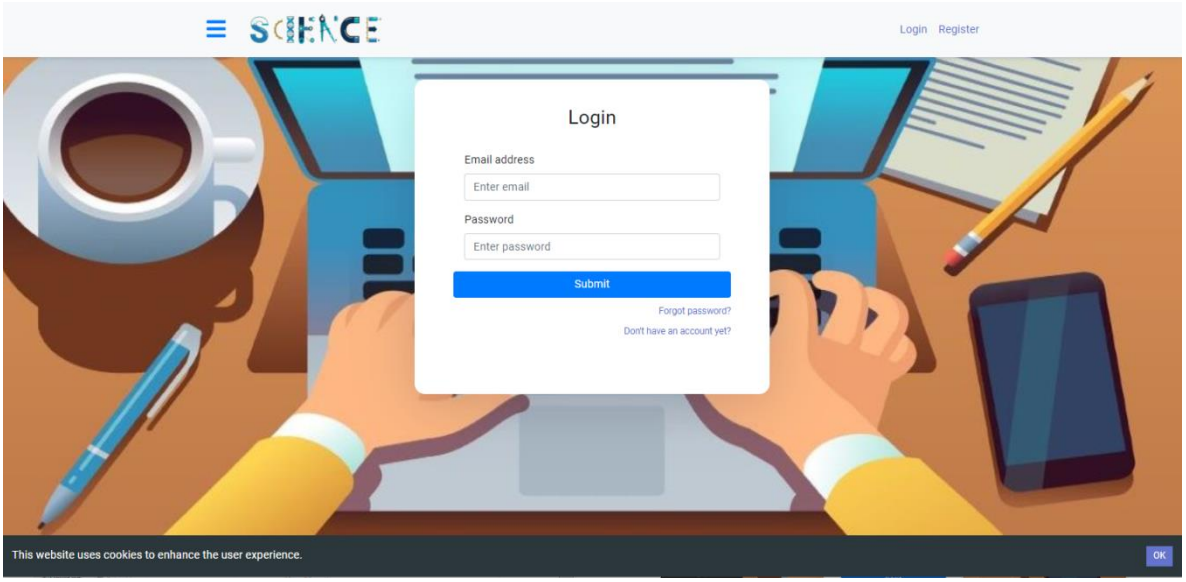
На наредној слици приказана је инфраструктура.



Слика 30: Инфраструктура блокчејн мреже

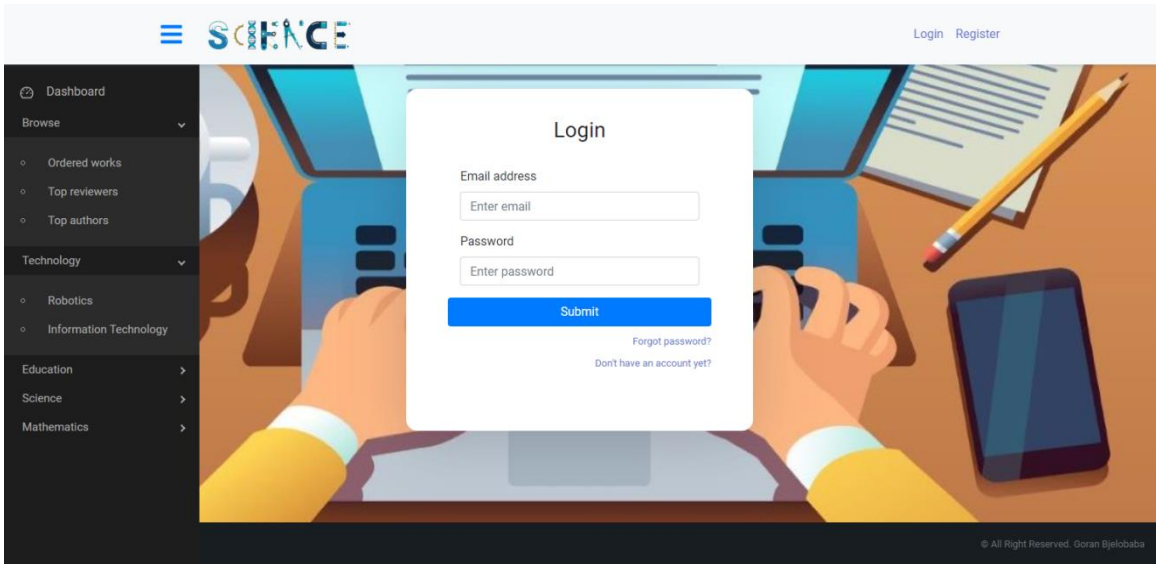
5.3.6 Приказ реализованог решења

Апликацији се приступа преко *URL*-а: *open-rev.com*. Почетни екран кориснику даје могућност да се региструје, логује, као и да прегледа радове по рангу или категоријама, да их отвори и прочита.

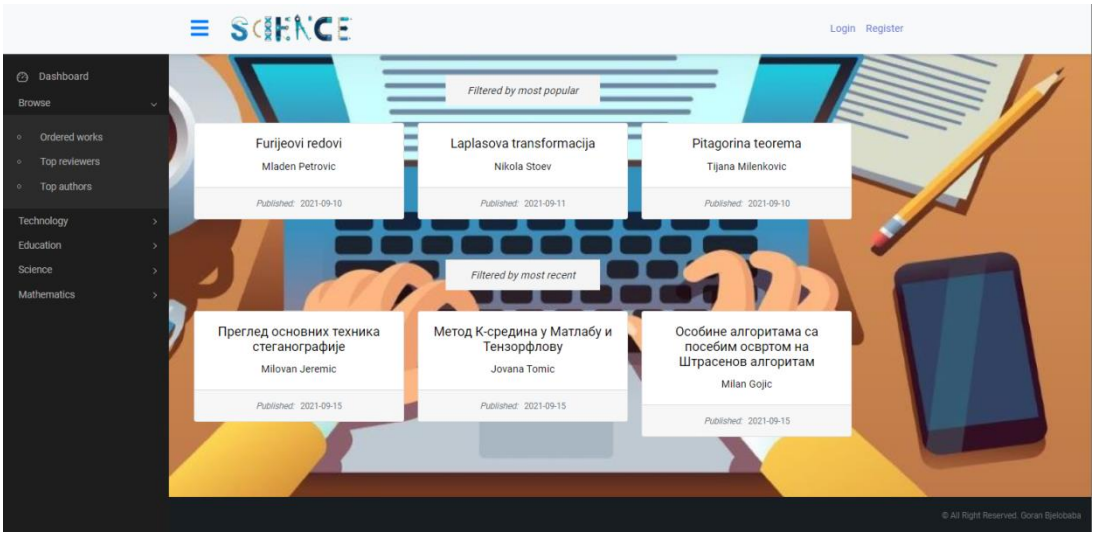


Слика 31: Почетни екран за пријављивање

Сајдбар нерегистрованог корисника приказан је на слици испод. Корисник може да се определи да радове ређа по највећој оцени или по категоријама.

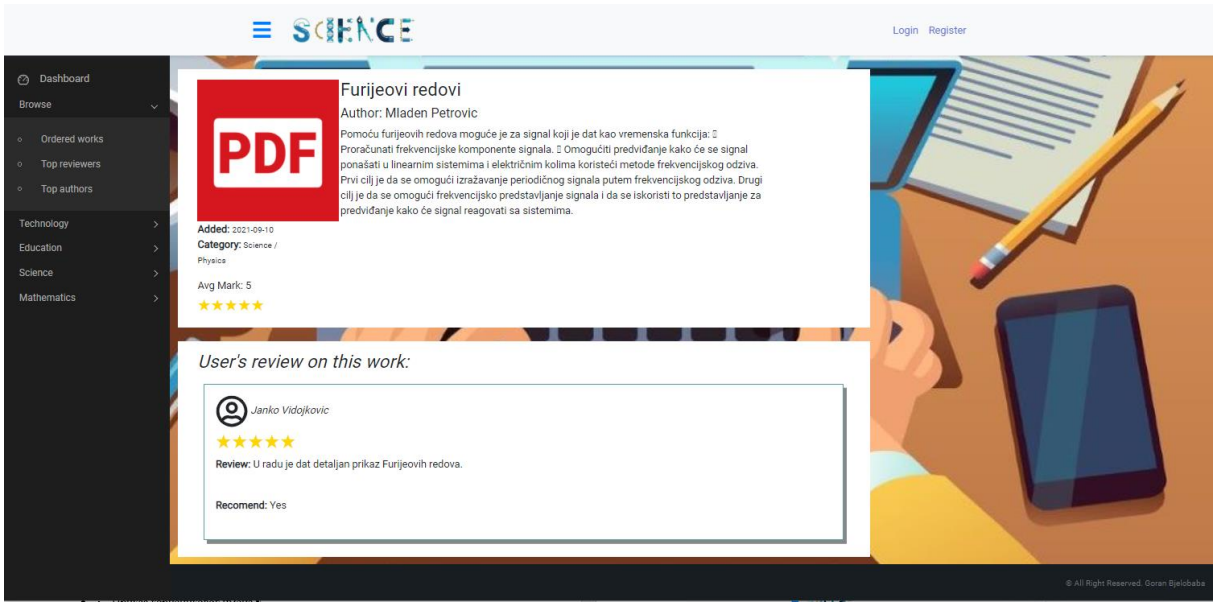


Слика 32: Почетни екран за пријављивање с приказом сајдбара



Слика 33: Приказ семинарских радова за нерегистрованог корисника

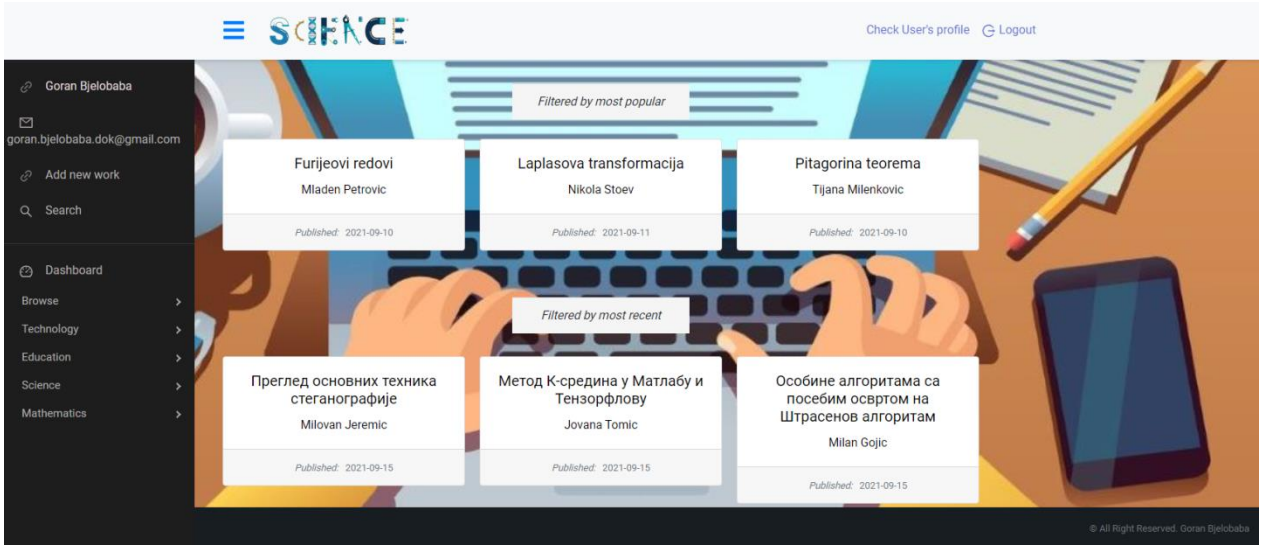
Екран за приказ семинарског рада и свих његових евалуација добија се одабиром једне од кућица на слици изнад. Нерегистровани корисник може да прочита семинарски рад и погледа све евалуације (Слика 34).



Слика 34: Семинарски рад и поглед евалуација

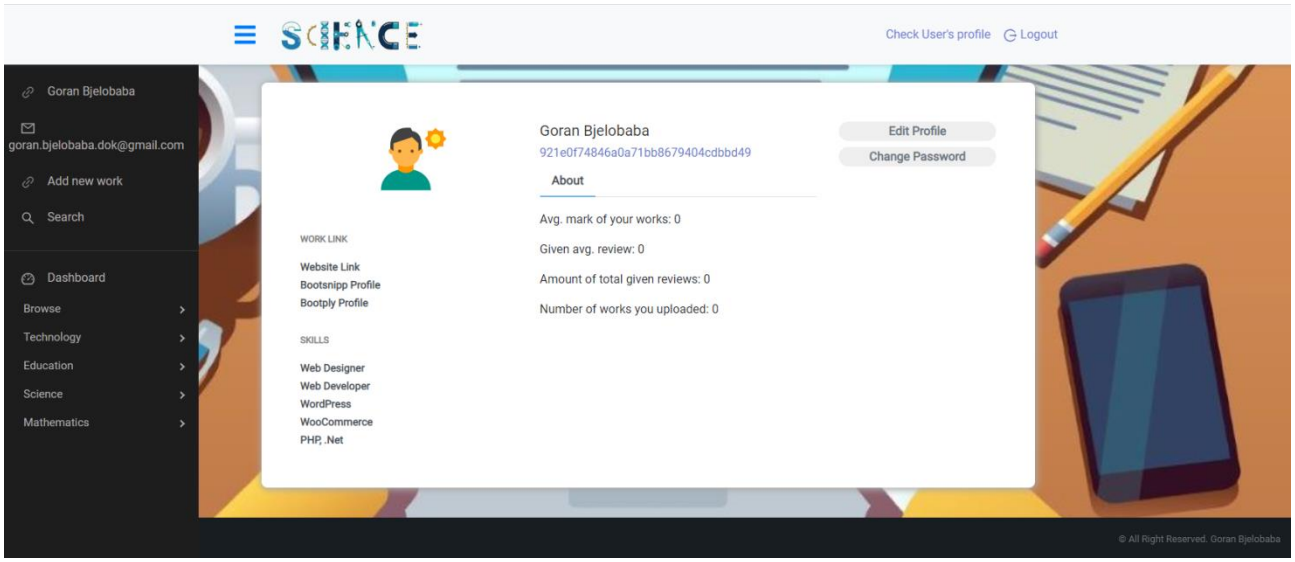
Улоговани корисник има нешто другачији приказ, као и сајдбар (Слика 35). Навигациони „сајдбар” садржи следеће елементе:

- приказ корисниковог имена,
- могућност „LogOut”;
- могућност одласка на администрациони панел (уколико је корисник администратор);
- приказ свих категорија и поткатегорија на чији се клик отварају радови.



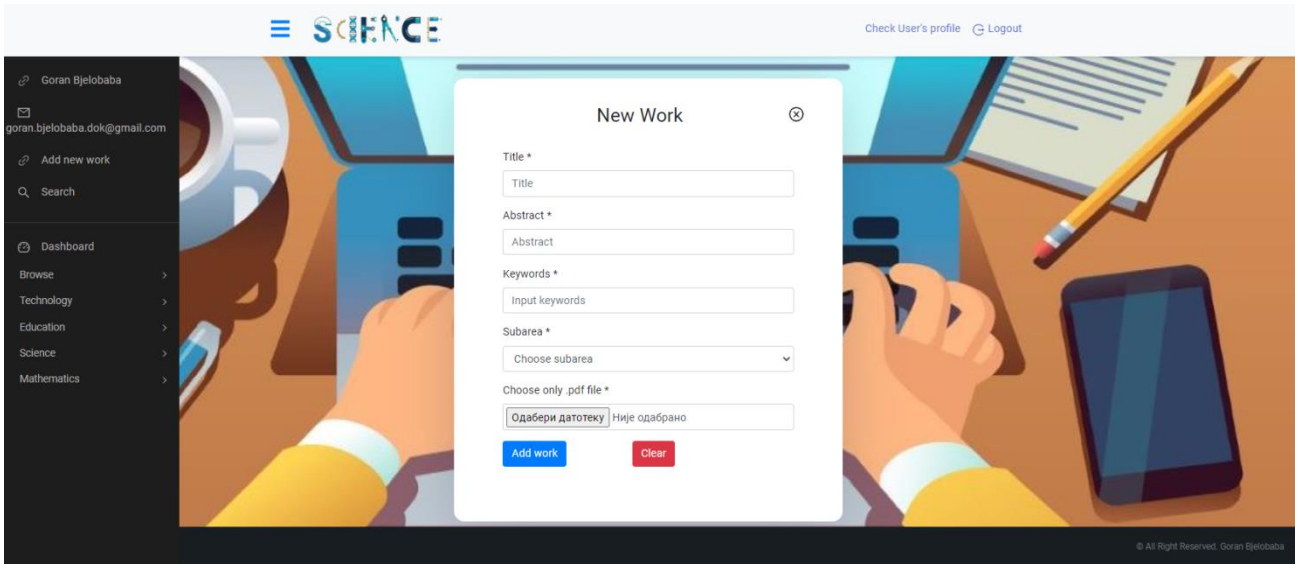
Слика 35: Приказ екрана пријављеног корисника

Корисник може погледати свој профил, а свој *GUID* копирати и послати уколико жели да га други корисник лако пронађе у апликацији.



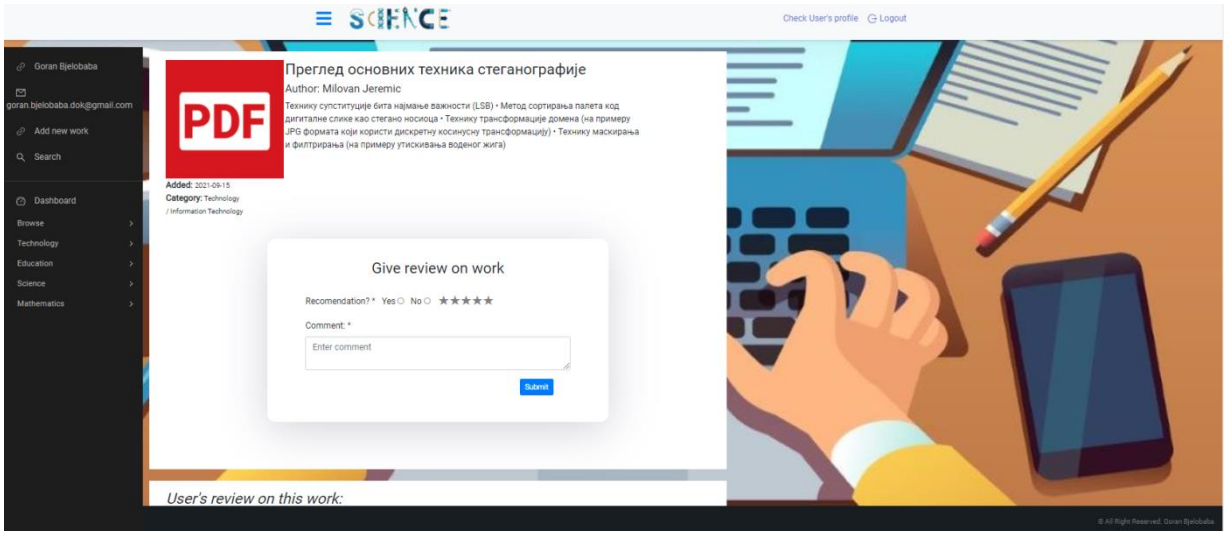
Слика 36: Приказ профила корисника

Корисник може да постави нови рад, при чему обавезно мора да унесе сва поља која су означена звездицом: наслов, апстракт, област и подобласт, кључне речи и документ у ПДФ формату.



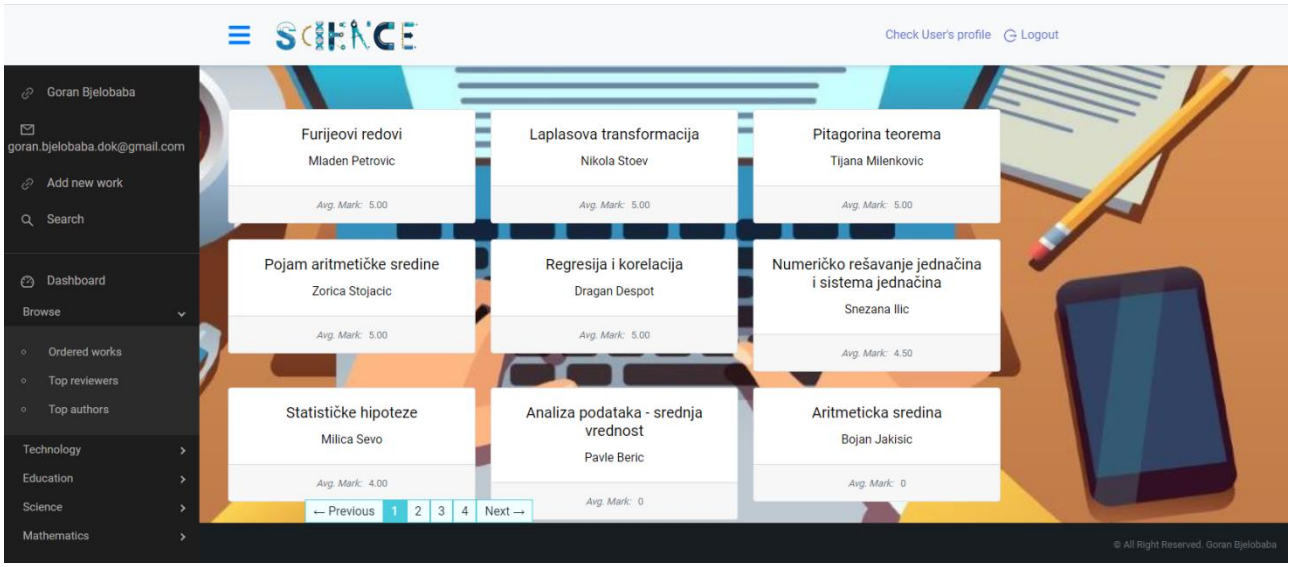
Слика 37: Приказ уноса новог рада пријављеног корисника

Пријављени корисник може да постави рецензију рада (Слика 38).

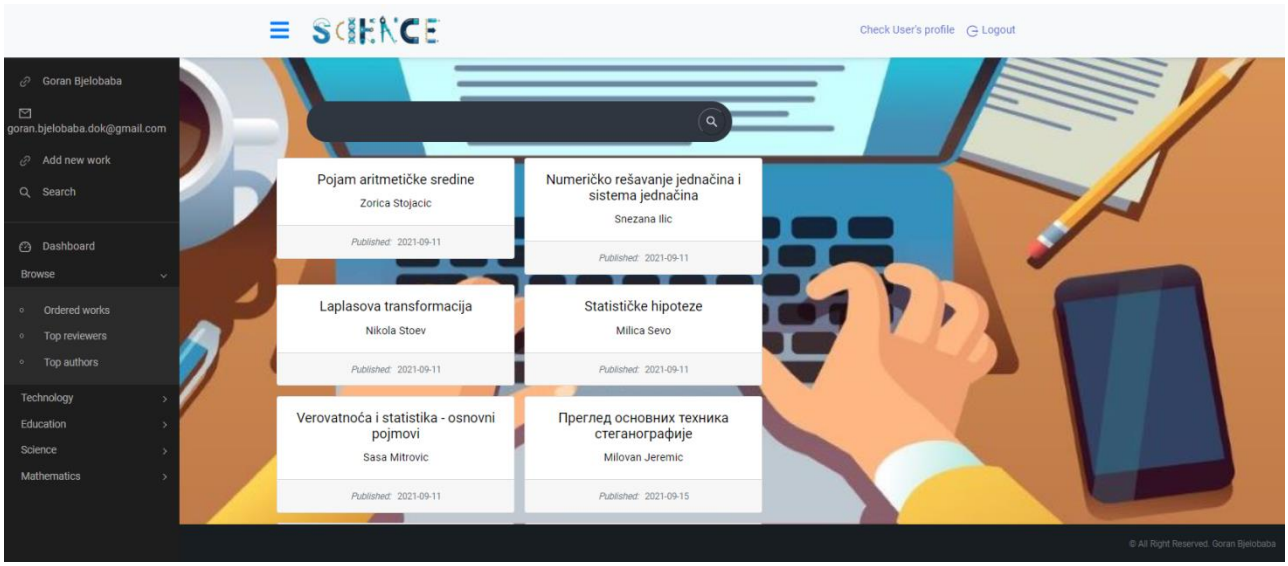


Слика 38: Евалуација рада

Корисник може да прегледа семинарске радове рангиране по најбоље добијеним оценама. Такође, може да претражује радове по кључним речима, притиском на тастер за претрагу у сајдбару.

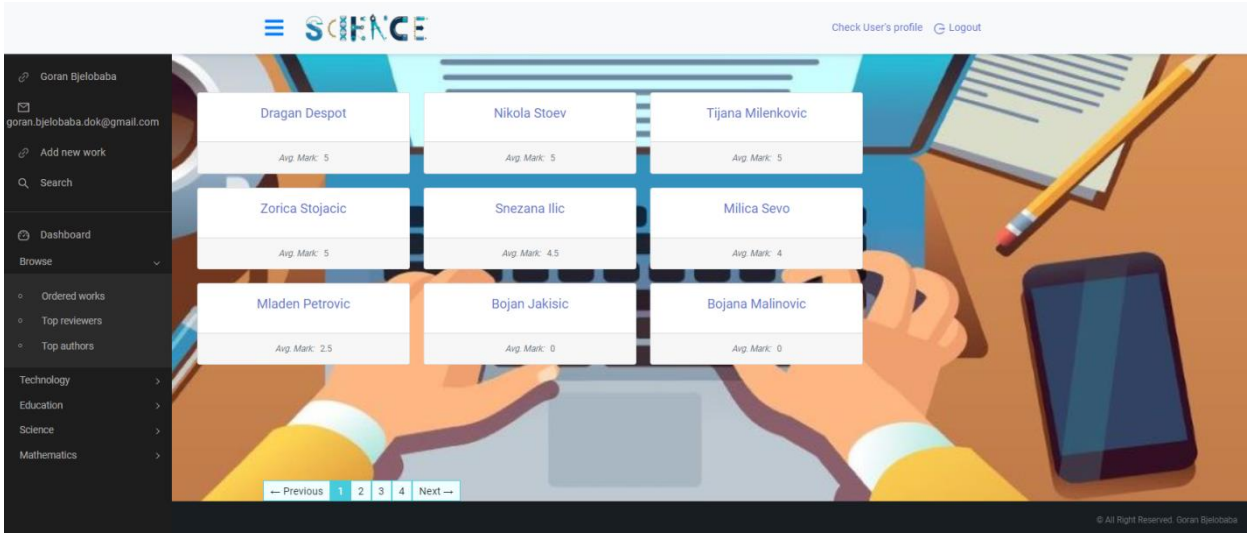


Слика 39: Преглед семинарских радова по оцени

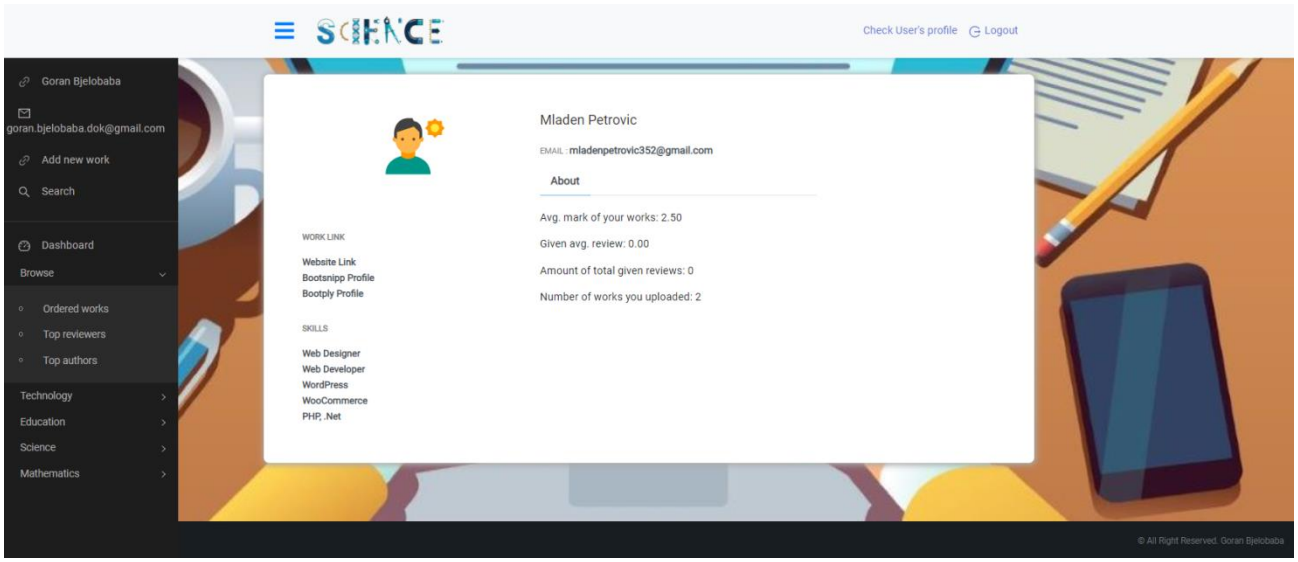


Слика 40: Претраживање радова по кључним речима

Корисник може да погледа листу аутора и евалуатора и да кликом на поље које приказује корисника уђе и погледа његове податке: објављене семинарске радове, евалуације које је дао, просечну оцену, квалификације и контакт линкове.



Слика 41: Приказ листе аутора и евалуатора

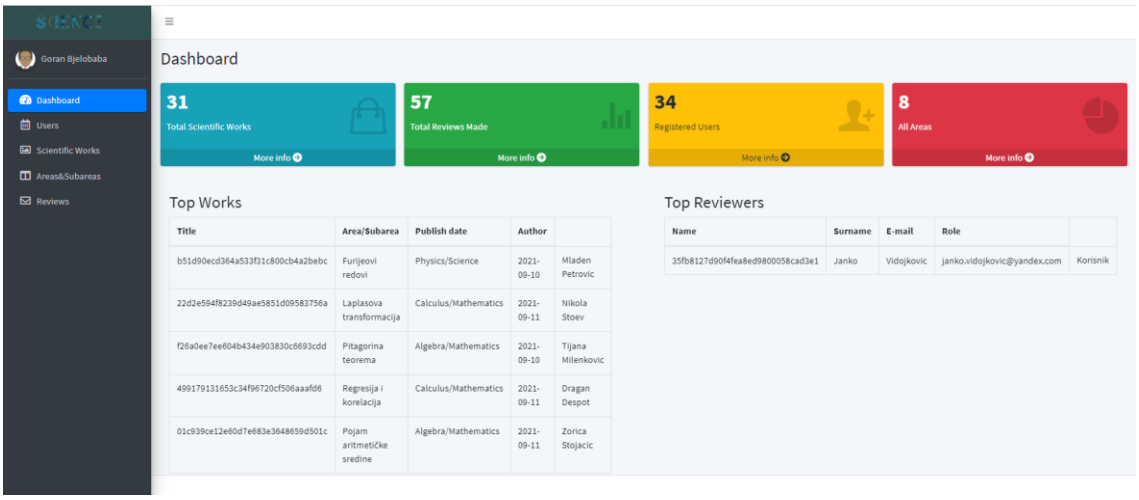


Слика 42: Профил аутора и евалуатора

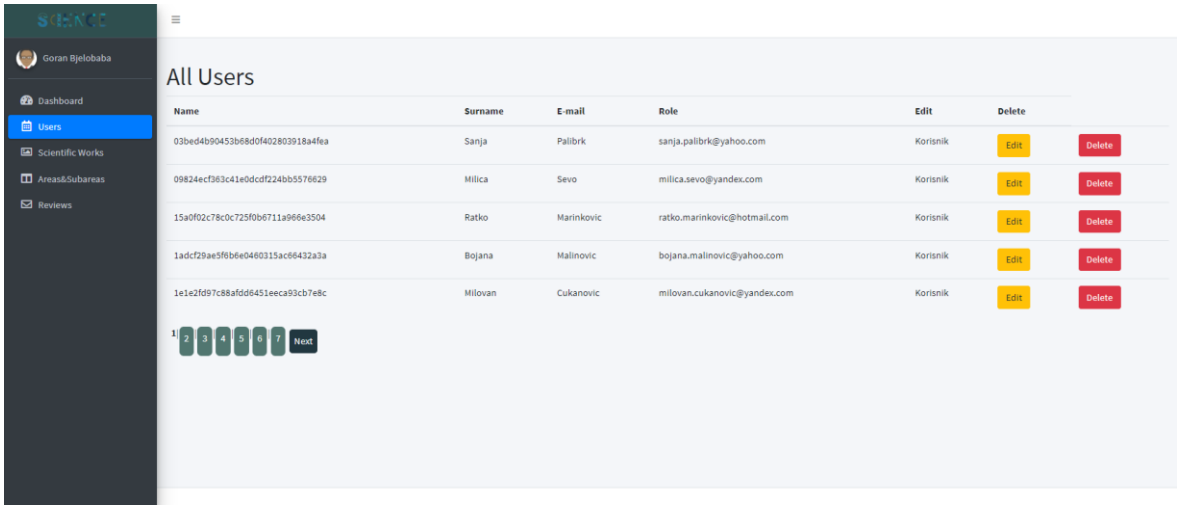
5.3.7 Администраторски панел

Омогућава администрацију преглед и администрацију корисника, радова и рецензија.

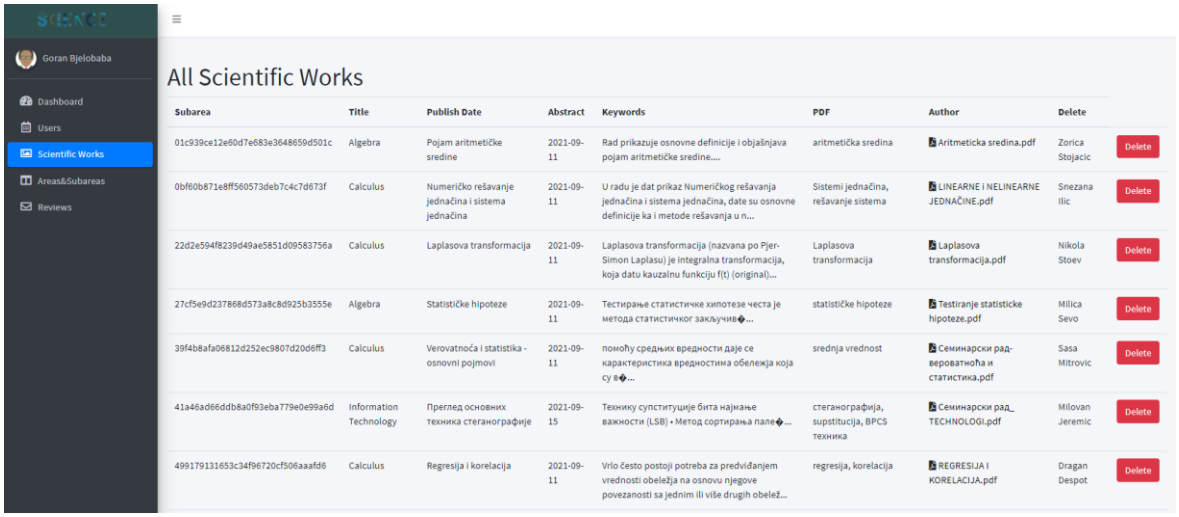
С обзиром на то да су улоге „администратор" и „администратор садржаја" обједињене, администратор има могућност да прегледа и администрира и научне области и подобласти.



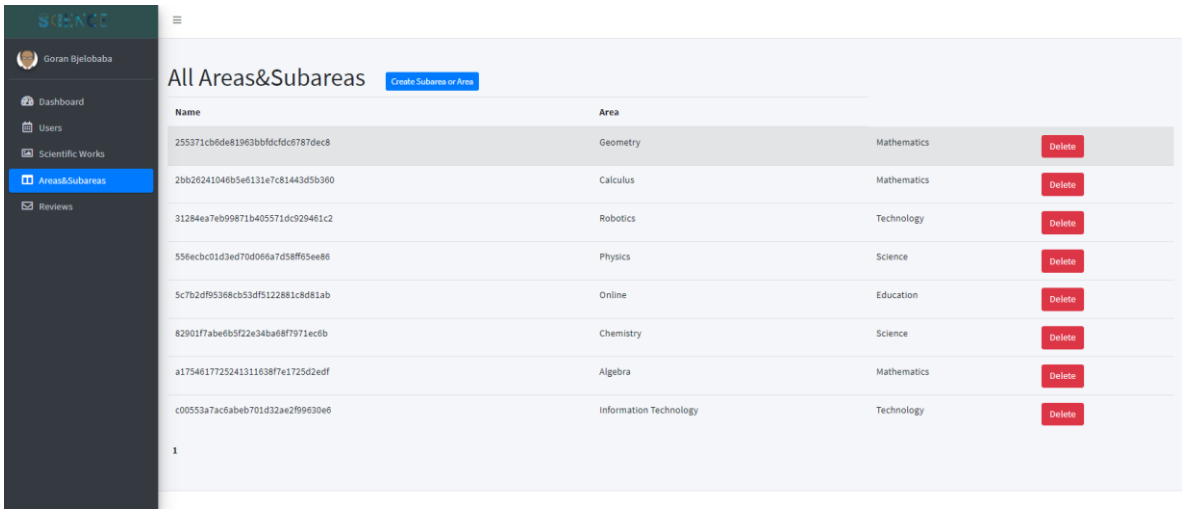
Слика 43: Приказ екрана пријављеног администратора апликације



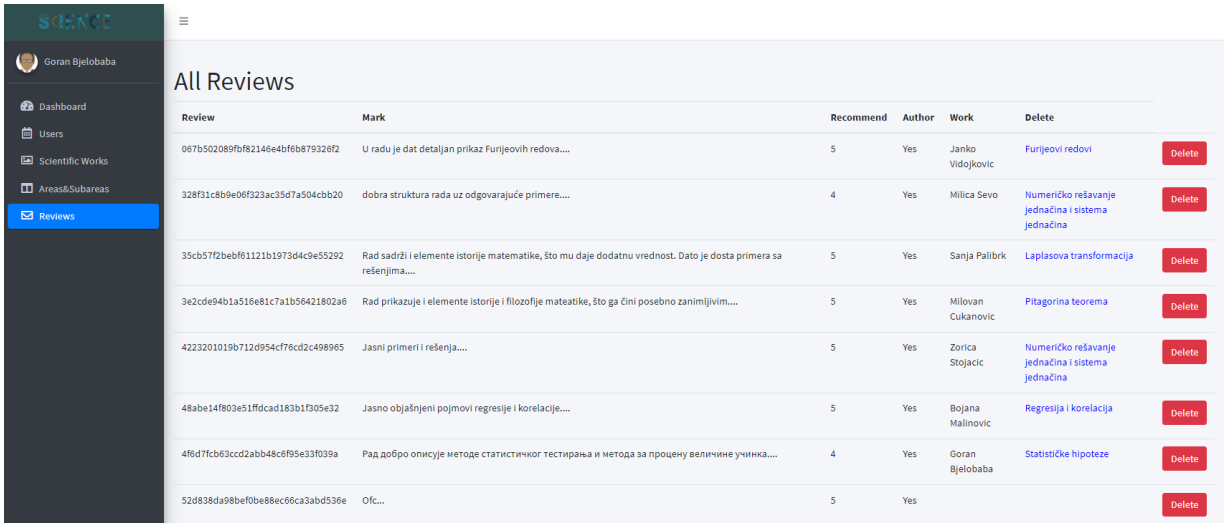
Слика 44: Администраторски приказ корисника



Слика 45: Администраторски приказ објављених радова



Слика 46: Приказ научних области и подобласти у апликацији



Слика 47: Приказ евалуација објављених радова

5.3.8 Одржавање апликације

За безбедан и непрекидан рад развијене апликације потребно је редовно одржавање:

- Једном недељно треба радити бекап апликације. У С-панелу постоје алати који то омогућавају;
- Препорука је да се на диску чувају бар две последње верзије бекапа. У случају да треба вратити неку од претходних верзија апликације, потребно је позвати техничку подршку хостинг провајдера;
- Ванредни бекап треба урадити уколико су предвиђене измене на апликацији или бази како би се у случају грешке могла вратити претходна верзија софтвера;
- Једном недељно треба проверавати попуњеност диска на С-панелу хостинг провајдера;
- Повремено ће бити потребно урадити ажурирање *SW* пакета који се користе. Поруке о новим верзијама *SW* пакета налазиће се на С-панелу;
- Хостинг провајдер нуди бесплатан *SSL* сертификат, тако да његово обнављање није потребно;
- Једном годишње треба обновити закуп хостинга и домена.

5.3.9 Блокчејн имплементација

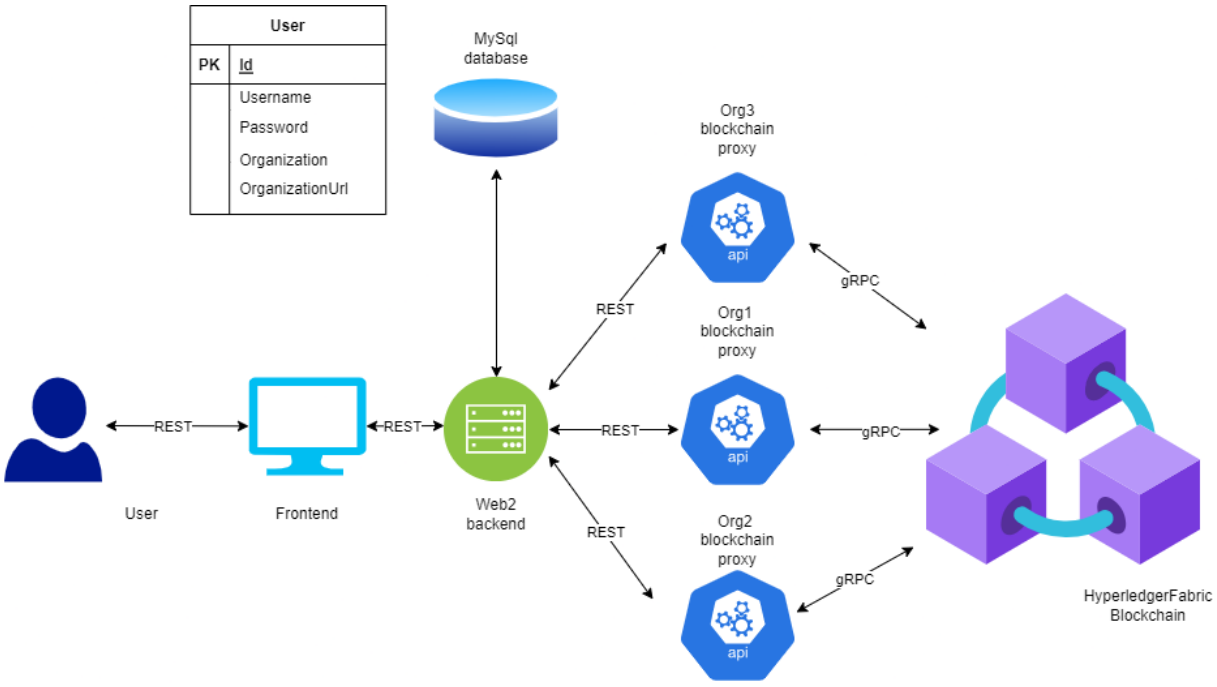
За блокчејн имплементацију коришћен је *HyperLedger Fabric*. *HyperLedger Fabric* је *open-source* платформа. Ова платформа се користи за развој приватних блокчејн решења. *HyperLedger Fabric* је један од најпознатијих и најкоришћенијих блокчејн фрејмворкова у свету. Развио га је *HyperLedger*, на иницијативу фондације *Linux*, с циљем да обезбеди отворен извор блокчејн технологије и подстакне иновације у овој области. *HyperLedger Fabric* је модуларни блокчејн фрејмворк који обезбеђује флексибилност и скалабилност апликацијама изграђеним на њему. Има архитектонски модел који омогућава многим организацијама да сарађују унутар једне блокчејн мреже,

нудећи им могућност дељења заједничке базе података и извршавања трансакција са изузетном транспарентношћу и сигурношћу [202].

Примери коришћења *HyperLedger Fabric*-а:

- *IBM Blockchain Platform* – користи *HyperLedger Fabric* као основну технологију за своју блокчејн платформу која омогућује клијентима да развијају, имплементирају и управљају блокчејн апликацијама у облаку;
- *Alibaba Cloud Blockchain Service* – нуди хостинг блокчејн мреже на *HyperLedger Fabric*-у, што клијентима омогућава да креирају своје сопствене блокчејн апликације и да их покрену у производном окружењу;
- *Digital Asset* – технолошка компанија која користи *HyperLedger Fabric* као основну блокчејн технологију за развој различитих апликација повезаних с трансакцијама и финансијама;
- *Walmart* – један од пионира у коришћењу блокчејн технологије за праћење хране у ланцу снабдевања. Користи *HyperLedger Fabric* да би се осигурали транспарентност и поузданост ове мреже;
- *Everledger* – користи *HyperLedger Fabric* за развој блокчејн апликација које прате драгоцено камење, попут дијаманата. Њихове апликације омогућавају управљање ризиком и заштиту [203].

На наредној слици приказана је *Open-Rev* архитектура.



Слика 48: Open-Rev архитектура

Тестна мрежа је подигнута са три организације по три *peer*-а. За подизање тестне мреже коришћен је алат *Docker-compose*, као и скрипте које је фондација *HyperLedger* пружила, које су промењене да би омогућиле овакву конфигурацију система. Паметни уговори (енг. *chaincode*) писани су у програмском језику *Golang*.

Комуникација према *ledger*-у врши се путем *RPC*-а (енг. *Remote Procedure Call*).

Како је идеја била да се мигрира с централизованог решења на дистрибуирани *ledger*, у оквиру тестне мреже, приликом иницијализације *ledger-a* мигрирани су тестни подаци, који су у продукционој верзији измењени. Они се на *ledger* уписују у *JSON* формату уз помоћ *TransactionContextInterface* из *HyperLedger*-ове библиотеке *contractapi*.

Функција задужена за упис на *ledger*:

```
err = ctx.GetStub().PutState(user.ID, userJSON)
```

где *err* представља грешку до које може доћи приликом позива методе *PutState*.

Сваки упис на *ledger* представља *key-value* пар, где кључ представља *ID* ентитета који се уписује на *ledger*, а вредност је формат *JSON* објекта који се уписује. Уколико се покуша уписати на *ledger* ентитет с кључем који већ постоји на *ledger*-у, настаће грешка.

Добављање сваког ентитета с *ledger*-а врши се путем методе *GetState*, која као параметар прима *ID* ентитета који се потражује.

У наставку је дат пример функције задужене за претрагу на *ledger*-у:

```
entity, err := ctx.GetStub().GetState(id)
```

Entity представља потенцијално пронађени ентитет, а *err* грешку која може настати приликом претраге. Такође, важна ставка је да *GetState* не чита стања која још увек нису уписана на *ledger* (али су *commit*-ована), односно уколико ентитет не постоји у оквиру *world state*, повратна вредност ће бити пар *nil, nil*.

Како су на самом *ledger*-у подаци уписани као *key-value* парови, а *value* је *JSON* објекат, не постоји опција да се прочитају само одређени објекти. Једно од решења за тако нешто је додавање поља које специфично препознаје одређену врсту објекта. У оквиру ове *HyperLedger Fabric*-ове имплементације, идентификациона поља у *Open-Rev chaincode*-у могу следеће имати вредности:

- *user*
- *role*
- *area*
- *subarea*
- *scientific-work*
- *review*
- *review-quality*

За потраживање низа објеката са *ledger*-а користи се метода *GetStateByRange.*

Пример позива:

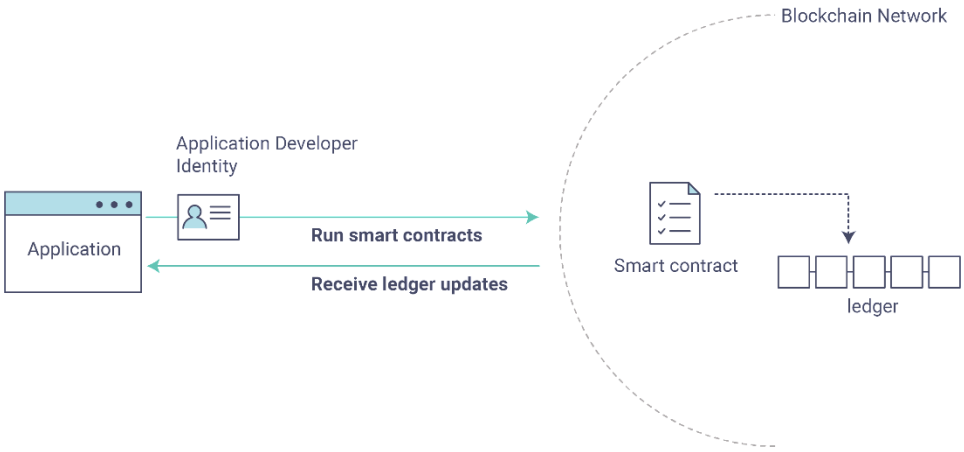
```
resultsIterator, err := ctx.GetStub().GetStateByRange("", "")
```

Проласком кроз итератор и *unmarshaling*-ом *JSON* објеката у жељене *Golang* структуре добија се низ структура које поседују специфичну вредност идентификатора.

Пример за добављање свих корисника у систему:

```
resultsIterator, err := ctx.GetStub().GetStateByRange("", "")
if err != nil {
  return nil, err
}
defer resultsIterator.Close()

var assets []*domain.OpenRevUser
for resultsIterator.HasNext() {
  queryResponse, err := resultsIterator.Next()
  if err != nil {
    return nil, err
  }

  var asset domain.OpenRevUser
  err = json.Unmarshal(queryResponse.Value, &asset)
  if err != nil {
    return nil, err
  }
  if asset.Type == "user" {
    assets = append(assets, &asset)
  }
}

return assets, nil
```

Паметни уговори се идентификују и позивају јединственим именом.



Слика 49: AppConceptsOverview

5.3.10 *Open-Rev gateway API*

Gateway је имплементиран коришћењем програмског језика *Golang* и *open-source* библиотеке *Gin*. (https://gin-gonic.com/).

Подаци битни за радно окружење чувани су у *.env* фајлу. Ту се налазе подаци попут путање до сертификата, порта на ком се покреће *Gin* сервер, мода у ком се покреће сервер, као и осталих битних података за сам *chaincode*.

У наредном делу дат је приказ основне архитектуре апликације.

```
src -
    |--- config
|--- config.go
    |--- domain
|--- Area.go
|--- OpenRevUser.go
…
    |--- helper
|--- error_handler.go
|--- formatter.go
…
    |--- http
|--- handler
   |--- area_handler.go
    |--- review_handler.go
    |--- scientific_work_handler.go
    |--- user_handler.go
|--- router
```

```
    |--- router.go
     |--- infrastructure
|--- dto
    |--- auth.go
    |--- confirm_acc_dto.go
    …
|--- seaweedFS_objects
    |--- seaweedFS_objects.go

     |--- interactor
|--- interactor.go

     |--- usecase
|--- area_usecase.go
|--- review_usecase.go
|--- scientific_work_usecase.go
|--- user_usecase.go
     |--- .env
     |--- go.mod
     |--- main.go
```

Овај директоријум представља основну архитектуру апликације написане у програмском језику *Go*. Приказ директоријума и датотека дат је у наредном делу:

- Директоријум *config* садржи датотеку *config.go*, која се користи за читање конфигурационих параметара апликације из окружења;
- Директоријум *domain* садржи *Go* датотеке, које представљају ентитете домена. Примери су *Area.go* и *OpenRevUser.go*;
- Директоријум *helper* садржи помоћне функције које се користе у апликацији. Примери су *error_handler.go* и *formatter.go*;
- *HTTP* директоријум садржи *HTTP* руковаоце (енг. *handlers*) и рутер (енг. *router*) који се користе за управљање *HTTP* захтевима. Руковаоци су у посебном директоријуму *handler*, док је рутер у директоријуму *router*;
- Директоријум *infrastructure* садржи датотеке које се користе за повезивање са спољним услугама и ресурсима. Ово укључује *DTO* фајлове (енг. *Data Transfer Objects*) који се користе за слање података преко мреже, као и датотеке које су одговорне за повезивање са системом за складиштење датотека *SeaweedFS*;
- Директоријум *interactor* садржи интеракторе (енг. *interactors*) који се користе за пословну логику апликације. Интерактори су одговорни за координацију употребе случајева (енг. *use cases*);

- Директоријум *usecase* садржи случајеве коришћења (енг. *use cases*) који представљају специфичну функционалност коју апликација пружа. Примери су area_usecase.go, review_usecase.go, scientific_work_usecase.go и user_usecase.go;
- .env датотека с параметрима конфигурације апликације је у формату кључ = вредност;
- Датотека *go.mod* дефинише модуле који су потребни за апликацију;
- Датотека *main.go* садржи главну функцију, главну функцију апликације која се покреће када се покрене апликација.

За само покретање сервера коришћене су *Gin* уграђене методе *Run* и *RunTLS*, а у зависности од мода у ком се покреће на *HTTP*-у или *HTTPS*-у.

```
if cfg.Mode == "development" {
  err = r.Run(":" + cfg.Port)
} else {
  err = r.RunTLS(":443", cfg.GinCertPath, cfg.GinKeyPath)
}
```

Приказани кôд користи уграђене *Run* и *RunTLS* методе у *Gin* фрејмворку за покретање сервера у *HTTP* или *HTTPS* режиму. У зависности од подешавања у конфигурационој датотеци, сервер ће се покренути у развојном (*HTTP*) или производном (*HTTPS*) режиму.

Ако је подешавање *development*, сервер ће се покренути на датом порту, који је дефинисан у конфигурационој датотеци коришћењем *HTTP* протокола:

err = r.Run(":" + cfg.Port).

Ако је подешавање *production*, сервер ће се покренути на стандардном *HTTPS* порту 443, користећи *SSL* сертификат и кључ дефинисан у конфигурационој датотеци:

err = r.RunTLS(":443", cfg.GinCertPath, cfg.GinKeyPath).

Ове методе аутоматски обрађују захтеве клијената и генеришу одговоре на основу крајњих тачака имплементираних у апликацији.

Као вид сигурности да ће захтев доћи са адресе на којој се налази *bekend Open-Rev* апликација, имплементиран је *CORS*, као такође уграђена *Gin* метода.

```
r.Use(cors.New(cors.Config{
  AllowOrigins:     []string{"*"},
  AllowMethods:     []string{"GET", "POST"},
  AllowHeaders:     []string{"Origin"},
  ExposeHeaders:    []string{"Content-Length"},
  AllowCredentials: true,
  AllowOriginFunc: func(origin string) bool {
    return origin == address_of_open_rev_backend
```

```
  },
  MaxAge: 12 * time.Hour,
}))
```

Приказани кôд представља имплементацију механизма *CORS* (*Cross-Origin Resource Sharing*), који омогућава контролу приступа ресурсима с других домена у веб-апликацијама.

Конкретно, овде су дефинисани одобрени извори захтева (*AllowOrigins*), одобрене *HTTP* методе (*AllowMethods*), одобрена *HTTP* заглавља (*AllowHeaders*) и експортована *HTTP* заглавља (*ExposeHeaders*).

Такође, имплементирана је провера да ли је извор захтева једнак адреси на којој се налази *Open-Rev backend* апликација (*AllowOriginFunc*). Ово је важно за спречавање напада с других локација, тзв. *cross-site request forgery* (*CSRF*).

Додата је и опција *AllowCredentials*, која указује на то да ли ће се током слања захтева с другог извора слати и подаци за аутентификацију (колачићи (енг. *cookies*), *HTTP* аутентификациони хедери).

Сва ова подешавања примењују се на све *HTTP* захтеве које клијенти шаљу ка *Open-Rev backend* апликацији.

Откривени ендпоинти су описани у фајлу *http/router.go*.

```
router.POST("/users/register", handler.Register)
router.POST("/users/edit", handler.EditUser)
router.POST("/users/confirmAccount", handler.ConfirmAccount)
router.POST("/sciWorks", handler.CreateScientificWork)
router.POST("/review", handler.CreateReview)
router.POST("/review/quality", handler.CreateReviewQuality)

router.GET("/users", handler.GetAllUsers)
router.GET("/users/:id", handler.GetUserById)
router.GET("/users/info/:id", handler.GetUserInfo)
router.GET("/users/:id/reviews", handler.GetAllReviewsByUser)

router.GET("/subareas", handler.GetAllSubAreas)
router.GET("/areas", handler.GetAllAreas)
router.GET("/dashboardAreas", handler.GetAllAreasAndSubAreas)

router.GET("/dashboard", handler.GetDashboardItems)
router.GET("/reviews", handler.GetAllReviews)
```

```
router.GET("/sciWorks", handler.GetAllScientificWorks)
router.GET("/sciWorks/:id/review", handler.GetAllReviewsByScientificWork)
router.GET("/sciWorks/:id/details", handler.GetScientificWorkDetails)
router.GET("/sciWorks/id/:id", handler.GetScientificWorkById)
router.GET("/sciWorks/userId/:userId",handler.GetAllScientificWorksByUser)
router.GET("/sciWorks/subareaId/:subareaId", handler.GetAllScientificWorksBySubareaId)
```

Ови ендпоинти су важни за функционалности које пружа апликација *Open-Rev*. Неки од њих служе за регистрацију и управљање корисницима, као што су */users/register*, */users/edit* и /users/confirmAccount. Остали ендпоинти су повезани с додавањем, добијањем и управљањем студентским радовима и рецензијама, као што су */sciWorks*, */review*, */review/quality* и */sciWorks/:id/review*. Такође, постоје ендпоинти који служе за добијање информација о корисницима, студентским радовима, областима и пописима подобласти. Ендпоинти за управљање областима и подобластима укључују */areas*, */subareas* и /*dashboardAreas*. Неки од ендпоинта имају параметре као што је /users/:id, што омогућава добијање података о кориснику са одређеним *ID*-јем. Сви ти ендпоинти су доступни кроз *HTTP* методе *GET* и *POST*.

Приликом иницијализације сервера, коришћени су *HyperLedger*-ови механизми идентификације на *ledger*-у. Остварена је сигурна *gRPC* конекција према једном од *peer*-ова путем сертификата добијених од сертификационог тела *HyperLedger Fabric*.

```
func newGrpcConnection(config *config.Config) *grpc.ClientConn {
  certificate, err := loadCertificate(config.TlsCertPath)
  if err != nil {
    panic(err)
  }

  certPool := x509.NewCertPool()
  certPool.AddCert(certificate)
  transportCredentials := credentials.NewClientTLSFromCert(certPool, config.GatewayPeer)

  connection, err := grpc.Dial(config.PeerEndpoint,
grpc.WithTransportCredentials(transportCredentials))
  if err != nil {
    panic(fmt.Errorf("failed to create gRPC connection: %w", err))
  }

  return connection
}
```

У овом коду користи се функција *newGrpcConnection* која приказује процес креирања сигурне *gRPC* конекције према *HyperLedger Fabric peer*-у. У току овог процеса прво се учитавају сертификати који се користе у криптографској заштити комуникације, а затим се користе за креирање *TLS* креденцијала (подешавањем опција *credentials.NewClientTLSFromCert*). Након тога, ови креденцијали користе се за креирање *gRPC* конекције позивом функције *grpc.Dial*. Функција *grpc.WithTransportCredentials* користи се да би се навело то да се користе *TLS* креденцијали при конекцији. Уколико процес конекције не успе, биће пријављен („бачен") изузетак. Тиме се осигурава да је комуникација сигурна, тј. да је сервер аутентификован и да су подаци енкриптовани.

Креиран је нови идентитет функцијом *newIdentity* и нови дигитални потпис помоћу функције *newSign*. Функција *newIdentity* користи *loadCertificate*, која учитава сертификате.

```
func newIdentity(config *config.Config) *identity.X509Identity {
  certificate, err := loadCertificate(config.CertPath)
  if err != nil {
    panic(err)
  }
  id, err := identity.NewX509Identity(config.MspID, certificate)
  if err != nil {
    panic(err)
  }
  return id
}

func loadCertificate(filename string) (*x509.Certificate, error) {
  certificatePEM, err := ioutil.ReadFile(filename)
  if err != nil {
    return nil, fmt.Errorf("failed to read certificate file: %w", err)
  }
  return identity.CertificateFromPEM(certificatePEM)
}
```

Функција *newIdentity* користи *X509* сертификат који се учитава из фајла чији је пут задат у конфигурационом фајлу (*config.CertPath*). Учитавање се врши функцијом *loadCertificate* која учитава *PEM* кодовани сертификат из фајла и конвертује га у *x509.Certificate* објекат користећи функцију *identity.CertificateFromPEM*.

За потписивање трансакције користи се функција *newSign*, која захтева два параметра: идентитет и поруку која се потписује. На основу идентитета добијају се потребни приватни и јавни кључеви, а потом се користи приватни кључ да се потпише порука.

У наредном делу дат је приказ кода за функцију *newSign*:

```
func newSign(identity *identity.X509Identity, message []byte) ([]byte, error) {
privateKey, err := identity.PrivateKey()
if err != nil {
return nil, fmt.Errorf("failed to get private key from identity: %w", err)
}

digest := sha256.Sum256(message)
signature, err := rsa.SignPKCS1v15(rand.Reader, privateKey.(*rsa.PrivateKey), crypto.SHA256, digest[:])
if err != nil {
return nil, fmt.Errorf("failed to sign message: %w", err)
}

return signature, nil
}
```

Ledger се иницијализује позивом трансакције *InitLedger* и иницијално попуњава тестним подацима, а како је немогуће два пута уписати ентитет са истим *ID*-јем на *ledger*-у, није потребно додатно оборити мрежу пре сваког поновног покретања сервера.

Трансакција *InitLedger* користи се да иницијализује *Ledger* и да у њега унесе тестне податке. Једном када су подаци унети, није потребно обарати мрежу пре сваког поновног покретања сервера јер је свака трансакција која је потписана и потврђена у *ledger*-у неизмењива. То значи да није могуће унети ентитет са истим *ID*-јем два пута, што гарантује конзистентност података на *ledger*-у. Самим тим, иницијално попуњени подаци остаће сачувани и доступни након поновног покретања сервера.

Како је једини корисник *ledger*-а заправо *backend Open-Rev* система, приликом покретања *API*-ја креира се дигитални потпис на основу сертификата које је издао *HyperLedger Fabric* за сваку поруку слату према *ledger*-у.

```
func newSign(config *config.Config) identity.Sign {
  files, err := ioutil.ReadDir(config.KeyPath)
  if err != nil {
    panic(fmt.Errorf("failed to read private key directory: %w", err))
  }
  privateKeyPEM, err := ioutil.ReadFile(path.Join(config.KeyPath, files[0].Name()))

  if err != nil {
```

```
    panic(fmt.Errorf("failed to read private key file: %w", err))
  }

  privateKey, err := identity.PrivateKeyFromPEM(privateKeyPEM)
  if err != nil {
    panic(err)
  }

  sign, err := identity.NewPrivateKeySign(privateKey)
  if err != nil {
    panic(err)
  }

  return sign
}
```

Приликом комуникације с *ledger*-ом, *backend Open-Rev* система користи свој дигитални потпис на основу сертификата које је издао *HyperLedger Fabric* како би се потврдио идентитет себе као корисника. Овај потпис је део механизма за потписивање трансакција и обезбеђује да само потписани корисници могу да извршавају трансакције на *ledger*-у. Када корисник са *backend-a Open-Rev* система шаље трансакцију на *ledger*, трансакција се потписује корисничким дигиталним потписом и шаље се на *ledger* за верификацију. Овај процес обезбеђује да само потписани корисници могу да извршавају трансакције на *ledger*-у и да све трансакције потврди и верификује *ledger*.

Ради спречавања неовлашћене измене података на *ledger*-у, предузети су следећи кораци: функција *newSign* учитава приватни кључ користећи функцију *ioutil.ReadFile* за читање фајлова у директоријуму задатом у *config.KeyPath*. Приватни кључ се претвара у објекат типа *identity.Sign* коришћењем функције *identity.NewPrivateKeySign*. Овај објекат се користи за потписивање сваке поруке која се шаље *ledger*-у, а функција се користи за креирање дигиталног потписа који служи за потписивање сваке поруке послате према *ledger*-у.

Функција почиње читањем директоријума који садржи приватни кључ за потписивање. Ако дође до грешке приликом читања директоријума, функција ће изазвати *panic* с грешком „неуспешно читање директоријума приватног кључа” (енг. *failed to read private key directory*).

Затим функција чита приватни кључ из датотеке користећи функцију *ioutil.ReadFile*. Ако дође до грешке при читању датотеке, функција ће изазвати *panic* с грешком „неуспешно читање датотеке приватног кључа” (енг. *failed to read private key file*).

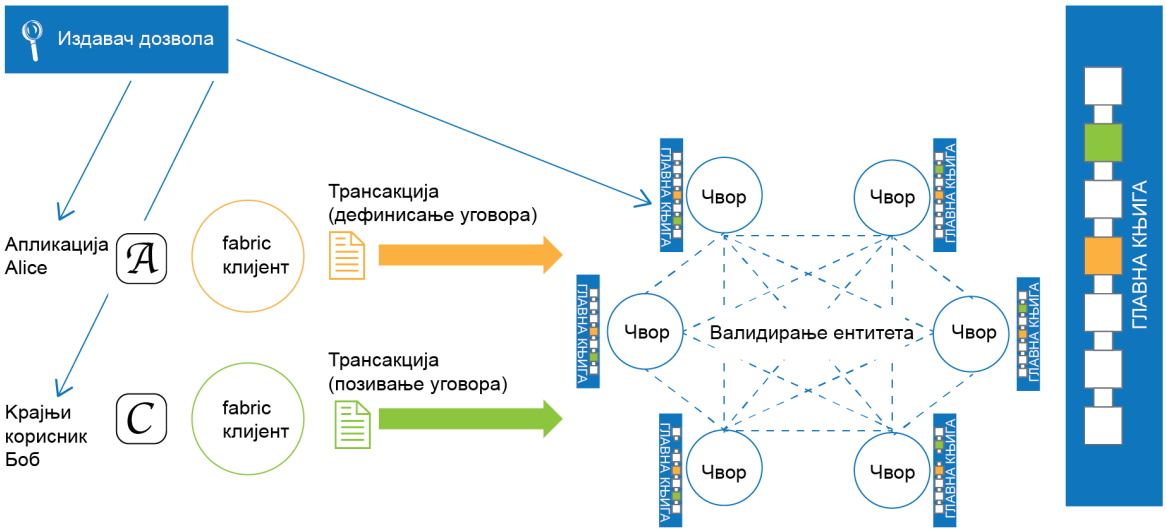
Након читања приватног кључа у *PEM* формату, функција користи функцију *identity.PrivateKeyFromPEM()* да креира инстанцу приватног кључа. Ако дође до грешке приликом парсирања *PEM* формата, функција ће изазвати *panic*.

Функција *newSign* користи функцију *identity.NewPrivateKeySign()* да креира дигитални потпис с приватним кључем корисника. Ако дође до грешке приликом

креирања дигиталног потписа, функција ће изазвати *panic*. Функција враћа креирани дигитални потпис као објекат типа *identity.Sign*.

У оквиру система *Open-Rev* блокчејн технологија имплементирана је коришћењем *HyperLedger Fabric*-а. Систему се приступа преко *API*-ја, а комуникација с *ledger*-ом одвија се преко *gRPC* конекције. Приликом иницијализације сервера, користе се *HyperLedger*-ови механизми идентификације на *ledger*-у и успоставља се безбедна *gRPC* конекција с једним од *peer*-ова система преко сертификата које обезбеђује сертификационо тело *HyperLedger Fabric*-а.

Open-Rev систем је једини корисник главне књиге (енг. *ledger*) и при покретању *API*-ја креира се дигитални потпис на основу сертификата које издаје *HyperLedger Fabric* за сваку поруку која се шаље према *ledger*-у. У склопу иницијализације главне књиге позива се трансакција *InitLedger*, која се користи за почетно попуњавање тест-подацима. Пошто није могуће два пута унети ентитет са истим *ID*-јем у главну књигу, није потребно додатно рушити мрежу пре сваког поновног покретања сервера.



Систем са дозволама; снажно управљање идентитетом
Различите улоге корисника и валидатора
Корисници постављају нове делове кода(chaincode) и позивају их путем трансакција за постављање (deploy) и позивање (invoke)
Валидатори процењују ефекте трансакције и постижу сагласност о новој верзији главне књиге
Ledger (Главна књига) = укупан редослед трансакција + хеш (глобалног стања)
Замењиви протоколи консензуса, као што су PBFT & Sieve

Слика 50: Hyperledger-fabric модел Workflow

Уколико се јави грешка приликом извршавања трансакције, *ledger* ће вратити одређену грешку. Постоји неколико типова грешака:

- *EndorseError*
- *SubmitError*
- *CommitStatusError*
- *CommitError*

Када настане грешка приликом извршавања трансакције, *ledger* ће вратити одговарајућу грешку (енг. *error*), која се може класификовати у један од четири наведена типа. Сваки *error* садржи детаље о грешци, који се обично налазе у објекту

status.Status. Да би се лакше руковало овим грешкама, може се користити функција *LedgerErrorHandler* имплементирана у помоћни пакет *helper*. Ова функција ће конвертовати *status.Status* објекат у један од предефинисаних типова грешке и вратити га као резултат.

Поред ових типова грешака које се јављају у *Hyperledger Fabric ledger*-у, могу постојати и друге врсте грешака које су специфичне за имплементацију апликације. У таквим случајевима треба поштовати препоруке произвођача за ефикасно руковање грешкама и одржавање стабилности и поузданости апликације.

Такође, важно је напоменути да су форма и садржај порука о грешци битни за кориснике апликације како би могли да разумеју и брзо реагују на могуће проблеме у систему. Добра пракса да се поруке о грешци формулишу доследно и јасно, тако да буду разумљиве и корисне корисницима, примењена је приликом развоја апликације *Open-Rev*, а ради будућих истраживања.

Руковање грешкама у оквиру апликације један је од кључних аспеката одржавања поузданости и стабилности система. Због тога се посебно водило рачуна о томе да имплементација система буде вођена добрим праксама у том погледу, као и да се редовно тестира и ажурира како би се избегли или минимизовали проблеми.

У апликацији *Open-Rev* сваки *error* у себи носи детаље грешке, које прво треба конвертовати помоћу уграђене методе *status.Convert* у оквиру пакета *grpc*. Функција *LedgerErrorHandler* која обрађује грешке налази се у оквиру пакета *helper*.

У наредном делу дат је приказ функције која ради обраду грешке:

```
func convertError(err error) error {
  statusErr := status.Convert(err)
  for _, detail := range statusErr.Details() {
    switch detail := detail.(type) {
    case *gateway.ErrorDetail:
      log.Printf("Error from endpoint: %s, mspId: %s, message: %s\n", detail.Address, detail.MspId, detail.Message)
      return fmt.Errorf(detail.Message)
    }
  }
  return nil
}
```

Функција *convertError* има задатак да обради грешку примљену приликом извршавања трансакције на главној књизи. Функција прво конвертује грешку користећи методу *status*.Convert из пакета *grpc* да би добила објекат типа *statusError*.

После тога функција пролази кроз све детаље грешке добијене позивањем методе *statusErr.Details()*. У случају да је деталь грешке типа *gateway.ErrorDetail*, функција евидентира поруку о грешци на конзоли, која садржи детаље о адреси *endpoint*-а, *mspId*-у и поруци грешке. Ако је грешка другог типа, функција враћа *nil*. Крајњи циљ ове

функције је да врати јасну поруку о грешци која се догодила током извршавања трансакције.

Како трансакције могу да се евалуирају (енг. *evaluate*) или поднесу (енг. *submit*), оне се извршавају помоћу функција *contract.EvaluateTransaction* и *contract.SubmitTransaction*. Повратна вредност тих функција је низ бајтова и потенцијална грешка. Након тога, низ бајтова треба *unmarshal*-овати у низ објеката које *Golang* може да користи.

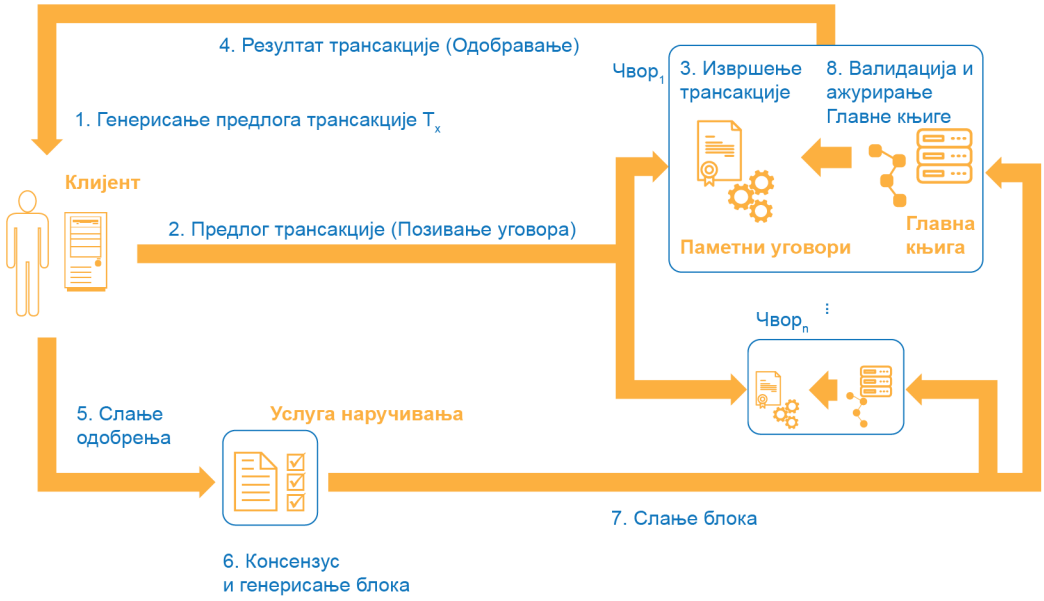
У наредном делу дат је пример позива:

```
evaluateResult, err := contract.EvaluateTransaction("RandomQueryTransaction")
if err != nil {
  return nil, helper.LedgerErrorHandler(&contract, err)
}

var objects []*domain.RandomObject
err = json.Unmarshal(evaluateResult, &objects)

if err != nil {
  return nil, err
}
```

Функције *contract.EvaluateTransaction()* и *contract.SubmitTransaction()* користе *gRPC* протокол за комуникацију с *ledger*-ом и извршавање одговарајуће радње (процену или подношење трансакције). Након што добије повратну вредност као низ бајтова, функција *json.Unmarshal()* користи се за декодирање података и добијање низа објеката које *Golang* може да користи.

Важно је напоменути да је функција *contract.EvaluateTransaction()* намењена само за процену стања у главној књизи, док се функција *contract.SubmitTransaction()* користи за извршавање стварних трансакција које ће променити стање у књизи.

Горенаведене методе користе *gRPC* како би се обратили *ledger*-у.



Слика 51: Модел система

5.3.11 Примена и евалуација развијеног решења

Ради евалуације развијеног модела, спроведено је истраживање како би се испитала функционалност оваквог система у пракси. За потребе таквог истраживања на Топличкој академији посматране су две групе студената.

Табела 15: Подаци о броју корисника и евалуација радова

Укупан број регистрованих корисника	Укупан број регистрованих студента	Укупан број постављених семинарских радова	Укупан број рецензија	Укупан број области у којима су постављени семинарски радови	Укупан број рецензија датих од стране студената	Укупан број рецензија датих од стране рецензената
34	31	31	57	8	45	12

Прва група, коју је чинило око 30 студената, у договору с предметним професором и асистентима у настави кроз програм вежби имала је задатак да на сваке две недеље напише есеј или краћи семинарски рад или реализује пројектни задатак на задату тему. Радови су постављени на представљену локацију и били су доступни другим студентима из групе за читање и евалуацију.

Први сегмент истраживања није укључио обавезу студената да евалуирају радове својих колега, већ је то студентима остављено као могућност избора, уз напомену да та активност доноси одређени број бодова, односно бенефите сходно упутствима и оквирним критеријумима за евалуацију студентских радова. Ово је омогућило сагледавање мотивисаност студената да учествују у оваквом процесу [178].

Други сегмент истраживања односио се на квалитет саме евалуације коју су спровеле колеге у поређењу са оном коју би одрадио наставни кадар.

Трећи део је упоредио резултате, оцене из матичног предмета студената из експерименталне групе која спроводи евалуацију рада колега с резултатима и оценама контролне групе која укључује исти број студената али без примене овог система.

Такође, спроведена је и анкета. Студенти и професори који су изабрани као репрезентативни предложили су питања за анкетни упитник.

У истраживању су анализирани подаци прикупљени применом одређених статистичких техника и метода. Табеларна презентација и анализа резултата истраживања прате одговарајући редослед примењених статистичких анализа, које претходе анализама прикупљених података путем одговарајућих статистичких тестова. Стога су у истраживању коришћене следеће методе и технике:

1. дескриптивна статистичка анализа демографских и психографских карактеристика испитаника ради израчунавања најважнијих показатеља дистрибуције фреквенција;

2. тест Хи-квадрат како би се испитала значајност разлике у фреквенцији посматраних карактеристика.

Применом ових статистичких метода могуће је донети закључке о прихватању и/или одбацивању постављених хипотеза. Подаци које су прикупили испитаници обрађени су у статистичком пакету СПСС 20.

У наредном делу дате су табеле фреквенција за карактеристична обележја истраживања.

Табела 16: Пол испитаника

Р. бр.	Пол
1	женски
2	мушки

pol_ispitanika

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	110	78.6	78.6	78.6
	2	30	21.4	21.4	100.0
	Total	140	100.0	100.0	

Табела 17: Године старости испитаника

Р. бр.	Године старости
1	од 18 до 23
2	од 24 до 29
3	од 30 до 35
4	од 36 до 41
5	од 42 до 47
6	више од 47

god_starosti

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	60	42.8	42.8	42.8
	3	70	50	50	92.8
	4	5	3.6	3.6	96.4
	5	5	3.6	3.6	100.0
	Total	140	100.0	100.0	

Табела 18: Ниво образовања испитаника

Р. бр.	Ниво образовања
1	Средње
2	Висока стручна спрема
3	Магистар наука / мастер
4	Доктор наука

stepen_obrazovanja

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	50	35.7	35.7	35.7
	2	40	28.6	28.6	64.3
	3	26	18.6	18.6	82.9
	4	24	17.1	17.1	100.0
	Total	140	100.0	100.0	

Полазећи од утврђеног предмета, циљева и сврхе истраживања, дефинисали смо хипотетички оквир који се састоји од основних и неколико посебних хипотеза.

Општа хипотеза, Х-0, на којој се темељи ово истраживање јесте: *Постоји статистички значајна разлика између демонстриране спремности наставника да допринесу примени технологија блокчејна у високошколским институцијама у Србији и њихових демографских карактеристика (пол, године и ниво образовања).* Теоријска подршка општој хипотези дефинисаној на овај начин произлази из признања бројних приступа важности система блокчејна у колаборативном учењу. Овај приступ активно укључује студенте у анализу и синтезу информација и концепата, уместо коришћења механичког учења и меморисања чињеница и бројева. Један од важнијих доприноса развоју колаборативног учења јесте образовни приступ коришћењу тимова ради оптимизације учења путем заједничког рада. Колаборативно учење у е-образовању користи мале групе студената у учионици, подстичући их да максимално унапреде своје и међусобно учење [178].

На основу анализе релевантне литературе, дефинисане су три специфичне хипотезе које могу бити операционализоване/раздвојене на следећи начин:

Х-1: Да ли су разлике у полу наставника статистички значајне за увођење и примену блокчејн технологија у високошколским институцијама?

Х-2: Да ли су разлике у нивоу образовања знатно утицале на спремност наставника ангажованих у високошколским институцијама Србије да примене модел колаборативног учења и евалуације радова студената, заснован на блокчејн технологијама?

Х-3: Да ли се примена блокчејн технологија које омогућавају повезивање с партнерима из високошколских институција статистички знатно разликује у зависности од старосне доби испитаника?

Главна карактеристика оцене утицаја демографских карактеристика наставника на њихову спремност да примене блокчејн технологије у високошколским институцијама Србије јесте да се ради о феномену који се не може квантитативно мерити и стога се може изразити само у облику фреквенција. Због тога се тестирање ове хипотезе спроводи путем теста Хи-квадрат. Суштина овог типа теста састоји се у утврђивању значајности разлике између оригиналних и теоретских фреквенција посматраног феномена, што омогућава доношење одговарајућих закључака. На овај начин остварује се један од циљева овог рада, а то је објективна процена сложене улоге савременог наставника у убрзаном развоју модерног образовања. Стога се примењује тест Хи-квадрат, који омогућава проверу исправности претпоставке у очекиваном специфичном окружењу, у већем броју модалитета посматраних карактеристика.

5.3.12 Анализа постигнутих резултата

За потребе тестирања прве посебне хипотезе Х-1 примењен је тест Хи-квадрат независности. Овим тестом је испитано да ли се оцене радова и пројеката студената заснованих на блокчејн технологијама у е-образовању статистички знатно разликују између мушких и женских испитаника. Статистичка значајност овог теста је изнад прага вредности од 0,05, због чега се закључује да не постоји статистички значајна разлика ($\chi^2 = 2{,}142$, df = 2) [178].

Ако се посматра табела, може се закључити да су мушки испитаници изузетно спремни да користе блокчејн технологију, јер верују да колаборативним учењем и учешћем у оцени радова колега студенти доприносе бољој оцени и студентских

пројектних радова, и квалитета образовног процеса у Србији. У случају испитаница, такође је постојала значајна отвореност за ову могућност, која се може побољшати колаборативним учењем, заснованим на блокчејн технологијама, аналогно процесу оцењивања резултата научноистраживачког рада.

На основу резултата добијених коришћењем теста Хи-квадрат, утврђено је да не постоје статистички значајне разлике у спремности наставника ангажованих у високошколским институцијама Србије да примене модел колаборативног учења и евалуације радова студената, заснован на блокчејн технологијама и различитим нивоима образовања ($\chi^2 = 2{,}077$, df = 2) [178].

Испитаници који су недавно завршили основне академске студије навели су као најчешћи разлог чињеницу да се блокчејн технологије у овом случају могу користити за развој сигурне платформе за складиштење и размену података о студентским пројектима и радовима, студентима-евалуаторима, рецензентима из праксе и евалуацијама. Када се подаци о оцени студената забележе, не могу се негирати нити их може променити било која страна.

Такође, примена блокчејн технологија омогућава да учествовање у оцени студентских радова постане део процеса развоја каријере. Оцене и евалуирани пројекти могу бити доступни заинтересованим послодавцима. Послодавац би имао информације о резултатима практичног рада студената и како су пројекат оценили други. Поред студената-евалуатора, може се обезбедити и рецензент из праксе за студентске радове и пројекте. Како би се изабрао компетентан рецензент, вештине рецензента су мапиране у односу на тему семинарског рада или пројекта коришћењем кључних речи и графикона. Информације о квалитету рецензија за сваког рецензента такође ће бити сачуване.

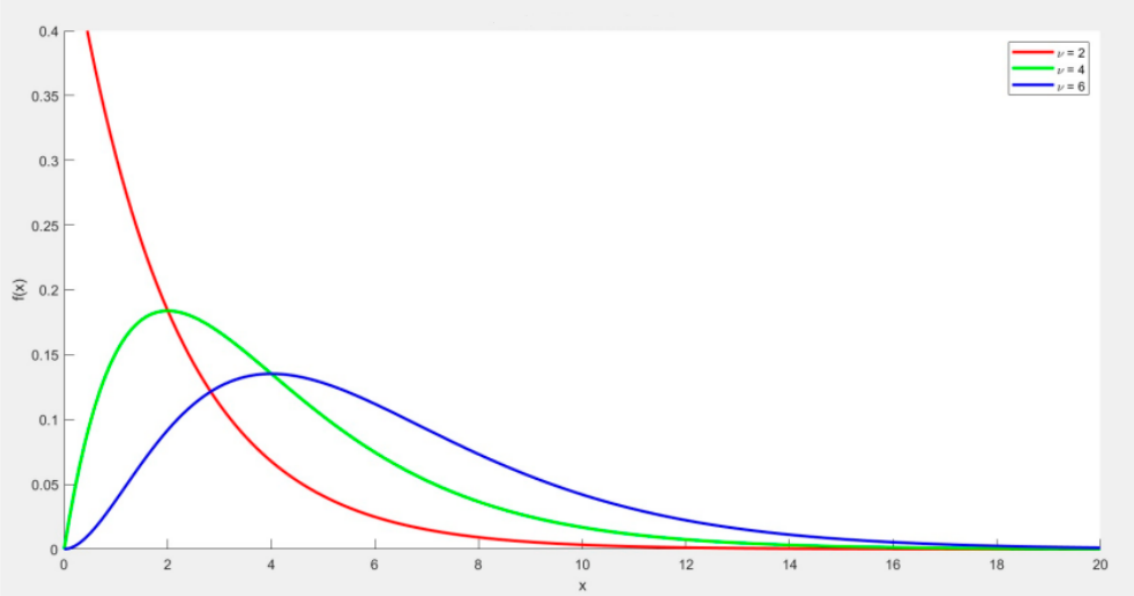
Коришћењем теста Хи-квадрат такође је испитано да ли се примена блокчејн технологија, која омогућава повезивање с партнерима из високошколских институција, статистички значајно разликује међу испитаницима у зависности од њихове старосне доби. Резултати теста ($\chi^2 = 2{,}106$, df = 2) указују на постојање статистички значајне разлике између старосних група.

Табела 19:Статус тестиране, посебне, Х-1 хипотезе и повезаних додатних хипотеза (извор: [178])

Хипотеза	Општа/додатна хипотеза	Статус	Вредност теста Хи-квадрат χ^2	Број степена слободе df
Х-0: Постоји статистички значајна разлика између показане спремности наставника да допринесу примени технологија блокчејна у високошколским институцијама у Србији и њихових демографских карактеристика (пол, године и ниво образовања).	Општа	Потврђено	2,142	2
Х-1: Да ли су разлике у полу наставника статистички значајне за увођење и примену технологија блокчејна у високошколским институцијама?	Додатна	Потврђено	2,142	2
Х-2: Да ли су разлике у нивоу образовања знатно утицале на спремност наставника ангажованих у високошколским институцијама Србије да примене модел колаборативног учења и евалуације радова студената заснован на технологијама блокчејна?	Додатна	Није потврђено	2,077	2
Х-3: Да ли се примена технологија блокчејна које омогућавају повезивање с партнерима из високошколских институција статистички значајно разликује у зависности од старосне доби испитаника?	Додатна	Потврђено	2,106	2

У дискусији су анализирани резултати истраживања и општа хипотеза Х-0 проверена је тестирањем помоћних хипотеза Х-1, Х-2 и Х-3. За проверу тачности ових допунских хипотеза коришћен је тест Хи-квадрат. Овај тест је омогућио да се истражи да ли постоји статистички значајна разлика између спремности наставника да допринесу примени блокчејн технологија у високошколским институцијама у Србији и њихових демографских карактеристика. С обзиром на то да су потврђене две од три допунске хипотезе, може се закључити да је општа хипотеза, Х-0, прихваћена [178].

На Слици 52 приказане су три различите криве које представљају тест Хи-квадрат за три степена слободе: 2, 4 и 6. Тест је коришћен ради истраживања утицаја демографских карактеристика на спремност наставника да користе блокчејн технологије у високообразовним институцијама.



Слика 52: Утицај демографских карактеристика наставника на њихову спремност за коришћење блокчејин технологија [178]

Примена блокчејн технологија омогућава да учествовање у оцени радова студената буде део процеса развоја каријере. Евалуације и оцењени пројекти могу бити доступни заинтересованим послодавцима. На тај начин послодавци могу добити информације о резултатима практичног рада студената, као и о начину на који су те пројекти оценили други. Поред студената који оцењују, може се обезбедити и стручњак из праксе за евалуацију радова и пројеката студената. Да би се изабрао одговарајући рецензент, анализираће се компетенције рецензента у односу на тему семинарског рада или пројекта коришћењем кључних речи и графикона. Такође, информације о квалитету рецензија за сваког рецензента биће сачуване [178].

Увођењем колаборативног учења у е-образовање омогућава се боља евалуација студентских радова, подстиче се учење оријентисано ка пројектима и унапређује се квалитет образовног процеса. Колаборативним учењем и учествовањем у оцени радова колега студенти стичу нова знања, вештине и компетенције и доприносе бољој евалуацији студентских радова и квалитету образовног процеса.

Студенти имају могућност да међусобно сарађују на пројектима, где морају деловати као тим како би разумели представљене концепте. Активности као што су одбрана својих ставова, преобликовање идеја, слушање различитих мишљења и изражавање сопствених мишљења омогућавају студентима да боље разумеју градиво као група него што би то могли појединачно. Тимови студената такође имају прилику да заједно решавају различите задатке, постављају проблеме или сарађују у савладавању нових концепата.

Анализа постигнутих резултата тежи да докаже оправданост примењивости система вршњачког оцењивања у високошколским програмима едукације путем више различитих критеријума, међу којима су најзначајнији:

- активност студената и стално ангажовање и повећање колаборативности;
- повећана мотивација за рад;
- виши ниво савладаности градива, ефикасност и ефективност стечених знања;
- бенефити у процесу оцењивања од стране наставног кадра;

- унапређење методолошког приступа за евалуацију студентских радова заснованог на одабраним концептима рецензирања научноистраживачких радова;
- компаративна анализа метода колаборативног учења и евалуације студентских радова;
- оправданост интеграције система за евалуацију студентских радова заснованог на блокчејн технологијама са системима за е-образовање и оцена перформанси [178].

6 НАУЧНИ И СТРУЧНИ ДОПРИНОС

Значајнији допринос ове докторске дисертације јесте развој модела колаборативног учења и евалуације студентских радова у е-образовању заснованог на блокчејн технологијама који ће омогућити квалитетнију евалуацију студентских радова и унапредити квалитет образовног процеса.

Научни доприноси огледају се у:

- развоју модела колаборативног учења и евалуације студентских радова заснованог на блокчејн технологијама;
- развоју новог методолошког приступа за евалуацију студентских радова заснованог на одабраним концептима рецензирања научноистраживачких радова;
- компаративној анализи метода колаборативног учења и евалуације студентских радова;
- моделу интеграције система за евалуацију студентских радова заснованог на блокчејн технологијама са системима за е-образовање;
- развоју методолошких поступака и метрика за оцену перформанси развијеног модела.

Стручни доприноси планираног истраживања огледају се у:

- утврђивању могућности развоја модела евалуације студентских радова заснованог на блокчејн технологијама;
- развоју софтверског система за колаборативно учење и евалуацију студентских радова;
- развоју блокчејн мреже за повезивање стејкхолдера и верификацију трансакција у систему за колаборативно учење и евалуацију студентских радова;
- испитивању могућности за примену развијеног модела у другим окружењима електронског образовања, као што је *Moodle*;
- обезбеђивању веродостојности података применом блокчејн технологија;
- прегледу и анализи технологија потребних за примену модела за евалуацију студентских радова заснованог на блокчејн технологијама.

Друштвени доприноси резултата истраживања односе се на могућност решавања различитих друштвених проблема, од којих су важнији:

- афирмација увођења модела колаборативног учења заснованог на блокчејн технологијама с циљем квалитетније евалуације студентских радова и унапређења образовног процеса;
- утврђивање потенцијала за квалитетнију евалуацију студентских радова усвајањем модела колаборативног учења подржаног блокчејн технологијама;
- унапређење сарадње између студената у формалном образовању;
- унапређење сарадње између студената и будућих послодаваца;

- унапређење сарадње између студената и стручњака из праксе;
- развој критичког мишљења студената;
- унапређење студентских вештина тимског рада;
- могућност да друге високошколске институције користе резултате истраживања с циљем ефикаснијег спровођења интеграције модела колаборативног учења и евалуирања студентских радова;
- омогућавање напретка е-образовања применом модела колаборативног учења и евалуацијом студентских радова.

Резултати и доприноси докторске дисертације објављени су у следећим радовима (категорија М22):

1. **Bjelobaba, G**.; Savić, A.; Tošić, T.; Stefanović, I.; Kocić, B. Collaborative Learning Supported by Blockchain Technology as a Model for Improving the Educational Process, Sustainability (ISSN 2071-1050), Special Issue "Blockchain and Agile Management – Important Tools for Circular Economy" 2023, 15, 4780. https://doi.org/10.3390/su15064780 импакт фактор за 2022=3.9, (М22).
2. **Bjelobaba, G.**; Paunovic, M.; Savic, A.; Stefanovic, H.; Doganjic, J.; Miladinovic Bogavac, Z. Blockchain Technologies and Digitalization in Function of Student Work Evaluation. Sustainability (ISSN 2071-1050), Special Issue "Blockchain and Agile Management – Important Tools for Circular Economy" 2022, 14, 5333. https://doi.org/10.3390/su14095333 импакт фактор за 2022=3.9, (М22).

Списак научних радова с међународних конференција категорија М30

3. H. Stefanović, A. Savić, **G. Bjelobaba**, N. Popović, *Simulation and Analysis of Blockchain Operations Model with RSA Algorithm in CrypTool2*, Conference "E-business technologies", Vol. 3 No. 1 (2023): E-business technologies Conferences Proceedings 2023, pp.171–175, Belgrade, Serbia, June, 15–17, 2023. (M33)
4. S. Ersoy; A. Savić; **G. Bjelobaba**; H. Stefanović, *Collaborative Learning of Mathematics Supported by Blockchain Technology in the Context of Mandelbrot and Julia Sets*, 13th International Scientific Conference Science and Higher Education in Function of Sustainable Development – SED 2023, Western Serbia Academy of Applied Studies, 5–8 June, 2023, Vrnjacka Banja, Serbia, ISBN 978-86-82078-18-0 (M33)
5. A. Savic, H. Stefanovic, **G. Bjelobaba**, N. Popovic, "The Simulation Model of Blockchain Transaction", XLIX International Symposium on Operations Research-SYM-OP-IS 2022, Proceedings of papers, pp. 143-148, Vrnjačka Banja, Serbia, September 19–22, 2022, ISBN: 978-86-403-1750-4 (M33)
6. Lj. Diković, **G. Bjelobaba**, A. Savić, N. Popović, *Mathematics for Informatics Education*, 12th International Conference Science and Higher Education in Function of Sustainable Development-SED 2021, Proceedings of papers, pp. 1–5 (1–6), Užice, Serbia, October 8, 2021, ISBN 978-86-82078-11-1 (M33)
7. A. Savic, **G. Bjelobaba**, N. Popovic, H. Stefanovic, "One-Time Pad Cipher (OTP) Use Cases and Simulation Examples for Electronic Financial Transactions", International

Conference on Business, Technology and Innovation-UBT 2021, Conference Book of Abstracts, pp. 187, Pristina, October 29–30, 2021, ISBN 978-9951-550-47-5 (M33)

8. N. Popovic, **G. Bjelobaba**, H. Stefanovic, "Primena zaštitnog kodovanja i kodova za kontrolu grešaka u sistemu za vrednovanje znanja", International Symposium on Operations Research-SYM-OP-IS 2021, Proceedings of papers, pp. 255–260, Banja Koviljača, Serbia, September 20–23, 2021, ISBN 978-86-7589-151-2 (M33)
9. N. Popovic, **G. Bjelobaba**, H. Stefanovic, A. Savic, N. Stefanovic, "*The Knowledge Evaluation System in Function of Achieving Competences*", 1st E-business technologies, "Modern e-business ecosystems" 2021, Department of a Business, Faculty of organizational sciences, University of Belgrade, Book of Abstracts, pp. 135–136, Belgrade, Serbia, July 10–11, 2021. (M33)
10. **G. Bjelobaba**, H. Stefanovic, A. Savic, N. Stefanovic, N. Popovic, "*A New Approach to Scientific-Research Paper Evaluation*", 1st E-business technologies, "Modern e-business ecosystems" 2021, Department of a Business, Faculty of organizational sciences, University of Belgrade, Book of Abstracts, pp. 129-131, Belgrade, Serbia, July 10–11, 2021. (M33)
11. **G. Bjelobaba**, N. Popovic, A.Savic, V. Vasiljevic, H. Stefanovic, M. Ilic, "Computer Networking Teaching and Learning Multimedia Education System", International Business Information Management Association-IBIMA, Proceedings of papers, pp. 8852-8862, Cordoba, Spain, May 30–31, 2021, ISBN: 978-0-9998551-6-4, ISSN: 2767-9640 (M33)
12. A. Savic, **G. Bjelobaba**, S. Strbac-Savic, I. Stefanovic, *Teaching and Learning of Mathematics in relation to the teaching program Electrical Engineering – traditional and distance approach*, International conference Quality of University Teaching and Learning, The Centre of the Republic of Slovenia for Mobility and European Educational and Training Programmes, Brdo kod Kranja, Slovenia April 6, 2016. CIP – 378.147(082)(0.034.2), Conference proceedings, ISBN 978-961-6628-50-1, pp. 232–240 (M33)
13. Kuka E., Kalemi E., Savic A., **Bjelobaba G.**, *Information Security in the public sector in Albania*, 6th International conference "Information Systems and Technology Innovations: inducting Modern Business Solutions" International Conference Proceedings ISTI 2015, 5–6 June 2015, Tirana, Albania, Proceedings Book, pp. 11 (M33)

7 БУДУЋА ИСТРАЖИВАЊА

Будућа истраживања су приказана кроз могућности интеграције развијеног софтверског система *Open-Rev* са сервисима система за е-образовање и примену развијеног приступа у образовном окружењу. Дат је предлог за евентуална побољшања развијеног система и приступа кроз мерење образовних и техничких индикатора перформанси система, анализу резултата примене система, конкретне идеје за унапређење система у будућности.

7.1 Интеграција развијеног софтверског система са сервисима система за е-образовање

Постоји много различитих система за е-учење који се могу интегрисати са развијеним системом *Open-Rev*. Наводимо неке могућности:

1. *Moodle* – платформа за е-учење отвореног кода која пружа низ функција за креирање курсева, управљање оценама и комуникацију између студената и наставника. *Moodle* има велику заједницу корисника и мноштво додатака који се могу користити за проширење функционалности;
2. *Blackboard* – један од најпопуларнијих система за е-учење који се широко користи у високом образовању. *Blackboard* омогућава креирање курсева, управљање оценама и распоредима и пружа низ додатака за проширење функционалности;
3. *Canvas* – е-образовна платформа која се широко користи у основним и средњим школама, као и на факултетима и универзитетима. *Canvas* пружа напредне алате за сарадњу, процену, аналитику и комуникацију;
4. *Google Classroom* – бесплатна алатка за учење и управљање учионицама која користи *Google* диск за складиштење и дељење датотека. *Google Classroom* пружа алате за сарадњу и комуникацију између наставника и ученика;
5. *Edmodo* – платформа за е-учење која се фокусира на интеракцију између наставника и ученика. *Edmodo* пружа алате за креирање курсева, додавање задатака и дељење садржаја.

Употреба блокчејн технологије у е-образовању може донети низ предности, али и неке недостатке. Предности су:

1. Повећана сигурност и транспарентност:

   Коришћењем блокчејн технологија подаци о студентима и њиховом напретку могу се чувати на безбедан и транспарентан начин. Сваки унос података трајно се чува и не може се избрисати, што повећава интегритет података;

2. Боље управљање идентитетом:

   Блокчејн технологије омогућавају боље управљање идентитетом студената, што помаже да се осигура да само овлашћени корисници могу приступити подацима;

3. Олакшано дељење података:

Коришћењем блокчејн технологија подаци о студентима и њиховом напретку могу се брзо и безбедно делити између различитих образовних институција и организација;

4. Побољшана сарадња:

   Блокчејн технологије омогућавају студентима и наставницима да сарађују на пројектима и задацима на безбедан и транспарентан начин, повећавајући квалитет образовања.

Недостаци су:

1. Сложеност:

   Блокчејн технологије могу бити сложене и захтевне за примену, што може представљати изазов за мање организације;

2. Високи трошкови:

   Примена блокчејн технологија може бити скупа, укључујући трошкове развоја, одржавања и безбедности;

3. Недостатак интероперабилности:

   Постоји ризик да различити блокчејн системи неће бити компатибилни један с другим, што може отежати дељење података између различитих организација;

4. Приватност:

   Пошто се подаци трајно чувају на блокчејну, постоји ризик да неке информације могу бити изложене јавности и нарушити приватност ученика.

На основу наведеног долази се до закључка да се мора пронаћи блокчејн систем који најбоље одговара потребама и који пружа неопходне алате за примену развијеног система.

Могуће је прилагодити развијени систем евалуације студентских радова подржаног блокчејн технологијом *Open-Rev* за интеграцију с платформом за е-учење *Moodle*. Интеграција система *Open-Rev* с платформом *Moodle* може пружити бројне предности, као што су:

1. Могућност повезивања с постојећим *Moodle* налозима: интегрисање *Open-Rev* блокчејн система с платформом *Moodle* може обезбедити да се повеже с постојећим корисничким налозима и подацима о студентима;
2. Безбедно складиштење и дељење података: интеграција са *Open-Rev* блокчејн системом омогућава безбедно складиштење и дељење података о студентима и њиховом напредовању кроз децентрализовану мрежу;
3. Транспарентност: блокчејн интеграција може да обезбеди транспарентност у процесу оцењивања и праћења напретка студената;
4. Аутоматизација: интеграција с блокчејном може аутоматизовати процес оцењивања и пратити напредак студената.

Интеграција блокчејн система *Open-Rev* с платформом *Moodle* може се постићи различитим методама, као што је развој прилагођених додатака или коришћење постојећих блокчејн додатака доступних за *Moodle*.

Неки од доступних блокчејн додатака за *Moodle* су:

1. *Moodle Blockchain Certificate* – омогућава генерисање дигиталних сертификата за студенте и чување њихових података у блокчејну. Сертификати се могу користити као доказ успешног завршетка курса;
2. *Open Badge Factory* – омогућава генерисање дигиталних отворених беџева који се чувају у блокчејну. Беџеви се могу користити као доказ о стеченим знањима и вештинама;
3. *EduCTX* – омогућава складиштење академских достигнућа студената у блокчејну. Подаци се могу користити као доказ о квалификацијама за запошљавање или даље образовање;
4. *Blockcerts* – омогућава издавање дигиталних сертификата и чување података о њима у блокчејну. Сертификати се могу користити као доказ о успешно завршеним курсевима или образовним програмима;
5. *Moodle Blockchain* – омогућава интеграцију платформе *Moodle* с различитим блокчејн мрежама, укључујући *Ethereum* и *Hyperledger Fabric*. Омогућава безбедно складиштење и дељење података о студентима и њиховом напредовању кроз децентрализовану мрежу.

Наведени додаци се могу разликовати по функцијама и могућностима које нуде, тако да треба проверити њихову компатибилност са одређеном верзијом платформе *Moodle*. Постоје и други блокчејн додаци доступни за *Moodle* који се могу прилагодити специфичним потребама.

Блокчејн додаци доступни за *Moodle* су и:

1. *BC LMS* – омогућава интеграцију платформе *Moodle* с биткоин блокчејном. Омогућава креирање и проверу дигиталних потписа за аутентичност докумената;
2. *VeriDegree* – омогућава креирање и издавање дигиталних сертификата за студенте и њихово складиштење у блокчејну;
3. *ProVerum* – омогућава чување академских достигнућа у блокчејну и њихову верификацију путем паметног уговора;
4. *ODEM* – омогућава креирање и издавање дигиталних сертификата за студенте и њихово складиштење у *Ethereum* блокчејну;
5. *CertUp* – омогућава генерисање и верификацију дигиталних сертификата ускладиштених у блокчејну. Сертификати се могу користити као доказ о успешном завршетку школовања или стицању одређених вештина.

Ови додаци нуде различите функције и карактеристике, тако да је важно проверити њихову компатибилност са одређеном верзијом платформе *Moodle* због одабира оне која најбоље одговара потребама.

Open-Rev користи популарну *open source* платформу за блокчејн *Hyperledger Fabric* која нуди бројне могућности за развој и примену различитих блокчејн апликација, с обзиром на то да се *Open-Rev* може интегрисати с платформом *Moodle* помоћу одговарајућих додатака (енг. *plugin*).

Hyperledger Fabric могућности:

1. *Hyperledger Fabric Connector* – омогућава платформи *Moodle* да се повеже на *Hyperledger Fabric* блокчејном и постигне двосмерну комуникацију;

2. *Certify Moodle* – омогућава креирање дигиталних сертификата за студенте и складиштење тих сертификата на *Hyperledger Fabric* блокчејну;
3. *EdChain* – омогућава интеграцију платформе *Moodle* с *Hyperledger Fabric* блокчејном за креирање и издавање академских диплома и сертификата;
4. *Moodle Hyperledger Plugin* – омогућава интеграцију платформе *Moodle* с *Hyperledger Fabric* блокчејном за креирање и издавање дигиталних сертификата.

7.2 Примена развијеног приступа у образовном окружењу

Примена *Open-Rev* развијеног модела у образовном окружењу зависи од многих фактора, као што су тип образовног програма, циљна публика, врста садржаја, доступност технологије и многи други.

Општи захтеви за примену модела у образовном окружењу су следећи:

1. Идентификација области у којој би развијени модел могао најбоље да допринесе побољшању образовања и где би био најефикаснији. Ово може укључивати области као што су процена учења, развој вештина, процена знања итд.;
2. Анализирање предности развијеног модела у поређењу с постојећим моделима у тој области. На тај начин може се јасније дефинисати постављени циљ и потенцијална корист развијеног модела у образовном окружењу;
3. Идентификација неопходних ресурса за примену развијеног модела, као што су технологија, инфраструктура, људски ресурси и финансије. На тај начин може се јасније одредити изводљивост модела;
4. Израда плана промене, који ће укључивати тестирање, праћење и процену развијеног модела. На овај начин модел ће моћи да се прилагођава на основу повратних информација добијених током тестирања;
5. Едукација и обука запослених који ће користити развијени модел. Потребно је уверити се да су корисници обучени да искористе предности развијеног модела и да разумеју како он функционише;
6. Континуирано праћење перформанси развијеног модела како би се осигурало да су постављени циљеви испуњени и да је примена развијеног модела ефикасна.

С обзиром на специфичности захтева, развијени систем *Open-Rev* за евалуације студентских радова подржан блокчејн технологијом, може бити веома користан за побољшање процеса евалуације на курсевима с великим броје студената. Наводимо неке примере за примену у таквом окружењу:

1. Обезбеђивање једноставног и интуитивног корисничког интерфејса. Требало би да и студенти и професори могу лако да користе систем, без специјализованог знања о блокчејн технологијама;
2. Укључивање функције објављивања и омогућавање студентима да евалуирају радове других студената, својих колега. Ово ће помоћи студентима да се активно укључе у процес евалуације и побољшају своје критичко мишљење;
3. Обезбеђивање сигурности и приватности података у систему. То се може постићи коришћењем безбедносних протокола уграђених у блокчејн технологије:

4. Коришћење паметних уговора да би се осигурало да су сви кораци у процесу евалуације транспарентни и да се оцене додељују према унапред дефинисаним правилима;
5. Обезбеђивање аналитике и статистике о процесу евалуације како би се омогућило професорима да боље разумеју како студенти евалуирају радове и да им олакшају процес оцењивања;
6. Обезбеђивање подршке корисницима развијеног система, укључујући обуку и техничку подршку, како би се осигурало да корисници могу лако да користе систем и решавају све проблеме;
7. Континуирано праћење перформанси развијеног система и коришћење повратних информација корисника да би се систем могао побољшати и прилагодити потребама одређеног окружења.

7.3 Мерење образовних и техничких показатеља перформанси

Мерење показатеља образовних и техничких перформанси од суштинског је значаја за правилно управљање образовним процесом, као и за праћење напретка студената и процеса учења.

Наведени су кораци који се могу предузети да би се реализовало и применило мерење образовних и техничких показатеља учинка:

1. Одредити циљеве мерења: Први корак у процесу мерења је одређивање циљева мерења – дефинисање шта се жели мерити и зашто је то важно за образовни процес;
2. Утврђивање релевантних показатеља учинка: Након одређивања циљева мерења, утврђују се релевантни показатељи учинка да би се пратили циљеви. Ови показатељи могу бити квалитативни или квантитативни [185];
3. Одабир одговарајућих инструмената за прикупљање података: У зависности од типа показатеља учинка који се жели пратити, бирају се одговарајући инструменти за прикупљање података (анкете, тестови, упитници, евалуације);
4. Упоређивање података: Упоређивање прикупљених података с дефинисаним циљевима мерења и показатељима учинка да би се утврдило колико добро функционише образовни процес [185];
5. Анализа података: Анализирање прикупљених података да би се открили трендови и обрасци у процесу учења;
6. Коришћење података за побољшање образовног процеса: Коришћење прикупљених података за доношење релевантних одлука о томе како да образовни процес буде побољшан. То може укључивати промену наставног материјала, реорганизацију наставног времена или увођење нових технологија и метода учења [204];
7. Континуирано надгледање и процењивање учинка: Континуирано праћење и процењивање учинка како би се могао прилагодити и побољшати образовни процес током времена [205].

7.4 Анализа резултата примене

Анализа резултата примене укључује следеће кораке:

1. Дефинисање циљева: Циљеви могу бити различити, као што је процена ефективности система, препознавање слабих тачака и предлога за побољшање, праћење напретка у односу на претходне перформансе итд.
2. Припрема података: Да би се извршила анализа, потребно је припремити релевантне податке. То могу бити подаци о перформансама система (на пример број корисника, број објављених радова, број евалуација итд.) и подаци о корисницима система (на пример године студија, успех на претходним испитима итд.). Подаци морају да буду доступни у структурираном формату и јасно дефинисани.
3. Избор метода и техника анализе: Избор метода и техника анализе зависиће од циљева и природе података. Неке од уобичајених метода укључују статистичке тестове, анализу трендова, кластер анализу и друге.
4. Извођење анализе: Када се припреме подаци и изаберу методе анализе, треба извршити анализу. Ово може укључивати употребу софтвера за статистичку анализу или програмских језика за обраду података.
5. Интерпретација резултата: Након што су подаци анализирани, резултате треба интерпретирати. Ово би могло укључити препознавање кључних фактора који утичу на перформансе система, утврђивање трендова, препознавање слабих тачака и предлога за побољшање, као и друге закључке.
6. Презентација резултата: Резултате анализе треба представити на јасан начин. Ово може укључивати припрему извештаја, графичких приказа и других материјала који ће помоћи у разумевању и тумачењу резултата.

7.5 Идеје за унапређење система у будућности

Наводимо неке од идеја за унапређење система у будућности:

- Побољшање скалабилности система: Иако је систем већ скалабилан, могу се истражити могућности за додатно побољшање скалабилности, на пример коришћењем технологије *sharding* или других метода.
- Повећање безбедности система: Безбедност система се увек може побољшати. Могу се истражити нове методе за заштиту од напада и рањивости, укључујући употребу нових механизама за шифровање и аутентификацију.
- Функција која ради обраду грешке могла би се унапредити. У функцију *convertError* било би добро додати обраду других врста грешака које се могу појавити при раду са *ledger*-ом, а нису укључене у тип *ErrorDetail*, који се обрађује у тренутно примењеној. Такође, уместо функције *log.Printf*, могла би се користити функција *log.Error* да би се грешка на адекватан начин приказала у системским логовима.

На пример, функција може изгледати овако:

```
func convertError(err error) error {
```

```
  statusErr := status.Convert(err)
  for _, detail := range statusErr.Details() {
    switch detail := detail.(type) {
    case *gateway.ErrorDetail:
      log.Errorf("Error from endpoint: %s, mspId: %s, message: %s\n", detail.Address, detail.MspId, detail.Message)
      return fmt.Errorf(detail.Message)
    default:
      log.Errorf("Unknown error occurred: %v", err)
      return err
    }
  }
  return nil
}
```

Функција ажурирана на овај начин може да обради различите врсте грешака које се могу јавити приликом рада с *ledger*-ом и адекватно их приказати у системским евиденцијама.

- У делу где се позивају функција *evaluate* и трансакције *submit* могло би бити корисно додати друге функционалности као што су:
  - Валидација улазних података: Пре него што се подаци проследе у трансакцију, важно је проверити да ли су валидни. Ово се може урадити додавањем функција за валидацију, које ће проверити да ли су подаци у складу са очекиваним форматом и да ли су уопште доступни;
  - Трансакције с више потписа: У случају када је потребан потпис више корисника да би се извршила трансакција, кôд треба да се прилагоди да подржи овај процес. Ово се може урадити коришћењем библиотека као што су *go-crypto-multisig* или *go-multisignature*;
  - Оптимизација перформанси: За веће и сложеније трансакције може бити корисно оптимизовати кôд како би се смањило време извршења. Ово се може урадити коришћењем функционалности као што је кеширање података или коришћењем вишенитног програмирања (енг. *concurrency*);
  - У зависности од потреба и захтева организације, можда ће бити потребно додати додатне безбедносне функционалности, као што је шифровање података или додатна аутентификација корисника;
  - У зависности од потреба, могуће је додати и друге функционалности као што су пријављивање, праћење статуса трансакција и слично;
- Побољшање перформанси система: Иако су перформансе система већ високе, увек постоје начини за побољшање, као што су оптимизација кода и коришћење напреднијих хардверских ресурса;
- Истраживање могућности за проширење система на друге области;

- Побољшање корисничког искуства истраживањем нове функционалности и алата за побољшање корисничког искуства, као што су бољи интерфејси, персонализација и друге функције;
- Развијање нове функционалност система које могу бити корисне у одређеним индустријама или за одређене групе корисника;
- Истраживање нових технологија и трендова: Систем се може проширити и побољшати коришћењем нових технологија и трендова у индустрији, као што су вештачка интелигенција, машинско учење, *IoT* и још много тога.

8 ЗАКЉУЧАК

У докторској дисертацији је изложен преглед теоријских основа колаборативног учења, евалуације студентских радова и блокчејн технологија. У експерименталном делу рада развијен је модел за колаборативно учење и евалуацију студентских радова заснован на блокчејн технологијама. Тестирање модела за колаборативно учење и евалуацију студентских радова реализовано је наменски развијеним софтверским системом *Open-Rev* примењеним у високошколској образовној институцији.

Допринос овог рада је нови модел за колаборативно учење и евалуацију студентских радова заснован на блокчејн технологијама. Развијени модел има за циљ квалитетнију евалуацију студентских радова, подстицање пројектно оријентисаног учења и унапређење квалитета образовног процеса. Резултати истраживања у овој докторској дисертацији објављени су у часописима међународног значаја и саопштени на научним скуповима у земљи и иностранству.

9 ЛИТЕРАТУРА

[1] T. T. Vu and G. Dall'Alba, "Students' experience of peer assessment in a professional course," *Assess. Eval. High. Educ.*, vol. 32, no. 5, pp. 541–556, 2007, doi: 10.1080/02602930601116896.

[2] J. Mok, "A case study of students' perceptions of peer assessment in Hong Kong," *ELT J.*, vol. 65, no. 3, pp. 230–239, Jul. 2011, doi: 10.1093/elt/ccq062.

[3] Y. Han, W. Wu, Y. Yan, and L. Zhang, "Human-machine hybrid peer grading in SPOCs," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3043291.

[4] F. Garcia-Loro, S. Martin, J. A. Ruipérez-Valiente, E. Sancristobal, and M. Castro, "Reviewing and analyzing peer review Inter-Rater Reliability in a MOOC platform," *Comput. Educ.*, vol. 154, Sep. 2020, doi: 10.1016/j.compedu.2020.103894.

[5] H. Luo, A. C. Robinson, and J.-Y. Park, "Peer Grading in a MOOC: Reliability, Validity, and Perceived Effects," *Online Learn.*, vol. 18, no. 2, pp. 454–460, Jun. 2014, doi: 10.24059/olj.v18i2.429.

[6] T. Hovardas, O. E. Tsivitanidou, and Z. C. Zacharia, "Peer versus expert feedback: An investigation of the quality of peer feedback among secondary school students," *Comput. Educ.*, vol. 71, pp. 133–152, 2014, doi: 10.1016/j.compedu.2013.09.019.

[7] M. Formanek, M. C. Wenger, S. R. Buxner, C. D. Impey, and T. Sonam, "Insights about large-scale online peer assessment from an analysis of an astronomy MOOC," *Comput. Educ.*, vol. 113, pp. 243–262, Oct. 2017, doi: 10.1016/j.compedu.2017.05.019.

[8] D. E. Paré and S. Joordens, "Peering into large lectures: Examining peer and expert mark agreement using peerScholar, an online peer assessment tool," *J. Comput. Assist. Learn.*, vol. 24, no. 6, pp. 526–540, Dec. 2008, doi: 10.1111/j.1365-2729.2008.00290.x.

[9] F. Liu, W. dong Zhu, Y. wang Chen, D. ling Xu, and J. bo Yang, "Evaluation, ranking and selection of R&D projects by multiple experts: an evidential reasoning rule based approach," *Scientometrics*, vol. 111, no. 3, pp. 1501–1519, Jun. 2017, doi: 10.1007/s11192-017-2278-1.

[10] K. J. Topping, "Peer assessment," *Theory Pract.*, vol. 48, no. 1, pp. 20–27, 2009, doi: 10.1080/00405840802577569.

[11] K. Topping, "Peer assessment between students in colleges and universities," *Rev. Educ. Res.*, vol. 68, no. 3, pp. 249–276, 1998, doi: 10.3102/00346543068003249.

[12] J. S. Kane and E. E. Lawler, "Methods of peer assessment," *Psychol. Bull.*, vol. 85, no. 3, May 1978, doi: 10.1037/0033-2909.85.3.555.

[13] G. Bjelobaba, H. Stefanović, A. Savić, N. Stefanović, and N. Popović, "A New Approach to Scientific-Research Paper Evaluation," in *E-business technologies conference proceedings*, 2021, vol. 1, no. 1, pp. 198–200, [Online]. Available: https://ebt.rs/journals/index.php/conf-proc/article/view/93.

[14] Z. Misic and B. Mrazovac, "Implementacija Programske Podrške za Manipulaciju Podacima Decentralizovane Aplikacije za Upravljanje Pristupom Zaštićenoj Zoni," *Zb. Rad. Fak. Teh. Nauk. u Novom Sadu*, vol. 35, no. 10, pp. 1818–1821, Oct. 2020, doi: 10.24867/09ih03misic.

[15] R. Chatterjee and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain," in *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*, Oct. 2017, pp. 126–127, doi: 10.1109/CINE.2017.33.

[16] P. Bhaskar, C. K. Tiwari, and A. Joshi, "Blockchain in education management: present and future applications," *Interactive Technology and Smart Education*, vol. 18, no. 1. Emerald Group Holdings Ltd., pp. 1–17, 2020, doi: 10.1108/ITSE-07-2020-0102.

[17] H. Sun, X. Wang, and X. Wang, "Application of blockchain technology in online education," *Int. J. Emerg. Technol. Learn.*, vol. 13, no. 10, pp. 252–259, 2018, doi:

10.3991/ijet.v13i10.9455.
[18] H. Hyvärinen, M. Risius, and G. Friis, “A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services,” 2017.
[19] V. J. Morkunas, J. Paschen, and E. Boon, “How blockchain technologies impact your business model,” *Bus. Horiz.*, vol. 62, no. 3, pp. 295–306, May 2019, doi: 10.1016/j.bushor.2019.01.009.
[20] M. Mettler, “Blockchain technology in healthcare: the revolution starts here,” Aug. 2016, Accessed: Jun. 12, 2021. [Online]. Available: https://sci-hub.do/https://ieeexplore.ieee.org/abstract/document/7749510/.
[21] W. Rashideh, “Blockchain technology framework: Current and future perspectives for the tourism industry,” *Tour. Manag.*, vol. 80, Oct. 2020, doi: 10.1016/j.tourman.2020.104125.
[22] M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100. Elsevier Ltd, pp. 143–174, Feb. 01, 2019, doi: 10.1016/j.rser.2018.10.014.
[23] T. I. Akaba, A. Norta, C. Udokwu, and D. Draheim, *A framework for the adoption of blockchain-Based e-Procurement systems in the public sector*, vol. 12066. Cham: Springer International Publishing, 2020.
[24] S. Mahankali and S. Chaudhary, “Blockchain in education: a comprehensive approach–utility, use cases, and implementation in a university,” in *Blockchain in Education*, IGI Global, 2020.
[25] M. Malekigorji, D. Corbett, L.-A. Hanna, and M. Hall, “An Investigation of Chinese Students Academic Performance, and Their Views on The Learning Experience, Associated with Flipped Team-Based Learning,” *Lit. Inf. Comput. Educ. J.*, vol. 9, no. 1, pp. 2788–2799, Mar. 2018, doi: 10.20533/licej.2040.2589.2018.0368.
[26] R. Bdiwi, C. De Runz, S. Faiz, and A. A. Cherif, “A blockchain based decentralized platform for ubiquitous learning environment,” in *Proceedings - IEEE 18th International Conference on Advanced Learning Technologies, ICALT 2018*, Aug. 2018, pp. 90–92, doi: 10.1109/ICALT.2018.00028.
[27] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 9891 LNCS, pp. 490–496, doi: 10.1007/978-3-319-45153-4_48.
[28] A. Savelyev, “Copyright in the blockchain era: promises and challenges,” 2018. [Online]. Available: http://www3.weforum.org/docs/WEFA_BlueprintforDigitalIdentity.pdf.
[29] K. Ito, “A critical examination of the application of blockchain technology to intellectual property management,” London, 2019, pp. 317–335.
[30] W. Zhao, K. Liu, and K. Ma, “Design of Student Capability Evaluation System Merging Blockchain Technology,” in *Journal of Physics: Conference Series*, Mar. 2019, vol. 1168, no. 3, doi: 10.1088/1742-6596/1168/3/032123.
[31] P. Williams, “Does competency-based education with blockchain signal a new mission for universities?”
[32] B. Duan, Y. Zhong, and D. Liu, “Education application of blockchain technology: Learning outcome and meta-diploma,” in *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, May 2018, vol. 2017-Decem, pp. 814–817, doi: 10.1109/ICPADS.2017.00114.
[33] A. Mikroyannidis, *Blockchain Applications in Education: A Case Study in Lifelong Learning*. 2020, pp. 21–25.
[34] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang, and Q. Li, “ECBC: A high performance educational certificate blockchain with efficient query,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10580 LNCS, pp. 288–304, doi: 10.1007/978-3-319-67729-3_17.
[35] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, “Blockchain-based applications

in education: A systematic review," *Applied Sciences (Switzerland)*, vol. 9, no. 12. MDPI AG, Jun. 01, 2019, doi: 10.3390/app9122400.
[36] M. Han, D. Wu, Z. Li, Y. Xie, J. S. He, and A. Baba, "A novel blockchain-based education records verification solution," in *SIGITE 2018 - Proceedings of the 19th Annual SIG Conference on Information Technology Education*, Sep. 2018, pp. 178–183, doi: 10.1145/3241815.3241870.
[37] D. J. Skiba, "The Potential of Blockchain in Education and Health Care," *Nurs. Educ. Perspect.*, vol. 38, no. 4, pp. 220–221, Jul. 2017, doi: 10.1097/01.NEP.0000000000000190.
[38] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, Jan. 2018, doi: 10.1109/ACCESS.2018.2789929.
[39] N. Bore, S. Karumba, J. Mutahi, S. S. Darnell, C. Wayua, and K. Weldemariam, "Towards Blockchain-enabled school information hub," in *ACM International Conference Proceeding Series*, Nov. 2017, vol. Part F1320, doi: 10.1145/3136560.3136584.
[40] H. Ali, "The effect of collaborative learning and self-assessment on self-regulation," *Educ. Res. Rev.*, vol. 10, no. 15, pp. 2164–2167, Aug. 2015, doi: 10.5897/err2015.2349.
[41] M. Laal and M. Laal, "Collaborative learning: What is it?," in *Procedia - Social and Behavioral Sciences*, 2012, vol. 31, pp. 491–495, doi: 10.1016/j.sbspro.2011.12.092.
[42] M. Laal and S. M. Ghodsi, "Benefits of collaborative learning," in *Procedia - Social and Behavioral Sciences*, 2012, vol. 31, pp. 486–490, doi: 10.1016/j.sbspro.2011.12.091.
[43] J. MacDonald, "Assessing online collaborative learning: Process and product," *Comput. Educ.*, vol. 40, no. 4, pp. 377–391, May 2003, doi: 10.1016/S0360-1315(02)00168-9.
[44] "A case study of students perceptions."
[45] J. Van Aalst, "Chapter 16 Assessment in Collaborative Learning." [Online]. Available: www.act21.org.
[46] I. Kollar and F. Fischer, "Peer assessment as collaborative learning: a cognitive perspective." [Online]. Available: https://hal.archives-ouvertes.fr/hal-00703943.
[47] H. P. Chan and I. King, "Leveraging social connections to improve peer assessment in MOOCs," in *26th International World Wide Web Conference 2017, WWW 2017 Companion*, 2017, pp. 341–349, doi: 10.1145/3041021.3054165.
[48] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *J. Comput. High. Educ.*, vol. 32, no. 1, pp. 109–134, Apr. 2020, doi: 10.1007/s12528-019-09209-y.
[49] S. Saurabh, H. Sanwar A. S. M., and Y. Byungun, "Blockchain Security Attacks, Challenges, andSolutions for the Future DistributedIoT Network," *Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network*, 2021. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9323061 (accessed Jun. 01, 2021).
[50] J. Xu, Q. Li, J. Liu, P. Lv, and G. Yu, "Leveraging cognitive diagnosis to improve peer assessment in MOOCS," *IEEE Access*, vol. 9, pp. 50466–50484, 2021, doi: 10.1109/ACCESS.2021.3069055.
[51] C. Piech, J. Huang, Z. Chen, C. Do, A. Ng, and D. Koller, "Tuned Models of Peer Assessment in MOOCs," Jul. 2013, doi: 10.48550/arXiv.1307.2579.
[52] H. Luo, A. C. Robinson, and J.-Y. Park, "Peer Grading in a MOOC: Reliability, Validity, and Perceived Effects," *Online Learn.*, vol. 18, no. 2, pp. 1–14, Jun. 2014, doi: 10.24059/olj.v18i2.429.
[53] C. Task and C. Clifton, "A guide to differential privacy theory in social network analysis," in *Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012*, 2012, pp. 411–417, doi: 10.1109/ASONAM.2012.73.
[54] IEEE Education Society, IEEE Computer Society, Institute of Electrical and Electronics Engineers, and King Mongkut's University of Technology North Bangkok,

Proceedings of 2016 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) : 7–9 December 2016, Dusit Thani Bangkok Hotel, Bangkok, Thailand. .
[55] I. Claros, R. Cobos, and C. A. Collazos, "An Approach Based on Social Network Analysis Applied to a Collaborative Learning Experience," *IEEE Trans. Learn. Technol.*, vol. 9, no. 2, pp. 190–195, Apr. 2016, doi: 10.1109/TLT.2015.2453979.
[56] H. Chen, "IEEE ISI 2008 Keynote Talk (III) Homeland Security Data Mining using Social Network Analysis."
[57] J. Lopez-Vargas, N. Piedra, J. Chicaiza, and E. Tovar, "OER Recommendation for Entrepreneurship Using a Framework Based on Social Network Analysis," *Rev. Iberoam. Tecnol. del Aprendiz.*, vol. 10, no. 4, pp. 262–268, Nov. 2015, doi: 10.1109/RITA.2015.2486387.
[58] M. Jamali and H. Abolhassani, "Different Aspects of Social Network Analysis."
[59] 1954- Halimah Badioze Zaman and Universiti Kebangsaan Malaysia. Fakulti Teknologi dan Sains Maklumat., *International Symposium on Information Technology 2008 : proceedings : Kuala Lumpur Convention Centre, Malaysia, 26–29 August 2008 : ITSIM '08, cognitive informatics, bridging natural and artificial knowledge*. Institute of Electrical and Electronics Engineers, 2008.
[60] Erlin, N. Yusof, and A. A. Rahman, "Students' interactions in online asynchronous discussion forum: A social network analysis," in *2009 International Conference on Education Technology and Computer, ICETC 2009*, 2009, pp. 25–29, doi: 10.1109/ICETC.2009.48.
[61] T. R. Coffman, "Pattern Classification in Social Network Analysis: A Case."
[62] F. Pozzi, S. Manca, D. Persico, and L. Sarti, "A general framework for tracking and analysing learning processes in computer-supported collaborative learning environments," *Innov. Educ. Teach. Int.*, vol. 44, no. 2, pp. 169–179, May 2007, doi: 10.1080/14703290701240929.
[63] Association for Computing Machinery. and Institute of Electrical and Electronics Engineers., *2009 31st International Conference on Software Engineering : May 16-24, 2009 Vancouver, Canada : proceedings*. IEEE, 2009.
[64] C. Y. Lin, N. Cao, S. X. Liu, S. Papadimitriou, J. Sun, and X. Yan, "SmallBlue: Social network analysis for expertise search and collective intelligence," in *Proceedings - International Conference on Data Engineering*, 2009, pp. 1483–1486, doi: 10.1109/ICDE.2009.140.
[65] D. Katsaros, "T T Social Network Analysis Concepts in the Design of Wireless Ad Hoc Network Protocols," 2010.
[66] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *IEEE Trans. Mob. Comput.*, vol. 8, no. 5, pp. 606–621, May 2009, doi: 10.1109/TMC.2008.161.
[67] N. Akhtar, "Social network analysis tools," in *Proceedings – 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, 2014, pp. 388–392, doi: 10.1109/CSNT.2014.83.
[68] C. Y. Lin *et al.*, "Social network analysis in enterprise," *Proc. IEEE*, vol. 100, no. 9, pp. 2759–2776, 2012, doi: 10.1109/JPROC.2012.2203090.
[69] K. Stepanyan, K. Borau, and C. Ullrich, "A social network analysis perspective on student interaction within the twitter microblogging environment," in *Proceedings – 10th IEEE International Conference on Advanced Learning Technologies, ICALT 2010*, 2010, pp. 70–72, doi: 10.1109/ICALT.2010.27.
[70] S. Ghani *et al.*, "Visual Analytics for Multimodal Social Network Analysis: A Design Study with Social Scientists," 2013.
[71] J. M. Spector, IEEE Technical Committee on Learning Technology., IEEE Computer Society., and Denki Tsūshin Daigaku., *The Seventh IEEE International Conference on Advanced Learning Technologies : proceedings : ICALT 2007 : July 18–20, 2007 : Niigata,*

Japan. IEEE Computer Society, 2007.
[72] P. A. Gloor, J. Krauss, S. Nann, K. Fischbach, and D. Schoder, "Web science 2.0: Identifying trends through semantic social network analysis," in *Proceedings – 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 2009, vol. 4, pp. 215–222, doi: 10.1109/CSE.2009.186.
[73] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9891 LNCS, pp. 490–496, 2016, doi: 10.1007/978-3-319-45153-4_48.
[74] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *J. Comput. High. Educ.*, vol. 32, no. 1, pp. 109–134, Apr. 2020, doi: 10.1007/S12528-019-09209-Y.
[75] P. Dillenbourg, "What do you mean by collaborative learning?," pp. 1–19, 1999, Accessed: Aug. 05, 2021. [Online]. Available: https://telearn.archives-ouvertes.fr/hal-00190240.
[76] M. Ibáñez, J. Rueda, D. Maroto, C. K.-J. of N. and, and undefined 2013, "Collaborative learning in multi-user virtual environments," *Elsevier*, no. 6, pp. 1566–1576, 2013, doi: 10.1016/j.jnca.2012.12.027.
[77] D. Johnson, R. Johnson, and M. Stanne, "Cooperative learning methods: A meta-analysis," 2000, Accessed: Aug. 05, 2021. [Online]. Available: https://sci-hub.do/https://www.academia.edu/download/33787421/Cooperative_Learning_Methods_A_Meta-Analysis.pdf.
[78] L. Lin, *Investigating Chinese HE EFL Classrooms - Using Collaborative Learning to Enhance Learning*. Springer , 2014.
[79] G. Jacobs and P. Seow, "Cooperative Learning Principles Enhance Online Interaction Paper 55-CTLT 2014."
[80] B. Rosenshine, C. M.-R. of educational research, and undefined 1994, "Reciprocal teaching: A review of the research," *journals.sagepub.com*, vol. 64, no. 4, pp. 479–530, 1994, Accessed: Aug. 05, 2021. [Online]. Available: https://sci-hub.do/https://journals.sagepub.com/doi/abs/10.3102/00346543064004479.
[81] E. A.-I. academic achievement and undefined 2002, "Building empathy, compassion, and achievement in the jigsaw classroom," *Elsevier*, 2002, Accessed: Aug. 05, 2021. [Online]. Available: https://sci-hub.do/https://www.sciencedirect.com/science/article/pii/B9780120644551500130.
[82] J. A. Larusson and R. Alterman, "Wikis to support the 'collaborative' part of collaborative learning," *Int. J. Comput. Collab. Learn.*, vol. 4, no. 4, pp. 371–402, 2009, doi: 10.1007/S11412-009-9076-6.
[83] M. Kordaki and H. Siempos, "Digital storytelling view project computational thinking and digital storytelling view project the jigsaw collaborative method within the online computer science classroom," 2010. [Online]. Available: https://www.researchgate.net/publication/221130399.
[84] M. Martić, D. Makajić-Nikolić, G. Savić, Faculty of Organizational Sciences (Beograd)., and Fakultet organizacionih nauka (Beograd)., *Proceedings Zbornik radova*. Faculty of Organizational Sciences, 2019.
[85] P. C. Blumenfeld, E. Soloway, R. W. Marx, J. S. Krajcik, M. Guzdial, and A. Palincsar, "Motivating Project-Based Learning: Sustaining the Doing, Supporting the Learning," *Educational Psychologist*, vol. 26, no. 3–4. pp. 369–398, 1991, doi: 10.1080/00461520.1991.9653139.
[86] N. Webb, M. Franke, T. De, … A. C.-C. J. of, and undefined 2009, "'Explain to your partner': teachers' instructional practices and students' dialogue in small groups," *Taylor Fr.*, vol. 39, no. 1, pp. 49–70, Mar. 2009, doi: 10.1080/03057640802701986.
[87] Littleton Karen and Light Paul, *Learning with computers: Analysing productive*

interaction. Florence: Florence, KY: Psychology Press , 1999.
[88] V. Chiang, S. Leung, C. Chui, … A. L.-N. education, and undefined 2013, "Building life-long learning capacity in undergraduate nursing freshmen within an integrative and small group learning context," *Elsevier*, Accessed: Aug. 05, 2021. [Online]. Available: https://sci-hub.do/https://www.sciencedirect.com/science/article/pii/S0260691712001396.
[89] S. Järvelä and A. F. Hadwin, "New Frontiers: Regulating Learning in CSCL," *Educ. Psychol.*, vol. 48, no. 1, pp. 25–39, Jan. 2013, doi: 10.1080/00461520.2012.748006.
[90] A. Hadwin and M. Oshige, "Self-Regulation, Coregulation, and Socially Shared Regulation: Exploring Perspectives of Social in Self-Regulated Learning Theory."
[91] H. Järvenoja, "Socially Constructed Self-Regulated Learning and Motivation Regulation in Collaborative Learning Groups," 2011. [Online]. Available: https://www.researchgate.net/publication/230555576.
[92] E. Aronson, "Building Empathy, Compassion, and Achievement in the Jigsaw Classroom," in *Improving Academic Achievement*, Elsevier, 2002.
[93] M. Laal, S. G.-P. and behavioral Sciences, and U. 2012, "Benefits of collaborative learning," *Elsevier*, Accessed: Aug. 06, 2021. [Online]. Available: https://sci-hub.do/https://www.sciencedirect.com/science/article/pii/S1877042811030205.
[94] C. N. Loes, "Applied Learning through Collaborative Educational Experiences," *New Dir. High. Educ.*, vol. 2019, no. 188, pp. 13–21, 2019, doi: 10.1002/he.20341.
[95] H. Jeong, C. H.-S.-E. Psychologist, and undefined 2016, "Seven affordances of computer-supported collaborative learning: How to support collaborative learning? How can technologies help?," *Taylor Fr.*, vol. 51, no. 2, pp. 247–265, Apr. 2016, doi: 10.1080/00461520.2016.1158654.
[96] B. Inpin, "Online Collaborative Learning Communities (OCLCs): Pathways to Promote Teachers' Professional Development in Transformative Educational System," 2021.
[97] J. L. Laufgraben and N. S. Shapiro, *Sustaining and Improving Learning Communities* , 1st Editio. Jossey-Bass, 2004.
[98] B. L. Smith and J. T. MacGregor, "Collaboration Learning: A Sourcebook for Higher Education," *Univ. Park. PA Natl. Cent. Postsecond. Teaching, Learn. Assess.*, pp. 159–189, 1992.
[99] M. Shonfeld and D. Gibson, *Collaborative learning in a global world*. New York: New York: IAP, 2018.
[100] B. Inpin, "Online Collaborative Learning Communities (OCLCs)," 2021, doi: 10.2991/assehr.k.210203.139.
[101] A. Aslan, "The evaluation of collaborative synchronous learning environment within the framework of interaction and community of inquiry: An experimental study," *J. Pedagog. Res.*, vol. 5, no. 2, pp. 72–87, 2021, doi: 10.33902/jpr.2021269326.
[102] T. Oktavia, H. L. H. S. Warnars, and S. Adi, "Integration model of knowledge management and social media for higher education," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 15, no. 2, pp. 678–685, 2017, doi: 10.12928/TELKOMNIKA.v15i2.3491.
[103] M. Rena, "Collaborating Online: Learning Together in Community.," vol. 32, pp. 3–18, 2010.
[104] T. Markham, *Project Based Learning - Teacher Librarian*, vol. 2. Teacher Librarian, 2011.
[105] K. Smith, "Project-Based Learning," 2015.
[106] J. Larmer, "Seven Essentials for Project-Based Learning," 2010, Accessed: Aug. 25, 2021. [Online]. Available: http://www.ascd.org/publications/educational_leadership/sept10/vol68/num01/Seven_Essentials_for_Project-Based_Learning.aspx.
[107] N. Rummel, "One framework to rule them all? Carrying forward the conversation started by Wise and Schwarz," *Int. J. Comput. Collab. Learn.*, vol. 13, no. 1, pp. 123–129,

Jan. 2018, doi: 10.1007/S11412-018-9273-2.
[108] K. Holstein, V. Aleven, and N. Rummel, “A conceptual framework for human–AI hybrid adaptivity in education,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12163 LNAI, pp. 240–254, 2020, doi: 10.1007/978-3-030-52237-7_20.
[109] Y. Han, W. Wu, Y. Yan, L. Z.-I. Access, and U. 2020, “Human-machine hybrid peer grading in SPOCs,” *ieeexplore.ieee.org*, Accessed: Aug. 06, 2021. [Online]. Available: https://sci-hub.do/https://ieeexplore.ieee.org/abstract/document/9286436/.
[110] J. Xu, Q. Li, J. Liu, P. Lv, G. Y.-I. Access, and U. 2021, “Leveraging Cognitive Diagnosis to Improve Peer Assessment in MOOCs,” *ieeexplore.ieee.org*, Accessed: Aug. 06, 2021. [Online]. Available: https://sci-hub.do/https://ieeexplore.ieee.org/abstract/document/9387359/.
[111] H. Luo, A. Robinson, J. P.-O. L. Journal, and undefined 2014, “Peer grading in a MOOC: Reliability, validity, and perceived effects,” *learntechlib.org*, Accessed: Aug. 06, 2021. [Online]. Available: https://sci-hub.do/https://www.learntechlib.org/p/183756/.
[112] L. Bouzidi, A. J.-J. of E. T. & Society, and U. 2009, “Can online peer assessment be trusted?,” *JSTOR*, Accessed: Aug. 26, 2021. [Online]. Available: https://sci-hub.do/https://www.jstor.org/stable/jeductechsoci.12.4.257.
[113] G. D.-C. Brief and undefined 2003, “The value of online student peer review, evaluation and feedback in higher education,” *Citeseer*, 2003, Accessed: Aug. 26, 2021. [Online]. Available: https://sci-hub.do/http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.1903&rep=rep1&type=pdf.
[114] J. Gikandi, D. Morrow, N. D.-C. & education, and undefined 2011, “Online formative assessment in higher education: A review of the literature,” *Elsevier*, 2011, doi: 10.1016/j.compedu.2011.06.004.
[115] A. L.-R.-C. S. Education and undefined 2009, “A systematic review of tools that support peer assessment,” *Taylor Fr.*, vol. 00, no. 00, pp. 1–19, 2009, doi: 10.1080/08993400903384844.
[116] K. Topping, “Peer assessment between students in colleges and universities,” *Rev. Educ. Res.*, vol. 68, no. 3, pp. 249–276, 1998, doi: 10.3102/00346543068003249.
[117] D. Babik, E. Gehringer, J. Kidd, and F. Pramudianto, “Probing the landscape: Toward a systematic taxonomy of online peer assessment systems in education,” 2016, Accessed: Aug. 26, 2021. [Online]. Available: https://sci-hub.do/http://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1053&context=teachinglearning_fac_pubs.
[118] Y. Reddy, H. A.-A. & evaluation in higher, and undefined 2010, “A review of rubric use in higher education,” *Taylor Fr.*, vol. 35, no. 4, pp. 435–448, 2010, doi: 10.1080/02602930902862859.
[119] C. S. Spetzler and C.-A. S. Staël Von Holstein, “Probability Encoding in Decision Analysis,” *Manage. Sci.*, vol. 22, no. 3, 1975, doi: 10.1287/mnsc.22.3.340.
[120] P. Davies, “Computerized Peer Assessment,” *Innov. Educ. Train. Int.*, vol. 37, no. 4, pp. 346–355, 2000, doi: 10.1080/135580000750052955.
[121] J. R. Douceur, “Paper rating vs. paper ranking,” *Oper. Syst. Rev.*, vol. 43, no. 2, pp. 117–121, Apr. 2009, doi: 10.1145/1531793.1531816.
[122] D. Babik, L. S. Iyer, and E. W. Ford, “Towards a comprehensive online peer assessment system: Design outline,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7286 LNCS, pp. 1–8, 2012, doi: 10.1007/978-3-642-29863-9_1.
[123] K. Cho, C. S.-C. & Education, and undefined 2007, “Scaffolded writing and rewriting in the discipline: A web-based reciprocal peer review system,” *Elsevier*, doi: 10.1016/j.compedu.2005.02.004.

[124] S. Joordens, S. Desa, D. P.-J. of Systemics, & C., and U. 2009, "The pedagogical anatomy of peer-assessment: Dissecting a peerScholar assignment," *iiisci.org*, Accessed: Aug. 26, 2021. [Online]. Available: https://sci-hub.do/http://www.iiisci.org/journal/CV$/sci/pdfs/XE123VF.pdf.
[125] H. Søndergaard, R. M.-C. S. Education, and undefined 2012, "Collaborative learning through formative peer review: Pedagogy, programs and potential," *Taylor Fr.*, vol. 22, no. 4, pp. 343–367, Dec. 2012, doi: 10.1080/08993408.2012.728041.
[126] R. Yadav, E. G.-S. and future directions of smart, and undefined 2016, "Metrics for automated review classification: What review data show," *Springer*, Accessed: Aug. 26, 2021. [Online]. Available: https://sci-hub.do/https://link.springer.com/chapter/10.1007/978-981-287-868-7_41.
[127] T. Gayvoronskaya and C. Meinel, *Blockchain*. Cham: Springer International Publishing, 2021.
[128] P. Ray, K. Saini, and C. Surianarayanan, *Blockchain technology and applications*, First 2021. London, New York: CRC press, 2021.
[129] G. Hileman and M. Rauchs, *Global Blockchain Benchmarking Study*, vol. 10, no. 2. 2017, pp. 37–38.
[130] P. Raj, K. Saini, and C. Surianarayanan, "Blockchain Technology and Applications."
[131] S. Krishnapriya and G. Sarath, "Securing Land Registration using Blockchain," in *Procedia Computer Science*, 2020, vol. 171, pp. 1708–1715, doi: 10.1016/j.procs.2020.04.183.
[132] "Banking Beyond Banks and Money A Guide to Banking Services in the Twenty-First Century." [Online]. Available: http://www.springer.com/series/6901.
[133] M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Electron. J.*, no. August, 2018, doi: 10.2139/ssrn.3230013.
[134] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," May 2017, doi: 10.14722/ndss.2016.23187.
[135] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in Bitcoin and Ethereum Networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10957 LNCS, pp. 439–457, 2018, doi: 10.1007/978-3-662-58387-6_24.
[136] D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, "Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector," *Vis. Comput. Ind. Biomed. Art*, vol. 4, no. 1, Dec. 2021, doi: 10.1186/s42492-021-00084-y.
[137] W. Yang, S. Garg, Z. Huang, and B. Kang, "A decision model for blockchain applicability into knowledge-based conversation system," *Knowledge-Based Syst.*, vol. 220, p. 106791, 2021, doi: 10.1016/j.knosys.2021.106791.
[138] R. Raimundo and A. Rosário, "Blockchain system in the higher education," *Eur. J. Investig. Heal. Psychol. Educ.*, vol. 11, no. 1, pp. 276–293, 2021, doi: 10.3390/ejihpe11010021.
[139] S. Alam *et al.*, "A Blockchain-based framework for secure Educational Credentials," 2021.
[140] S. F. Fahmy, "Blockchain and its uses," 2018.
[141] R. Chatterjee, R. C.-2017 3rd I. Conference, and undefined 2017, "An overview of the emerging technology: Blockchain," *ieeexplore.ieee.org*, 2017, doi: 10.1109/CINE.2017.33.
[142] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org.
[143] Y. Zheng, "Design of a Blockchain-Based e-Portfolio Evaluation System to Assess the Education and Teaching Process," *Int. J. Emerg. Technol. Learn.*, vol. 16, no. 5, pp. 261–280, 2021, doi: 10.3991/ijet.v16i05.21081.

[144] R. Johari and V. Kumar, “BLOSOM : Blockchain technology for security of medical records,” *ICT Express*, Jun. 2021, doi: 10.1016/j.icte.2021.06.002.
[145] M. Finck, “Blockchains and Data Protection in the European Union,” *Eur. Data Prot. Law Rev.*, vol. 4, no. 1, pp. 17–35, Mar. 2018, doi: 10.21552/edpl/2018/1/6.
[146] H. Yi, “Securing e-voting based on blockchain in P2P network,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1473-6.
[147] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm,” in *Materials Today: Proceedings*, 2020, vol. 37, no. Part 2, pp. 2653–2659, doi: 10.1016/j.matpr.2020.08.519.
[148] G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” *Smart Learn. Environ.*, vol. 5, no. 1, Dec. 2018, doi: 10.1186/s40561-017-0050-x.
[149] Szabo Nick, “The Idea of Smart Contracts,” *“Formalizing and Securing Relationships on Public Networks,”* 1997. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (accessed Jul. 26, 2021).
[150] De Filippi Primavera and Wright Aaron, *Blockchain and the Law The Rule of Code*. Harvard University Press, 2018.
[151] J. P. Quintais and V. Ferrari, “Stanford Journal of Blockchain Law & Policy Blockchain and the Law: A Critical Evaluation,” 2019. [Online]. Available: https://stanford-jblp.pubpub.org/pub/blockchain-and-law-evaluation/release/2.
[152] F. Loukil, M. Abed, and K. Boukadi, “Blockchain adoption in education: a systematic literature review,” *Educ. Inf. Technol.*, 2021, doi: 10.1007/s10639-021-10481-8.
[153] A. Qasim and F. F. Kharbat, “Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum,” *J. Emerg. Technol. Account.*, vol. 17, no. 1, pp. 107–117, Mar. 2020, doi: 10.2308/jeta-52649.
[154] “Structure of a Contract.” https://docs.soliditylang.org/en/v0.5.10/structure-of-a-contract.html (accessed Jul. 26, 2021).
[155] M. Drijvers and G. Neven, “Pixel : Multi-signatures for Consensus.” .
[156] H. Stefanović, G. Bjelobaba, and N. Popović, “Simulation and Analysis of Blockchain Operations Model with RSA Algorithm in CrypTool2,” in *E-business technologies*, 2023, pp. 171–175.
[157] A. Savic, H. Stefanovic, G. Bjelobaba, and N. Popovic, “The Simulation Model of Blockchain Transaction,” in *XLIX International Symposium on Operations Research-SYM-OP-IS 2022*, 2022, pp. 601–612.
[158] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.10016848.
[159] “Blockchain Platforms Reviews 2021 | Gartner Peer Insights.” https://www.gartner.com/reviews/market/blockchain-platforms (accessed Sep. 14, 2021).
[160] “Public vs Private Blockchain - Innovation & Technology Blog.” https://www.e-zigurat.com/innovation-school/blog/public-vs-private-blockchain-whats-the-difference/ (accessed Sep. 14, 2021).
[161] “Permissioned and Permissionless Blockchains | Freeman Law.” https://freemanlaw.com/permission-and-permissionless-blockchains/ (accessed Sep. 14, 2021).
[162] “Hyperledger – Open Source Blockchain Technologies.” https://www.hyperledger.org/ (accessed Sep. 14, 2021).
[163] “Hyperledger vs Corda vs Ethereum: The Ultimate Comparison.” https://101blockchains.com/hyperledger-vs-corda-r3-vs-ethereum/ (accessed Sep. 14, 2021).

[164] G. Greenspan, “MultiChain Private Blockchain-White Paper,” Accessed: Sep. 14, 2021. [Online]. Available: http://coinsecrets.org/.
[165] “A Comprehensive Guide to Enterprise Blockchain -.” https://www.blockchain-council.org/blockchain/a-comprehensive-guide-to-enterprise-blockchain/ (accessed Sep. 14, 2021).
[166] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing,” *Futur. Internet*, vol. 14, no. 11, p. 341, 2022, doi: 10.3390/fi14110341.
[167] A. Deshmukh, N. Sreenath, A. K. Tyagi, and U. V. E. Abhichandan, “Blockchain Enabled Cyber Security: A Comprehensive Survey,” *2022 Int. Conf. Comput. Commun. Informatics, ICCCI 2022*, 2022, doi: 10.1109/ICCCI54379.2022.9740843.
[168] M. del P. Ramos-Sosa, D. Cabrera, and B. Moreno, “Blockchain and Smart contracts for Education,” *Mpra*, no. 101518, 2020, [Online]. Available: https://mpra.ub.uni-muenchen.de/101518/.
[169] R. Pethuru, S. Kavita, and S. Chellammal, *Blockchain Technology and Applications*. Auerbach Book CRC Press, 2021.
[170] G. MATEI, “Blockchain Technology – Support for Collaborative Systems,” *Inform. Econ.*, vol. 24, no. 2/2020, Jun. 2020, doi: 10.24818/issn14531305/24.2.2020.02.
[171] K. Al Harthy, F. Al Shuhaimi, and K. K. Juma Al Ismaily, “The upcoming Blockchain adoption in Higher-education: requirements and process,” in *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, Jan. 2019, pp. 1–5, doi: 10.1109/ICBDSC.2019.8645599.
[172] E. E. Bessa and J. S. B. Martins, “A Blockchain-based Educational Record Repository,” pp. 1–8, 2019, doi: 10.5281/zenodo.2567524.
[173] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, “Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections,” *Electron.*, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203359.
[174] T. Y. Lam and B. Dongol, “A blockchain-enabled e-learning platform,” *Interact. Learn. Environ.*, vol. 30, no. 7, pp. 1229–1251, 2022, doi: 10.1080/10494820.2020.1716022.
[175] M. Jirgensons and J. Kapenieks, “Blockchain and the Future of Digital Learning Credential Assessment and Management,” *J. Teach. Educ. Sustain.*, vol. 20, no. 1, pp. 145–156, 2018, doi: 10.2478/jtes-2018-0009.
[176] S. Ersoy, A. Savić, G. Bjelobaba, and H. Stefanović, “Collaborative Learning of Mathematics Supported by Blockchain Technology in the Context of Mandelbrot and Julia Sets,” 2023.
[177] G. Bjelobaba, M. Paunovic, A. Savic, H. Stefanovic, J. Doganjic, and Z. M. Bogavac, “Blockchain Technologies and Digitalization in Function of Student Work Evaluation,” *Sustain.*, vol. 14, no. 9, pp. 1–22, 2022, doi: 10.3390/su14095333.
[178] G. Bjelobaba, A. Savić, T. Tošić, I. Stefanović, and B. Kocić, “Collaborative Learning Supported by Blockchain Technology as a Model for Improving the Educational Process,” *Sustainability*, vol. 15, no. 6, p. 4780, Mar. 2023, doi: 10.3390/su15064780.
[179] D. Tapscott and A. Tapscott, “Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money ...,” *Sage Publ. Inc.*, p. 384, 2018.
[180] V. Buterin, “A next-generation smart contract and decentralized application platform,” *Etherum*, no. January, pp. 1–36, 2014, [Online]. Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf.
[181] H. F. Korth and A. Silberschatz, *Database system concepts*. 1991.
[182] Z. Gao and X. Wang, “Deep learning,” *EEG Signal Process. Featur. Extr.*, pp. 325–333, 2019, doi: 10.1007/978-981-13-9113-2_16.
[183] T. Electronic and P. M. Scheme, “Portfolio Management Scheme,” 2022.
[184] Andreas M, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies,” 2014, [Online].

Available: https://sci-hub.do/https://books.google.com/books?hl=zh-CN&lr=&id=IXmrBQAAQBAJ&oi=fnd&pg=PR4&dq=Antonopoulos,+Andreas+M.+2014&ots=9C9UrwGrNX&sig=3l49cnJsCUpJcR51eJK10_OaH-E.
[185] C. Farchi, B. Touzi, F. Farchi, and A. Mousrij, "Sustainable performance assessment: A systematic literature review," *J. Sustain. Dev. Transp. Logist.*, vol. 6, no. 2, pp. 124–142, 2021, doi: 10.14254/jsdtl.2021.6-2.8.
[186] Z. Dodevski, S. Filiposka, A. Mishev, and V. Trajkovik, "Real time availability and consistency of health-related information across multiple stakeholders: A blockchain based approach," *Comput. Sci. Inf. Syst.*, vol. 18, no. 3, pp. 927–955, 2021, doi: 10.2298/CSIS200426017D.
[187] F. Ortega and E. L. Cano, "Sensor Data Analytics: Challenges and Methods for Data-Intensive Applications," *Entropy*, vol. 24, no. 7, pp. 18–19, 2022, doi: 10.3390/e24070850.
[188] G. Marcus, "Deep Learning: A Critical Appraisal," pp. 1–27, 2018, [Online]. Available: http://arxiv.org/abs/1801.00631.
[189] F. Provost and T. Fawcett, "Data Science for Business," no. August 2013, p. 387, 2013.
[190] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.10016848.
[191] Ryan, Cooper, and Tauer, "Data Science for Business," *Pap. Knowl. . Towar. a Media Hist. Doc.*, pp. 12–26, 2013.
[192] T. Alladi, V. Chamola, R. M. Parizi, and K. K. R. Choo, "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019, doi: 10.1109/ACCESS.2019.2956748.
[193] M. Vukolić, "The Quest for Scalable Blockchain Fabric : Proof-of-Work vs . BFT Replication Marko Vukolić To cite this version : HAL Id : hal-01445797 The Quest for Scalable Blockchain Fabric :," 2017.
[194] Y.-L. Cheng *et al.*, "We are IntechOpen , the world ' s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %," *Intech*, vol. 11, no. tourism, p. 13, 2016, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics.
[195] B. F. Klimova, "Evaluation Methods as an Effective Tool for the Development of Students' Learning," *Procedia - Soc. Behav. Sci.*, vol. 152, pp. 112–115, 2014, doi: 10.1016/j.sbspro.2014.09.165.
[196] D. Rowntree, *Assessing Students-How Shall We Know Them?* London: Routledge, 2015.
[197] P. Lameras and S. Arnab, "Power to the Teachers: An Exploratory Review on Artificial Intelligence in Education," *Information*, vol. 13, no. 1, p. 14, Dec. 2021, doi: 10.3390/info13010014.
[198] Н. Поткоњак and П. Шимлеша, *Педагошка стварност*. Београд: Завод за уџбенике и наставна средства и др., 2011.
[199] Г. Гојков, *Докимологија – приручник*, vol. 27, no. 7. Вршац: четврто допуњено издање, Висока школа струковних студија за образовање васпитача"Михаило Палов, 2009.
[200] Н. Хавелка, Е. Хебиб, and А. Бауцал, *Оцењивање за развој - приручник за наставнике*. Б: Евалуација за развој, Београд: Министарство просвете и спорта Републике Србије - сектор за развој образовања и међународну просветну сарадњу и British Council, 2003.
[201] Ј. Д. Стаматовић, "Самовредновање Наставника У Функцији Унапређивања Васпитно - Образовног Рада," *Dokstorska Disert.*, 2012.
[202] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art

Advancements, Challenges and Future Research Directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022, doi: 10.1109/ACCESS.2022.3189998.
[203] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proc. 13th EuroSys Conf. EuroSys 2018*, vol. 2018-Janua, 2018, doi: 10.1145/3190508.3190538.
[204] L. Dearden and C. Emmerson, "Education Subsidies and School Drop-Out Rates Christine Frayne Costas Meghir," no. January, pp. 1–40, 2006.
[205] S. You, E. Kim, and K. Shin, "Teachers' Belief and Efficacy Toward Inclusive Education in Early Childhood Settings in Korea," *Sustainability*, vol. 11, no. 5, p. 1489, 2019, doi: 10.3390/su11051489.

ПРИЛОГ 1: СПИСАК ТАБЕЛА

ПРИЛОГ 2: СПИСАК СЛИКА

ПРИЛОГ 3: СПИСАК ГРАФИКОНА

БИОГРАФИЈА

Горан Бјелобаба је рођен 16. фебруара 1975. године у Бихаћу, где је завршио основну школу. Гимназију, математички смер, завршио је у Бањалуци. Дипломирао је на Факултету организационих наука, Универзитет у Београду, 2006. године с темом „Утицај и подршка интернет и веб-технологије традиционалном образовном процесу". Школовање је наставио на мастер-студијама, на Факултету организационих наука, Универзитет у Београду, и 2009. године одбранио мастер-рад „Компаративна анализа софтверских решења у е-образовању". Докторске студије на Факултету организационих наука, Универзитет у Београду, уписује 2015. године на студијском програму – Информациони системи и квантитативни менаџмент, модул – Електронско пословање.

Од 1999. до 2003. године радио је на Вишој електротехничкој школи у Београду у својству лаборанта на више предмета (Математика, Рачунарске мреже). Од 2003. до 2006. године радио је на Вишој школи унутрашњих послова у Београду као систем инжењер на одржавању информационог система. Радио је на пројектовању и имплементацији сигурносних мера информационог система и процени сигурносних ризика. Радио је на пројекту „Даљинско учење" за потребе студената Више школе унутрашњих послова у Београду и пословних организација. Комплетан пројекат имплементиран је на платформи ЛОТУС.

Од 2006. до 2013. године радио је у предузећу „Parallel" на пословима инсталације, креирања базе података, обезбеђивања, клонирања, надгледања перформанси, подешавања и оптимизације, као и на безбедносној провери. У појединим пројектима обављао је послове који се односе на дизајн базе података, шему оптимизације, миграцију базе података, миграцију оперативног система кроз различите платформе, репликацију података, осмишљавање стратегије чувања и опоравка података. Радио је на пројекту имплементације *Oracle E-Business Suite* као консултант (на модулу *Enterprise Asset Management*).

Од 2013. до 2014. године радио је у предузећу „Сага". Био је ангажован на пројекту имплементације „Централног регистра обавезног социјалног осигурања". У току 2014. године радио је у предузећу „Финбет". Тренутно је запослен у Народној банци Србије на месту директора Одељења за безбедност и заштиту. Ради на примени препорука и смерница за корпоративну и информациону безбедност. Објављује радове из делокруга послова који су му поверени.

СТЕЧЕНО НАУЧНОИСТРАЖИВАЧКО ИСКУСТВО

У наставку ће бити приказане научноистраживачке активности кандидата. Оне обухватају радове објављене на конференцијама и у часописима од године уписа докторских студија, као и преглед положених испита.

Током досадашњег рада Горан Бјелобаба је објавио је више радова у земљи и иностранству и учествовао на више међународних и домаћих скупова и конференција.

РЕЗУЛТАТИ И ДОПРИНОСИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ ОБЈАВЉЕНИ СУ У СЛЕДЕЋИМ РАДОВИМА (КАТЕГОРИЈА M22):

1. **Bjelobaba, G.**; Savić, A.; Tošić, T.; Stefanović, I.; Kocić, B. Collaborative Learning Supported by Blockchain Technology as a Model for Improving the Educational Process, Sustainability (ISSN 2071-1050), Special Issue "Blockchain and Agile Management – Important Tools for Circular Economy" 2023, 15, 4780. https://doi.org/10.3390/su15064780. импакт фактор за 2022=3.9, (M22).
2. **Bjelobaba, G.**; Paunovic, M.; Savic, A.; Stefanovic, H.; Doganjic, J.; Miladinovic Bogavac, Z. Blockchain Technologies and Digitalization in Function of Student Work Evaluation. Sustainability (ISSN 2071-1050), Special Issue "Blockchain and Agile Management – Important Tools for Circular Economy" 2022, 14, 5333. https://doi.org/10.3390/su14095333. импакт фактор за 2022=3.9, (M22).

РАДОВИ У ЗБОРНИЦИМА МЕЂУНАРОДНИХ СКУПОВА (M30):

1. S. Zeković, **G. Bjelobaba**, S. Štrbac-Savić, "*Analiza uticaja operativnih problema kod učesnika u platnom sistemu*", Naučno-stručni Simpozijum-INFOTEH 2015, Proceedings of papers, Vol. 14, pp. 664–669, Jahorina, Bosna i Hercegovina, 18–20 mart, 2015, ISBN 978-99955-763-6-3 (M33)
   https://infoteh.etf.ues.rs.ba/zbornik/2015/radovi/RSS-4/RSS-4-4.pdf
2. Kuka E., Kalemi E., Savic A., **Bjelobaba G.**, *Information Security in the public sector in Albania*, 6th International conference "Information Systems and Technology Innovations: inducting Modern Business Solutions" International Conference Proceedings ISTI 2015, 5–6 June 2015, Tirana, Albania, Proceedings Book, p. 11 (M34)
   http://www.conference.ijsint.org/sites/default/files/Agenda_ISTI2015.pdf
3. A. Savic, **G. Bjelobaba**, S. Strbac-Savic, I. Stefanovic, *Teaching and Learning of Mathematics in relation to the teaching program Electrical Engineering – traditional and distance approach*, International conference Quality of University Teaching and Learning, The Centre of the Republic of Slovenia for Mobility and European Educational and Training Programmes, Brdo kod Kranja, Slovenia April 6, 2016. CIP – 378.147(082)(0.034.2), Conference proceedings, ISBN 978-961-6628-50-1, p. 232-240 (M33)
   http://eng.cmepius.si/wp-content/uploads/2015/08/1-ZBORNIK-OBLIKOVANJE-final-5.pdf
4. **G. Bjelobaba**, A. Savić, "Smart building, the National Bank of Serbia", XV International symposium Reshaping the Future Through Sustainable Business Development and Enteproureship SymOrg 2016, June 10–13, Zlatibor, Symposium proceedings ISBN 978-86-7680-326-2, p.415-422 (M33)
   http://symorg.fon.bg.ac.rs/proceedings/2016/
5. **G. Bjelobaba**, A. Savic "Methodology for preparing a project application for curriculum master studies in Information security", EEE 2017, Economic and Technological Development and Information Technology, 19–21 October 2017, Belgrade, Serbia, ISBN 978-1-912009-85-5, p 124- 141 (M33)
   https://vspep.edu.rs/fileadmin/user_upload/EEE/EEE_2017/eee_2017_book_4.pdf

6. **G. Bjelobaba**, A. Savic, *Cloud Computing And Economic Analysis*, 8th INTERNATIONAL CONFERENCE, "Information Systems and Technology Innovations: Fostering the As-A-Service Economy", International Conference Proceedings ISTI 2017, Tirana, Albania, June 23–24, 2017, Proceedings Book, ISBN: 978-9928-148-67-4, p. 18–19 (M34)
http://www.conference.ijsint.org/sites/default/files/Proceedings_ISTI2017.pdf

7. **G. Bjelobaba**, A. Savic, *Big Data in Banking*, 8th International conference, "Information Systems and Technology Innovations: Fostering the As-A-Service Economy", International Conference Proceedings ISTI 2017, Tirana, Albania, June 23–24, 2017, Proceedings Book, ISBN: 978-9928-148-67-4, p.67 (M33)
http://conference.ijsint.org/sites/default/files/Proceedings_ISTI2017.pdf

8. **G. Bjelobaba**, A. Savic, H. Stefanovic, "Analysis of central banks platforms on social networks", *International Conference on Computer Science and Communication Engineering & Information Systems and Security-IC–UBT 2017*, *Proceedings of papers*, pp. 17–21, Durres, Albania, October 27–29, 2017, ISBN 978-9951-437-60-8 (M33)
http://conferences.ubt-uni.net/2018/wp-content/uploads/2018/09/ICCSEISS.pdf

9. **G. Bjelobaba**, A. Savic, H. Stefanovic, "Crypto-currency in the digital economy as a challenge to centralized money issuing", *International Scientific Conference–UNITECH 2017*, *Proceedings of papers*, Vol. 2, pp. 256-261, Gabrovo, Bulgaria, November 17–18, 2017, ISSN 1313-230X (M33)

10. A. Savić, **G. Bjelobaba**, H. Stefanović, "Programska rešenja pri proceni broja Pi Monte Carlo metodama uz interaktivne animacije", *Međunarodni naučnostručni Simpozijum-INFOTEH 2018, Proceedings of papers*, Vol. 17, pp. 418–422, Jahorina, Bosnia and Herzegovina, March 21-23, 2018, ISBN 978-99976-710-1-1 (M33)
http://www.infoteh.rs.ba/zbornik/2018/radovi/RSS-3/RSS-3-7.pdf

11. H. Stefanović, R. Veselinović, **G. Bjelobaba**, A. Savić, "An adaptive car number plate image segmentation using K-means clustering", *International Scientific Conference on Information Technology and Data Related Research-SINTEZA 2018, Proceedings of papers*, pp. 74–78, Belgrade, Serbia, April 22, 2018 DOI: https://doi.org/10.15308/Sinteza-2018-74-78 (M33)
http://portal.sinteza.singidunum.ac.rs/Media/files/2018/74-78.pdf

12. **G. Bjelobaba**, A. Savić, H. Stefanović, "Primena težinske metode najmanjih kvadrata (WLMS) pri proceni rasta broja Twitter pratilaca u komunikaciji sa centralnim bankama", *International Symposium on Operations Research-SYM-OP-IS 2018*, *Proceedings of papers*, ISBN 978-86-403-1567-8, pp. 81–87, Zlatibor, Serbia, September 16-18, 2018, (M33)
https://symopis2018.ekof.bg.ac.rs/razno/Zbornik_radova_SYM-OP-IS_2018.pdf

13. **G. Bjelobaba**, A. Savić, R. Veselinović, H. Stefanović, "An implementation of Weighted Least Squares method in Central Bank Twitter accounts grew prediction", *International Conference on Computer Science and Communication Engineering & Information Systems and Security-IC–UBT 2018, Proceedings of papers*, pp. 71–78, Pristina, Kosovo, October 26-28, 2018, ISBN 978-9951-437-74-5 (M33)
http://conferences.ubt-uni.net/2019/wp-content/uploads/2019/05/Book-of-Proceedings_CSE_IS_2018.pdf

14. H. Stefanovic, S. Janicijevic, **G. Bjelobaba**, A Savic, "An application of K-means clustering for customer segmentation in one luxury goods company", *International Conference Science and Higher Education in Function of Sustainable Development-SED 2019*, *Proceedings of papers*, pp. 2–15 – 2–21, Mecavnik-Drvengrad, Uzice, Serbia, May 24–25, 2019, ISBN 978-86-83573-95-0 (M33)

http://sed.vpts.edu.rs/CD%20Proceedings%202019/proceedings/2-3.pdf

15. H. Stefanovic, R. Veselinovic, **G. Bjelobaba**, A. Savic, "Primena Hough-ove transformacije i različitih tehnika povezivanja detektovanih ivica prilikom izdvajanja registarskih tablica u digitalnoj slici", *International Symposium on Operations Research-SYM-OP-IS 2019, Proceedings of papers*, pp. 226–231, Kladovo, Serbia, September 15–18, 2019, ISBN 978-86-7680-363-7 (M33)
http://symopis2019.fon.bg.ac.rs/download/SYM-OP-IS%202019%20Proceedings.pdf
16. A. Savic, **G. Bjelobaba**, S. Janicijevic, H. Stefanovic, "An application of PCA based K-means clustering for customer segmentation in one luxury goods company", *International Conference on Computer Science and Communication Engineering&Information Systems and Security-IC–UBT 2019, Proceedings of papers*, pp. 85–92, Pristina, Kosovo, October 26-28, 2019, ISBN 978-9951-437-84-4 (M33)
http://conferences.ubt-uni.net/2019/wp-content/uploads/2018/09/Book-of-Proceedings_CEIE_2019-1.pdf
17. A. Savic, **G. Bjelobaba**, R. Veselinovic, H. Stefanovic, "Visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images", *International Conference on Business, Technology and Innovation-UBT 2020, Conference Book of Abstracts*, pp. 566, Lipjan, Kosovo, October 30–31, 2020, ISBN 978-9951-437-96-7, DOI: 10.33107/ubt-ic.2020.1 (M33)
https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=3122&context=conference
18. H. Stefanovic, R. Veselinovic, **G. Bjelobaba**, A. Savic, "Primena vizuelne kriptografije u procesu deljenja informacija o vozilima parkiranim u krugu kompanije", *International Symposium on Operations Research-SYM-OP-IS 2020, Proceedings of papers*, pp. 143-148, Belgrade, Serbia, September 20–23, 2020, ISBN 978-86-7395-429-5 (M33)
https://symopis.sf.bg.ac.rs/download/Zbornik%20SYMOPIS%202020.pdf
19. H. Stefanovic, A. Savic, R. Veselinovic, **G. Bjelobaba**, "An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images", International Journal of Engineering Inventions–IJEI, Vol. 10, Issue 2, pp. 1–11, February 2021, e-ISSN: 2278-7461, p-ISSN: 2319-6491, IF 6.7 (M33)
http://www.ijeijournal.com/papers/Vol10-Issue2/A10020111.pdf
20. **G. Bjelobaba**, N. Popovic, A.Savic, V. Vasiljevic, H. Stefanovic, M. Ilic, "Computer Networking Teaching and Learning Multimedia Education System", International Business Information Management Association-IBIMA, Proceedings of papers, pp. 8852-8862, Cordoba, Spain, May 30–31, 2021, ISBN: 978-0-9998551-6-4, ISSN: 2767-9640 (M33)
21. N. Popovic, A. Savic, **G. Bjelobaba**, R. Veselinovic, H. Stefanovic, M. Ilic, "The Implementation of Hierarchical and Nonhierarchical Clustering for Customer Segmentation in One Luxury Goods Company", International Business Information Management Association-IBIMA, Proceedings of papers, pp. 8370–8381, Cordoba, Spain, May 30–31, 2021, ISBN: 978-0-9998551-6-4, ISSN: 2767-9640 (M33)
22. N. Popović, **G. Bjelobaba**, H. Stefanović, A. Savic, N. Stefanović, "The Knowledge evaluation system in function of achieving competences", 1st E-business technologies, "Modern e-business ecosystems" Department of a Business, Faculty of organizational sciences, University of Belgrade, 10–11 July 2021. https://ebt.rs/journals/index.php/conf-proc/issue/view/1 (M33)
23. **G. Bjelobaba**, H. Stefanovic, A. Savic, N. Stefanovic, N. Popovic, N. Stefanović, "A New Approach to Scientific-Research Paper Evaluation", 1st E-business technologies,

"Modern e-business ecosystems" Department of a Business, Faculty of organizational sciences, University of Belgrade, 10–11 July 2021. https://ebt.rs/journals/index.php/conf-proc/issue/view/1 (M33)

24. N. Popović, **G. Bjelobaba**, H. Stefanović "Primena zaštitnog kodovanja u sistemu za vrednovanje znanja", SYM-OP-IS 2021, XLVIII Međunarodni simpozijum o operacionim istraživanjima, Matematički fakultet Univerziteta u Beogradu i Matematički institut SANU, pp 255–260, Banja Koviljača, 20–23. septembar 2021 http://symopis2021.matf.bg.ac.rs/download/Zbornik-SYM-OP-IS2021.pdf (M33)
25. H. Stefanovic, A. Savic, N. Popovic, **G. Bjelobaba**, " Application of the One-Time Pad (OTP) Cipher in Business Communications", *Science and Higher Education in Function of Sustainable Development – SED 2021*, Uzice, Serbia, October 8th , 2021, (M33)
26. Lj. Dikovic, **G. Bjelobaba**, A. Savic, N. Popovic, "Mathematics for informatics education", *Science and Higher Education in Function of Sustainable Development – SED 2021*, Uzice, Serbia, October 8th , 2021 (M33)
27. A. Savic, **G. Bjelobaba**, N. Popovic, H. Stefanovic, "One-Time Pad Cipher (OTP) Use Cases and Simulation Examples for Electronic Financial Transactions", International Conference on Business, Technology and Innovation-UBT 2021, Conference Book of Abstracts, pp. 187, Pristina, October 29–30, 2021, ISBN 978-9951-550-47-5 (M33)
28. N. Popovic, **G. Bjelobaba**, H. Stefanovic, "Primena zaštitnog kodovanja i kodova za kontrolu grešaka u sistemu za vrednovanje znanja", International Symposium on Operations Research-SYM-OP-IS 2021, Proceedings of papers, pp. 255-260, Banja Koviljača, Serbia, September 20–23, 2021, ISBN 978-86-7589-151-2 (M33)
29. **G. Bjelobaba**, H. Stefanovic, A. Savic, N. Stefanovic, N. Popovic, "A New Approach to Scientific-Research Paper Evaluation", 1st E-business technologies, "Modern e-business ecosystems" 2021, Department of a Business, Faculty of organizational sciences, University of Belgrade, Book of Abstracts, pp. 129–131, Belgrade, Serbia, July 10–11, 2021. (M33)
30. A. Savic, H. Stefanovic**, G. Bjelobaba**, N.Popovic, "The Simulation Model of Blockchain Transaction", XLIX International Symposium on Operations Research-SYM-OP-IS 2022, Proceedings of papers, pp. 143–148, Vrnjačka Banja, Serbia, September 19-22, 2022, ISBN: 978-86-403-1750-4 (M33)
31. H. Stefanović, A. Savić, **G. Bjelobaba**, N. Popović, *Simulation and Analysis of Blockchain Operations Model with RSA Algorithm in CrypTool2*, Conference "E-business technologies", Vol. 3 No. 1 (2023): E-business technologies Conferences Proceedings 2023, pp.171–175, Belgrade, Serbia, June, 15–17, 2023. (M33)
32. S. Ersoy; A. Savić; **G. Bjelobaba**; H. Stefanović, *Collaborative Learning of Mathematics Supported by Blockchain Technology in the Context of Mandelbrot and Julia Sets,* 13th International Scientific Conference Science and Higher Education in Function of Sustainable Development – SED 2023, Western Serbia Academy of Applied Studies, 5–8 June, 2023, Vrnjačka Banja, Serbia, ISBN 978-86-82078-18-0 (M33)
33. H. Stefanovic, A. Savic, **G. Bjelobaba**, "An Application of Bound-Constrained Quadratic Programming in Optimization Problem", International Symposium on Operations Research-SYM-OP-IS 2023, Proceedings of papers, pp. 461–466, Tara, Serbia, September 18-21, 2023, ISBN 978-86-335-0836-0, (M33) http://www.symopis2023.mod.gov.rs/download/Zbornik_radova_SIM-OP-IS_2023.pdf

РАДОВИ ОБЈАВЉЕНИ У ЧАСОПИСИМА НАЦИОНАЛНОГ ЗНАЧАЈА (M50):

1. H. Stefanovic, R. Veselinovic, **G. Bjelobaba**, A. Savic, „Optimizacija algoritmskih rešenja za izdvajanje obeležja registarskih tablica u uslovima otežane detekcije”, *Info M 64/2017*, pp. 33–37, 2017, ISSN 1451-4397, UDC 004.42:681.3.06 (M53) https://infom.fon.bg.ac.rs/index.php/infom/article/view/2255/2227
2. **G. Bjelobaba**, A. Savic, H. Stefanovic, „Integracija različitih oblika komunikacije u poslovanju primenom internet telefonije“, *Trendovi u poslovanju, Sves. 1, Br. 11 (2018)*, pp. 87–94, 2018, ISSN (Štampano izd.) 2334-816X. ISSN (Online) 2334-8356 (M53) http://trendovi.indmanager.org/index.php/tp/article/view/154/115
3. **G. Bjelobaba**, A. Savic, S. Janicijevic, H. Stefanovic, „Kombinovana primena hijerahijskih i nehijerarhijskih metoda klasterizacije u cilju segmentacije kupaca u jednom trgovinskom lancu”, *Trendovi u poslovanju, Sves. 1, Br. 13 (2019)*, pp. 61–72, 2019, ISSN (Štampano izd.) 2334-816X. ISSN (Online) 2334-8356 (M53) http://trendovi.indmanager.org/index.php/tp/article/view/171/129

Изјава о ауторству

Име и презиме аутора **Горан Бјелобаба**

Број индекса **5024/2015**

Изјављујем

да је докторска дисертација под насловом

Модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, _____

_____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора **Горан Бјелобаба**

Број индекса **5024/2015**

Студијски програм **Информациони системи и квантитативни менаџмент**

Наслов рада **Модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама**

Ментор **проф. др Зорица Богдановић**

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањивања у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, _____

_____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Модел колаборативног учења и евалуације студентских радова заснован на блокчејн технологијама

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

Потпис аутора

У Београду, _____

_____

1. **Ауторство.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.
2. **Ауторство – некомерцијално.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.
3. **Ауторство – некомерцијално – без прерада.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.
4. **Ауторство – некомерцијално – делити под истим условима.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.
5. **Ауторство – без прерада.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.
6. **Ауторство – делити под истим условима.** Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.