УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Даниел Л. Бјелица

МОДЕЛ ДИГИТАЛНОГ ЗДРАВСТВЕНОГ ЕКОСИСТЕМА ЗАСНОВАН НА *BLOCKCHAIN* ТЕХНОЛОГИЈИ

докторска дисертација

Београд, 2023.

UNIVERSITY OF BELGRADE
FACULTY OF ORGANIZATIONAL SCIENCES

Daniel L. Bjelica

MODEL OF A DIGITAL HEALTHCARE ECOSYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

Doctoral Dissertation

Belgrade, 2023.

МЕНТОР:

Др Александра Лабус,
редовни професор Факултета организационих наука Универзитета у Београду

ЧЛАНОВИ КОМИСИЈЕ:

Др Маријана Деспотовић Зракић,
редовни професор Факултета организационих наука Универзитета у Београду

Др Зорица Богдановић,
редовни професор Факултета организационих наука Универзитета у Београду

Др Саша Лазаревић,
редовни професор Факултета организационих наука Универзитета у Београду

Др Радмила Јаничић,
редовни професор Факултета организационих наука Универзитета у Београду

Др Марија Јевтић,
редовни професор Медицинског факултета Универзитета у Новом Саду

Датум одбране: _____

Модел дигиталног здравственог екосистема заснован на blockchain технологији

Апстракт:

Расположивост информација и њихов транспарентан ток унутар здравственог система и између свих стејкхолдера су неопходни за заједничко доношење одлука и обезбеђење одговорности. Продуктивна интеракција између информисаних пацијената и медицинских експерата омогућава пацијентима да активно учествују у процесу пружања/коришћења услуга здравствене заштите. У контексту протока података у комплексном здравственом екосистему, неопходна и веома битна је чврста гаранција безбедности података.

Истраживачки задатак ове докторске дисертације представља развој модела дигиталног здравственог екосистема који се базира на *blockchain* технологији. Детаљно је анализиран проблем сајбер сигурности у области пословања здравственог система у дигиталном окружењу и предложен је модел дигиталног здравственог екосистема базиран на *blockchain* технологији, у функцији обезбеђења функционалног система са досегом максималних нивоа сигурности. Предложени модел обухватио је кључне стејкхолдере дигиталног здравственог екосистема и размене података у пословним процесима, чија ће сигурност бити обезбеђена применом *blockchain* технологије.

Предложена су и развијена техничка решења којима се обезбеђује функционисање модела дигиталног здравственог екосистема заснованог на *blockchain* технологији. Наведена решења су тестирана и евалуирана у односу на квалитет система, сервиса, информација, перформанси као и процене задовољства корисника кроз оквир дефинисаних кореспондентних индикатора. Анализа добијених резултата анкетирањем у пост-имплементационом периоду указује на високо задовољство применом предложених и тестираних креираних апликација, што представља основ за даље развијање свих сегмената модела дигиталног здравственог екосистема базираног на *blockchain* технологији, као и пратећих апликативних софтверско-техничких решења.

Кључне речи: *дигитални екосистеми, е-здравство, мобилно здравство, blockchain технологија*

Научна област: *Информациони системи и технологије*

Ужа научна област: *Електронско пословање*

УДК број:

Model of a Digital Healthcare Ecosystem Based on Blockchain Technology

Abstract:

The availability of information and its transparent flow within the healthcare system and between all stakeholders are necessary for functioning of joint decision-making and maintenance of responsibility. Productive interaction between informed patients and medical experts enables patients to be empowered as active partners in the core of the process of providing/using health care. In the context of data flow in the complex healthcare ecosystem, a firm guarantee of data security is of extreme importance.

The subject of the doctoral dissertation research is the development of a digital healthcare ecosystem model based on blockchain technology. The problem of cybersecurity in the field of healthcare system operations in a digital environment was analyzed in detail and a model of a digital healthcare ecosystem based on blockchain technology was proposed, in order to ensure a functional system with the maximum level of security. The proposed model included key stakeholders of the digital healthcare ecosystem and data exchange in business processes with the security ensured by the application of blockchain technology.

Technical solutions have been proposed and developed to ensure the functioning of the developed digital healthcare ecosystem model. The solutions were tested and evaluated in relation to the system quality, information quality, service quality, system usage and user satisfaction through the defined appropriate key performance indicators. The analysis of the results of acceptance of the proposed model and tested applications obtained by surveying in the post-implementation period revealed a high satisfaction of the users involved in the survey. The results are the basis for further development of all segments of the digital healthcare ecosystem model based on blockchain technology and accompanying applied software-technical solutions.

Keywords: *digital ecosystems, e-health, mobile health, blockchain technology*

Scientific field: *Information Systems and Technology*

Narrow scientific field: *E-business*

UDK number:

САДРЖАЈ

1. УВОД

1.1. Дефинисање предмета истраживања

Истраживачки задатак ове докторске дисертације представља развој модела дигиталног здравственог екосистема који се базира на *blockchain* технологији. Основни проблем који се анализира је испитивање могућности коришћења *blockchain* технологије у савременим облицима, моделима, инфраструктури, сервисима и технологији електронског пословања у оквиру дигиталног здравственог екосистема за унапређење, пре свега, сигурности комуникације и сарадње стејкхолдера укључених у пословање у здравственом сектору. Предложени модел може да буде основ одговора и да представља акцију на неоспорну потребу за променом функционисања пословања здравствених установа у Републици Србији.

Интеграција дигиталних технологија у сва подручја пословања, што резултира значајном променом у пословном систему, позната је као дигитална трансформација (Coté, 2020). Несумњиво је да је и појава *COVID-19* инфекције, која је попримила пандемијске размере током 2020/2021. године, утицала на све аспекте живота људи али и на пословање у свим гранама индустрије.

Дигитална трансформација пословања је апсолутно пресудна за развој компанија у актуелном моменту. Као најзначајнији промотивни фактори за дигиталну трансформацију се наводе (Zangiacomi et al., 2020):

1. Побољшана ефикасност. Свака организација тежи бољој ефикасности што дигитална трансформација неоспорно нуди. На тај начин, компанија може да се дистанцира од традиционалних поступака и људских интервенција јер електронске интервенције успешно замењују мануелне, нудећи квалитативну равномерност, бржи и балансирани ток процеса, чинећи организацију ефикаснијом.
2. Искуство клијената. Клијенти су свакако све захтевнији па се из тог разлога у фокус ставља њихово задовољство. Примена дигиталних метода омогућава бољу процену степена задовољства клијената и остваривање веће лојалности.
3. Унапређено доношење адекватних одлука. У циљу постизања веће ефикасности и задовољства клијената, потребно је доносити што прецизније одлуке у датом моменту. Примена дигиталних технологија пружа добро планиране податке, што у дугорочном плану повећава шансе за постизање организационих циљева, дајући здраве основе за пословни успех.
4. Побољшани наступ на тржишту. Продор на неистражена тржишта је пресудан за придобијање нових клијената постојећим пословним нормама. Спровођење сегментације за процену квалитета циљног тржишта је од пресудног значаја. Дубински увиди, заједно са побољшаним доношењем одлука, чине процес освајања тржишта знатно ефикаснијим.
5. Повећана профитабилност. Дигитална трансформација повећава профит побољшањем задовољства постојећих клијената, као и стицањем нових.

Сектор здравства је показао потребу за иминентном променом и брзим преласком на значајни удео дигиталног функционисања. Медицински радници могу да користе дигиталне технологије за пружање телемедицинских услуга и консултација, што смањује потребу за посетама здравственим установама које су преоптерећене и рестриктивно примају пацијенте. Додатно, велики број пацијената, нарочито од појаве пандемије *COVID-19,* због развијеног страха од инфекције избегава или одлаже посете лекару, посредно дајући тиме значајан подстицај дигиталној трансформацији у здравству. Очекује се да ће здравствени сектор забележити сложену годишњу стопу раста (енг. *Compound Annual Growth Rate – CAGR*) од 15,1% током предвиђеног периода 2020-2027. године (BusinessWire, 2020).

Дигитална трансформација у здравству постаје приоритет овог сектора ради постизања унапређеног и бољег искуства клијената, јер пацијенти нису само пасивни примаоци здравствених услуга већ они желе да буду третирани као клијенти, како би могло да се чује њихово мишљење, а такође очекују и персонализована решења за своје здравствене проблеме. На тај начин долазимо до преласка са организацијски усмереног здравства на пацијентима усмерено здравство, што несумњиво намеће потребу за новим технолошки омогућеним екосистемима односно дигиталним здравственим екосистемима (Sinhasane, 2020).

Дигитални екосистеми су инспирисани природним екосистемима а по дефиницији представљају адаптивне, отворене, социо-техничке системе са карактеристикама самоорганизације, скалабилности и одрживости (Briscoe & De Wilde, 2006). Дигитални здравствени екосистем је инфраструктура која подржава прелазак са организационог на ка пацијенту оријентисан модел пружања здравствених услуга помоћу дигиталних платформи. Примарни циљ овог система је подстицање пружања здравствене заштите у више организационих, мултидисциплинарних и колаборативних облика. У основи, инфраструктура се састоји од интернет платформе која нуди дигиталне здравствене услуге. С друге стране, дигитални здравствени екосистем промовише интероперабилност, омогућавајући међусобну комуникацију здравствених радника. Такође, омогућава дељење *VHR* (енг. *Virtual Healthcare Record*) за 360-степено сагледавање здравственог статуса пацијената (Sinhasane, 2020).

Концепт дигиталних здравствених решења катализује систематско усвајање здравствених технологија где пацијенти заузимају централно место. Дигитални здравствени екосистем, заправо, доноси промену парадигме у здравственом сектору јер (Serbanati et al., 2011; Marini, 2019; Sinhasane, 2020):

- даје могућност кућног лечења, лако управљање хроничним болестима, контролу стања након отпуста и оснаживање и повезивање пацијената са вишеструким стејкхолдерима,
- ствара могућност за економску одрживост унапређеног квалитета здравствених услуга,
- помаже у контроли трошкова здравствене заштите,
- нуди неопходан квалитет, приступ, сигурност и исплативост здравствених токова и процеса.

Унутар дигиталних здравствених екосистема омогућена је компатибилност података као и могућност интеракције, тако да различити актери могу понудити допуне дигиталних

здравствених производа и услуга. Студија коју је спровела Witte (2020), дедуктивно је извела пет главних концепата (стварање и задржавање вредности, активност, актери, архитектура и управљање) и девет потконцепата (подаци, услуге, интеграција, стејкхолдери, улоге, инфраструктура, технологија, основна правила и политика).

Дигитални здравствени екосистем образују три учесника: пружаоци услуга (енг. *Providers*), пацијенти (енг. *Patients)* и платиоци услуга (енг. *Payers*). Ова три учесника се обично називају три *P* здравствене заштите (Sinhasane, 2020; Credihealth, 2023):

1. Пружаоци услуга. То су здравствене установе – болнице, поликлинике, ординације, лабораторије и апотеке. Пружаоци здравствене заштите суочавају се са бројним препрекама у пружању здравствене заштите: болнице и ординације имају често недостатак особља и непотпуне податаке о пацијентима, апотеке се боре да испуне све већу потражњу за лековима, лабораторијама је тешко да тестирају и пријаве понекад и стотине узорака дневно. Дигитални здравствени екосистем растерећује пружаоце услуга, јер усмеравањем фокуса на пацијенте пружаоцима услуга омогућава заједнички рад у мултидисциплинарним тимовима који нуде побољшане здравствене третмане и услуге.
2. Пацијенти. Главни фокус дигиталног екосистема су пацијенти. Дигитални здравствени екосистем ради на моделу превентивне неге, а не на куративном моделу. Овакав модел омогућује пацијентима приступ персонализованим здравственим услугама и побољшаној превентивној дијагностици. Здравствени систем може упозорити пацијенте на све здравствене проблеме и пружити адекватну медицинску помоћ. Аутоматизација овог процеса доприноси независности пацијената од пружалаца здравствених услуга.
3. Платиоци услуга. Дигитални здравствени екосистем се фокусира и на смањење трошкова здравствене заштите и давање обухватнијег приступа квалитетној здравственој заштити широј популацији. Платиоци, укључујући осигураваче, сада могу искористити свој централни положај у борби против растућих трошкова здравствене заштите.

Компоненте дигиталног здравственог екосистема су:

- Компоненте усмерене ка клијентима/пацијентима, које садрже дигиталне приступне тачке попут портала и уређаја за размену порука, како би се пацијентима омогућио персонализовани приступ здравственим услугама у датом временском тренутку. Најрепрезентативнији пример је употреба телемедицине.
- Компоненте везане за пружаоце услуга, које садрже два елемента: слој података напредне генерације за *API* приступ и управљање дистрибуираним подацима. Добро организована дистрибуирана база података великог обима пресудна је за чување, организовање и размену података.
- Унутрашње компоненте. Аутоматизован дигитални *core* је основ добро утемељених унутрашњих компоненти и садржи обимне аналитичке моделе за извештавање, анализу и побољшање квалитета лечења као и саме исплативости лечења.

С обзиром на обимност података које садржи сваки дигитални екосистем, питање које се нужно намеће је њихово складиштење.

Развој *cloud* рачунарства даје могућност организацијама/компанијама да своју постојећу информациону и комуникациону инфраструктуру мигрирају на спољне платформе. *Cloud computing* омогућава складиштење великих количина података и извршавање сложених апликација на робусним, скалабилним хардверским ресурсима, без потребе да се поседује и одржава такав хардвер.

И поред несумњивих предности (флексибилност и економичност) које нуде услуге *cloud* рачунарства, неке компаније, ипак, не прихватају овакав вид складиштења информација из безбедносних разлога условљених сајбер претњама и сајбер криминалом. Главни провајдери *cloud* решења примењују високо стандардизоване и проверене сигурносне протоколе усклађене са регулативама о заштити података. *AWS, Google* и *Microsoft* услуге подржавају главне безбедносне стандарде, покривајући релевантне сертификате и прописе, укључујући *PCI-DSS, HIPAA, GDPR* и *NIST 800-171*. Ипак, сајбер сигурност никада неће моћи да буде 100-процентно обезбеђена.

Здравствене организације такође су дошле до увида користи од *cloud computing*-а. Пружаоци услуга здравствених осигурања, велике фармацеутске компаније и велике здравствене установе почињу у значајној мери да се ослањају на екосистеме засноване на *cloud*-у.

Важно је истаћи да дигитални екосистеми засновани на *cloud*-у нису само ствар креирања производа или услуге. Екосистеми све више подржавају компаније у потрази и испуњавању корпоративних циљева, бавећи се исходима које деле више заинтересованих страна, попут побољшања здравља клијената, омогућавања неометане логистике, побољшања сигурности и добробити запослених или пак смањења емисије угљен-диоксида (Chatterjee, 2020).

С обзиром да је људски фактор и даље водећи узрок угрожавања безбедности података, спасоносно решење за сајбер сигурност података може да представља *blockchain* технологија.

Blockchain технологија, иницијално започета као технологија за *Bitcoin* криптовалуту, представља дистрибуирани и децентрализовани систем главног регистра (енг. *ledger system*) који може да снима трансакције између више рачунара. Може се користити у готово свим секторима, јер се било која врста дигиталног средства или трансакције може инкорпорирати у *blockchain*. Нова технологија се сматра поузданим протоколом са аспекта сајбер сигурности због својих могућности указивања на сваки покушај угрожавања, пружајући тако сигурност интегритета трансакција. Иновативна *blockchain* технологија је по свом дизајну транспарентна, не нудећи приватност или поверљивост било каквих трансакција извршених на овај начин. Сигурност потиче не од приватности, већ од интегритета трансакција. *Blockchain* представља низ записа који континуирано расте. Они представљају „блокове", повезани су и заштићени криптографијом. Сваки од ових блокова садржи криптографско хеширање, укључујући информације о претходном блоку, уз временску ознаку и информације у вези са трансакцијом.

Blockchain бележи трансакције на трајан, ефикасан и поверљив начин и отпоран је на било који облик неовлашћеног приступа или модификовања података. Управљање *blockchain*-ом врши се путем *peer-to-peer* (*P2P*) мреже која се придржава одређеног протокола за валидацију сваког блока. Једном забележени подаци не могу се накнадно уређивати или мењати без промене свих блокова који су претходили.

Blockchain технологија налази употребу у бројним областима, па и у здравственом сектору. Најочигледнији пример за могућност употребе *blockchain* технологије у здравственом сектору су здравствени подаци о пацијентима који захтевају апсолутну тајност и приватност (Garg, 2020; Aunger, 2020).

У дигиталном екосистему који је пацијент-центричан, они који здравствене податке морају да поседују, да њима управљају и да имају дозволу да их користе и деле, су пацијенти а не здравствене установе. Ово представља кључни концепт интероперабилности која је усредсређена на пацијента, и која се суштински и дијаметрално разликује од конвенционалне интероперабилности вођене институцијама. Оваква поставка интероперабилности која је усмерена на пацијента, поред технолошких питања (скалабилност и брзина, подстицаји и управљање), доноси бројне изазове као што су: стандарди података, сигурност и приватност (Yoon, 2019).

Blockchain технологија може олакшати прелазак са интероперабилности вођене институцијом на интероперабилност усмерену на пацијента јер омогућава пацијентима да додељују право приступа својим медицинским подацима, омогућавајући чак и приступ појединим деловима својих података на одређено време. Применом *blockchain* технологије пацијенти се могу повезати са другим здравственим установама и аутоматски прикупљати своје медицинске податке (Gordon & Catalini, 2018).

Међутим, примена *blockchain* технологије у здравственом сектору не ограничава се само на управљање здравственим подацима већ се може применити и на: мониторинг ланца набавке лекова (олакшани процеси верификације количине и квалитета ланца испоруке фармацеутских производа, на основу ажурирања у стварном времену шифрованог, децентрализованог *ledger*-а), сигурност *IoMT* (енг. *Internet of Medical Things*) путем спречавања губитка, хаковања и неовлашћене измене података, обезбеђујући тако поуздано функционисање, управљање потраживањима и обраду плаћања, јер паметни уговори омогућавају аутоматизацију и убрзани процес ауторизације (Aetsoft, n.d.).

1.2. Циљеви истраживања

Циљ истраживања је развој модела дигиталног здравственог екосистема базираног на *blockchain* технологији. Развијени модел треба да обухвати све идентификоване стејкхолдере дигиталног здравственог екосистема и размене података у пословним процесима, чија ће сигурност бити обезбеђена применом *blockchain* технологије. Развој модела подразумева следеће кораке:

- идентификацију свих стејкхолдера у дигиталном здравственом екосистему,
- дефинисање протока здравствених информација и података који се односе на пословање здравствене установе,
- креирање техничко-технолошког решења,
- дефинисање индикатора од значаја за евалуацију предложеног решења.

Ток истраживачког процеса треба да обухвати све кораке, од сондирања о потреби и препознатом значају оваквог модела од стране стејкхолдера, преко процеса пројектовања

и моделирања до имплементације модела дигиталног здравственог екосистема базираног на *blockchain* технологији и његове евалуације.

Непосредни истраживачки задаци, у односу на наведене циљеве, су:

- утврђивање потребе за применом *blockchain* технологије у дигиталном здравственом екосистему, пре свега са аспекта препознавања значаја сигурности података,
- анализа постојећих модела дигиталних здравствених екосистема,
- анализа могућности примене *blockchain* технологије у здравственом сектору,
- анализа постојећих софтверских решења у домену *blockchain* технологије,
- концептуализација модела дигиталног здравственог екосистема заснованог на *blockchain* технологији,
- моделирање инфраструктуре модела дигиталног здравственог екосистема заснованог на *blockchain* технологији,
- имплементација развијеног модела дигиталног здравственог екосистема заснованог на *blockchain* технологији,
- развој система метрика за евалуацију имплементираног модела дигиталног здравственог екосистема заснованог на *blockchain* технологији.

1.3. Полазне хипотезе

Као главна хипотеза која ће бити тестирана у раду се издваја:

Развојем и применом модела дигиталног здравственог екосистема заснованог на *blockchain* технологији постиже се већа сигурност функционисања електронског пословања, проток и координација података, управљање подацима, интерабилност, кооперабилност стејкхолдера у здравственом сектору.

Посебне хипотезе у истраживању које проистичу из главне истраживачке хипотезе су:

Х0.1. Могуће је развити модел дигиталног здравственог екосистема заснован на *blockchain* технологији.

Х0.1.1. Процесом имплементације предложеног модела може се подићи сигурност функционисања, квалитет и ефикасност електронског пословања здравствених установа.

Х0.1.2. Пословни процеси и функционисање здравствених установа се могу прилагодити предложеном моделу.

Х0.2. Могуће је интегрисати предложени модел у актуелно електронско пословање здравствених установа.

Х0.2.1. Примена предложеног модела може допринети повећаном квалитету и побољшаном функционисању здравствених установа у Републици Србији.

Х0.2.2. Интеграцијом се постиже веће поверење стејкхолдера у сигурност функционисања електронског пословања у здравственом сектору.

1.4. Методологија истраживања

Методологија истраживања представља комплексан и организован процес који се спроводи кроз утврђене фазе а полази од логичких начела и принципа. Након опсежне експлорације доступне литературе, коришћене су опште научне методе анализе досадашњих научних резултата и достигнућа, као и аналитичко-дедуктивне и статистичке методе анализе података. Процес моделирања искоришћен је за израду предлога модела здравственог екосистема базираног на *blockchain* технологији.

Метода аналитичке дедукције употребљена је за обраду података о већ постојећим решењима, технологијама и смерницама за развој софтверских компоненти од значаја за модел. Тестирање података од значаја за истраживање и анализа резултата спроведени су помоћу одговарајућих статистичких метода. Истраживање се може класификовати као: сложено (балансирани удео теоријског и емпиријског истраживања), према временској појавној одредници као трансверзално (пресек појаве у датом временском интервалу), као интердисциплинарно, јер разматра практичну примену информационих технологија и решења у здравственом сектору, према актуелности предмета се може окарактерисати као иновативно и актуелно, према сврси и циљевима иновативно-хеуристичко (усмерено на откривање непознатих односно, неидентификованих фактора, њихових својстава и међусобног односа а који се тичу предмета истраживања), док у функционалном смислу у домену развоја науке представља акционо истраживање, јер даје практично решење за конкретан актуелни проблем који се темељи на изграђеном научном сазнању.

Резултати истраживања приказани су путем текстуалног излагања и описа, табеларно, путем слика и дијаграма. Процеси синтезе, апстракције, генерализације и класификације, уз друге адекватне методе научног објашњења, биће примењени за закључивање на бази индуктивно-дедуктивног закључивања.

2. ЗДРАВСТВЕНИ СИСТЕМИ

Систем се дефинише као скуп међусобно делујућих или међузависних компоненти које чине интегрисану целину (Backlund, 2000). Заправо, под системом се подразумева „скуп међусобно повезаних елемената који заједничком акцијом доводе до постизања циљева у средини у којој систем егзистира" (Jovanović et al., 2015). Систем обухвата комплексност свих припадајућих елемената. Сектор здравства је за сваку државу један од најзначајнијих, јер ефикасан здравствени систем доприноси напретку државе кроз учешће у значајном делу привреде, доприносећи развоју и индустријализацији једне земље.

2.1. Модели и форме електронског пословања у здравственом сектору

Електронско пословање (е-пословање) доводи до великих, фундаменталних промена у бројним секторима, док један сектор остаје релативно неискоришћен. Према мишљењу експерата *Forbes*-а, здравствени сектор је последња граница е-пословања, препун могућности раста која је вођена практичношћу, нижим трошковима и приступом производима (Ashbey, 2017).

Здравствени сектор се налази под великим притиском да побољша здравствену заштиту пацијената, управља улазним трошковима, технологијама, квалитетним услугама и оперативним маржама. Брзе промене у технологији, одлукама владе и осигуравајућих кућа, јака конкуренција и медицински напредак, учинили су пацијенте забринутијим и захтевнијим. Као императив се намеће да здравствена заштита буде приступачна, одговорна и доступна широкој популацији (Lee et al., 2011).

Постоје бројне класификације модела е-пословања. Прегледом литературе, доминатна је класификација базирана на трансакцијама односно тзв. *X2X* модели. У табели 1 дат је приказ основних модела е-пословања.

Табела 1. *X2X* модели е-пословања (Извор: E-commercetoolbox (n.d.); Bjelica, 2020)

	Клијенти/физичка лица	**Пословни систем/ организација**	**Влада**
Клијенти/физичка лица	*Customer-to-Customer* (*C2C*)	*Business-to-Customer* (*B2C*)	*Government-to-Customer* (*G2C*)
Пословни систем/ организација	*Customer-to-Business* (*C2B*)	*Business-to-Business* (*B2B*)	*Government-to-Business* (*G2B*)
Влада	*Customer-to-Government* (*C2G*)	*Business-to-Government* (*B2G*)	*Government-to-Government* (*G2G*)

Предности које нуди е-пословање у здравственом сектору су (KBK Communications, 2020):

- већи избор продуката по мањим ценама,
- већа помоћ пацијентима, уз мање оптерећење професионалаца,

- већа сигурност у обезбеђивању приватности пацијената и информација,
- олакшан и једноставан приступ.

Пословни модели у здравственом сектору базирају се углавном на примењеним технологијама. Дефинисање пословног модела у здравству односи се на идентификовање области здравства где се примењује предвиђена технологија. Најчешћи модели су (Bjelica, 2020):

1. *Government-to-Business* (*G2B*) модел, који представља комуникацију ресорног министарства и других државних органа са:
   - институцијама здравственог осигурања,
   - здравственим установама свих нивоа здравствене заштите,
   - институцијама које едукују профиле здравственог усмерења.

   Модел обухвата системско планирање, праћење и контролу употребе ресурса у здравственом сектору, мониторинг здравственог статуса како јединке тако и целе популације, усаглашавање и интеграцију активности од заједничког интереса, планирање потрошње расположивих финансијских средстава, са циљем смањења непотребних и понављајућих информација, што свакако води повећању поузданости и избегавању кашњења.
2. *Business-to-Business* (*B2B*) модел, који се у домену е-здравства појављује у комуникационим процесима:
   - здравствених осигуравајућих кућа и радних организација,
   - здравствених осигуравајућих кућа и установа које пружају здравствене услуге,
   - здравствених осигуравајућих кућа и фармацеутских компанија, добављача медицинских средстава, лекова итд.,
   - хоризонталним комуникационим процесима (између здравствених установа истог ранга) и/или трансверзалним (између организација различитих нивоа здравствене заштите).

   Овим моделом су обухваћени типови трансакција који се односе на новчани проток као и ток информација између појединачних правних субјеката у процесу пружања здравствене заштите, добављача опреме, материјала, медицинских средстава и лекова, здравствених установа свих нивоа заштите, осигуравајућих друштава и других организација. *B2B* модел у здравственом сектору представљен је путем ланаца набавки, промета робе уз тежњу ка повећању ефикасности, редукцију трошкова трансакција уз усмеравање ка правилним протоцима информација у реалном времену за све учеснике у ланцу.
3. *Business-to-Customer* (*B2C*) модел се у е-здравству користи од стране:
   - клијената/пацијената за заказивање прегледа и медицинских услуга,
   - корисника здравствене заштите приликом пријаве за здравствено осигурање,
   - здравствених организација приликом провере статуса и нивоа здравственог осигурања,
   - корисника здравствене заштите за добијање информација везаних за обим права која проистичу из актуелног нивоа здравственог осигурања,

- здравствених радника и/или сарадника у циљу повезивања са појединцима на истом или вишем нивоу здравствене заштите,
- здравствених радника у циљу усавршавања у образовним институцијама које пружају едукацију из медицинске струке.

4. *Government-to-Customer* (*G2C*) модел се у е-здравству користи за:
    - комуникацију са корисницима здравствене заштите у вези са остваривањем права из домена осигурања, процедуром лечења у иностранству, улагањем жалби итд.
    - поступке прибављања информација од стране надлежних институција о болестима, употреби лекова и медицинских средстава,
    - промотивне активности из домена здравог стила живота,
    - информисање здравствених радника/сарадника о постојећим континуираним едукацијама, стручним усавршавањима, ужим специјализацијама, научним и стручним скуповима, као и едукационим семинарима и курсевима.

Здравство почиње да доживљава помак ка *C2B* (*Consumer-to-Business*) моделу, јер се пацијенти све више укључују због нарастајућих очекивања и захтева корисника здравствене заштите. Као основе за експанзију *C2B* модела наводе се (Chigrinetc, 2019):

- **Пацијенти се фокусирају на превенцију** – људи су спремнији да траже информације о начину живота, алергијама, симптомима и боље су упућени и заинтересовани да преузму контролу над својим здрављем. Као резултат тога, пацијенти све чешће траже здравствену заштиту знатно проактивније, избегавајући чекање на специфичне симптоме.
- **Пацијенти желе да поседују своје медицинске податке** – сада пацијенти постају равноправни актери у процесу здравствене заштите. Историјски гледано, пацијенти су морали да прођу кроз дуг процес да би затражили да виде своје медицинске информације, али модерна времена мењају ту традицију.
- **Пацијенти траже повезаност** – пацијенти желе да приступе информацијама о симптомима, стањима и превенцији било када и било где, па чак и да добију персонализовану помоћ од вештачке интелигенције. Они желе да остану у контакту са својим пружаоцем здравствене заштите и својом осигуравајућом компанијом на најједноставнији могући начин (преко апликације) и да чак могу да разговарају са својим лекаром у тренутку. Они очекују једноставне интеракције прилагођене кориснику, где је технологија од помоћи.
- **Пацијенти желе персонализацију** – здравствене установе ће морати да иду у корак са временом, тражећи начине да надограде и персонализују искуство пацијената, било да се узима у обзир собна температура и преференције у погледу оброка, или да се дозвољавају специфичне посете у установама, укључујући чак и медицинске сестре које говоре матерњи језик пацијента.
- **Пацијенти желе удобност** – медицинске установе ће морати да признају да је удобност пацијената постала веома важна и да понуде мобилне резервације, термине за исти дан, телемедицину, испоруку лекова, флексибилно радно време итд., као стандардне функције.

- **Пацијенти захтевају транспарентност** – купци су нестрпљиви и очекују да имају потпуно власништво над производом који су платили, укључујући информације о процесима који стоје иза његове припреме и испоруке. Здравствену заштиту, међутим, карактерише неравнотежа информација, где се пацијент третира као део производне линије и нема информације о производном процесу. Међутим, ситуација се драстично мења.

Једно од чуда дигиталне економије је оснаживање потрошача које је она донела, где су потрошачи у могућности да узму значајно учешће у стварању вредности за производе до којих им је стало и слободни су да размењују информације са произвођачима. И здравство иде у правцу либерализације пацијената. Вероватно је да ће током века пацијенти и необучени неговатељи постати активнији у пружању неге захваљујући развоју вештачке интелигенције и ширењу информација. Баш као што сада можемо да поправимо рачунар у свом дому пратећи *Youtube* туторијал или *WikiHow* упутство, у наредним деценијама обични људи ће моћи да управљају хроничним стањима и лакшим болестима код куће уз помоћ вештачке интелигенције, која се заузврат заснива на колективном медицинском знању. Без обзира на могуће будуће сценарије, међутим, јасно је да ће се ниво технолошке софистицираности у малопродајном свету и здравству приближити прилично брзо (пре него што „миленијалци" оду у пензију), пошто очекивања потрошача расту експоненцијално, а болнице треба да почну да се припремају за будућност управо сада.

Погодност, једноставност, брзина и тренутно задовољство су основе економске тежње. Пословне активности које омогућују развијене технолошке платформе, испуњавајући потражњу клијената кроз тренутну набавку добара и услуга, су неминовност која се намеће у здравственом сектору. Здравство има тенденцију да себе сматра јединственим и имуним, али економско оријентисани захтеви су неизбежни у сектору здравства. Развој функционалних платформи на захтев превазилази *B2B* и *B2C*. Нове *C2B* платформе ће кориснике оснажити за изградњу захтевних система здравствених услуга (Birch, 2018).

2.2. Е-здравство

Електронско здравство или е-здравство је настало укрштањем медицинских информационих технологија, јавног здравља и процеса који се односе на пружање здравствених услуга и пренос генерисаних података путем интернета и одговарајућих комуникационих протокола (Eysenbach, 2001). Европска комисија је 2015. године дала дефиницију електронског здравства као „примену информационо-комуникационих технологија за задовољење потреба грађана, пацијената, здравствених радника, пружалаца здравствених услуга и креатора здравствене политике" (European Parliament, 2015). Светска здравствена организација (СЗО) дефинише е-здравље као „употребу информационих и комуникационих технологија за подршку здравству и здравственим областима" (WHO, 2019).

Е-здравство представља употребу информационо-комуникационих технологија са циљем (Rodić Trmčić, 2018):

- унапређивања и побољшања превенције болести, дијагностичких процедура, лечења и праћења тока опоравка, као и управљања обољењима и здравственим стањима,
- побољшања доступности здравствених услуга и подизања квалитета услуга путем побољшане ефикасности у целокупном здравственом систему,
- протока информација између клијената/пацијената и институција које пружају здравствене услуге,
- коришћења телемедицине и преносних уређаја помоћу којих је могуће праћење стања пацијената и размена прикупљених информација.

Е-здравство може да се посматра и као спој следећих основних компоненти (Obradović, 2009):

- информационо-комуникационе технологије (ИКТ), које представљају основу процеса побољшања перформанси активности везаних за очување и унапређење здравља,
- пацијент, односно корисник здравствених услуга,
- радне организације (државни органи и правни субјекти) које за своје кориснике уплаћују доприносе за здравствено и социјално осигурање,
- установе за пружање здравствених услуга (дом здравља, општа болница, поликлиника, клинички центар, приватне здравствене ординације итд.),
- државне и приватне установе здравственог осигурања,
- здравствено регулаторно тело (министарство здравља),
- институције образовања из области здравства,
- здравствени радници,
- информације, као основни елемент целокупне здравствене мреже.

Електронско здравство се уопштено дефинише као примена технологија и специфичне електронске комуникације у области здравства, користећи погодности које пружа интернет у процесу преноса здравствених информација, података и пружања услуга. Поред неизбежног стационарног компјутера, користе се и мобилни уређаји (телефон и таблет), и тада се говори о м-здравству. Ако се пак лекарске услуге, процене, консултације и сл. спроводе уз помоћ телекомуникационе технологије, онда се говори о телемедицини. У систем су укључени корисници здравствених услуга, пружаоци услуга (медицинско особље и медицинске установе), као и фондови и појединци који плаћају услуге.

Актуелно е-здравство обухвата широку палету – од мобилног здравства (м-здравство) до телемедицине. Широк дијапазон е-здравства илуструје слика 1, приказујући домене е-здравства.

Слика 1. Домени е-здравства (адаптирано из: Cowie et al., 2016)

Сматра се да технологија е-здравства доприноси побољшању здравља и искуства пацијената у процесу здравствене заштите, уз смањење трошкова здравственог система (Asthana et al., 2020).

Предности које нуди е-здравство су (Iberdrola, n.d.):

- **Унапређено праћење пацијената.** Дигитални канали комуникације олакшавају спону између лекара и пацијената. Примена савремених технолошких достигнућа омогућава праћење стања пацијента у реалном времену.
- **Информисанији пацијенти.** Пацијенти могу доносити боље здравствене одлуке када их разумеју и када им се омогући управљање сопственим здрављем. ИКТ омогућавају приступ водичима и најбољој пракси доступној на тржишту здравствених услуга.
- **Подстицање здравих навика.** Нове технологије мењају начин на који се пацијенти брину о себи помоћу апликација и уређаја који прате шта једу, колико вежбају, какава је хигијена сна, уз праћење стања организма.
- **Олакшано доношење одлука код здравственог особља.** Е-здравство такође трансформише начин на који се професионалци баве болешћу. ИКТ могу помоћи, на пример, да се лакше идентификују оптимални третмани или да се открију болести у раној фази.
- **Доступнија и равноправнија здравствена заштита.** Приступ здравственој заштити више није ограничен временом и простором. Технологија доприноси пружању здравствене заштите већем броју људи.
- **Ефикасније болнице и здравствене установе.** Повезаност здравствених установа значи модернизован здравствени систем који нуди минимизирање могућности људске грешке и смањење трошкова. Поред тога, велики број процеса се аутоматизује.

2.2.1. Компоненте е-здравства

Увођење електронског пословања у постојеће здравствене системе доводи до унапређења ефикасности протока информација, активности доношења одлука као и побољшања квалитета пословних процеса, док се положај и улога пацијента у тим процесима мења и он добија активну улогу, уместо досадашње пасивне (WHO and International Telecommunication Union, 2012).

Све активности и појмови који су постојали (или још негде постоје) у области традиционалних здравствених система имају своје е-варијанте. Тако нпр. постоје: електронски здравствени картон (е-картон), електронски упут (е-упут), електронски рецепт (е-рецепт), систем за подршку у клиничким одлукама, телемедицина и м-здравство, здравствени информациони системи итд. Све ове поменуте подсистеме не треба посматрати изоловано већ интегрисане у један општи систем, чиме се постиже синергијски ефекат и подиже вредност целокупног система.

Као елементи система е-здравства наводе се (Radenković et al., 2015; Scott & Mars, 2013; Steinhubl et al., 2015):

1. Е-картон – структурирана колекција електронских информација о здравственом стању једног пацијента или популације, која се чува ради лакшег приступа информацијама, обрачуна лечења, прегледа историје болести и смањивања потреба за класичном администрацијом.
2. Е-рецепт – замена за класичан рецепт који издају лекари. Има предности над класичним рецептом, јер се смањују трошкови администрације и избегавају се могући проблеми који настају код класичних рецепата.
3. Е-упут – за слање електронским путем захтева од лекара до лабораторије са назначеним потребним анализама и пријем резултата, или за консултацију код лекара других специјалности.
4. Е-здравствена картица – мултифункционална паметна картица која се израђује као замена за класичну здравствену књижицу, са могућношћу измене података осигураника, као и додавања информација о електронским рецептима, лабораторијским налазима итд.
5. Дијагностички информациони систем – интерактивни софтвер који представља подршку приликом постављања дијагнозе.
6. М-здравство – подразумева примену мобилних телефона у медицинској пракси и јавном здрављу.
7. Телемедицина – коришћење информационо-комуникационих технологија у циљу пружања здравствених услуга на даљину.

2.2.2. Електронски здравствени картон (е-картон)

Електронски здравствени картон се може дефинисати као дигитална верзија пацијентовог папирног картона (CIS Consulting, n.d.). Он садржи све релевантне информације о пацијенту, којима могу приступити једино овлашћени корисници. Ту спадају: медицинска историја пацијента, дијагнозе, називи лекова, планови лечења, датуми имунизације, алергије, радиолошки снимци и лабораторијски резултати. Док

појединачни е-картон садржи историје о свим медицинским третманима пацијента, системи базирани на е-картону омогућавају да се клиничке и друге информације прикупљене на једном месту могу користити шире, тако да други пружаоци здравствених услуга у оквиру исте здравствене организације или других системски повезаних институција могу квалитетније да брину о здрављу пацијента. Системи засновани на е-картону укључују разне могућности али су три функционалности од битног значаја за побољшање квалитета здравствене заштите и смањење трошкова здравственог система, а то су: алати који подржавају клиничке одлуке (енг. *clinical decision support tools*), системи компјутеризованог лекарског упута (енг. *computerized physician order entry systems*) и системи размене здравствених информација (енг. *health information exchange*) (Menachemi & Collum, 2011).

И поред тога што постоји велики број чланака у којима се приказују користи које доноси увођење е-картона, неки аутори наводе и потенцијалне мањкавости које су повезане са овом технологијом. Ове мане се односе на финансијске проблеме, промене у уходаном радном току, привремено смањену продуктивност због уходавања система итд. Посебно треба истаћи бригу о приватности и сигурности података и могућности појаве нежељених последица. Такође, треба напоменути да и одржавање система е-картона може бити скупо због потребе замене хардвера и усавршавања софтвера, за шта се крајњи корисници е-картона морају редовно обучавати.

Подаци садржани у е-картону представљају поуздану основу за спровођење лонгитудиналних студија неког здравственог проблема у оквиру одређене регије. Као пример може се навести рад Zhao и сар. (2019). У првом делу истраживања аутори су анализирали податке о конвенционалним факторима ризика (старост, крвни притисак, укупни холестерол, индекс телесне масе, креатинин, глукоза итд.) прикупљене у 10-годишњем периоду из скоро 110 хиљада е-картона, док су у другом делу те податке комбиновали са генетским подацима за 10162 испитаника. Сложеним поступцима аутори су анализирали различите утицаје, а све то је било могуће захваљујући постојању е-картона за испитанике обухваћене студијом.

У недавно објављеном чланку у *Harvard Business Review*, аутори наводе да су системи базирани на е-картону намењени интегрисаним здравственим мрежама често нефлексибилни, неподесни за употребу и скупи, јер се обично добијају од комерцијалних испоручилаца који настоје да што више зараде путем њихове имплементације и оптимизације (Davenport et al., 2018). Постојећи системи електронског здравственог картона (ЕЗК) отвореног типа обично су дизајнирани за мање институције и није их лако подићи на скалу да задовољавају потребе великих здравствених система. Зато се као обећавајућа опција заговара увођење вештачке интелигенције (енг. *Artificial Intelligence - AI*) „како би се системи са е-картонима учинили флексибилнијим и интелигентнијим". У овом правцу се крећу и настојања произвођача оваквих система.

2.2.3. Електронски упут (е-упут)

Електронски упут представља преносиви електронски систем који омогућава изабраном лекару да директно уноси налоге за тестирање и лечење пацијента и да их електронски шаље одговарајућој установи ради извршења. Наравно, коришћење стационарног компјутера или мобилног уређаја омогућава ефикасну комуникацију, смањује могуће

грешке узроковане нечитким рукописом и пружа низ других погодности у раду, а све у корист пацијента (Ludwick & Doucette, 2009).

Електронски упут знатно повећава ефикасност када су у питању захтеви да се изврше лабораторијски тестови и радиолошки прегледи, као и само лечење пацијента. Примењен у тандемском систему са е-рецептом, електронски упут упозорава лекара и клиничаре на могућу алергичност пацијента на одређене лекове.

Систем електронског упута пружа низ погодности, као што су (Khanna & Yen, 2014):

- **Подршка у одлучивању фокусирана на пацијента.** Интегрисан са електронским картоном, електронски упут даје могућност клиничарима да имају ажуриране податке о пацијенту као и целокупну медицинску историју пацијента, што омогућава доношење бољих одлука о конкретним питањима лечења.
- **Сигурност пацијента.** Систем електронског упута омогућава лекарима и медицинским сестрама да идентификују пацијента у реалном времену, добију увид у препоручене дозе лекова и провере потенцијалне нежељене ефекте алергије на одређене лекове и интеракције лекова.
- **Усклађеност са прописима и сигурност.** Приступ подацима мора бити безбедан и у складу са одговарајућим прописима.
- **Преносивост.** Систем електронског упута може да прихвати захтеве из свих одељења, употребом преносивих уређаја (лаптоп, таблет, паметни мобилни телефон).
- **Управљање.** Генерисани извештаји могу се анализирати и процењивати, што може помоћи у доношењу одлука о евентуалним променама у саставу особља и продуктивности. Треба напоменути да постоје извештаји о томе да неки учесници у процесу пружају отпор увођењу овакве новине.

Увођење система електронског упута захтева знатна финансијска средства која укључују не само набавку него и обуку и одржавање система, те се зато овој проблематици поклања значајна пажња. Испитивања зависности између каталошке цене испоручилаца интегрисаних система електронског упута и електронског картона и квалитета здравствене услуге (ефикасност, погодност примене, сигурност пацијента, равноправност у третману, правовременост и сл.) су показала да не постоји нека значајна веза између ових фактора (Mummadi & Mishra, 2018).

2.2.4. Електронски рецепт (е-рецепт)

Електронски рецепт (енг. *e-prescribing*) представља компјутеризовану варијанту традиционалног папирног лекарског рецепта коју лекар, користећи специјални софтвер инсталиран на неком од типова компјутера (стационарни, лаптоп или таблет), прослеђује мрежи апотекарских установа на реализацију, тј. издавање одговарајућих лекова кориснику. Овде је сувишно наглашавати да оваква новина представља значајно олакшање како за лекаре, тако и за кориснике њихових услуга.

Porterfield и сар. (2014) наводе предности које пружају системи електронског рецепта који, мада наведени за америчке услове, вероватно сви важе и на овим просторима, и то су:

- Елиминишу се грешке у прописивању лекова. Код ручно исписиваних рецепата постојала је могућност да због нечитког рукописа дође до грешке. Чињеница да и лекар и апотекар имају увид у историју прописивања лекова за конкретног пацијента такође смањује могућност грешке.
- Аутоматизована подршка клиничким одлукама. Многи лекови постоје у различитим облицима и са различитим садржајем активне супстанце. Електронско прописивање лека отклања нагађања, јер су дозе, начини и фреквенције узимања лека јасно наведени. Електронски рецепт такође укључује проверу дозе и упозорење о дуплираној терапији. Већина апликација користи стандардне речнике лекова и бира параметре са одговарајућих листа, што такође смањује ризик у електронском прописивању лекова.
- Убрзава се усклађени процес лечења. Клиничари у сваком тренутку могу имати увид у историју лечења пацијента и не морају да усклађују листе лекова или да се ослањају на информације из своје меморије, као што су лек-лек интеракције.
- Обезбеђује се тренутно обавештење о алергијама, интеракцији лекова, дуплираним терапијама и другим клиничким упозорењима. Електронско прописивање омогућава лекарима пун увид у документоване алергије пацијента и раније прописиване лекове. Систем ће упозорити лекара о алергијама, интеракцијама са другим лековима које узима пацијент, као и о томе да се неки лек не сме давати трудницама, малој деци или старијим особама.
- Прати се испуњавање прописаног. Када лекар испише рецепт ручно, не постоји могућност да се провери његова реализација, јер пацијент може да на њега заборави, да га изгуби, не може да приушти његово плаћање, или једноставно одустане од узимања лека због тога што се тренутно осећа боље и без њега. Електронски рецепт даје могућност провере, тако да лекар може да утиче на пацијентов став.
- Смањује се број изгубљених рецепата. Када пацијент добије папирни рецепт постоји могућност да га загуби и зато мора да се поново исписује. У електронској верзији то не постоји јер се рецепт шаље директно апотеци.
- Омогућава се да лекар електронски пропише контролисане супстанце у јединственом поступку. Одговарајући софтвер омогућава директно поручивање контролисаних супстанци, чиме се постиже увид у њихову употребу.
- Омогућава се бољи мониторинг рецепата за контролисане супстанце. Електронско прописивање даје могућност лекару да прати колико је издато рецепата за контролисане супстанце, што смањује вероватноћу злоупотребе. Ово омогућава да се контрола може вршити на нивоу државе у складу са одговарајућим прописима.
- Запослени троше мање времена за поновно исписивање рецепата. Једно од највећих административних оптерећења лекара и клиничара јесте потреба да се одговори на захтеве за поновним испуњавањем рецепата. Одговарајући софтвер омогућава да се обнављање рецепата обави у врло кратком времену, што је од посебне користи пацијенту који путује или је већ потрошио лекове.
- Смањује се ризик од поновног пријема. Постоје сигурносна упозорења на дуплу терапију и смањује се ризик од нежељених реакција на лек. Процењује се да је око 20% поновних пријема у болнице последица негативних реакција на лекове.

- Побољшава се правилно узимање лека. Најчешћи облик непридржавања прописаног начина узимања лека јесте узимање мањих доза од прописаних и прерано прекидање терапије. Испитивања су показала да електронско прописивање лека даје побољшање од 10% у успешности терапије, што представља значајан корак с обзиром на процене да се око једне половине терапија не извршава онако како је то прописано.
- Омогућава се лакша провера осигурања. Електронско прописивање олакшава избор одговарајућег лека са позитивне листе лекова.

2.3. М-здравство и телемедицина

Модерне информационо-комуникационе технологије дале су могућност контроле пацијената на даљину (енг. *Remote Patient Monitoring – RPM*), што за последицу има појаву иновативних облика активности и развоја услуга у области е-здравства, као што су телемедицина и м-здравље.

Према Америчком националном институту здравља (енг. *National Institute of Health – NIH*) „м-здравље подразумева примену мобилних и бежичних уређаја (лаптоп, таблет, паметни мобилни телефон и др.) за унапређење исхода лечења, услуга здравствене заштите и спровођење истраживања у здравству" (Park, 2016).

Телемедицина и м-здравство су, заправо, елементи е-здравства који се у великој мери преклапају. Како наводи Collier (2018), м-здравство, у ужем смислу, представља облик телемедицине, са апликацијама које често и не укључују медицинске раднике. С друге стране, телемедицина представља коришћење технологија за пружање здравствених услуга пацијенту од стране здравствених професионалаца.

Прву дефиницију термина м-здравства су дали Istepanian и Lacal (2003), као употребу нових технологија мобилних и мрежних комуникација у здравству. У том погледу, м-здравство се ослања на три главна елемента:

- сензори за примену у здравству,
- комуникациони системи (*5G*, *IoT*),
- рачунарство и интернет (вештачка интелигенција, *cloud* рачунарство, *big data* итд.).

Најједноставнији облици м-здравства, који могу да се примењују употребом јефтиних, класичних мобилних телефона су:

- гласовна комуникација (са другом особом или са системом снимљених одговора путем интерактивног навођења),
- слање текстуалних порука.

Без обзира на техничку једноставност, и овакав начин комуникације може да донесе бољитке у лечењу стања као што су дијабетес, астма, повишен крвни притисак итд., кроз самоконтролу од стране пацијената и адекватно навођење на примену терапије, што може бити од посебног значаја у слабо развијеним земљама и руралним подручјима.

Са развојем технологије, у последње две деценије је и тржиште мобилних телефона доживело експанзију, у смислу масовне појаве паметних мобилних телефона, који из генерације у генерацију имају побољшане карактеристике и перформансе, ширећи могућности примене и пружајући боље корисничко искуство. Самим тим, и употреба паметних мобилних телефона је доживела експоненцијалан раст, отварајући врата за примену бројних апликација које подржавају услуге м-здравства, а усмерене су на праћење и побољшање здравља корисника, односно пацијената.

Dicianno и сар. (2015) категоришу апликације м-здравства у следеће групе:

- Апликације усмерене на побољшање животног стила – које помажу корисницима да прилагоде своје животне навике и нуде могућност праћења активности вежбања, плана исхране, напретка губитка килограма итд. Овакав тип апликација најчешће не подразумева надзор од стране лекара.
- Апликације оријентисане ка пацијентима – које појединцима са медицинским проблемима омогућавају управљање својим здравственим стањем, кроз савете и упутства за самоконтролу и рано откривање симптома, као и праћење и придржавање прописане терапије. Овакав тип апликација не нуди могућност директне комуникације са лекаром, тако да њихова примена захтева додатан опрез.
- Апликације намењене лекарима – које им пружају подршку у управљању здравственим стањима пацијената помоћу информација едукативног карактера, смерница које потпомажу лакше доношење медицинских одлука, алата за мерење и прорачуне итд. Примери за овај тип апликација обухватају електронске верзије медицинских енциклопедија, приручника за рехабилитационе процедуре, регистре лекова итд.
- Апликације за управљање болестима – представљају најчешће веб базиране портале, који користе класичне рачунаре и сталну интернет везу, и пружају лекарима могућност праћења хроничних стања пацијената. Могу бити интегрисане у електронске здравствене картоне и фармацеутске апликативне системе, нудећи често алате за подршку у доношењу одлука, али без могућности прикупљања података о пацијентима путем преносивих уређаја за мониторинг.
- Традиционални системи телездравља – представљају електронску комуникацију за пренос информација и пружање услуга на даљину. Овакви системи подразумевају интеракцију пацијента и лекара, и укључују употребу уређаја као што су мерач крвног притиска и пулса, апарат за проверу нивоа шећера у крви итд., који су повезани на класичан рачунар или лаптоп, а не паметни мобилни телефон.
- Апликације м-здравства – које су по начину функционисања сличне традиционалним системима телездравља, али подразумевају употребу паметних мобилних телефона и таблет уређаја уместо класичних десктоп односно лаптоп рачунара. Употребом овог типа апликација, пацијенти имају могућност интеракције са лекарима и помоћи у праћењу здравственог стања (нпр. повишен крвни притисак, висок ниво шећера у крви), придржавању прописане терапије, рехабилитационим саветима итд. Пацијентима се пружа могућност и мултимедијалне интеракције, где помоћу камере паметног мобилног телефона могу нпр. показати лекару неке уочене промене на кожи, или пружити повратну информацију о начину зарастања ране после неке хируршке интервенције. Овај

тип апликација захтева приступ интернету, али у условима слабе покривености сигналом мрежног оператера може и да складишти податке у интерну меморију телефона, који ће бити послати након поновног успостављања активне конекције.

Несумњиво је да услуге м-здравства пружају бројне погодности за праћење и унапређење здравља, али се свакако морају узети у обзир и мане које са собом носи ова технологија.

Bajwa (2014) као главне баријере за примену услуга м-здравства наводи:

- отпор према иновацијама,
- недостатак одговарајуће инфраструктуре и
- трошкове набавке и одржавања неопходне технологије.

С обзиром да апликације м-здравства подразумевају размену осетљивих медицинских информација, брига за сигурност протока података је и већа него код традиционалних жичних мрежних система, јер се за приступ користе паметни мобилни телефони, који комуницирају путем бежичне и мобилне конекције, а такође се за складиштење користи и интерна меморија у оваквом типу уређаја.

Апликације м-здравства и услуге које оне пружају често нису контролисане од стране лекара (клиничара, специјалиста итд.), што у неким случајевима може довести и до погоршања стања појединаца, јер могу испољити нежељена дејства терапије која би за њих била контраиндикована у случају надзора од стране одговарајућих здравствених стручњака.

Телемедицина представља термин који подразумева употребу технологије у пружању услуга здравствене неге и заштите на даљину (Balingit, 2022). Основни циљ овакве примене технологије јесте да пацијент добије одговарајућу здравствену негу када год је то потребно, без обзира на његову физичку локацију, која би иначе била лимитирајући фактор. Телемедицина обухвата видео конференције у реалном времену, праћење на даљину здравствених података који се прикупљају и евалуирају (крвни притисак, засићење кисеоником, пулс, стопа респираторног система итд.), као и системе складиштења и дељења медицинских информација (снимци радиографије, магнетне резонанце, компјутеризоване томографије, слике и видео записи о пацијентовом здравственом стању итд.).

Као главне предности телемедицине истичу се (Ahamed, 2022):

- повећање приступа здравственој заштити (нарочито за пацијенте у руралним и подручјима која нису довољно покривена системом здравствене заштите),
- побољшање континуитета здравствене заштите (пружање чешћих и редовнијих контаката између пацијената и медицинског особља),
- уштеда трошкова (смањење потребе за путовањем и смештајем),
- флексибилност термина и локација,
- омогућена удобност пацијената (комуникација се одиграва из њихових домова),
- побољшање задовољства пацијената (практично усмерена и персонализована здравствена заштита),
- проширење и олакшан приступ медицинским стручњацима разних специјалности (који нису доступни на актуелним локалитетима где живе корисници услуга),
- побољшана комуникација,

- побољшана координација здравствене заштите,
- повећана ефикасност (смањење листе заказивања и времена чекања на преглед).

Као главни недостаци телемедицине наводе се: проблем техничке природе (обука и опрема), редукција контаката са истим медицинским стручњаком, смањење персоналних консултација (eVisit, 2018). Такође, недостаци телемедицине обухватају и ограничења у спровођењу интегративног клиничког прегледа, појаве могућности техничких ограничења и потешкоћа, сигурност здравствених информација и регулаторне баријере (Balestra, 2018).

Поједини елементи е-здравства – електронски здравствени картон, електронски упут, електронски рецепт и сл. су ушли у широку примену у савременој медицинској пракси. Наравно, поставља се питање њихове интеграције у јединствен систем, чему се поклања посебна пажња у одговарајућој литератури. Тако је у књизи „*e-Health Systems, Theory, Advances and Technical Applications*" (Rodrigues et al., 2016) дат глобални преглед свих делова е-здравственог система као и главних трендова у побољшању квалитета и ефикасности управљања здравственим системом. Аутори се фокусирају на апликације ИКТ технологија и њихову имплементацију у е-здравствене системе, посебно се осврћући на бежичне мреже и сигурносне протоколе у њима. При томе се посебна пажња посвећује проблему побољшања квалитета и смањењу трошкова здравствене заштите и заговара приступ да би сваки појединац требало да, у случају потребе, добије помоћ од ауторизоване особе, било где и у било које време.

2.4. Организација здравственог система

Према дефиницији Светске здравствене организације (WHO, 2000), систем здравствене заштите је базиран на здравственој инфраструктури која пружа широки спектар програма и услуга, које имају за циљ обезбеђивање здравствене заштите за појединце, чланове њихових породица као и целокупну друштвену заједницу.

Светска здравствена организација је предложила четири главне функције за систем здравствене заштите. То су:

- пружање здравствених услуга,
- стварање здравствених ресурса (улагање и обука),
- финансирање здравства,
- управљање.

Према СЗО, главни циљ здравственог система представља побољшање здравља људи. Најважнија функција коју систем треба да даје је пружање здравствених услуга, а друге функције су помоћне али веома значајне јер обезбеђују пружање услуга. Неуспех у генерисању ресурса може урушити концепт пружања услуга. Понекад се услуге не испоручују потенцијалним корисницима јер су оне саме недовољно финансиране. Пружање услуга је оно што здравствени системи спроводе а то су специфичне услуге или интервенције. Стварање ресурса се односи на три главна инпута здравственог система: људски ресурси, физички капитал и потрошна средства. Одговорност за

функционисање и свеукупни учинак здравственог система у земљи се налази у рукама владајућих структура у држави (Papanicolas et al., 2013; Ferreira et al., 2018).

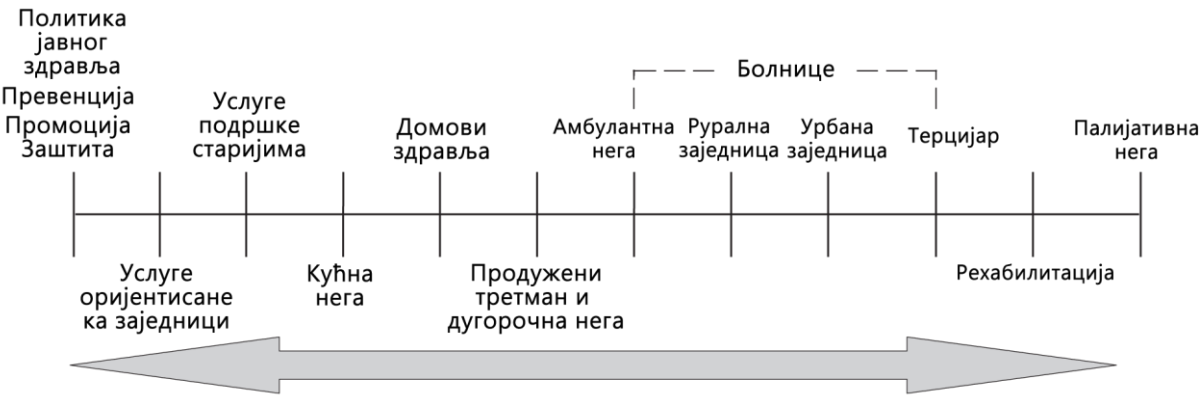
Интегрисани здравствени систем представља организацију и управљање здравственим услугама на начин да људи добију здравствену заштиту која им је потребна, када им је потребна, на начине који су прилагођени корисницима, да се постижу жељени резултати и обезбеђење вредности за новац (Integrated Health Systems: Definition & Types, 2021). Примарни фокус интегрисаних здравствених система је да обезбеде беспрекорну здравствену заштиту односно координисану здравствену заштиту за пацијенте и њихове породице. На тај начин, постићи ће се виши квалитет здравствене заштите као и бољи здравствени исходи за пацијенте, јер ће се осигурати да они на одговарајући начин буду усмерени кроз здравствени систем.

Постоје различити типови интеграције, и то:

- Функционална интеграција – постоје вишеструки односи који су координисани кроз различите јединице и одељења на начин да се пацијентима пружи најбоља вредност и услуга. Овакав концепт премашује основну бригу о пацијентима и односи се на помоћна одељења, као и на ИТ одељење и одељења за осигурање квалитета. Чврста веза ових одељења и одељења за здравствену заштиту пацијената омогућава боље искуство здравствене неге за пацијенте, као и несметану транзицију кроз све аспекте здравствене заштите.
- Интеграција лекара односи се на интеграцију у којој лекари и организације са којима раде и/или су повезани деле исте вредности, визије и циљеве, како би се ограничиле разлике у пруженој здравственој заштити пацијената. Лекар и организација треба да су савезници који раде заједно на истом циљу који им омогућава да пруже ефикаснију и бољу услугу, што заједно води ка бољим укупним здравственим исходима за пацијенте.
- Клиничка интеграција – у којој услуге које се пружају пацијентима могу потицати од различитих пружалаца услуга и организација. Ове услуге се координишу преко координатора неге, како би се максимизирао квалитет здравствене заштите коју пацијент добија, као и да би се обезбедила ефикаснија и делотворнија здравствена заштита.

2.4.1. Дефинисање здравствених организација

Постоји много различитих здравствених услуга. Поједине услуге спречавају проблеме, неке их дијагностикују, неке лече проблеме, а неке помажу људима на крају живота. Стотине различитих здравствених услуга могу се груписати у категорије, као што су превентивне услуге, дијагностичке услуге, услуге лечења, рехабилитационе услуге итд. (Olden, 2019). Ове категорије представљају континуум здравствене заштите који је координисан у циљу постизања што здравије популације (Tulchinsky & Varavikova, 2015). Слика 2 даје приказ континуума здравствене заштите.



Слика 2. Континуум здравствених услуга (адаптирано из: Tulchinsky & Varavikova, 2015)

Здравствене организације су, заправо, организације које пружају услуге из наведеног континуума. Оне се разликују по својој основној делатности, сложености, обиму и другим одредницама. Здравствена организација подразумева велики комплекс заинтересованих страна и учесника – добављача и клијената, регулаторних тела и директних пружалаца услуга, као и појединачних пацијената и њиховог доношења одлука.

Здравствене организације могу се класификовати према њиховој мисији, услугама које пружају и према томе да ли представљају јавно или приватно власништво. Здравствене установе у јавном власништву су обично владине које подржавају порези, за разлику од приватних здравствених организација које раде ван граница државне контроле и примају средства од пацијената и њихових полиса осигурања. Други начин за класификацију је заснован на њиховој финансијској класификацији – као профитне или непрофитне. Ипак, оба типа остварују приходе кроз здравствене услуге које пружају (Arias, 2021).

Здравствене организације се непрестано мењају услед технолошког напретка, старења популације, променљивих образаца болести као и нових открића у лечењу болести. Организационе промене су неопходне да би се постигле еволуирајуће друштвене норме и вредности, које носе већа очекивања за приступ здравственој заштити, побољшано искуство пацијената и повећано учешће пацијената у доношењу одлука о здравственој заштити (WHO, 2018).

Као нова тенденција намеће се увођење логике менаџерства у здравствену заштиту, што практично значи да би рад требало да организују и контролишу менаџери, како би се постигли организациони циљеви одрживе и ефикасне здравствене заштите. Здравствени радници више нису само једноставни пружаоци услуга, већ се од њих очекује да максимално документују свој рад, преузму одређене административне задатке и учествују у иницијативама за побољшање квалитета (Nilsen et al., 2020).

2.4.2. Дефинисање кључних стејкхолдера у здравственим организацијама и системима

Кључни актери су важни у здравству, као и у свим другим секторима. Главни стејкхолдери здравственог сектора су: лекари, медицинско особље, чланови одбора,

волонтери и донатори. Они представљају интерне стејкхолдере који се дефинишу као појединци који су посвећени пружању услуга у здравственом сектору или организацији.

Лекари играју кључну улогу у обезбеђивању адекватне здравствене заштите, али и у контроли растућих трошкова у здравству. Број особља у здравственој установи је условљен тиме да ли институција припада амбулантном или болничком типу здравствене организације. Сваки појединац особља у здравственој организацији игра важну улогу као интерни актер. Чланови одбора усмеравају организацију ка одрживој будућности усвајањем здраве, етичке и законске политике организационог и финансијског управљања, обезбеђујући да непрофитна организација има адекватне ресурсе да унапреди своју мисију. Волонтери и донатори су такође део категорије интерних стејкхолдера, због улагања у организацију свог времена и/или финансијских ресурса.

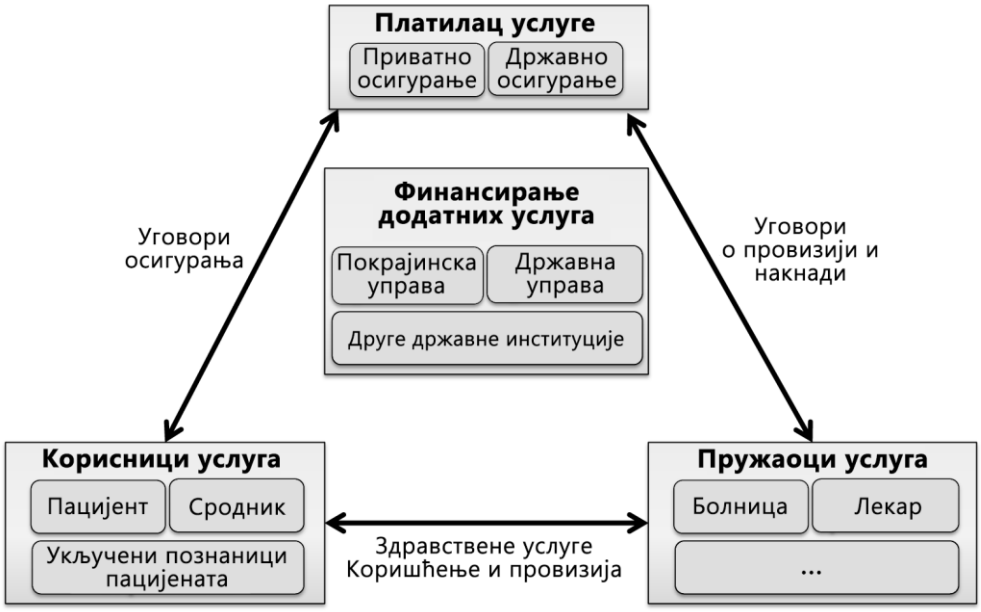
Кључни екстерни стејкхолдери обухватају пацијенте, осигуравајућа друштва, фармацеутске компаније и компаније за дистрибуцију лекова и медицинске опреме. Сектор здравствене заштите је заправо тржиште потрошача. Из тих разлога искуство пацијената је важно да здравствени системи односно организације привуку што већи број пацијената. Фармацеутске компаније обезбеђују неопходне лекове које лекари преписују својим пацијентима, док компаније за медицинску опрему доприносе тако што производе медицинску опрему коју лекари и особље користе у процесу пружања здравствених услуга. Осигуравајућа друштва доприносе као спољни актери, обезбеђујући здравствено осигурање за пацијенте, где пружаоци услуга добијају надокнаду за своје услуге.

Пацијенти и лекари представљају директну комуникацију интерних и екстерних стејкхолдера. Јединствени симбиотски однос је неминован јер ако спољни актери односно пацијенти не би тражили медицинску помоћ, потреба за лекарима не би постојала. Са друге стране, ако интерни актери – лекари не би постојали, пацијенти не би имали начин да се лече. Заправо, интерни и екстерни актери имају важну улогу у сектору здравствене заштите. Без комбинације сваког од њих, здравствена заштита не би била функционална. Успех у сектору здравствене заштите је директно повезан са виталном улогом свих стејкхолдера и савеза који су међу њима остварени (Nowak, 2021).

Effective Health Care Program Агенције за здравствена истраживања и квалитет (енг. *Agency for Healthcare Research and Quality*) дефинише стејкхолдере као особу или групу са сопственим интересом за одређену клиничку одлуку и доказе који подржавају ту одлуку. Ту спадају (Cottrell et al., 2014):

- пацијенти, пружаоци здравствене заштите и организације за заступање пацијената,
- клиничари односно медицински профеционалци и њихова професионална удружења,
- институционални пружаоци здравствених услуга, као што су болнички системи и медицинске организације,
- владине агенције,
- клијенти и платиоци, као што су послодавци и јавни и приватни осигуравачи,
- представници здравствене индустрије,
- креатори политике здравствене заштите на државном и локалном нивоу,
- истраживачи здравствене заштите и истраживачке институције.

Графички приказ главних стејкхолдера у здравственом сектору и њихов међусобни однос дат је на слици 3.



Слика 3. Однос између кључних стејкхолдера у здравственом сектору (адаптирано из: Görlitz, 2014)

3. ДИГИТАЛНИ ЗДРАВСТВЕНИ ЕКОСИСТЕМ

Дигитални екосистеми, аналогно биолошким екосистемима, су сложени и међузависни системи са сопственом инфраструктуром помоћу које сви елементи комуницирају и представљају целину која је самоорганизована, скалабилна и одрживог понашања (Li et al., 2012).

Стратегије многих организација подвргнуте су дигиталној трансформацији. Од суштинског је значаја да се успостави дигитални екосистем како би се побољшао учинак и помогле интеракције изван компаније. Дигитални екосистем омогућава организацији да фокусира своје ресурсе на омогућавање пословне вредности уклањањем свих недостатака које носе традиционалне *B2B* услуге. Заправо, дигитални екосистеми додају вредност односима са клијентима, помажући компанијама да доследно испуњавају уговорени ниво услуга и обезбеђују брзе акције уз ефикасно откривање очекивања (Brush, n.d.).

3.1. Дигитална трансформација и дигитална револуција у пословању

Под дигиталном трансформацијом се подразумева непрекидна повезаност свих области економије на начин на који се различити актери прилагођавају новим условима који преовлађују у дигиталној економији (Roland Berger Strategy Consultants, 2015).

Дигитална трансформација пословања омогућује компанијама континуитет, флексибилност, пренос знања и способност да се задовољи повећани обим потражње. Представља интеграцију дигиталних технологија у сва подручја пословања. Дигитална трансформација пословања превазилази једноставно покретање веб странице или присуство у друштвеним медијима. Заправо, дигитална трансформација је транскултурна промена која подстиче пословне организације и системе да измене традиционалне пословне процесе (Coté, 2020).

Дигиталне технологије односно обим и начин на који их користимо у свакодневном животу, послу и друштву несумњиво мењају организацију компанија. Темпо којим се напредак дигиталних технологија одиграва се све више убрзава и знатно је бржи од темпа трансформације у организацијама. Сам термин дигитална транформација није довољно прецизан. Можда је коректнији и конкретнији термин – дигитална пословна трансформација, што више одговара пословном аспекту. Термин дигитална трансформација се такође користи за промене у значењима које се не односе строго на пословни сектор већ подразумева и промене друштва у целини, владе, прописа и економских услова, што понекад може да буде отежавајући фактор трансформације. Сасвим је јасно да промене у друштву имају утицаја на организације и као такве могу бити врло инфлуентне када се на трансформацију гледа из холистичке перспективе. Ипак, ниједна компанија, индустрија, сектор, економски актер или стејкхолдер и подручје целокупног друштва не (по)стоји самостално.

Дигитална транформација представља процес у којем дигиталне технологије имају централну улогу у креирању и јачању турбулентних промена које се одигравају у индустријском сектору и друштву (Vial, 2019). Такве промене доводе до стратегијских одговора – да би остале конкурентне, компаније користе дигиталне технологије приликом стварања вредности. Како би се савладали изазови у процесу трансформације, компаније истовремено морају да спроводе и структурне промене, које могу да производе позитивне организационе ефекте, али могу да доведу и до нежељених резултата, као што су: смањење интерперсоналне комуникације, зависност од модерних технологија, крађа пословних података, скупе технологије и неопходна обука запослених, безбедност и приватност података итд.

Дигитална трансформација обухвата два елемента – дигиталну технологију и дигиталну иновацију (Kozarkiewicz, 2020). Из овог аспекта, дигитална трансформација може се представити као скуп промена у организацији које су изазване развојем дигиталних технологија, које укључују како коришћење тренутно доступних технологија са циљем унапређења постојећих процеса, тако и истраживање дигиталних иновација које потенцијално могу да доведу до промене пословног модела организације. Дигитална трансформација има значајан утицај не само на технологије које се већ користе, него и на стратегије, процесе, односе са потрошачима, ставове и очекивања запослених.

Циљ дигиталне трансформације није једноставно насумично додавање нових технологија у пословање, већ представља стратегију укључивања тих технологија на начин који ће крајњим корисницима донети већу вредност од постојеће.

Дигитална трансформација је другачија за сваку компанију, што у пракси значи да не постоји јасно дефинисана стратегија за њену имплементацију (Laoyan, 2022). У самом процесу имплементације, кључни су смисленост и систематичност. Први корак у дигиталној трансформацији јесте постављање глобалних циљева, што тимовима даје могућност избора одговарајуће стратегије и разумевање и дефинисање циља конкретног пројекта. У процесу имплементације, треба водити рачуна не само о утицају промена на потрошаче/кориснике, већ и на запослене који учествују у процесу. Спровођење великих промена у оквиру компаније може изазвати отпор запослених, па је веома битна добро дефинисана стратегија управљања променама. С друге стране, уколико се планирају промене које драстично утичу на потрошаче, добра стратегија је објављивање мањих, пробних верзија, да би се тестирала њихова реакција. На тај начин, могу се прикупити повратне информације у почетним фазама, што омогућава бољу идентификацију захтева потрошача и начина на који они могу бити задовољени. Евалуацију успешности примењене стратегије дигиталне трансформације најбоље је спроводити праћењем метрика пословног успеха, јер су некада крајњи резултати невидљиви за потрошаче – на пример, брже учитавање веб странице или краћа времена испорука производа.

O'Brien (2022) наводи да постоје 4 типа дигиталне трансформације:

- Трансформација процеса – фокусира се на промене које доводе до смањења трошкова и повећања операционе ефикасности пословања и подразумева податке, аналитику, вештачку интелигенцију итд.
- Трансформација пословног модела – односи се на фундаменталне промене у начину вођења пословања или организације и може обухватити запослене, процесе и технологије.

- Трансформација домена – прихватањем нових технологија, компанија може да прошири пословање на нову област у којој до сада није била присутна.
- Организациона/културална трансформација – подразумева редефинисање начина размишљања, процеса, способности и вештина тако да буду прилагођени новом, дигиталном окружењу.

Да би се разумео појам дигиталне револуције, мора се узети у обзир да се ради о процесу промена које друштво доживљава сваког дана. Појава најпре аналогних, па затим механичких, електронских и дигиталних технологија кроз процесе индустријских револуција, довела је до великих промена како у друштву, тако и у економији.

Трећа светска индустријска револуција донела је ширење дигитализације и аутоматизације помоћу електронских, телекомуникационих и информационих система и може се сматрати почетком дигиталне револуције (Schwertner, 2021). Под дигитализацијом се у овом случају подразумева чисто претварање података из аналогног у дигитални облик, омогућавајући аутоматизацију и бољу и лакшу доступност информација и докумената.

Даљи напредак технологије довео је до дигитализације организационих, односно пословних процеса, спајајући на тај начин физички свет са виртуелним технологијама. Сведоци смо тренутно Четврте светске индустријске револуције, или како се назива – Индустрија 4.0, која представља прелазак на дигитална, потпуно аутоматизована окружења и сајбер-физичке системе. Индустрија 4.0 обухвата много различитих технологија и иновација, које се примењују у бројним секторима (Paul, Riffat et al., 2021).

Дигиталну трансформацију, као саставни део Индустрије 4.0, карактеришу следећи принципи (Schwab, 2016):

- флексибилност, односно динамични пословни процеси,
- скраћење времена извршавања,
- прилагођавање купцима, у погледу планирања, конфигурације, поручивања, дизајна и производње,
- ефикаснији процеси и услуге као резултат анализе великих количина података,
- адаптивност у организацији, уместо формалне поделе посла.

Кључне технологије које Индустрија 4.0 обухвата су:

- *big data* аналитика,
- вештачка интелигенција и аутономни роботи,
- индустријски *IoT*,
- сајбер безбедност и сајбер-физички системи,
- симулација,
- адитивна производња,
- системска интеграција,
- *cloud* и мобилне технологије,
- проширена реалност.

Big data аналитика

Сам термин „*big data*" је почео да се користи за означавање великих количина података, које су толико обимне да управљање њима употребом класичних система за базе података постаје не само компликовано, већ и готово немогуће. *Big data* аналитика се односи на нову генерацију технологија, архитектуре и стратегија за прикупљање и складиштење великих количина података из различитих извора и њихову анализу великом брзином која не би могла да се спроведе помоћу традиционалних метода, а са циљем креирања нових извора пословних вредности.

Elgendy & Elragal (2014) наводе три главне карактеристике *big data* система, које се називају и *3V*:

- Обим (енг. *Volume*) – односи се на величину података и представља главну карактеристику *big data* система. Величина скупова података може да износи од неколико терабајта (TB) до чак више петабајта (PB).
- Разноврсност (енг. *Variety*) – велика обимност података највише потиче од великог броја извора података, који могу да обухватају и евиденционе датотеке, „веб клик" информације и друштвене мреже. Поред тога, постоје и информације које се прикупљају из аудио и видео извора, као и мултидимензиони подаци, који обезбеђују историјски контекст.
- Брзина (енг. *Velocity*) – означава брзину генерисања или испоруке података. Посебно је битна код садржаја који се у реалном времену преузимају са веб сајтова (енг. *streaming data*).

Неки аутори предлажу и четврту карактеристику *big data* система – тачност (енг. *Veracity*), и тиме допуњују модел на *4V*. Тачност се фокусира на квалитет *big data* података.

Вештачка интелигенција и аутономни роботи

Ribeiro (2021) дефинише вештачку интелигенцију као „комбинацију више технологија, које омогућавају софтверу и машинама да опажају, разумеју, реагују и уче самостално или да проширују људске активности".

Вештачка интелигенција, налик људској, има за циљ да помогне приликом решавања проблема различите природе. Ова технологија има велику могућност примене у роботизованим системима у производњи. Нове генерације аутономних робота које су опремљене напредним софтвером, вештачком интелигенцијом и сензорима, могу да препознају, анализирају и адекватно реагују на информације које добијају из окружења.

Уз помоћ машинског учења (енг. *machine learning*), различити фактори (као што су тип садржаја, методе производње, буџетска и временска ограничења) могу да се анализирају и искористе за даље унапређење алгоритама вештачке интелигенције. Применом у фабрикама, управљање осетљивим индустријским машинама добија могућност предикције отказа, како би администрација на време могла да рехабилитује опрему и избегне скупе непланиране застоје (Javaid et al., 2021).

Главне предности примене вештачке интелигенције у индустријској производњи су (Ribeiro, 2021):

- смањење грешака – интелигентни алгоритми, након одговарајућег програмирања, могу да извршавају задатке који су подложни људским грешкама, због независности од спољних утицаја,
- смањење трошкова – компаније могу да смање потребе за радницима, тако што ће увести у употребу роботизоване системе, где се људска интервенција захтева само за комплексне задатке. На тај начин се могу смањити финансијска издвајања за раднике, или они могу бити преусмерени на друга одељења у оквиру компаније,
- раст прихода – руководство компаније може да се фокусира на даље унапређење пословања, у условима где је смањен обим грешака а запослени фокусирани на обављање критичних процеса.

Индустријски *IoT*

Термин *IoT* (енг. *Internet of Things*) се односи на технологију повезивања на интернет уређаја који се користе у свакодневном животу, помоћу интеграције одговарајућих сензора. На тај начин, уређаји могу да прикупљају, размењују и обрађују информације из свог окружења, чиме се обезбеђује додатна вредност за кориснике.

Примена *IoT* технологије у индустријском окружењу назива се *IIoT* (енг. *Industrial Internet of Things*) и односи се на сензоре, инструменте и аутономне уређаје који су, путем интернета, повезани са индустријским апликацијама (AuraQuantic, n.d.). Овако креирана мрежа омогућава прикупљање, размену и анализу података, и има за циљ повећање ефикасности и безбедности, уз смањење трошкова.

Са сталним унапређивањем сензорске технологије, прикупљени подаци могу да се упарују са предиктивном аналитиком у реалном времену, вештачком интелигенцијом и машинским учењем, чиме се стиче бољи увид у функционисање машина и производних линија, и могу да се предвиде откази опреме и на време изврше превентивни сервиси. Велика предност примене ове технологије огледа се у могућности трансформације постојећих производних линија у тзв. „паметне фабрике", уз повећање производне ефикасности, мањи степен отказивања опреме, смањење трошкова што, с друге стране, доноси и предност за потрошаче, у виду бржег добијања квалитетнијих производа и услуга (Gilchrist, 2016).

Два највећа изазова примене *IIoT* технологије су (Smith, 2018):

- интероперабилност – уређаји и машине имају другачију архитектуру и користе различите протоколе. Ово може да се превазиђе имплементацијом одговарајућих *API* (енг. *Application Programming Interface*) интерфејса, где уређаји и машине могу да комуницирају путем *API* позива.
- безбедност – примена *IIoT* технологије значи и прелазак на *cloud* решења складиштења података, што са собом носи потенцијалне ризике од крађе података и сајбер напада, и може довести до прекида и застоја у производњи.

Сајбер безбедност и сајбер-физички системи

Раст захтева за коришћењем *cloud* рачунарства и сервиса базираних на интернету довео је до повећања потребе заштите компјутерских система од крађе и оштећења хардвера, софтвера или података, као и од прекида или неправилног рада услуга које пружају. Сајбер безбедност подразумева како контролу физичког приступа системском хардверу,

тако и заштиту од сигурносних ризика неовлашћеног мрежног приступа и извршавања нежељеног и малициозног програмског кода (Weallans, 2018).

Упоредо са ширењем употребе технологија које доноси Индустрија 4.0, сектор индустријске производње постаје све већа потенцијална мета за сајбер нападе, јер хакери, у случају успешног пробоја, путем мреже унутар компаније имају могућност да неовлашћено приступе како информационим, тако и операционим системима. Исти безбедносни ризици који постоје у класичким рачунарским мрежама су и овде могући: искоришћавање сигурносних „рупа", вируси, онемогућавање услуга мреже услед превеликог броја упита итд.

Безбедносни ризици са којима се организације сусрећу у ери Индустрије 4.0 су (Cybalt, n.d.):

- сваки повезан уређај представља потенцијални ризик,
- индустријски контролни системи су посебно рањиви на сајбер нападе,
- Индустрија 4.0 повезује системе који су до тада били изоловани, чиме се повећава обим потенцијалних напада,
- надоградње се због комплексности система често спроводе у етапама, остављајући поједине делове и даље рањивим на нападе,
- сектор производње има мање регулисаних стандарда усклађености од других,
- одвојени системи и изолована окружења отежавају могућност надгледања и заштите.

Симулација

Алати за симулацију у оквиру Индустрије 4.0 су намењени оптимизацији индустријских пословних процеса. Омогућавају креирање виртуелних процеса односно дигиталних копија техничких система из стварног света, унутар контролисаног и поновљивог окружења. Помоћу симулације је могуће идентификовати уска грла и оптимизовати производњу, анализирати критичне тачке у процесима, смањити време потребно за имплементацију и снизити трошкове, чиме пословање постаје конкурентније и отпорније на утицаје (AuraQuantic, n.d.).

Симулација омогућава евалуирање ефеката и утицаја акција у безбедном окружењу, чиме се повећавају ефекти учења и унапређује процес доношења одлука. Промене понашања у зависности од конфигурације машина, тока производње и дизајна постројења могу да се анализирају у симулираном окружењу, без потребе за извођењем акција у стварном свету. Симулациони модели су паметни, самокоративни, са могућношћу учења на основу анализе информација из претходних искустава. Такође, могу да се комбинују и са аналитичким системима, чиме се ствара могућност избора одговарајућих акција приликом доношења одлука, на основу резултата симулације (Ibrahim et al., 2020).

Адитивна производња

Адитивна производња је скуп производних технологија које омогућавају израду физичких објеката кроз процес генерисања и сукцесивног наношења слојева материјала (Bromberger et al., 2022).

Предности коришћења адитивне производње у оквиру Индустрије 4.0 су (ESA Automation, 2020):

- генерисање мање отпадног материјала – у односу на класичну производњу супстракцијом материјала (нпр. бушење или обрада на стругу), процес производње је обрнут, односно, производ настаје наношењем само потребне количине материјала у слојевима;
- скраћује се време израде прототипова и смањују трошкови – друге технике израде прототипова укључују веће трошкове материјала и прилагођавање производне опреме, док се у овом случају прототип веома брзо може креирати, тестирати и додатно усавршавати, уз готово тренутне увиде у начињене измене;
- промовише се дигитализација пословања – адитивна производња захтева сталну комуникацију између уређаја, машина и робота, тако да компанија мора улагати у модерне дигиталне технологије;
- синтетише се процес склапања производа у један део – време потребно за склапање односно монтирање финалног производа је знатно скраћено, јер се група делова може произвести у једном комаду.

Системска интеграција

Хоризонтална и вертикална интеграција промовишу стварање ланаца колаборативних система, који могу укључивати различите комбинације делова и одељења као што су инжењеринг, производња, маркетинг, добављачи итд. Постоје категорије интеграције система (Vaidya, 2018):

- хоризонтална интеграција дуж целе мреже креирања вредности,
- вертикална интеграција и умрежени производни системи,
- *end-to-end* инжењеринг током целог животног циклуса производа.

Хоризонтална интеграција односи се на повезивање различитог софтвера и хардвера који се користе у производњи, без обзира на број различитих добављача опреме и апликација. Ово пружа могућност паметним фабрикама да динамички одговарају на нове производне захтеве и врше предиктивно одржавање. Код произвођача који имају више производних постројења, хоризонтална интеграција укључује и координацију производног процеса између њих (Buchberger, 2021).

Вертикална интеграција се односи на интеграцију система на различитим хијерархијским нивоима у организацији, од производње до менаџмента. Укључује повезивање свих пословних јединица и процеса унутар организације, односно свих слојева. Код ове интеграције, подаци теку између свих пословних јединица и свима су на располагању. Први корак је дигитализација физичких објеката у производном погону помоћу сензора, актуатора и *PLC* (енг. *Programmable Logic Controller*) контролера. Подаци се затим прикупљају помоћу *SCADA* (енг. *Supervisory Control And Data Acquisition*) система и прослеђују у софтвер за извршавање производње *MES* (енг. *Manufacturing Execution System*) (операциони слој), ради контроле и оптимизације производних радних токова. Резултат у виду информација о статусу производње се шаље у *ERP* (енг. *Enterprise Resource Planning*) систем (корпоративни слој). Сваки од наведених система има своје техничке специфичности, и пре појаве Индустрије 4.0 компаније су их најчешће набављале и имплементирале не водећи рачуна о

потенцијалним будућим интеграцијама. Различите софтверске архитектуре отежавају имплементацију концепата Индустрије 4.0, па избор одговарајућих информационих система за вертикалну интеграцију захтева јасан модел усвајања нових технологија (Tabim et al., 2021).

Cloud и мобилне технологије

Cloud рачунарство описује начин складиштења и приступа подацима, софтверу и сервисима на удаљеним серверима, путем интернета. Тиме је компанијама омогућено да користе јаке компјутерске ресурсе, без потребе за поседовањем самог хардвера. Главне карактеристике *cloud* система су: скалабилност, брзина, исплативост и складишни простор.

Cloud рачунарство представља основу за примену других савремених технологија попут вештачке интелигенције, машинског учења, *IoT* система итд. У паметним фабрикама, где се генеришу велике количине података, *cloud* пружа могућност њиховог складиштења и коришћења од стране свих система који учествују у компанији, и чије одлуке зависе од сталне расположивости неопходних информација.

Пружаоци *cloud* услуга користе један од следећих модела (Buchberger, 2021):

- *SaaS* (енг. *Software as a Service*) – корисник плаћа пружаоцу услуге за коришћење *cloud*-базираног софтвера;
- *PaaS* (енг. *Platform as a Service*) – корисник плаћа пружаоцу услуге за коришћење ИТ ресурса и инфраструктуре која им је потребна за развој, извршавање и контролу сопствених апликација;
- *IaaS* (енг. *Infrastructure as a Service*) – корисник плаћа пружаоцу услуге за коришћење и складишни простор који им је потребан за смештање сопствених платформи.

Нови трендови показују да корисници желе да имају прилагођене производе, мобилне индустријске апликације и флексибилне производне линије. До сада су се ови сервиси испоручивали путем класичних, жичних комуникационих канала, али присуство сензора, дронова, робота и бројних нових уређаја захтева бежичну комуникацију напредних карактеристика. Ове потребе се могу задовољити применом *5G*, а у скоријој будућности и већ најављене *6G* комуникационе мреже. За *5G* и наредне мреже се очекује да обезбеде готово тренутно повезивање и веома поуздану конекцију са изузетно малим вредностима латенције (Tsaramirsis, 2022).

Проширена реалност

Проширена реалност је технологија која премошћава јаз између физичког и дигиталног света додавањем, односно, преклапањем информација и виртуелних слика преко физичког објекта.

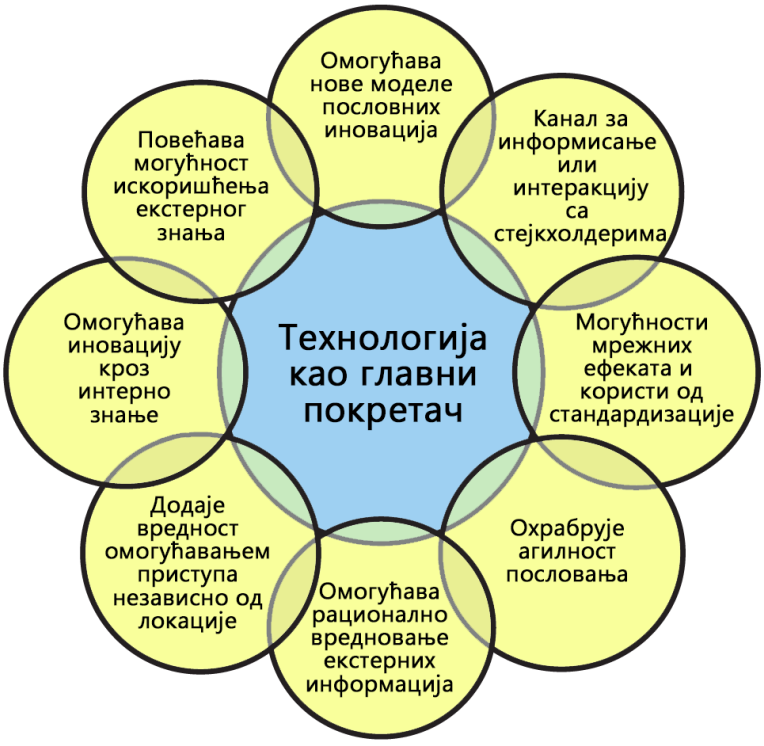
Начини за имплементацију ове технологије су (Weallans, 2018):

- на мобилним телефонима/таблетима – када се мобилни телефон или таблет са активираном камером упери према одређеном предмету, на екрану се преко слике приказује дигитални слој са додатним информацијама о посматраном објекту, који укључује текстуалне и графичке податке, кључне индикаторе перформанси, шематске приказе итд.,

- носиви уређаји за помоћ у реалности – пример су *Google Glass* наочаре, код којих се на стаклу испред једног ока пројектује компјутерски екран са тренутним информацијама,
- носиви уређаји за проширење реалности – најчешће у облику наочара које покривају већину видног поља корисника, и приказују кључне индикаторе перформанси, графичке и текстуалне информације, моделе дигитално клонираних објеката из стварног света итд.

У производној индустрији, проширена реалност подржава напредни облик аутоматизације и налази примену у процесима као што су: одржавање опреме, дизајнирање производног процеса, просторно рачунарство, логистика, монтажа, комуникација између одељења и запослених за решавање проблема, контрола квалитета, обука запослених, експертска корисничка подршка итд.

На основу приказаних технолошких решења Индустрије 4.0, може се закључити да је технологија главни покретач дигиталне трансформације, као и различитих предности које организације и компаније могу остварити њеним увођењем у своје стратегије пословања (Kraus et al., 2021). На слици 4 је дат графички приказ предности које могу бити остварене.



Слика 4. Предности увођења технологије у пословне стратегије (адаптирано из: Kraus et al., 2021)

Практично посматрано, у светлу е-пословања, дигитални екосистеми су заправо повезани са пословним екосистемима, платформским екосистемима и платформском економијом. Овај став деле и аутори као што су Valdez-De-Leon (2019), Bygstad и Dulsrud (2020), Koch и сар. (2022).

Дигитални екосистем подстиче сарадњу изградњом мрежних ефеката којим се постижу повезивање потрошача и добављача средстава. Поред заједничке (дигиталне) платформе, сарадња чини саставни део дигиталног екосистема (Koch et al., 2022).

3.2. Изазови дигитализације здравствених екосистема

Дигитална трансформација здравства се у различитим деловима света другачије спроводи и генерално је више заступљена у приватном сектору него државном. Приватни сектор здравства углавном има већа финансијска средства на располагању, а менаџмент и запослени показују већу спремност за веома обимне промене које дигитализација носи са собом.

Lennon и сарадници су 2017. године у Великој Британији спровели студију и идентификовали факторе од значаја за прихватање дигитализације здравства. То су: клиничко одобрење, истакнути промотери дигиталног здравства и друштвена и професионална спремност. Као фактори који негативно утичу наводе се: недостатак ИТ инфраструктуре, неизвесност управљања информацијама, недостатак подстицаја за давање приоритета интероперабилности, недостатак предности у погледу одговорности у комерцијалном сектору и тржиште које се доживљава као компликовано за управљање.

Дигитално здравство је веома брзо растућа област медицине која се највећим делом ослања на здравствене податке пацијената. Здравствени подаци се прикупљају помоћу дијагностичких уређаја којима управљају здравствени радници у клиникама, по установљеном протоколу. Мобилно здравство, телемедицина, паметни уређаји повезани на интернет постају све више избор за прикупљање здравствених података пацијената. Са напретком технологије, долази до минијатуризације здравствене опреме, али и ширења примене на свакодневне уређаје као што су паметни телефони и носиви уређаји опремљени одговарајућим сензорима, помоћу којих пацијенти сами могу да прикупљају своје податке код куће. Сви ови уређаји генеришу велике количине медицинских података, које примена *cloud* рачунарства, *big data* аналитике, вештачке интелигенције и других модерних технологија у здравству може да искористи за ефикасније праћење тока болести и прилагођене третмане лечења пацијената (Manteghinejad & Javanmard, 2021).

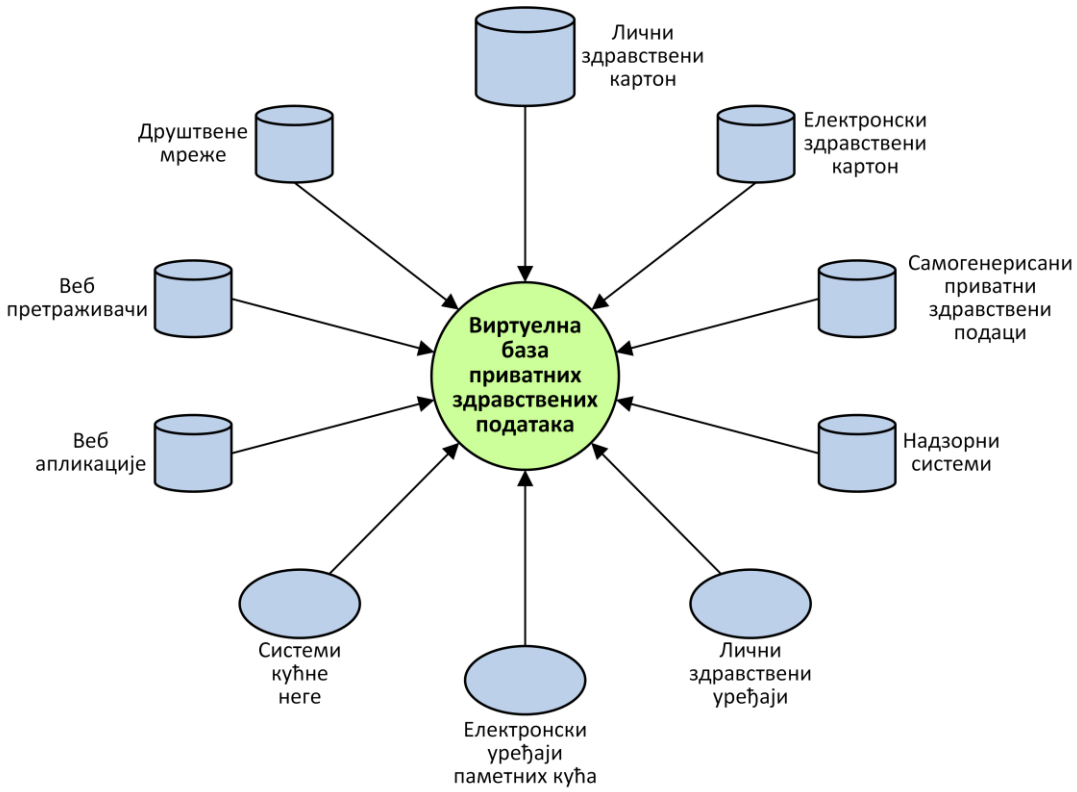
Као изазови процеса дигитализације здравственог сектора наводе се (Kaur, 2021):

- Приступ здравственим подацима је углавном веома компликован. Без обзира на чињеницу да велики број пружалаца здравствених услуга има имплементирану неку врсту система за електронски запис медицинских података о пацијенту, потребно је уложити још пуно средстава и времена како би подаци били лакше доступни, као и интероперабилни.
- Медицински подаци о пацијентима нису конзистентни између различитих здравствених установа. За пружаоце здравствених услуга, недостатак ефикасног електронског приступа медицинским подацима о пацијентима значи и ограничену количину информација приликом лечења. За пацијенте, недостатак обједињеног приступа сопственим медицинским подацима значи и ограничење могућности једноставне промене здравствене установе у којој се лече, а у циљу проналажења јефтиније услуге.

- Забринутост за приватност података о пацијенту. У случајевима лонгитудиналних медицинских података који су ускладиштени у различитим здравственим центрима и ИТ системима, постоји забринутост за безбедност и приватност информација о пацијентима приликом њиховог преноса између установа и њихову могућу рањивост на сајбер нападе.
- Финансијска ограничења за развој. Имплементација дигиталне трансформације здравственог сектора се не односи само на набавку најновијег ИТ система већ подразумева и велика улагања, како за технологију тако и за запошљавање довољног броја стручних лица.
- Закони који још увек нису прилагођени за регулисање организационе бриге која се односи на одговорност везану за пружену негу као и на аутономију пацијената. У скоријој будућности се очекује све већа примена предиктивних система базираних на вештачкој интелигенцији. Када установа почне да користи такву врсту система, неопходно је да буде законски јасно дефинисана медицинска одговорност (на пример: у случају да систем направи грешку на штету пацијента, да ли је одговоран лекар, установа која је увела ту технологију, компанија која је развила технологију итд.). Пацијенти морају бити информисани о технологији како би могли да доносе одлуке о начину свог даљег лечења.
- Организациона спремност. Због свог специфичног начина функционисања, за здравствени сектор се не очекује да процес дигитализације буде брзо и једноставно имплементиран. Између осталог, постоје и проблеми у виду отпора (културолошког и у начину размишљања) према новим технологијама, чије превазилажење захтева средства и време. То се може постићи обукама запослених и спровођењем кампања од стране надлежних државних здравствених институција, како би се свест пацијената усмерила ка подржавању нових технологија, кроз јасно наглашавање предности које модернизација здравства доноси.

Модеран дигитални здравствени екосистем треба да прикупља медицинске податке пацијената не само у току лечења, приликом њиховог боравка у здравственим установама, већ и када су они здрави, у смислу превенције и подизања свести о сопственом здрављу, формирајући на тај начин виртуелне, обједињене дигиталне картоне. С обзиром на то да се приватни здравствени подаци пацијената прикупљају из различитих извора, који укључују и социјалне мреже, паметне телефоне, носиве уређаје, системе надзора и комерцијалне апликације (слика 5), Ruotsalainen и Blobel (2022) као кључне изазове за дигитализацију здравства наводе сигурност, приватност и поверење, који могу бити сагледани из више перспектива, као што су:

- Екосистем. Екосистем комбинује различите стејкхолдере, који имају своје бизнис моделе и политике сигурности и приватности. То отежава кориснику сервиса екосистема да зна која се правила безбедности и приватности примењују, када и ко користи њихове приватне здравствене податке, и како се контролише њихово разоткривање. Такође, пошто се здравствене информације које се користе у екосистему прикупљају из пуно различитих извора, питање које се намеће јесте власништво над њима, где организације често себе сматрају власницима података које су генерисали (Evans, 2017). Наведени проблеми отежавају управљање власништвом над подацима и приватношћу у екосистемима.



Слика 5. Извори приватних здравствених информација (адаптирано из: Ruotsalainen & Blobel, 2022)

- Субјект извора података. Пре откривања својих здравствених података неком од стејкхолдера у екосистему, пацијент мора да верује да су у потпуности имплементирани сви неопходни захтеви безбедности и приватности, прописани од стране законодавних тела земље у којој живи. Одлука о откривању сопствених података често није резултат слободне воље, јер пружаоци услуга често прикупљају бихевиоралне податке о корисницима помоћу „обавезних" колачића (енг. *cookies*) на својим веб сајтовима (Waldman, 2018). Пример је *big data* окружење, где пацијентов пристанак често није довољан да се заштити приватност здравствених података, јер на њу утичу и одлуке других страна (Evans, 2017).
- Модели приватности и поверења. Истраживања су показала да је немогуће измерити ризике приватности, па се често перцепција мишљења користи као замена за стварне ризике. У пракси, перцепцију често чине убеђења или туђа мишљења. Приватност, као приступ контекстуалног интегритета, је често недовољан, јер контексти у здравственим екосистемима углавном немају јасне границе, и правила приватности су често дефинисана од стране стејкхолдера, а не од корисника тј. пацијената. Слично је и са поверењем, које је често само мишљење, тако да је подједнако непоуздано као и приватност.
- Законске регулативе. Постојеће законске регулативе о заштити података прописују стејкхолдерима који учествују у екосистемима како се здравственим информацијама приступа, као и како се имплементирају и обрађују. Међутим, не постоји законска обавеза да се пацијентима објасни како се ово спроводи и који се тачно механизми заштите користе (Sanchini & Marelli, 2020).

- Архитектурни, безбедносни и рачунарски изазови. Унутар екосистема, приватни здравствени подаци су криптовани. Та чињеница отвара питање начина претраге криптованих података и безбедног управљања кључевима неопходним за енкрипцију/декрипцију. Корисници екосистема најчешће не припадају истом домену, и потребна су им различита права приступа здравственим подацима. Такође, неопходно је гарантовати и дугорочну расположивост и интегритет приватних здравствених података. *Cloud* базирани системи често користе виртуализацију, односно више корисника користи апликације које се извршавају на истом хардверу, тако да постоје ризици везани за сигурност и приватност, како саме инфраструктуре, тако и корисника (Ren et al., 2012).
- Услуге стејкхолдера. Истраживачким и комерцијалним организацијама које нуде системе базиране на вештачкој интелигенцији и машинском учењу се приватни здравствени подаци често шаљу без енкрипције, ради анализе и предикције. Ово ствара забринутост по питању безбедности и поверења. Такође, медицинска истраживања су често мултидисциплинарна и интернационална, па је тешко пратити ко су ауторизовани корисници, колико су безбедни информациони системи које користе и како се управља питањима приватности здравствених података (Yu et al., 2018).

Ефекти које дигитализација здравства доноси су (Bocas, 2022):

- Дигитална револуција доноси нове начине да се контактирају лекари и пацијенти.
- Нове технологије ће утицати на начине дељења здравствених информација и интеракције између лекара и пацијената.
- Пацијенти ће моћи безбрижно да деле своје медицинске информације од куће, а лекари ће моћи да им приступају једноставно, без обзира где се тренутно налазе, уз помоћ паметног телефона, таблета или персоналног рачунара.
- Медицински подаци ће постати глобални ресурс расположив свима, што ће пацијентима омогућити контролу сопствених здравствених одлука путем паметног телефона или таблета.
- Лекари ће користити нове технологије за унапређење интеракција са пацијентима, смањујући баријере на релацији лекар-пацијент, тако што ће им омогућити да приступају својим медицинским картонима путем паметних мобилних телефона.

Концепт дигиталних здравствених решења олакшава прилагођавање системских здравствених технологија, стављајући пацијенте у центар. У здравственом сектору, дигитални здравствени екосистем производи ефекте као што су (TIGA Healthcare Technologies, n.d.):

- стварање услова за опоравак код куће, лако управљање хроничним болестима и оснаживање пацијената,
- помоћ да се економски одржи напредни квалитет здравствених услуга,
- помоћ у борби против нерационалних трошкова здравствене заштите,
- сигурност да се токови рада и процеси здравствене заштите нуде у оквирима потребног квалитета, приступа и сигурности.

Дигиталне здравствене системе могу користити стејкхолдери у здравственом сектору у континуираном пружању здравствене заштите – од превенције до дугорочних лечења

болести и као катализатор промена у подршци пружања квалитетних здравствених услуга. Оваква стратегија повећава потенцијал за постизање универзалног здравственог осигурања. Влади и креаторима здравствене политике даје се могућност приступа подацима из популације који су неопходни за активирање прилагођених програма превенција и доношења информисаних одлука о здравственом систему. С друге стране, здравствени радници могу ефикасније да пружају медицинске услуге користећи релевантне информације и дигиталне алате за побољшање пружања здравствене заштите уз прилагођене програме обуке. Предности које дигитални здравствени екосистем даје пацијентима јесте да они постају значајан фактор, да их подстиче да остану здрави, управљају својим подацима о болестима и да чешће користе услуге здравствене заштите (Broadband Commission, 2018).

3.3. Концептуалне основе дигиталног здравственог екосистема

Дигитални здравствени екосистеми унели су револуцију у здравство – фокус је стављен на пацијенте, који су охрабрени да прате, управљају и унапређују своје лечење, што их чини информисаним, независним и захтевним. С друге стране, пружаоци здравствених услуга имају могућност да креирају персонализоване планове лечења и лекове. Дигитални здравствени екосистеми, као спој информација, технологија, људи и могућности повезивања, представљају будућност здравства. Потребно је направити дистинкцију између појмова е-здравства (које је организацијски усмерено, и подржава клиничко доношење одлука, уз помоћ нпр. електронских медицинских картона) и дигиталног здравства (које је пацијент-центрично, нудећи нпр. здравствене апликације за самостално праћење стања хроничних болести) (Deetjen et al., 2020). На слици 6 је графички приказана разлика између ова два појма.

Слика 6. Е-здравство и дигитално здравство (адаптирано из: Deetjen et al., 2020)

Нови дигитални екосистем довео је до повећаног нивоа интеракције између корисника здравствене заштите и пружалаца услуга. Дигитална здравствена решења постају нова норма доносећи промене односа у новом систему (Sinhasane, 2020):

- Однос клијената и пружалаца услуга. Размена података путем дигиталних решења повећала је интеракцију између клијената и пружалаца услуга, осигуравајући прилагођена примарна и не-примарна медицинска решења.
- Форме за пружање услуга основне здравствене заштите. Пружаоци услуга здравствене заштите, дијагностичке службе и апотеке чине окосницу компоненте означене као пружалац услуга. Нови екосистем нуди размену података у реалном времену, осигуравајући тачну испоруку услуга.
- Однос између корисника и више тачака. Иако је нови екосистем претежно дигитализован, корисници остају главни ентитет. Примарни циљ ове дигитализације здравствене заштите је промовисање једноставне и сигурне интеракције између различитих корисника система, укључујући лекаре, апотеке, осигуравајућа друштва и клијенте односно пацијенте.

Прелазак на Здравствену Индустрију 4.0 (енг. *Healthcare Industry 4.0*) подразумева електронску медицинску документацију, дигитализацију података о пацијентима, базе података, мобилни интернет, *IoMT* (енг. *Internet of Medical Things*), *big data*, здравствену вештачку интелигенцију, *machine learning* и *blockchain* (Agarwal et al., 2020; Sarwal et al., 2021).

Актуелни тренд у дигиталним решењима за здравствени сектор је прелазак са сегментираних услуга на интегрисане услуге које пружају више стејкхолдера путем технолошких платформи екосистема (Marcos-Pablos et al., 2019).

Дигитализација здравства отворила је врата за употребу нових технологија као што су (Iberdrola, n.d.):

- *Internet of Things* (*IoT*) односно *Internet of Medical Things* (*IoMT*). Омогућује помоћ у прилагођавању здравствене заштите, уштеди трошкова, смањењу вероватноће погрешне дијагнозе и скраћивању времена чекања.
- *Big data* аналитика. Анализа макро података омогућава прилагођене третмане и помаже у откривању фактора ризика и потенцијалних нежељених ефеката лекова.
- Вештачка интелигенција. Вештачка интелигенција може помоћи здравственим радницима да донесу исправније одлуке и пруже бољи третман.
- *Blockchain.* Омогућава безбедан приступ здравственом картону пацијента, што чини администрацију ефикаснијом и безбеднијом. Такође омогућава фармацеутској индустрији вођење прецизније евиденције у процесу производње лекова.
- 3Д и 4Д. Употреба 4Д прегледа у ултразвучној дијагностици даје нпр. прецизнији увид у структурни и функционални развој нервног система фетуса.
- *Chatbots*. Ова алатка омогућава брзу и директну комуникацију на релацији лекар-пацијент.
- Виртуелна реалност. Предности које даје технологија виртуелне реалности огледају се нпр. у помоћи рехабилитацији пацијената и лечењу психолошких поремећаја.

Једна од дефиниција дигиталног здравственог екосистема првенствено се фокусира на стејкхолдере, услуге и активности унутар екосистема и дефинише га као дигитални ланац здравствених радника и здравствених установа, који пружају клиничке услуге (превенција, лечење, дијагностика, опоравак) и активности подршке пацијентима (апотека, лабораторија) (Isakovic et al., 2015).

Архитектура дигиталног здравственог екосистема одређује технолошке интеракције које управљају разменом између две стране. *Cloud computing* је често неизоставни оквир за пружање здравствених услуга пацијентима или складиштење, дељење и анализу здравствених података у оквиру дигиталног здравственог екосистема (Hein et al., 2019; Witte, 2020). Други кључни елемент су скалирање/мрежни ефекти који описују скалирање међузависних група заинтересованих страна, како би се омогућили позитивни мрежни или екстерни ефекти (Fürstenau et al., 2019; Witte, 2020).

Инфраструктура дигиталног здравственог екосистема је стабилно језгро архитектуре екосистема. Састоји се од три елемента: софтвера, комуникационе мреже и хардвера. Комуникацију унутар дигиталног здравственог екосистема углавном омогућавају технологије засноване на интернету, нпр. алат за управљање и прегледање заснован на вебу или мобилно повезивање нпр. за коришћење мобилних података за апликације м-здравства, од којих свака укључује различите протоколе (Denoo & Yli-Renko, 2019; Witte, 2020).

У дигиталном здравственом екосистему изузетно важан аспект је приватност и безбедност платформи. Регулација и политика управљања здравственим подацима су предмет интензивних расправа. Евидентни проблем је ко треба да преузме чување података, чак и када су прикупљени подаци јавни или де-идентификовани. Иако је пристанак пацијената потребно добити кад год је то могуће да би се заштитили подаци, забринутост за њихову сигурност је истакла важност овог проблема од стране свих стејкхолдера у области здравства у погледу управљања безбедношћу и власништвом над информацијама (Filkins et al., 2016).

Дигитални здравствени екосистем има следеће карактеристике (Kaur, 2021):

- аутоматско управљање подацима пацијената и запослених,
- висока компетентност у здравственом сектору,
- унапређени комуникациони канали за бољу интеракцију пацијената, пружалаца здравствене заштите и других партнера екосистема,
- унапређене могућности за негу на даљину, како би се обезбедио континуитет пословања у условима спречености доласка у ординацију или услуга по позиву за пацијенте,
- брзо дијагностиковање и брже лечење за висок ниво задовољства пацијената,
- смањен ризик од људских грешака и побољшана укупна брига о пацијентима,
- развијене *big data* стратегије за омогућавање персонализованих прогностичких и дијагностичких налаза.

4. ЗНАЧАЈ САЈБЕР СИГУРНОСТИ У ЕЛЕКТРОНСКОМ ПОСЛОВАЊУ ЗДРАВСТВЕНИХ ЕКОСИСТЕМА

Информациона безбедност обухвата технике и методе чувања података од неовлашћеног приступа, откривања, употребе, модификације и деструкције (Barrett et al., 2020). У данашње време, већина савремених пословних података се налази у електронском облику на серверима, десктоп рачунарима, лаптоповима или у *cloud*-у, али смо сведоци да и даље постоје папирне форме докумената које садрже поверљиве податке. Информациона безбедност се брине о томе да подаци, неовисно од начина њиховог чувања, буду безбедни.

Кључни концепти успешне заштите информација су (Holmes, 2022):

- Поверљивост – заштита приступа подацима од стране било ког неовлашћеног лица.
- Интегритет – одржавање и обезбеђивање тачности и потпуности података током целог животног циклуса, што у пракси значи да неовлашћена лица не могу и не смеју да мењају податке.
- Доступност – могућност приступа и коришћења података када год је то потребно.

Ова три принципа заједно чине *CIA* (енг. *Confidentiality, Integrity, Availability*) тројство и представљају основу информационе безбедности сваке организације (слика 7).

Слика 7. *CIA* тројство као основа безбедности (адаптирано из: Kelley, 2023)

4.1. Појам и значај сајбер сигурности

Рапидна имплементација напредних информационих, комуникационих и сензорских технологија има огроман ефекат на економију, индустрију, функционисање државних институција, али и на свакодневни живот људи. Технолошки напредак доноси све већи број услуга и онлајн сервиса електронске управе, бржу и лакшу испоруку добара, роботизована постројења и дронове, аутономна возила, али и примену у области безбедности, транспорта, персонализованог здравства итд. Милијарде уређаја су

тренутно повезане на интернет, а процењује се да ће до 2025. године тај број достићи један трилион, спајајући на тај начин физичке и виртуелне светове. Све лакши приступ онлајн информацијама мења начин на који људи живе, раде и доживљавају окружење, јер се све више ослањају на информационе и комуникационе технологије, сензорску технологију, изворе података. Безбедност ових система представља велики изазов модерног друштва (Tagarev et al., 2017).

Сајбер безбедност је умеће заштите мрежа, уређаја и података од неовлашћеног приступа или криминалне употребе као и пракса обезбеђивања поверљивости, интегритета и доступности информација (CISA, 2019).

Бројни аутори су давали детаљније дефиниције сајбер сигурности. Schatz и сарадници (2017) су дали једну од најкомплекснијих и најсвеобухватнијих. Сајбер сигурност дефинишу као приступ и акције повезане са процесима управљања безбедносним ризицима које спроводе организације и државе да заштите поверљивост, интегритет и доступност података и средстава која се користе у сајбер простору. Концепт укључује смернице, акционе планове и регистре ризика/заштите, технологије, алате као и обуку за пружање најбоље заштите сајбер окружења и његових корисника.

У табели 2 је дат приказ кључних карактеристика односно разлике између сајбер сигурности и информационе сигурности.

Табела 2. Поређење сајбер сигурности и сигурности информација (адаптирано из: Simplilearn, 2022)

Сајбер сигурност	Информациона сигурност
Штити податке у сајбер простору	Омогућава сигуран пут до информација
Ризици укључују нежељени софтвер и мрежне нападе	Штити од дезинформација
Обезбеђени подаци помоћу енкрипције	Узима у обзир усклађености и политике

Потребно је споменути и појмове *cloud* и мрежне сигурности. Сигурност у *cloud*-у и мрежи су два најважнија аспекта заштите и сигурности података. Они укључују шифровање и друге безбедносне мере за заштиту података од приступа неовлашћених особа.

Cloud безбедност означава заштиту онлајн података ускладиштених на *cloud* платформама од крађе, цурења и брисања. Практично је то ситуација да само овлашћена лица могу да приступе подацима и да су сви подаци ускладиштени у *cloud*-у шифровани. *Cloud* безбедност је веома битна карактеристика већини корисника који су забринути за сигурност својих података, ускладиштених онлајн на некој од *cloud* платформи. Људи често сматрају да су њихови подаци безбеднији на личним, локалним серверима, где имају осећај веће контроле. Подаци ускладиштени у *cloud*-у могу бити чак и безбеднији, јер провајдери *cloud* услуга имају напредне сигурносне технике и њихови запослени су стручњаци у области информационе заштите. Злонамерни софтвер и социјални инжењеринг, као искоришћавање слабости људи да би се добио приступ њиховим личним информацијама, представљају претњу за сваку врсту складишног система, али

су генерално локални подаци рањивији, јер особе задужене за управљање њима најчешће имају мање искуства у препознавању безбедносних претњи (Frankenfield, 2022).

С обзиром на то да су *cloud* окружења веома комплексна, изложена су широком спектру могућих сајбер претњи, па је готово немогуће креирати једно безбедносно решење које би штитило од свих врста напада. Већина сигурносних сервиса је усмерена на специфичне врсте напада. Неки од најчешћих типова *cloud* сигурносних сервиса су (Bonuccelli, 2022):

- Превенција губитка података. Због огромних количина података који се складиште и генеришу у *cloud* сервисима, као и бројних апликација и уређаја који им приступају, постоје велике шансе за њихов губитак. Сервиси за превенцију губитка података могу да детектују осетљиве информације (кредитне картице, матични бројеви итд.) и да спрече да се неовлашћено открију.
- Управљање идентитетима и приступом. Према врсти корисничког налога, одређује се право приступа ресурсима на *cloud*-у као и активности које су дозвољене.
- Имејл безбедност. Корисници су честа мета сајбер напада, јер представљају најслабију карику у сигурносном ланцу. С обзиром да готово сви користе имејл, напади путем овог канала комуникације могу значајно компромитовати *cloud* окружење – нпр. да се придобију администраторска права приступа.
- Веб безбедност. Повећана употреба *cloud* сервиса значи и много већи број веб конекција и проток информација, чиме се отварају додатни ризици за сајбер нападе. Веб сигурносна решења нуде администраторима обезбеђење тих конекција и заштиту од потенцијалних напада.
- Детекција упада. Ови сервиси врше надгледање долазног и одлазног саобраћаја у потрази за сумњивим активностима и потенцијалним сајбер нападима. Детектовањем сајбер напада пре него што се искористе рањивости система, компаније могу да заштите своје пословне податке.

Мрежна сигурност представља заштиту мреже од неовлашћеног приступа, укључујући обезбеђивање да само овлашћени корисници могу приступити мрежи и да су сви подаци који пролазе кроз мрежу шифровани. Безбедност мреже такође укључује заштитне слојеве који блокирају неовлашћени приступ мрежи (White et al., 2017; Kumar & Goyal, 2019; Simplilearn, 2022).

Постоје четири уобичајена типа мрежне сигурности (Clancy, 2022):

1. Заштитни зид (енг. *Firewall*) – представља хардверски уређај или софтверски алат за контролу саобраћаја између мрежа и заштиту од спољних претњи.
2. Мрежна сегментација – процес дељења мреже у мање сегменте, ради веће сигурности, бољих перформанси и изоловања појединих делова.
3. *VPN* (енг. *Virtual Private Network*) – служи за безбедан удаљени приступ приватним мрежама. *VPN* користи енкрипцију да се заштити конекција између корисника и приватне мреже.
4. Имејл заштита – вид заштите имејл порука од пресретања и приступа од стране неовлашћених лица помоћу енкрипције, аутентификације и онемогућавања извршавања нежељеног софтвера.

Сајбер сигурност може да се примењује на различите контексте, од економског до примене мобилне технологије и укључује (Giansanti & Monoscalco, 2021; Giansanti, 2021):

- безбедност мреже (поступци за безбедно коришћење мреже),
- безбедност апликација (решења за безбедно коришћење апликација),
- информациона безбедност (управљање информацијама на безбедан начин који обезбеђује приватност),
- оперативна сигурност (сигурност у ИТ операцијама и трансакцијама),
- обезбеђивање континуитета рада (процедуре за поновно покретање система након проблема који су нарушили рутински рад система као и процедурални процеси за обезбеђивање континуитета рада),
- обука крајњих корисника (специфична обука за актере).

Информациона безбедност, која је више технички фокусирана, је у широкој употреби у рачунарској науци већ дуги низ година. Али, како живимо у дигиталном свету, питање сајбер сигурности је постало друштвена брига и одговорност (Veale & Brown, 2020). Сајбер сигурност је глобални феномен који представља сложен друштвено-технички изазов за органе управљања, али захтева учешће појединаца. Нарастајућа потреба за сајбер сигурношћу је услед све већег продора и наше зависности од информационих и комуникационих технологија у свим аспектима сајберфизичког друштва. Од суштинског је значаја за појединце, организације, и друштво у целини. Питање безбедности није ограничено на извршну власт, већ је такође релевантно за политичке странке, добављаче енергетске инфраструктуре, одборе, органе управљања, министарства, административне организације, невладине организације, здравствене организације, па чак и спортске организације. Из овога произилази да нарушавање сајбер безбедности утиче на све стејкхолдере у нашем друштву (de Bruijn & Janssen, 2017).

Релевантни оквири за сајбер сигурност базирани су, пре свега, на степену ризика. Да би се овде постигла скалабилност, захтевани ниво заштите се дефинише за сваку категорију података који се обрађују, у зависности од сврхе анализе. Ови нивои се дефинишу на следећи начин (Koerpe, 2020):

- Уобичајени ниво – означава личну референцу која има мали потенцијал за злоупотребу или стигматизацију у односу на појединца.
- Високи ниво – односи се на то да подаци који имају повећан интерес не буду обелодањени, неконтролисани или незаконито присвојени.
- Веома висока потреба за заштитом – мора бити обезбеђена за посебне категорије личних података и за податке који подлежу посебној законској обавези чувања тајности као што су нпр. личне здравствене информације.

Као стална претња која може да има разарајуће последице попут финансијских губитака, провала у информационе системе и крађе поверљивих података, прекида функционисања система, итд. стоји сајбер криминал.

Сајбер криминал се дефинише као свака неовлашћена активност која укључује рачунар, уређај или рачунарску мрежу. Постоје генерално три препознате класификације сајбер криминала (Kelley, 2023):

- криминална радња уз помоћ компјутера,
- криминална радња где је компјутер мета напада,

- криминална радња где је компјутер посредно а не директно повезан са злочином.

Према намери односно жељеном исходу нападача, сви сајбер напади се деле на (Taylor, 2023):

- нападе ради стицања финансијске користи,
- нападе ради прекида у раду неког система,
- нападе ради шпијунирања (укључујући и корпоративну шпијунажу).

У погледу технике сајбер напада, нападачима су на располагању бројни хакерски алати и апликације. Главни типови претњи безбедности информација су (Cassetto, 2023):

- Напади помоћу нежељеног софтвера (енг. *Malware*). Напади су усмерени на обезбеђивање да се нежељени софтвер имплементира на корисников рачунар или уређај, најчешће путем отварања линка из прилога имејл поруке. Након успешне инсталације, *malware* може да надгледа активности корисника, шаље поверљиве податке нападачима као и да им помогне да нападну друге уређаје у мрежи. Неки од најчешћих типова *malware*-а су:
  - тројански вируси – варају корисника да се ради о безопасној датотеци, након чега могу да нападну податке;
  - *ransomware* – онемогућавају кориснику да приступи својим подацима, где они могу бити и обрисани, уколико се не плати откуп који траже сајбер нападачи;
  - црви (енг. *Worms*) – проналазе рањивости и пропусте у безбедности како би допрли до оперативног система, након чега могу да извршавају разне нападе;
  - *spyware* – нападачи могу да дођу до поверљивих података као што су шифре за пријављивање, подаци о кредитним картицама итд.
- Напади помоћу социјалног инжењеринга. Ова врста напада психолошки наводи кориснике да изврше радње које ће открити њихове поверљиве податке. Најчешћи типови су:
  - „фишинг" (енг. *Phishing*) напади – нападачи, углавном путем имејла, шаљу лажне поруке кореспонденције које изгледају као да потичу из легитимних извора, и наводе корисника да унесе поверљиве информације или отвори линк;
  - лажни безбедносни софтвер – претвара се да претражује корисников рачунар у потрази за нежељеним софтвером и увек приказује лажне детекције. Кориснику се нуди да плати и региструје софтвер, чиме открива своје финансијске податке.
- Напади на ланце испоруке софтвера – за напад се искоришћава поверење које организације имају у своје добављаче софтвера, нарочито приликом ажурирања и исправљања грешака (мета су алати за надгледање мрежа, индустријски контролни и други системи који су присутни на мрежи и имају сервисне налоге).
- Напредни дуготрајни напади (енг. *Advanced persistent threats*) – када нападачи добију неовлашћен приступ мрежи и успеју да остану неоткривени дужи период, при чему могу да остваре приступ поверљивим информацијама. Оваква врста напада је изузетно софистицирана, и углавном се користи за нападе на велике корпорације.
- Напад ускраћивања услуге (енг. *Distributed Denial of Service*) – циљ ове врсте напада је да се преплаве ресурси система који је мета, што може да доведе до

престанка функционисања, и немогућности опслуживања корисника. Често се користе у комбинацији са другим сајбер нападима, да се одвуче пажња обезбеђења од правог напада.

- Напади помоћу посредника (енг. *Man-in-the-middle attack*). Када уређај или корисник приступа неком систему путем интернета, претпоставља се да комуницира директно са одговарајућим сервером. Напад помоћу посредника има за циљ да пресретне ту комуникацију, преузима поверљиве податке и шаље различите одговоре кориснику.
- Напади на лозинке за приступ. Нападачи могу да покушају да добију приступ лозинкама шпијунирањем конекције преко мреже, искоришћавањем социјалног инжењеринга, погађањем, или остваривањем приступа бази за лозинкама.

Како би се корисници и њихово окружење заштитили од сајбер напада, потребно је придржавати се следећих принципа (Shred-it, 2022):

- Заштита компјутерских система – потребно је користити антивирус и *firewall* програме, као и редовно ажурирати софтвер.
- Коришћење сложених лозинки, које се састоје од минимум 8 карактера и комбинују слова, бројеве и специјалне карактере; потребно је често мењати лозинке.
- Избегавање употребе јавних *Wi-Fi* мрежа за онлајн плаћања и слање поверљивих информација.
- Обазривост са непожељним имејл и текстуалним порукама – не отварати линкове, слике и видео садржаје који су стигли од непознатих пошиљалаца.
- Заштита личних информација на друштвеним мрежама – пажљиво делити личне информације (име и презиме, адреса становања, број телефона итд.).
- Ограничавање физичког приступа поверљивим информацијама – на пример, кућни рачунар искључивати када се излази из куће.
- Обазривост са свим уређајима – увек водити рачуна где се остављају мобилни уређаји јер су честа мета крађе.
- Избегавање нагомилавања података – потребно је брисати старе и непотребне верзије фајлова; хард дискове из старих рачунара треба одложити на безбедно место или уништити.

4.2. Здравствени подаци и њихов проток

Под здравственим подацима односно здравственим информацијама подразумева се свака лична информација или мишљење о здрављу, болести, повреди или инвалидности појединца. Најчешћи примери за здравствене информације су (Abdelhak et al., 2014):

- информације о симптомима, дијагностичком процесу и коначној дијагнози,
- информације о здравственој услузи,
- специјалистички извештаји и резултати испитивања,
- стоматолошки картони,

- лекарски рецепти као и друге набавке лекова и медицинских средстава,
- информације о потенцијалном донирању органа,
- статус здравственог осигурања,
- потврде термина и обрачуни пружених услуга, као и
- било који други лични подаци прикупљени од стране пружалаца здравствене заштите.

Ток здравствених информација је механизам преноса дигиталних здравствених информација о корисницима/пацијентима из једног организационог ентитета у други. Овај механизам има врло јасну, технолошки дефинисану архитектуру. Ентитет који генерише или прикупља здравствене информације о корисницима и чува их у дигиталном облику назива се пружалац здравствених информација (здравствене установе, дијагностичке лабораторије, апотеке или друге организације које покрећу софтверске системе за прикупљање, обраду и чување здравствених информација појединаца). Ентитет који тражи здравствене информације о пацијентима назива се корисником здравствених информација. То могу бити здравствене установе, осигуравајућа друштва, компаније за медицинска истраживања и мноштво других организација које су заинтересоване за обраду информација у вези са здрављем прикупљених из различитих извора. Заправо, ток здравствених информација укључује њихов пренос са пружалаца на кориснике здравствених информација.

Неки токови здравствених информација укључују пренос информација које садрже личне податке корисника или се лако могу повезати са одређеним појединцем. Оваква врста протока информација се назива ток личних здравствених информација. Динамички генерисане колекције дигиталних здравствених докумената добијених од више пружалаца појединачних здравствених информација о једном пацијенту из више различитих извора, води у креирање личног здравственог картона те особе.

Постоји и ток здравствених информација који се односи на пренос информација које се не могу лично идентификовати. Такве информације могу бити неличне по својој природи (нпр. детаљи о профилу здравствене установе која прикупља здравствене информације пацијената) или су пак применом техника анонимизације конвертоване у неличне здравствене информације. Овакав ток информација представља проток неличних здравствених информација (iSPIRT, 2020).

Доступност информација и њихов транспарентан ток, у оквиру система здравствене заштите и између свих стејкхолдера, су неопходни за унапређено заједничко доношење одлука и одговорности. Продуктивна интеракција између информисаних пацијената и медицинских стручњака омогућује да се пацијенти оснаже као активни партнери у самом процесу пружања односно коришћења здравствене заштите (Zonneveld et al., 2018; Kneck et al., 2019).

Графички приказ протока здравствених информација дат је на слици 8.

Слика 8. Проток здравствених информација (адаптирано из: Kissi et al., 2018)

Неоспорно је да су електронски здравствени картони широко распрострањени у лекарској пракси и здравственим системима (HealthIT, 2021). Ипак, технолошка еволуција која се одиграва у дигиталном здравству, уз повећање обима и опсега дигиталних трансакција, повећава сигурносни ризик.

Значај унапређивања приступа и размене здравствених информација уз успостављање транспарентних и функционалних система заштите појединачних, односно личних здравствених информација је од кључног значаја за функционисање здравственог екосистема.

Овакво функционисање намеће потребу за успостављањем баланса интереса индивидуе са потенцијалним коришћењем здравствених информација за унапређење здравствене заштите. На индивидуалном нивоу, појединци црпе корист од приступа и размене сопствених информација између лекара и установа где спроводе своје лечење. С друге стране, сваки корисник здравствене заштите у дигиталном систему мора бити у могућности да зна и контролише како здравствени систем и други субјекти приступају, користе и откривају његове личне здравствене информације (Sulmasy et al., 2017).

На ширем, друштвеном нивоу појединци могу да црпе корист од размене сопствених здравствених информација ако се оне користе у циљу унапређења здравствене заштите. Такву ситуацију срећемо у примени иновативних технологија (*big data* аналитика, вештачка интелигенција и алгоритми машинског учења). У оваквом случају појединци морају да имају чврсте гаранције да добијају потребну здравствену заштиту и учествују у дигиталном здравственом екосистему без неприкладног откривања или коришћења сопствених информација, да неповерење у систем здравствене заштите не би довело до ускраћивања релевантних здравствених информација, како на ширем тако и, још значајније за појединца, на индивидуалном нивоу (Price & Cohen, 2019).

4.3. Функционисање дигиталног здравственог екосистема и пословни процеси са аспекта сајбер сигурности

У здравственом сектору, концепт приватности који је широко прихваћен и распрострањен, а који дефинише приватност као комбинацију безбедности и транспарентности избора, није одржив, а институционално поверење засновано на уверењима не може функционисати у динамичном, несигурном, дистрибуираном окружењу са више стејкхолдера у дигиталном окружењу здравственог екосистема (O'Connor et al., 2017).

Дигитални здравствени екосистем подразумева процесе здравствене заштите и здравствене информационе системе као веома динамичне и потпуно дистрибуиране, што омогућава да се здравствене информације динамички прикупљају, користе и дистрибуирају између стејкхолдера. Величина података варира – од података из једне апликације где се информације прикупљају помоћу сензора, премештају у облак, процесирају путем алгоритама а резултати приказују на мобилном телефону корисника, до великих дигиталних здравствених информационих система базираних на дигиталним платформама и комуникационим мрежама, користећи машинско учење и вештачку интелигенцију (Ruotsalainen & Blobel, 2019).

Када је безбедносна политика у здравственом сектору угрожена, било намерно или ненамерно, повећан је ризик од злоупотребе информација које сајбер нападачи могу да искористе и на тај начин нанесу неизмерну штету здравственој индустрији (Sanghyun & Kyungho, 2014).

Наводи се да је током 2021. године 45 милиона појединаца било погођено нападима на своје здравствене информације, што је повећање од 32% у односу на 34 милиона у 2020-ој години. Број сајбер напада у 2021-ој години је, практично, утростручен за само три године, ако имамо у виду чињеницу да је ова бројка 2018. године износила 18 милиона (Landi, 2022).

Ови подаци указују на изузетан значај организације функционисања дигиталног здравственог екосистема са аспекта безбедности информација и њиховог протока. Сајбер напади на електронске здравствене картоне и друге системе такође представљају ризик за приватност пацијената, јер сајбер нападачи приступају здравственим картонима и другим осетљивим информацијама.

Оно што је најважније, безбедност пацијената и пружање услуга здравствене заштите такође могу бити угрожени. Губитак приступа медицинској документацији и медицинским уређајима онемогућавају способност ефикасне бриге о пацијентима. Приступ сајбер нападача приватним подацима о пацијентима не само да им отвара врата за крађу информација, већ даје и могућност да намерно или ненамерно измене податке, што може довести до озбиљних последица по здравствене исходе предузетих здравствених мера у лечењу пацијената (Riggi, n.d.).

Безбедност је један од главних проблема који омета усвајање *cloud computing*-а у здравственом сектору. Предности *cloud computing*-а далеко превазилазе опасности и претње које оно носи. Ипак, безбедносне захтеве је све теже испунити без значајних

улагања у инфраструктуру и особе задужене за сигурност сајбер података (Al-Issa et al., 2019).

Акције које се спроводе у здравству обухватају специфично прожимање система елаборације, информатике, биомехатронике, биоинжењеринга, електронике, умрежавања, е-здравства, м-здравства. У таквом окружењу, сајбер сигурност у здравству укључује мрежну безбедност, безбедност апликација, безбедност информација, оперативну безбедност, оперативни континуитет, обуку крајњих корисника али подразумева и прилагођене и специјализоване аспекте за здравствени сектор услед примене преносивих дијагностичких и терапијских уређаја, постојања сложених интероперабилних и хетерогених система (болнички информациони систем; радиолошки информациони систем; наменска здравствена мрежа) и с тога обухвата и следеће специфичности (Giansanti, 2021):

- Чување података – процедуре које обезбеђују чување података на дужи период које користе адекватне и стабилне системе архивирања.
- Приступ подацима и модификација – спровођење ових радњи остварује се помоћу посебно осмишљених процедура за аутентификацију и ауторизацију приступа.
- Размена података – било да се ради о интерној размени (у здравственој установи) или екстерној (спољних актера, као што су пацијенти, други лекари, и/или друге здравствене установе), размена података треба да се одвија на безбедан начин, у складу са дефинисаним безбедносним специфичностима, уз примену одговарајућих мера заштите података.
- Интероперабилност и усклађеност – интероперабилност омогућава и здравственом раднику и пацијентима да размењују податке између више система и уређаја на заједнички начин.

У табели 3 су приказани актери здравственог екосистема који стриктно морају поштовати кодексе сајбер сигурности.

Као сајбер претње у дигиталном здравственом екосистему најчешће се наводе (Nivarthi & Akhilesh, 2020):

- Крађа података – крађа података за финансијску добит као и крађа података ради утицаја.
- Оштећени подаци – намерно оштећење података као што је промена информација заинтересованих страна ради професионалне или личне користи.
- Онемогућавање приступа подацима – примена вируса да се корисницима онемогући приступ подацима.
- Претња ускраћивања услуге – услугу коју мрежа одбија због превише захтева и неовлашћеног садржаја.
- Застарели системи – мрежни проблеми или проблеми система који доводе до губитка података због ненамерних радњи особља које користи застареле верзије софтвера.

Табела 3. Актери здравственог екосистема за које се очекује стриктно поштовање кодекса сајбер сигурности (адаптирано из: Rockwern et al., 2021)

Листа актера здравственог екосистема
Све врсте клиничких лекара
Јавна и приватна осигурања
Рачуноводство у здравству
Софтверске куће које развијају електронске здравствене картоне
Пацијент портали
Брокери података
Оглашивачи
Веб сајтови и претраживачи
Интегрисана складишта података
Мреже и размена података у здравству
Програмери технологија за кориснике (м-здравствене апликације, праћење фитнес резултата, лични здравствени картони)
Произвођачи медицинских уређаја
Фармацеутске куће
Компаније за кућна лабораторијска тестирања и компаније за генетска тестирања

Здравствене организације могу да допринесу у решавању наведених рањивости тако што ће уградити сајбер безбедност у сам темељ своје ИТ инфраструктуре. Следеће смернице треба да буду испоштоване (Meyers & Tone, 2022):

- Позабавити се сајбер безбедношћу од старта и интегрисати је са корисничким искуством. ИТ одељења треба да се консултују са стручњацима из области сајбер безбедности пре сваке значајније ИТ одлуке, како би сваки вид модернизације приоритизовао расположивост и сигурност података, као и максимално корисничко искуство.
- Побољшати поверење пацијената. Имплементацијом архитектуре „нултог поверења" (енг. *Zero Trust Architecture – ZTA*) за сајбер безбедност, здравствене организације могу побољшати поверење пацијената у размену медицинских података.
- Променити културу и ресурсе. Потребно је развити свест да сви запослени у здравственим организацијама имају своју улогу у заштити медицинских података од сајбер напада. Спровођењем редовних обука запослених, као и сталним праћењем стања ресурса и адекватним решавањем уочених недостатака, може се допринети смањењу безбедносних пропуста и могућности да сајбер нападачи угрозе податке пацијената и пословања здравствене организације.

5. *BLOCKCHAIN* ТЕХНОЛОГИЈА

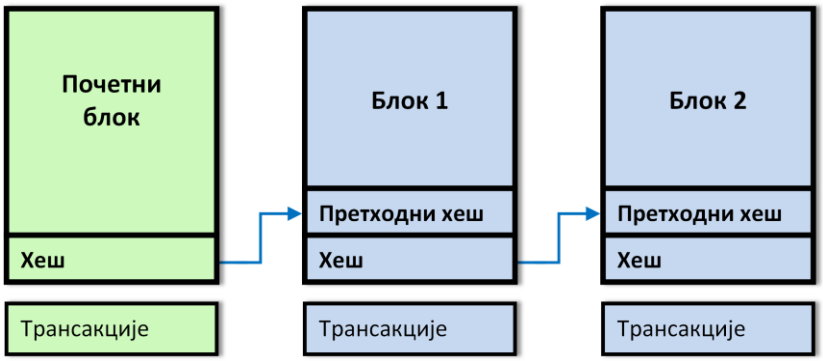
Blockchain, као поуздан и транспарентан механизам за складиштење и дистрибуцију података, представља технолошко достигнуће за које се предвиђа да може значајно да унапреди људске активности и интеракције. Иницијално је развијен за *Bitcoin* криптовалуту, која представља и најуспешнију примену ове технологије. Главне предности *Bitcoin*-а као што су децентрализација, велика отпорност на сајбер нападе и анонимност корисника привукле су пажњу бројних истраживачких заједница, што је резултовало применом *blockchain* технологије у разним сферама пословања као што су: управљање ланцима снабдевања, е-гласање, банкарство, паметни градови, ауто и авио индустрија, здравство (Ghiro et al., 2021). Оваква широка могућност примене *blockchain*-а чини ову технологију готово универзалном.

5.1. Појам, значај и предности *blockchain* технологије

Blockchain технологија се дефинише као дистрибуирани и децентрализовани систем главне књиге (енг. *ledger*) за *peer-to-peer* (*P2P*) мрежне трансакције података, који на поуздан и проверљив начин могу бити ускладиштени и јавно или приватно дистрибуирани свим корисницима (Rennock et al., 2018; Gaggioli, 2018). Поред главних концепата који обухватају постојаност, транспарентност и анонимност података без потребе за посредником, *blockchain* уводи и концепт паметних уговора, правно обавезујућих полиса које садрже прилагодљив скуп правила под којим различите стране врше међусобну интеракцију (Macrinici et al., 2018). *Blockchain* представља низ хронолошки сортираних записа који су организовани у блокове и повезани, евидентирани у главној књизи и заштићени криптографијом. Сваки блок садржи криптографски хеш код, временску ознаку и информације о самој трансакцији. Хеш код заправо представља резултат математичке функције трансформације улаза произвољне дужине у енкриптовани излаз фиксне дужине и основни је алат модерне криптографије. То је једносмерна функција, тј. не постоји обрнути алгоритам којим би се из хеш кода на излазу, добио оригинални улазни податак. Криптографске хеш функције имају велику примену у апликацијама у домену сигурности и дигиталном потписивању података, па је њихова примена у *blockchain* платформама један од основа безбедности и неизмењивости трансакција. Поред сопственог хеша, сваки блок садржи и хеш код претходног блока, чиме се гарантује интегритет података, јер би свака накнадна измена података у *blockchain*-у захтевала измену свих претходних блокова. На слици 9 је дат приказ основне архитектуре *blockchain* мреже.

Главна књига евидентираних трансакција се налази на различитим чворовима у оквиру мреже, који су повезани *peer-to-peer* протоколом, и сваки од чворова садржи исту копију података. Улога чворова је да обављају верификацију аутентичности записа у *blockchain* на основу консензус алгоритама за усвајање новог блока. Овакав децентрализован начин чувања података на чворовима је безбеднији у односу на централизован, јер би сваки

покушај насилне измене података подразумевао покушај неовлашћеног приступа и измене података на већем броју чворова, који је неопходан да се постигне консензус.



Слика 9. Архитектура *blockchain* мреже

Из горе наведеног, могу се индентификовати кључне компоненте *blockchain* архитектуре (Manu et al., 2020**)**:

- **чвор** – корисник или компјутер у оквиру *blockchain* мреже, где сваки поседује копију целе главне књиге *blockchain*-а,
- **трансакција** – најмањи градивни елемент *blockchain* система (записи, информације),
- **блок** – структура података која се користи за чување скупа трансакција које се дистрибуирају свим чворовима у мрежи,
- **ланац** – скуп блокова у одређеном редоследу,
- **рудари** – специфични чворови који извршавају процес верификације блокова пре него што се они додају у *blockchain*,
- **консензус протокол** – сет правила за извршавање *blockchain* операција.

Консензус алгоритми омогућавају *blockchain*-у додавање нових блокова, односно синхронизацију података, валидацију информација и обраду трансакција. Два тренутно најраспрострањенија консензус алгоритма су:

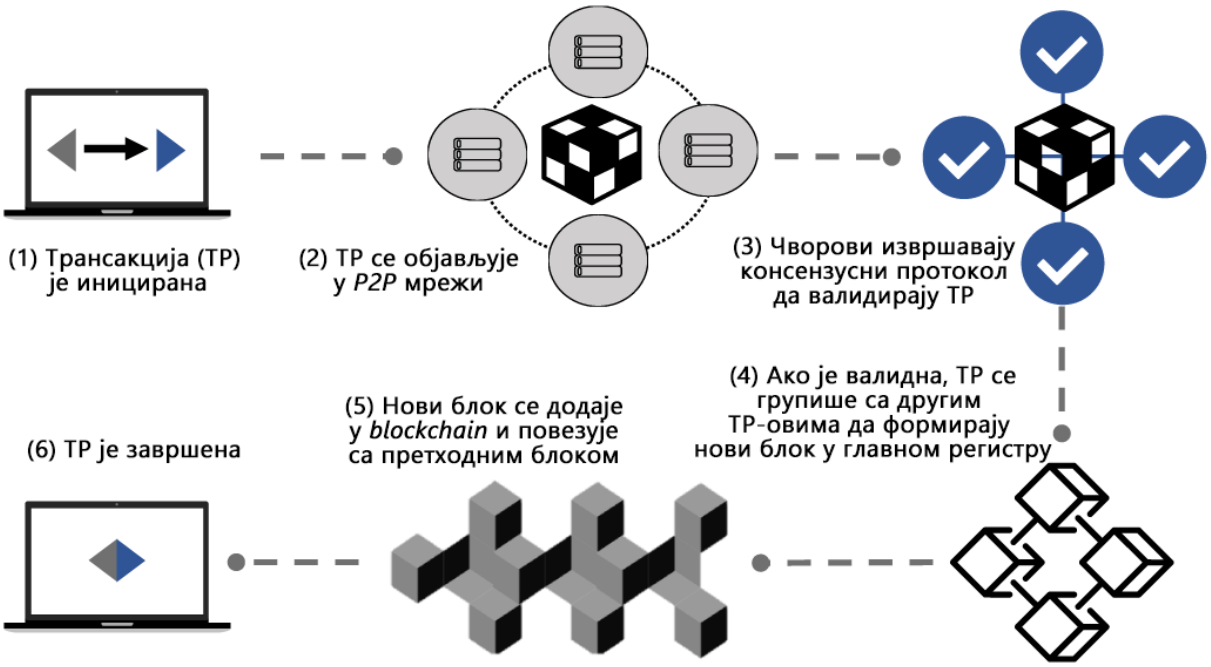
- доказ посла (енг. *Proof of Work – PoW*) и
- доказ улога (енг. *Proof of Stake – PoS*).

Код *PoW* алгоритма, креатори нових блокова се називају рудари. Рудари морају да поседују обимне компјутерске ресурсе уз помоћ којих рачунају криптографски хеш и тиме верификују трансакцију. Заузврат, они бивају награђени са одређеном количином криптовалуте, у зависности од тога у којој *blockchain* мрежи раде. Трошкови набавке специјализованог хардвера и неопходног утрошка електричне енергије су значајни, чиме се ограничава приступ рударењу, а самим тим се повећава и сигурност мреже. Рудари зарађују за свој рад добијањем криптовалута у одређеној вредности, али, с друге стране, троше прави новац за плаћање електричне енергије а често и за рентирање простора у који се смештају и читаве фарме са опремом за рударење. Потрошња електричне енергије често премашује потрошњу мањих држава у свету (Frankenfield, 2023).

Код *PoS* алгоритма, креатори блокова се називају валидатори (Smith, 2022). Валидатор проверава трансакције, верификује активности, гласа приликом избора и води евиденцију. Да би чвор постао валидатор, мора да уложи одређену количину

криптовалуте. У случају *Ethereum* мреже, тај износ је 32 *ETH*. Када одговарајући број валидатора потврди тачност блока, он се уписује у ланац. Систем насумично бира валидаторе па самим тим и ко ће добити провизију, за разлику од *PoW*-а, где се награђује рудар који први пошаље валидиран блок са израчунатим хешом. *PoS* је дизајниран да смањи загушења мреже и негативан утицај на екологију који има *PoW*, јер се електрична енергија и даље највећим делом добија из фосилних горива. Што се тиче сигурности, и код *PoS*-а постоји бојазан од „51-процентног напада", мада је то скоро немогуће, јер би подразумевало да хакери морају да поседују 51% уложених криптовалута. Такође, легитимни валидатори у том случају могу да изгласају одбацивање компромитованог *blockchain*-а, па чак и да одузму сав износ криптовалуте из новчаника нападача.

Пре самог уписа трансакције у *blockchain*, врши се њено процесирање. Све започиње захтевом за трансакцију, који се објављује у *P2P* мрежи, и који преузимају чворови за валидацију. На основу консензус протокола, чворови утврђују валидност трансакција. Уколико се постигне консензус односно сагласност већине чворова, трансакција се сматра валидном и, заједно са скорије одобреним трансакцијама, формира се нови блок који ће бити регистрован у главној књизи и уписан у *blockchain*. На крају, о успешно извршеној трансакцији се обавештавају сви учесници у процесу и измене се шаљу свим чворовима како би се ажурирала локална копија података. Уколико консензус није постигнут, предложени блокови података се одбацују. На слици 10 је приказан животни циклус трансакције приликом уписа у *blockchain*.



Слика 10. Обрада трансакције пре уписа у *blockchain* (адаптирано из: Ghiro et al., 2021)

Према начину приступа, *blockchain* мреже се деле на (Wegrzyn & Wang, 2021):

- мреже без дозволе – омогућавају било ком кориснику да се прикључи и постане чвор,
- мреже са дозволом – ограничавају приступ мрежи на само одређене чворове, као и права тих чворова у оквиру мреже.

Blockchain мреже без дозволе су углавном безбедније од оних са дозволом, јер постоји велики број чворова који врше валидацију, и покушај неког сајбер напада би захтевао пробој у велики број ентитета. С друге стране, мреже без дозволе доста споро обрађују трансакције, баш из разлога великог броја чворова који валидирају бројне трансакције. Насупрот томе, мреже са дозволом су углавном ефикасније, због мањег броја чворова, што омогућава краће време извршавања трансакција, услед брже валидације.

С аспекта отворености приступа, постоје 3 основна типа *blockchain* мрежа (Paul, Aithal et al., 2021):

- јавна,
- приватна,
- хибридна.

У јавном *blockchain*-у свако може да чита, уписује и надгледа мрежу. Овакве мреже су отворене и трансакције у њима су транспарентне, али анонимне. Одлуке у овом типу *blockchain* мрежа се доносе на основу бројних децентрализованих консензус механизама. Примери јавних *blockchain* мрежа су *Bitcoin, Ethereum, Zcash, Dash* итд.

Приватни *blockchain* представља личну имовину појединца или организације. У оваквој мрежи постоје ограничења за приступ, учешће у трансакцијама и валидацију. Приватне *blockchain* мреже се највише користе за управљање и надгледање база података, и користе се интерно у појединачним организацијама које не желе да њихови подаци буду јавно доступни. Главна предност оваквог типа мрежа су минимални трошкови трансакције и одсуство редундантности података али, с друге стране, оне су рањиве на сајбер нападе једнако као и уобичајени централизовани системи.

Хибридна *blockchain* мрежа представља комбинацију јавне и приватне, где неки чворови контролишу протокол консензуса док неки други имају могућност учествовања у трансакцијама.

У табели 4 је дато поређење главних карактеристика јавних и приватних *blockchain* мрежа.

Табела 4. Карактеристике јавних и приватних *blockchain* мрежа

ЈАВНА *BLOCKCHAIN* МРЕЖА	**ПРИВАТНА *BLOCKCHAIN* МРЕЖА**
Свако може да учествује	Учесници су унапред одабрани
Захтева криптовалуте	Не захтева криптовалуте
Висок степен децентрализације	Низак степен децентрализације
Мали пропусни опсег	Велики пропусни опсег
Висока потрошња електричне енергије	Ниска потрошња електричне енергије

Архитектура *blockchain*-а се састоји од 5 слојева (Pandey, 2022):

1. Хардверски слој. Први слој *blockchain*-а се састоји од хардвера односно самих рачунара, мрежних конекција и сервера података. Подаци у *blockchain*-у се складиште на серверима, и рачунари у *blockchain* мрежи размењују међусобно ове податке, формирајући *P2P* мрежу за валидацију трансакција.

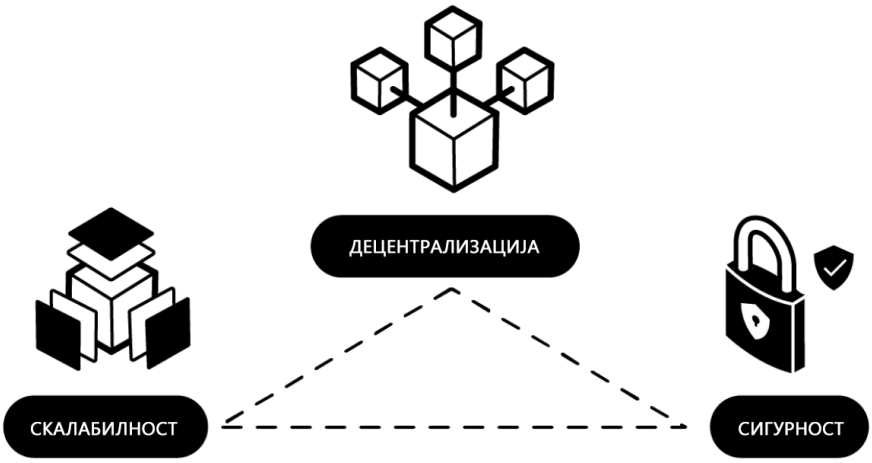
2. Слој података. Овај слој управља подацима у *blockchain*-у. Састоји се од блокова информација где је сваки блок повезан са претходним, сем почетног (енг. *genesis*), који представља први блок у мрежи.
3. Мрежни слој. Овај слој омогућава комуникацију између чворова унутар *blockchain*-а и у њему се креирају блокови и додају у мрежу.
4. Слој консензуса. Овај слој се брине о очувању униформности унутар мреже, кроз обавезност примене консензусних алгоритама. Чвор не може додати трансакцију у *blockchain* а да она пре тога није одобрена од стране осталих чворова у мрежи.
5. Апликациони слој. Овај слој омогућава примену *blockchain*-а за различите намене. Састоји се од паметних уговора (енг. *Smart contracts*) и децентрализованих апликација (енг. *Decentralized Application – DApp*). Овај слој представља заправо оно са чим се корисник сусреће приликом коришћења *blockchain* мреже.

С порастом употребе *blockchain*-а, важност скалабилности тог екосистема све више добија на значају. *Blockchain* мреже могу да прихвате нове апликације и већи број трансакција, али су за то потребне измене у системској пропусној моћи. С тог аспекта, *blockchain* може да се подели у следеће слојеве (Nguyen, 2022):

- **Слој 0 (*L0*)** – то је основни слој, који обухвата хардвер и софтвер који чине окосницу *blockchain* екосистема. *L0* омогућава међуланчану интеракцију, односно омогућава *blockchain* мрежама да међусобно комуницирају, што помаже у решавању проблема скалабилности наредних слојева.
- **Слој 1 (*L1*)** – већина пројеката у овом слоју је широко позната – ту спадају нпр. *Bitcoin* и *Ethereum*. *L1* је слој у коме се одвија највише активности, као што су консензус механизми, програмски језици, правила и параметри који осигуравају основне функције *blockchain* мреже. С порастом броја корисника у конкретној *blockchain* мрежи расте и број задатака које овај слој мора да опслужи, што доводи до проблема скалабилности.
- **Слој 2 (*L2*)** – покушава да реши проблеме скалабилности *L1* слоја на следеће начине:
  - канал стања – ажурира статус *blockchain*-а. Може се посматрати као посебан ланац (канал) који обрађује трансакције и у *L0* уписује само валидне статусне информације,
  - споредни ланац – то су посебне *blockchain* мреже које се извршавају паралелно са постојећим *L0* слојем, повезане двосмерним каналом са *L0* токеном. Споредни ланац користи своје протоколе, консензус алгоритме, параметре блокова али користи токене од *L1* (нпр. *Ethereum* споредни ланац користи tokene *Ethereum L0* ланца),
  - угњежђени ланац – представља интерни *blockchain*, где примарни *blockchain* поставља параметре мреже, а само извршавање трансакција се одвија у подланцима.
- **Слој 3 (*L3*)** – је слој који је видљив од стране корисника, у облику апликација. Обезбеђује једноставност и лакоћу коришћења слојева *L1* и *L2*. Чине га кориснички интерфејс и алати за извршавање трансакција.

Поред скалабилности, битне карактеристике које су пожељне у *blockchain* мрежи су децентрализација и сигурност. Ова три елемента заправо и чине тзв. „*blockchain*

трилему”, термин који је популаризовао Виталик Бутерин, оснивач *Ethereum blockchain* мреже. *Blockchain* трилема представља изазов с којим се сусрећу програмери а односи се на чињеницу да је у овим мрежама тешко постићи оптималну заступљеност све три наведене карактеристике, јер повећање једне најчешће доводи до смањења друге (Musharraf, 2022). На слици 11 је дат графички приказ овог концепта.



Слика 11. *Blockchain* трилема (адаптирано из: Musharraf, 2022)

Децентрализација представља померање и поделу контроле са једног ентитета ка мањим групама на управљање. У *blockchain*-у, децентрализација омогућава удаљеним чворовима да управљају мрежом уместо централне контроле коју спроводи један ентитет.

Са аспекта сигурности, *blockchain* мреже су по дефиницији безбедне, али нису у потпуности имуне на сајбер нападе, јер би хакерско преузимање више од половине чворова могло да омогући манипулацију трансакција и крађу информација.

Скалабилност *blockchain*-а се односи на могућност раста мреже уз очување пропусне моћи обраде трансакција.

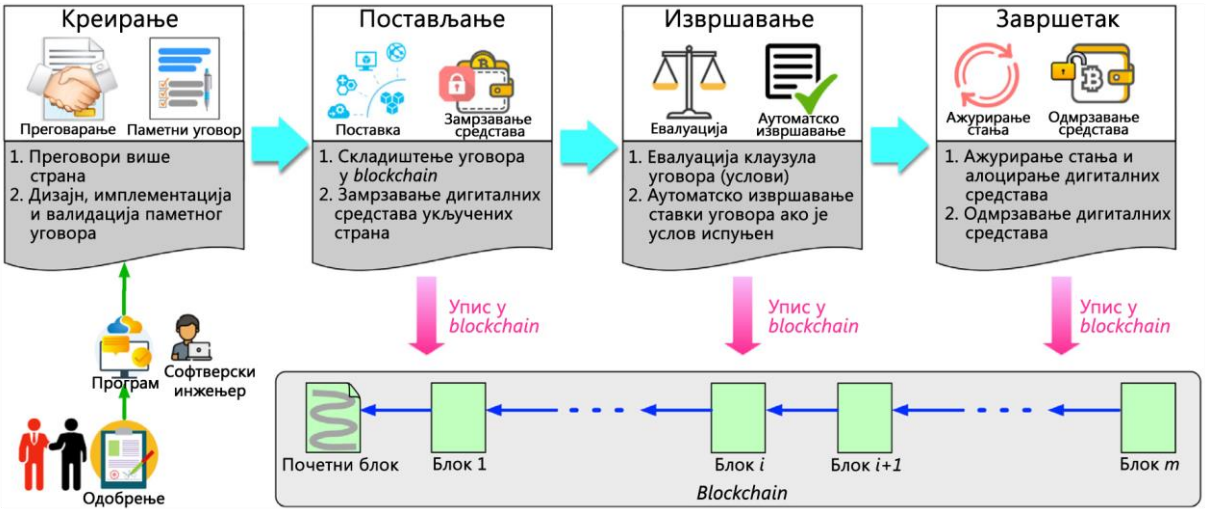
Децентрализација омогућава искључивање главног посредника који управља пројектом и омогућава трансакције, као што је то случај нпр. са банкама, које су у центру и представљају страну која стоји између клијената и њиховог новца и омогућава новчане трансакције. *Blockchain* уз помоћ самоизвршавајућих правила нуди алтернативу оваквом посредничком приступу. Свака од трансакција мора бити валидирана од стране више од половине чворова у мрежи, где са порастом њиховог броја, мрежа постаје све више децентрализована и сигурнија. С друге стране, повећање броја чворова доводи до смањења пропусне моћи због већег броја трансакција које је потребно обрадити. Да би *blockchain* мрежа и даље имала довољну пропусну моћ за растући број трансакција, неопходно је скалирање. Како скалирање мреже не би довело и до угрожавања безбедности мреже, неопходно је применити неке од раније споменутих концепата *L2* слоја.

Паметни уговори представљају кључну компоненту бројних платформи и апликација које су развијене на *blockchain*-у. Представљају компјутерски код који аутоматски извршава услове из споразума између заинтересованих страна, без потребе за надгледањем или посредовањем (Levi & Lipton, 2018). Код је реплициран на бројним чворовима у *blockchain* мрежи па је из тог разлога безбедан, постојан и неизмењив.

Већина паметних уговора је написана у неком од програмских језика директно прилагођених за одређену *blockchain* мрежу, нпр. *Solidity* за *Ethereum*.

Тренутно се за паметне уговоре не може баш рећи да су „паметни", јер се њихово извршавање своди на крајње једноставне наредбе типа „ако се појави X, изврши Y", као нпр. пребацивање одређеног износа криптовалуте из новчаника једне стране другој, у случају задовољења одређеног критеријума. Са све већом применом *blockchain* мрежа, расте и комплексност паметних уговора, односно њихова способност да извршавају софистицираније трансакције.

Пре него што се искомпајлирани паметни уговор изврши на конкретном *blockchain*-у, мора се платити трансакциона провизија за додавање у ланац. Код *Ethereum* мреже, паметни уговори се извршавају у оквиру *Ethereum* виртуелне машине (енг. *Ethereum Virtual Machine – EVM*), и провизија се плаћа у припадајућој *ETH* криптовалути, а означена је као гас (енг. *gas*) (Zheng et al., 2020). Износ цене гаса зависи од комплексности трансакција, односно броја наредби који је потребно извршити у оквиру једне трансакције. Провизија представља својеврсну одбрану од извршавања сувише комплексних трансакција или прекомерног извршавања нпр. у бесконачној петљи. На слици 12 је приказан процес извршавања једног паметног уговора.



Слика 12. Паметни уговор – животни циклус (адаптирано из: Zheng et al., 2020)

Предности примене *blockchain*-а се заснивају на главним карактеристикама ове технологије а то су:

- децентрализација,
- висока сигурност података и трансакција,
- транспарентност трансакција,
- неизмењивост података,
- примена паметних уговора.

Као главни бенефити могу се издвојити (Geroni, 2021):

- употребом *blockchain*-а пословни процеси су боље заштићени због високог нивоа сигурности,
- претња од сајбер напада на пословне процесе је у великој мери смањена,

- *blockchain* је децентрализована платформа, па се не морају плаћати услуге централизованих институција и посредника,
- приватне *blockchain* мреже омогућавају различита права приступа,
- организације могу брже да обављају трансакције,
- измирење уговорних обавеза може бити аутоматизовано,
- извршене трансакције су транспарентне и лаке за праћење.

5.2. Основе примене *blockchain* технологије

Захваљујући непроменљивости, децентрализацији и транспарентности, *blockchain* технологија се може применити у свим областима где је могуће искористити концепте паметних уговора и сигурности података са циљем повећања брзине, ефикасности и равноправности у пословању. *Blockchain* налази примену у следећим пословним секторима (слика 13):

Слика 13. Примена *blockchain* технологије (адаптирано из: Refat, 2022)

- Банкарство. Примена *blockchain*-а пружа решење главних изазова у сектору банкарства као што су неефикасно вођење документације, сигурносни ризици, неконзистентан надзор, високе цене провизија и велик утрошак времена (Takyar, n.d.). Сваки стејкхолдер представља чвор у банкарском систему који користи *blockchain*, чиме се избегавају посредници а употреба паметних уговора омогућава брже извршавање трансакција уз мање трошкове.
- Некретнине. *Blockchain* може да скрати дуг процес куповине/продаје некретнина који обухвата обимну документацију, проверу и пренос власништва помоћу паметног уговора који се извршава чим се обе стране усагласе око услова.
- Дигитална идентификација. *Blockchain* може корисницима да обезбеди пуну контролу сопствених дигиталних идентитета и информација и отвара могућност за

увођење *SSI* (енг. *Self-Sovereign Identity*) модела идентификације (Grech et al., 2021). Велике корпорације су препознале потребу за развојем апликација које омогућавају креирање дигиталних идентитета за своје запослене и становништво. У будућности се очекује увођење интернационалних дигиталних идентитета, који би се заснивали на *blockchain*-у и тиме обезбеђивали сигурност.

- Платни промет. Омогућава верификацију трансакција и међународна плаћања у реалном времену без учешћа посредника.
- Ланци снабдевања. *Blockchain* може да замени спор, често мануелни процес који се углавном ослања на папирну документацију са брзим процесом спајања крајњих корисника, нудећи видљивост и транспарентност у праћењу активности у ланцима снабдевања као што су: плаћања добављачима, смањивање броја фалсификованих производа, безбедност хране, логистика итд.
- *IoT.* Широка примена *IoT* технологије су суочава са проблемима мрежне безбедности, потенцијално несигурним *IoT* уређајима и подацима из различитих извора (Canorea, 2022). Компромитовани *IoT* уређај може бити искоришћен за хакерски напад на друге уређаје у мрежи, док разнородни извори података отежавају интеграцију, очување приватности, власништва и сигурности. *Blockchain* може да помогне у решавању ових проблема својим концептима: неизмењивости података да би се обезбедила њихова аутентичност, праћењем уређаја уз помоћ јединствених идентификатора, паметним уговорима за брже трансакције и децентрализацијом за повећану безбедност.
- Криптовалуте. Ово је свакако најпознатија примена *blockchain* технологије. Криптовалуте су дигиталне валуте односно тзв. токени, помоћу којих могу да се плаћају производи и услуге. За разлику од готовог новца, криптовалуте користе *blockchain* у смислу централног регистра са напредним криптографским сигурносним системом, тако да су све трансакције снимљене и обезбеђене (Daley & Whitfield, 2022).
- Спровођење закона. Неке *blockchain* мреже као нпр. *Bitcoin,* могу бити коришћене и за илегалне активности, баш због карактеристике одсуства посредника, односно, стране која надгледа трансакције. С друге стране, и полиција и друге агенције за спровођење закона су у могућности да анализирају јавно доступну *blockchain* мрежу, у потрази за форензичким материјалом који се може искористити за покретање поступака против извршилаца криминалних радњи.
- Здравство. Највећи проблеми са којима се здравство сусреће су спорост, грешке у подацима и административна комплексност (Refat, 2022). Као решење, *blockchain* нуди системе за управљање подацима о пацијентима, праћење ланаца набавке лекова, генетска истраживања, лакше обављање плаћања медицинских услуга, уз високу сигурност информација и транспарентност трансакција.

Сумирано, пословна примена *blockchain*-а има 3 главне предности:

- уштеде у времену,
- уштеде у трошковима,
- већу сигурност.

5.3. Софтверско-технолошка решења у домену *blockchain* технологије

За развој апликација које се извршавају на *blockchain*-у постоје бројне платформе, а избор зависи од критеријума као што су (Spiewak, 2022):

- Брзина извршавања трансакција и скалабилност. Брзина саме *blockchain* платформе показује колико трансакција у секунди може да обезбеди (енг. *Transactions per Second – TPS*). За развој апликације која обавља велики број плаћања, мора се изабрати платформа са већом пропусном моћи.
- Потребан ниво приватности. *Blockchain* мрежа може бити јавна или приватна. Приватне мреже се често користе у великим компанијама, где само корисници и партнери могу да читају и уписују у ланац. Власник мреже може чак и да мења и брише непотребне уносе. Јавне мреже могу сви да користе, и оне се фокусирају на непромењивости једном унетих података у ланац и анонимности, где се корисници идентификују помоћу јединственог криптографског кода (јавни и приватни кључеви). Приватне мреже су углавном и много брже, због мањег броја чворова неопходних за постизање консензуса.
- Величина мреже. Што је више чворова у мрежи, она је и безбеднија. С друге стране, повећање броја чворова често има негативан утицај на брзину извршавања трансакција („*blockchain* трилема").
- Потребе са криптовалутама. У приватним *blockchain* мрежама углавном нису потребне криптовалуте. Међутим, временом може да дође до потребе транзиције на јавну мрежу, која користи систем награђивања помоћу новчића криптовалуте. У том случају се јавља питање трошкова извршавања трансакција, због захтеване провизије мреже.
- Расположиве функционалности. Неке *blockchain* мреже се превасходно користе у сфери криптовалута, док је код других акценат стављен на паметне уговоре за децентрализоване апликације. Неке мреже су због велике пропусне моћи и прилагођених технологија више погодне за примену код обимних финансијских трансакција. У зависности од врсте пословања за коју се пише апликација, зависиће и избор одговарајуће *blockchain* платформе.
- Сигурност. Нису све *blockchain* платформе једнако сигурне. Уколико је потребно развити апликацију која треба да чува и размењује податке који су осетљиви и приватни, мора се узети у обзир и тачно које криптографске технике и консензусне алгоритме користи одређена *blockchain* платформа, као и колико често бива ажурирана.

Ethereum

Ethereum је дистрибуирана софтверска платформа отвореног кода, заснована на *blockchain* технологији. Представља једну од најпопуларнијих *blockchain* платформи. Поред тога што представља другу по величини криптовалуту (одмах иза *Bitcoin*-а), *Ethereum* се све чешће користи као платформа за креирање паметних уговора и развијање децентрализованих апликација (Cointelegraph, n.d.).

Ethereum мрежа, као и друге *blockchain* мреже, не постоји на једном централном компјутеру, већ је распрострањена на хиљаде компјутера широм света, који се називају чворови, чинећи је имуном на нападе и неочекивана заустављања у раду. *Ethereum* је у суштини један децентрализовани систем који покреће виртуелни *EVM* компјутер и сваки чвор поседује копију тог компјутера. Свака трансакција мора бити верификована и затим уписана као блок у *blockchain,* након чега се копија на сваком чвору ажурира. Рудари валидирају блокове пре слања на мрежу и за то добијају награду у облику новчића *ETH* криптовалуте. Сваки блок има јединствени 64-цифрени хеш код који га идентификује а рудари морају поседовати јак хардвер за његово комплексно рачунање. Овакав алгоритам се назива „доказ посла" (*PoW*) јер је компјутерска снага хардвера који рудари користе заправо доказ рада израчунавања кода. Насупрот овом консензус алгоритму, постоји „доказ улога" (*PoS*), где чворови уместо јаког хардвера морају имати значајну суму *ETH* криптовалуте, да би могли да буду валидатори трансакција за њихово уписивање у *blockchain*. *Ethereum* је у септембру 2022. године прешао на *PoS* консензусни алгоритам и тај помак је обележио као *Ethereum 2.0*. *PoS* протокол је мање енергетски захтеван, и омогућује нове нивое скалабилности.

Све трансакције су јавне и потврђени блокови се не могу мењати, тако да представљају комплетну историју свих мрежних трансакција. За сваку трансакцију потребно је да се плати провизија у *ETH* криптовалути, која се назива гас, и њу плаћа страна која је иницирала трансакцију. Поред плаћања провизије чворовима за калкулације, гас служи и као безбедносни механизам, ограничавајући број операција које корисник може да иницира у оквиру трансакције.

Интеракција са *Ethereum*-ом захтева поседовање криптовалуте, која је ускладиштена у новчанику који је повезан са децентрализованим апликацијама (*DApp*).

Паметни уговори представљају основу *Ethereum*-а. За писање *DApp* апликација које се извршавају на *blockchain*-у, развијен је посебан програмски језик *Solidity*.

Hyperledger Fabric

Hyperledger Fabric је *blockchain* платформа отвореног кода (енг. *Open source*), развијена од стране *Linux Foundation,* која подржава развој *blockchain* базираних апликација. Има модуларну архитектуру која омогућава кориснику да мења елементе као што су консензус, дизајн валидације трансакције, складиштење централног регистра и индентификатора. То је приватна мрежа са дозволом, што значи да је приступ ограничен и не може свако да буде члан *blockchain*-а. У *Hyperledger*-у, управљачки ентитети (најчешће група учесника) дају дозволу другим чворовима за било који тип трансакција. За валидацију трансакција, користе се посебни консензус алгоритми – *Kafka* и *Raft*. Платформа не поседује сопствену криптовалуту, и извршавање трансакција не захтева провизије, јер се цео пројекат финансира од стране непрофитне *Linux* фондације. *Hyperledger* омогућава симултано извршавање више трансакција, што значајно подиже перформансе система. За развој паметних уговора може да се користи готово било који стандардни програмски језик као што је *GoLang, Java, Node.js, Python*. У суштини, рад са *Hyperledger Fabric* паметним уговорима се реализује путем *API* интерфејса, где корисници валидирају улазне параметре, форматирају податке, и врше читање/упис у

базу. Ауторизација и полисе приступа могу бити дефинисане декларативно, приликом инсталација кода у ланац, или на нивоу кода (Derecha, n.d.).

Corda

Corda је прва платформа дистрибуираног главног регистра (енг. *Distributed Ledger Technology – DLT*) посебно дизајнирана за финансијску индустрију. Развијена је од стране *R3* компаније као платформа отвореног кода са циљем да омогући бележење, управљање и аутоматизацију правних уговора између пословних партнера (Newton, 2018). Кључне карактеристике обухватају стриктну приватност, ефикасност и директне трансакције помоћу технологије паметних уговора.

Corda главни регистар се разликује од система регистара које користе традиционалне *blockchain* технологије, и функционише као граф, где су сви чворови графа међусобно повезани, директно или преко других чворова. Сви могу да комуницирају један са другим, уколико то желе. Овим је искључена потреба јавног објављивања трансакција и оне су тајне. Чворови се откривају помоћу мрежне мапе, која садржи метаподатке о локацији свих сервиса (101 Blockchains, 2021).

R3 компанија је развила и *Corda Enterprise,* комерцијалну верзију која нуди додатне сигурносне механизме и професионалну подршку.

За писање паметних уговора на *Corda blockchain*-у користи се програмски језик *Kotline,* који је компатибилан са *Javascript*-ом и *JVM* (енг. *Java Virtual Machine*) језицима.

Algorand

Algorand је развио *Silvio Micali*, професор са *MIT* универзитета и светски признати стручњак из области криптографије и информационе сигурности, са визијом да демократизује финансије и тиме испуни обећање *blockchain*-а (Algorand Developer Portal, n.d.). Algorand платформа има за циљ да покуша да реши *blockchain* трилему, односно да истовремено постигне брзину, сигурност и децентрализацију. *Algorand* је децентрализована *blockchain* мрежа отвореног кода, која користи двостепену структуру и јединствену варијацију *PoS* консензусног механизма са циљем повећања брзине извршавања трансакција. Дизајниран је као мрежа фокусирана на плаћања, са брзим трансакцијама и фокусом на остваривање њихових готово тренутних финализација. *Algorand* мрежа је способна за брзине од преко 1000 трансакција у секунди, и финализацију трансакције за мање од 5 секунди (Cryptopedia Staff, 2022).

Као јавна *blockchain* мрежа за подршком за паметне уговоре, *Algorand* се намеће као алтернатива *Ethereum* мрежи за развој децентрализованих *Dapp* апликација и трговину у оквиру децентрализованих финансија *DeFi*, поготово у условима раста цене провизије у виду износа гаса у *Ethereum*-у.

Као консензусни алгоритам, *Algorand* користи посебну варијанту *PoS*-а коју назива *Pure-Proof-of-Stake (PPoS). PPoS* је механизам који захтева минималан улог криптовалуте за учешће и обезбеђење мреже – потребан је само један *ALGO* новчић, за разлику од *Ethereum*-а, где је тренутно потребно 32 *ETH* (Reiff, 2022). *ALGO* је нативна *Algorand* криптовалута, и представља основу целе платформе. Специфичност се огледа у томе што се награда за валидацију блокова дели на све имаоце *ALGO* криптовалуте, уместо да се

исплаћује искључиво валидаторима. Дистрибуција награде се врши на сваких 10 минута, и има за циљ да мотивише кориснике да се прикључе *Algorand* платформи, и тиме убрзају пут ка децентрализацији.

За развој дистрибуираних апликација и писање паметних уговора који се извршавају на *Algorand blockchain* мрежи, подржани су *Java, JavaScript* (*Node.js* и *browser*), *GoLang, Python, Rust, Swift, PHP, C#* итд.

5.4. Примена *blockchain* технологије у здравственом сектору

Blockchain мреже се користе у здравственом систему за чување и размену података о пацијентима између здравствених установа, дијагностичких лабораторија, апотекарских установа и лекара. *Blockchain* апликације могу прецизно идентификовати озбиљне грешке, које могу бити веома опасне у области медицине. Применом *blockchain* технологије може се побољшати учинак, сигурност и транспарентност размене медицинских података у систему здравствене заштите. Путем примене ове технологије медицинске институције стичу бољи увид и унапређују анализу медицинске документације (Haleem et al., 2021).

У здравству, *blockchain* има широк спектар апликација и функција. *Ledger* технологија обезбеђује сигуран пренос медицинске документације пацијената, пружа безбедност управљању ланцем снабдевања лековима и медицинским средствима. Заштита здравствених података, електронско управљање подацима, медицински картони, интероперабилност, дигитализовано праћење и слично, неке су од технички изведених и врло импресивних примена *blockchain* технологије (Chanchaichujit et al., 2019).

Ток процеса *blockchain* трансакције у здравству може се сажети у четири главна корака (Alkhushayni et al., 2019):

1. Здравствена организација складишти информације на *blockchain*-у. Здравствена организација пружа услуге пацијенту и снима податке о пацијенту у постојећи здравствени ИТ систем. Подаци и пацијентов јавни *ID* се преусмеравају на *blockchain* преко *API*-ја.
2. Трансакција је завршена и јединствено идентификована. Свака трансакција је шифрована и додељен јој је идентитет који је ускладиштен на *blockchain*-у, који садржи пацијентов јавни (неидентификујући) *ID*.
3. Здравствене организације могу директно да контактирају *blockchain*. Да би затражили податке, здравствене организације шаљу своје упите путем *API*-ја и користе пацијентов јавни *ID* на *blockchain*-у за преузимање шифрованих података. Информације о пацијенту су сада видљиве и могу се анализирати да би се стекао нови увид.
4. Пацијенти могу посебно овластити сваког појединца да приступи њиховим медицинским информацијама. Приватни кључ пацијента повезује њихов идентитет са подацима у *blockchain*-у. Овај приватни кључ може да се дели са другим здравственим организацијама, које могу да га користе за дешифровање података о пацијенту. Они који не поседују кључ не могу да идентификују податке.

Као главне предности примене *blockchain*-а у здравству наводе се ([x]cube LABS, 2022):

- Електронски здравствени картони усмерени на пацијента. Здравствени системи у свакој земљи сусрећу се са проблемом огромне количине података, што указује на то да пацијенти и њихови здравствени радници имају нејасну представу о свеобухватној историји болести. Као једно потенцијално решење намеће се креирање система заснованог на *blockchain*-у за медицинске картоне повезане са постојећим софтвером за електронске медицинске записе, који ће да фигурира као свеобухватни, јединствени поглед на здравствени картон пацијента.
- Транспарентност ланца снабдевања. Примарни изазов у целом здравственом сектору је обезбеђивање порекла медицинских средстава како би се гарантовала аутентичност. Помоћу система заснованог на *blockchain*-у може се пратити свако медицинско средство – од производње до сваке фазе кроз ланац снабдевања. На овај начин се клијентима/пацијентима омогућава потпуна видљивост и транспарентност артикала које купују.
- Управљање и дељење података о пацијентима. Управљање подацима о пацијентима коришћењем традиционалног приступа може бити сложен задатак, пошто се информације најчешће налазе у различитим базама здравствених података. *Blockchain* решава ове проблеме тако што пружа јединствену платформу за складиштење и управљање свим релевантним подацима на једној локацији, уз очување безбедности и контроле приступа.
- Праћење лека. *Blockchain* представља поуздано решење за осигурање аутентичности лека, јер омогућава праћење сваког лека до самог корена. Трансакције у *blockchain*-у ће бити видљиве свим овлашћеним странама, а кретање лека од једне стране до друге може се пратити у реалном времену. Купци лекова ће такође обезбедити аутентичност купљених производа скенирањем *QR* кода и тражењем података о произвођачу и другим релевантним странама у ланцу снабдевања. Дистрибуција лажног лека биће скоро немогућа у таквој поставци.
- Плаћања криптовалутама. Постоји могућност плаћања здравствених услуга путем криптовалута.

Транспарентност ланца снабдевања је главна предност, посебно на тржиштима у развоју где лажни лекови на рецепт изазивају десетине хиљада смртних случајева годишње. То је све више неопходно и за медицинске апарате, чији се број убрзано повећава усвајањем даљинског праћења здравља, а самим тим расте и интересовање лошенамерних актера.

С обзиром да је реч о новој технологији, може се поставити питање који су то фактори који утичу на имплементацију *blockchain*-а у здравственом сектору. Bali и сар. (2022) наводе да су три најзначајнија фактора који утичу на имплементацију *blockchain* технологије у здравствени екосистем: транспарентност података, праћење уз могућност увида у појединачне кораке као и подршка владе. Њихово истраживање је указало да је трошак имплементације имао најмање утицаја.

С друге стране, Aich и сар. (2021) идентификују да су кључни фактори који утичу на имплементацију *blockchain* технологије у здравству: регулаторна јасноћа и управљање, још увек нова технологија, високи инвестициони трошкови, програмери *blockchain*-а и поверење међу стејкхолдерима.

Као најзначајнији фактор за имплементацију *blockchain*-а у домену здравствених информација јесте очекивање перформанси које укључује препознавање технолошких и релативних предности. Фактор поверења утиче на прихватање, док идентификовани низак ризик има позитиван утицај на имплементацију *blockchain* технологије (Wanitcharakkhakul & Rotchanakitumnuai, 2017).

У погледу примене *blockchain* технологије у ланцу снабдевања, као три кључне димензије утицаја на имплементацију се наводе: операције и процеси, односи у ланцу снабдевања и иновације и приступ подацима. Ове димензије су међусобно повезане и у неким областима се преклапају унутар себе, што доводи до синергијских и контрасинергетских ефеката (Tokkozhina et al., 2022).

6. РАЗВОЈ МОДЕЛА ДИГИТАЛНОГ ЗДРАВСТВЕНОГ ЕКОСИСТЕМА ЗАСНОВАНОГ НА *BLOCKCHAIN* ТЕХНОЛОГИЈИ

Основни градивни елементи сваког дигиталног здравственог екосистема су медицински подаци. Подаци морају ефикасно да се прикупљају и размењују на погодан начин. Стандардизација података и могућност повезивања су омогућиле програмерима да раде унутар екосистема и да развијају апликације које се на њега ослањају. Искоришћеност података у оквиру дигиталног здравства увелико повећава продуктивност здравствених установа и побољшава исходе лечења (Domnisch, 2022):

- квалитетнији медицински подаци у облику електронских здравствених картона воде до повећања продуктивности пружалаца здравствених услуга,
- веб-оријентисани здравствени портали омогућавају пацијентима бољу комуникацију са пружаоцима здравствених услуга, што доводи до већег задовољства и бољих исхода лечења.

Свако унапређење концептуалне структуре дигиталних здравствених екосистема доноси побољшање квалитета услуга за постојеће кориснике а такође и охрабрује нове да почну да их користе.

Blockchain представља технологију која омогућава дистрибуирано, транспарентно и непроменљиво складиштење и размену података. Те карактеристике *blockchain* чине погодним за примену у здравственим дигиталним екосистемима, што за резултат може да има већу сигурност како медицинских података, тако и комуникације између стејкхолдера.

6.1. Концептуални циљеви и захтеви

Циљ ове докторске дисертације је да се да предлог модела дигиталног здравственог екосистема базираног на *blockchain* технологији. Развијени модел треба да обухвати све идентификоване стејкхолдере и пословне процесе који се одвијају у дигиталном здравственом екосистему. Треба да пружи већи степен аутоматизације трансакција, боље поверење у здравствени систем и приватност података, а самим тим и позитиван утицај на спремност стејкхолдера на размену информација. Приступ здравственим подацима мора бити строго контролисан, у смислу давања дозволе само овлашћеним стејкхолдерима, уз вођење евиденције о свим спроведеним трансакцијама.

Blockchain технологија треба да омогући развој сигурне платформе за чување и размену медицинских података и докумената пословне кореспонденције између идентификованих стејкхолдера у моделу дигиталног здравственог система.

Развијени систем треба да има могућност лаког проширења функционалности, у смислу повезивања и размене информација са *IoMT* уређајима, као и директне комуникације пацијената са лекарима у оквиру концепта телемедицине.

6.2. Модел и архитектура система

У данашње време, под савременим пословањем се подразумева пословање које се базира на управљању односима са стејкхолдерима. Теорија стејкхолдера скреће пажњу на синергијски потенцијал за стварање вредности међу групама заинтересованих страна компаније. Динамичке способности се састоје од процеса и активности усмерених на идентификацију могућности, мобилизацију ресурса и уношење неопходних промена за стварање вредности (Murphy & Wilson, 2022).

У светлу теорије стејкхолдера, иницијални корак је њихова идентификација у дигиталном здравственом систему. Идентификовани стејкхолдери у здравственом екосистему су приказани на слици 14.

Слика 14. Стејкхолдери у дигиталном здравственом екосистему
(адаптирано из: Moro-Visconti, 2021)

На глобалном нивоу, системи здравствене заштите актуелно настоје да се реконфигуришу, као и да иновирају своје процесе како би постигли и одржали сталну равнотежу између побољшања квалитета и рационализације трошкова (Sharma, 2021).

Blockchain технологија представља иновативни приступ ремоделирању здравственог система који нуди широк спектар интегрисаних функција: флексибилност приступа подацима, безбедност, приватност, децентрализовано складиштење, транспарентност, непроменљивост, аутентификацију, дисинтермедијацију, проверљивост, програмабилност и интерконекцију (Hasselgren et al., 2020).

Као почетни корак у пројекту планирања примене *blockchain* технологије неопходно је одредити кључне стејкхолдере који ће бити укључени у имплементацију. За пројекте који се базирају на *blockchain*-у, чворови (енг. *Nodes*) представљају основу *blockchain*

мреже. Типични чворови у руковању електронским здравственим информацијама су лекари и друго медицинско особље, фармацеути, здравствене установе, лабораторије. Сваки од наведених ентитета односно чворова има захтев да подаци буду сигурни, поуздани и ефикасно обрађени у оквиру обједињене комплетне медицинске историје (Burke, 2018). Поред тога, у планирању примене *blockchain* технологије у дигиталном здравственом екосистему у разматрање треба узети у обзир и спремност стејкхолдера за темељну имплементацију пројеката заснованих на *blockchain*-у. Искуство о спремности стејкхолдера за примену *blockchain*-а може да се црпи из истраживања о примени *blockchain*-а у другим секторима (Ozturan et al., 2019).

Студија коју су спровели Nicolai и сар. (2022) је идентификовала типове стејкхолдера – чворове и не-чворове и како њихов ниво спремности утиче на имплементацију пројеката заснованих на *blockchain*-у у погледу електронских здравствених података. Стејкхолдери који су чворови (нпр. пацијенти и лекари) су кључни за то да мрежа функционише након што је изграђена, док стејкхолдери које нису чворови играју кључну улогу у фази пре имплементације пројекта.

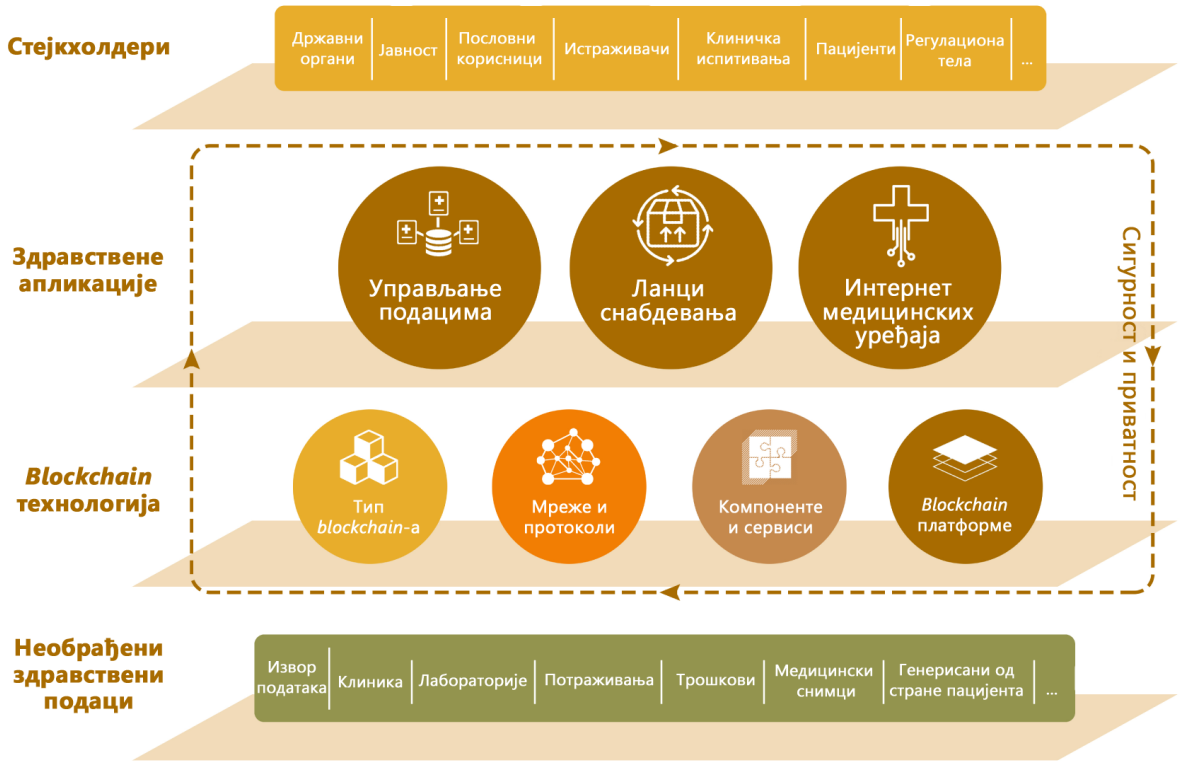
Студија спроведена на нашим просторима идентификовала је факторе од значаја за процес развоја дигиталног здравственог екосистема заснованог на *blockchain* технологији и то су: знање о *blockchain*-у, свест о сајбер безбедности, перципирана лакоћа коришћења, уочени кредибилитет, компатибилност, друштвени утицај и спремност на промене (Bjelica et al., 2021).

Из напред наведеног може се закључити да, заправо, сви идентификовани стејкхолдери у сфери здравства у одређеној мери доприносе у процесима креирања, имплементације и самог функционисања дигиталног здравственог екосистема заснованог на *blockchain*-у.

У погледу архитектуре система, нове здравствене технологије засноване на *blockchain*-у концептуално инфраструктурно су организоване у четири слоја (Khezr et al., 2019):

1. Слој здравствених података. Иницијално, све информације из медицинских уређаја, лабораторија, друштвених мрежа итд. се прикупљају и оне чине слој необрађених података, који представљају изворе информација и основу *blockchain* базираног здравственог система.
2. *Blockchain* слој. Овај слој својим одговарајућим концептима обезбеђује сигурност архитектуре.
3. Слој *blockchain* базираних здравствених апликација. Обухвата 3 велике групе апликација за:
   - управљање подацима,
   - управљање ланцима снабдевања,
   - *IoMT* системе за медицинске уређаје, сигурност података и вештачку интелигенцију.
4. Слој стејкхолдера. Налази се на врху хијерархије. Обухвата све стејкхолдере који имају корист од *blockchain* базираних здравствених апликација (пацијенти, пословни корисници, истраживачке институције итд).

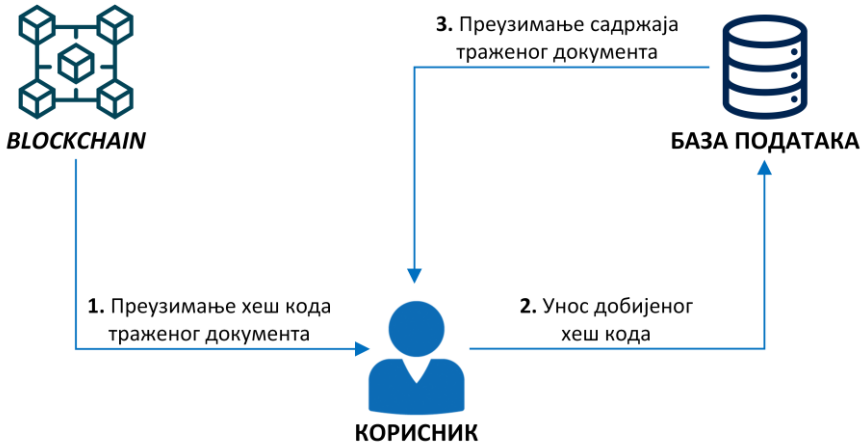
Слика 15 приказује типичну архитектуру *blockchain* базираног дигиталног здравственог система.



Слика 15. Архитектура *blockchain* базираног система за здравство (адаптирано из: Khezr et al., 2019)

6.3. Компоненте модела

Главна идеја за избор *blockchain*-а као платформе која представља основу развијеног модела дигиталног здравственог екосистема лежи у могућности да се искористи карактеристика непромењивости једном уписаних података у овакав тип мреже. Да би се то постигло, у *blockchain* није потребно складиштити комплетан садржај података, већ само њихов хеш код (слика 16). Тај хеш код се накнадно може искористити као доказ да су подаци, који су преузети из система, верни оригиналу, јер у случају да су мењани, аутоматски би се променио и њихов хеш код.



Слика 16. Основа концепта складиштења података у систему заснованом на *blockchain* технологији

У развоју модела дигиталног здравственог екосистема заснованог на *blockchain* технологији неопходно је укључити следеће компоненте које ће бити инкорпориране. То су:

1. Архитектура система за складиштење електронских здравствених картона:
   - База података;
   - Управљање подацима о пацијентима;
   - Архивирање података;
   - Сигурност и заштита података.
2. Архитектура система за складиштење документације пословних трансакција:
   - База података;
   - Управљање подацима пословних трансакција;
   - Архивирање података;
   - Сигурност и заштита података.
3. Архитектура *blockchain* технологије:
   - Тип *blockchain* платформе;
   - Отвореност мреже и права приступа;
   - Идентификација чворова мреже;
   - Консензусни протокол.
4. Интеграција *blockchain* платформе са системима за складиштење података:
   - Интерфејс за повезивање са базама података;
   - Комуникациони протоколи;
   - Сигурност и заштита података.
5. Интеграција корисничких апликација са *blockchain* платформом:
   - Интерфејс за комуникацију са *blockchain*-ом;
   - Сервиси за размену података;
   - Сигурност и заштита података.

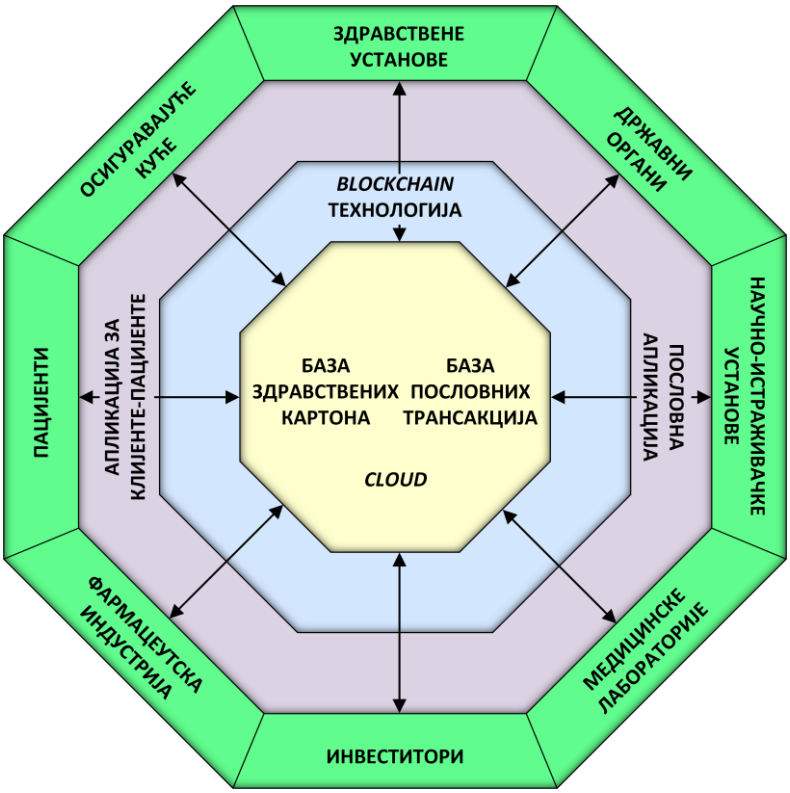
6.4. Предложени модел дигиталног здравственог екосистема заснован на *blockchain* технологији

Развијени модел дигиталног здравственог екосисистема базиран на *blockchain* технологији има следеће карактеристике:

- *Core* модела представљају две базе података – здравствени картони пацијената и подаци о пословним трансакцијама које остварује здравствена установа са осталим стејкхолдерима у дигиталном здравственом екосистему.
- Модел подржава два нивоа интероперабилности података: пацијент-центричну и институционалну интероперабилност.
- У односу на пацијенте, формулација модела је пацијент-центрична, чиме се промовише квалитативно нови ниво интероперабилности података.

- Институционална интероперабилност података подржана је у предложеном моделу путем размене информација здравствене установе са осталим стејкхолдерима.
- Кључне трансакције података у предложеном моделу базирају се на примени *blockchain* технологије.
- Примена *blockchain* технологије у датом моделу омогућава управљање и верификацију података без посредника, без угрожавања аутентичности, уз континуирану доступност, проверљивост података и постојање потпуне транспарентности.

На слици 17 је дат приказ предложеног модела дигиталног здравственог екосистема заснованог на *blockchain*-у.



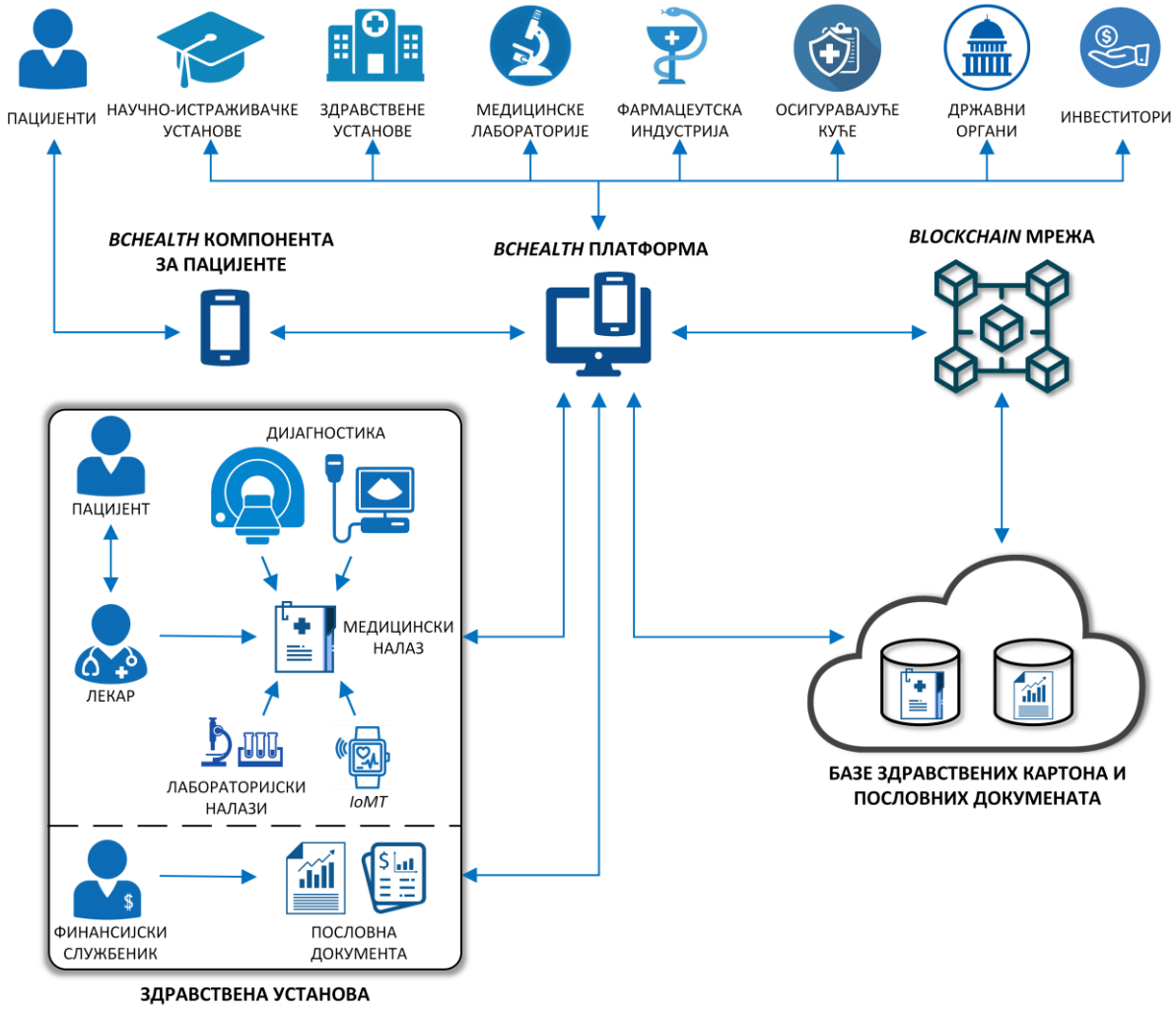
Слика 17. Предложени модел *blockchain* базираног система

Предложен модел дигиталног здравственог екосистема заснован на *blockchain* технологији нуди предности као што су:

- Безбедност. Базира се на основној логици *blockchain* технологије, јер када се блок дода у ланац, биће потребан консензус већине других чворова у мрежи да би се променили подаци у блоку.
- Децентрализација. Овакав модел нуди децентрализовану мрежу чворова у којој није неопходно веровање или познавање било кога другог у мрежи.
- Аутокорекција. У случају да се подаци у једном од блокова у мрежи промене, други чворови у мрежи спроводе проверу својих блокова и међусобно се повезују да би се исправила грешка.
- Дистрибуција. Независни рачунари бележе, деле и синхронизују трансакције у својим одговарајућим електронским књигама.

6.5. Архитектоника и инфраструктура предложеног модела

На слици 18 је дат приказ инфрастуктуре предложеног модела дигиталног здравственог екосистема заснованог на *blockchain* технологији.



Слика 18. Инфраструктура предложеног модела

Радни ток је следећи:

- Лекар прегледа пацијента и генерише нови медицински извештај. Поред лекара, извори информација за медицински извештај могу бити снимци са радиолошких модалитета, лабораторијски налази, подаци са *IoMT* уређаја. Медицински извештаји се уписују у *cloud* базу здравствених картона, и јединствени криптовани хеш код се уписује у *blockchain* ланац.
- Приликом прегледа или консултација, лекар има могућност приступа здравственом картону пацијента на основу дозволе пацијента путем прилагођене *blockchain* апликације. Пацијент може да дозволи приступ целокупном картону или само одређеним деловима.
- Пацијент уз помоћ посебног дела апликације може да дозволи приступ својим здравственим подацима свим заинтересованим стејкхолдерима, нпр.

истраживачким институцијама, фармацеутским компанијама, осигуравајућим друштвима итд.

- Документација везана за пословне трансакције између здравствене установе и осталих стејкхолдера се чува у *cloud* бази, а криптографски хеш код за приступ подацима се складишти у *blockchain* ланац, формирајући регистар свих трансакција.
- Стејкхолдери приступају бази пословних докумената путем посебне компоненте апликације, помоћу које могу да обављају трансакције са осталим заинтересованим стејкхолдерима.

6.6. Преглед постојећих решења

У традиционалним системима у здравству, када пацијент жели да подели своје медицинске податке са другим заинтересованим странама (истраживачка компанија, друга болница итд.), обично се сусреће са сложеном процедуром писаних захтева и одобрења, што процес преноса документације из једне установе у другу чини спорим и административно компликованим. Такође, питање приватности и сигурности медицинских информација све више добија на значају, јер напади на базе здравствених података наносе велике финансијске губитке и отежавају процесе квалитетног и правовременог лечења пацијената. *Blockchain* технологија, са својим основним концептима (децентрализована инфраструктура, безбедност, аутентификација и интегритет података), нуди могућност имплементације у софтверске системе управљања медицинским подацима, која имају за циљ да реше горенаведене проблеме. С друге стране, *blockchain* технологија се не сме схватити као решење за апсолутну сигурност података, јер постоје ризици од нпр. губитка приватног кључа за енкрипцију/декрипцију или рањивости паметних уговора, који могу довести до угрожавања здравствених информација пацијената.

У стручној литератури и експериментима проналази се већи број решења примене могућности *blockchain* технологије у здравственим информационим системима.

MedRec представља решење које предлажу Azaria и сарадници (2016), а односи се на примену *blockchain* технологије на постојеће централизоване системе за електронске медицинске записе. *MedRec* је изграђен на *Ethereum* мрежи, уз употребу *Python* програмског језика за креирање паметних уговора. *MedRec* користи концепт смештања медицинских записа ван *blockchain* мреже, и за то користи *SQL* засновану локалну базу података. Привилегије за приступ подацима се чувају у *blochchain* мрежи, заједно са јединственим хеш кодовима медицинских записа. Оваква имплементација олакшава интеграцију са постојећим системима који су у употреби и користе сопствена решења за смештај података. Мана предложеног система је што није имплементирана никаква врста енкрипције података записаних ван *blockchain* мреже, али аутори наводе важност овог аспекта за будућа унапређења система.

Ancile представља још једно *Ethereum* базирано решење које користи паметне уговоре за складиштење хеш кодова докумената са медицинским записима пацијената (Dagher et al., 2018). Хеш кодови се памте у *blockchain* мрежи, док се већина података и даље чува у

постојећим базама података које користе здравствене установе, али је примењена заштита ускладиштених информација уз помоћ одговарајућих техника енкрипције. Као и код *MedRec* решења, примена локалних база података на дуже стазе отвара питања скалабилности система.

Roehrs и сарадници (2017) су развили *OmniPHR* систем који покушава да обједини медицинске информације пацијената из више извора, које се чувају у базама података различитих пружалаца здравствене заштите. Здравствени подаци пацијената се у овом систему деле на блокове података, који се уписују у посебно развијену *P2P* мрежу. Потенцијални недостаци система су непостојање могућности да пацијенти имају контролу над приступом сопственим подацима, као и недовољна функционалност компоненте која врши спајање информација из хетерогених извора података, и захтева додатна унапређења.

Uddin и сарадници (2021) предлажу решење које се заснива на примени *HyperLedger blockchain*-а, и за своју имплементацију користе приватну мрежу са дозволама. Подаци о здравственим картонима пацијената се складиште комплетно унутар *blockchain* блокова. С обзиром да је у питању приватна *blockchain* мрежа, транспарентност уписаних информација не представља фактор ризика, али је свакако примењена и заштита података применом симетричне енкрипције.

У моделу који предлажу Shahnaz и сарадници (2019), за смештај информација о пацијентима користи се *IPFS* дистрибуирана платформа, а хеш кодови ускладиштених података се бележе у *Ethereum blockchain* мрежи. На овај начин је покушано да се реши питање скалабилности модела, али аутори не наводе никакве информације о евентуалној енкрипцији података пре смештања у *IPFS* систем. Овако ускладиштене информације су мање безбедне, јер пацијентовим здравственим подацима може приступити свако ко дође у посед *CID* (енг. *Content Identifier*) хеш кодова. Једина заштита коју овакво решење пружа се односи на саму природу неизмењивости једном ускладиштених података у *IPFS*.

Сумирано, главни проблеми код анализираних здравствених система базираних на *blockchain* технологији представљају:

- Питање локације за складиштење података о пацијентима. У неким решењима подаци се комплетно складиште у *blockchain*-у, што је економски неисплативо у решењима заснованим на јавним *blockchain* мрежама, а свакако утиче и на перформансе система, јер се рапидно повећава количина информација у дигиталном главном регистру. Уколико се подаци уписују ван *blockchain* мреже, у *cloud* бази података или у постојећој бази коју користи здравствена установа, ускладиштене информације су изложене безбедносним ризицима готово једнако као и у класичним, централизованим системима. Нека од решења која користе искључиво децентрализоване системе за складиштење, поред везе са документима, у *blockchain* уписују и информације које се напредним техникама анализе могу довести у везу са пацијентом, и на тај начин угрозити анонимност његових личних података и тока лечења.
- Питање скалабилности система. У решењима која податке о пацијентима чувају у постојећим локалним базама пружалаца здравствене заштите, поред безбедносних ризика временом може доћи до проблема везаних за скалабилност система, јер се

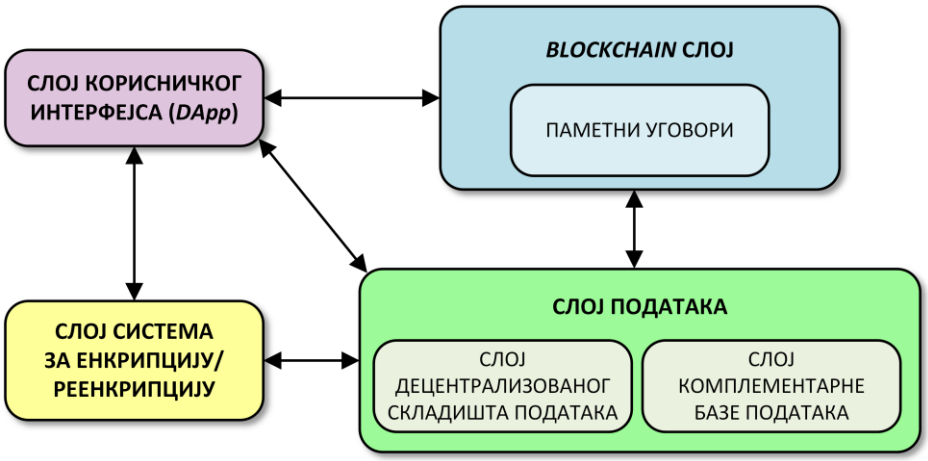
количина информација коју треба уписати и складиштити на дуги временски рок значајно повећава, нарочито уз примену нових дијагностичких модалитета и преносних уређаја, који генеришу податке све већег обима.

- Питање контроле приступа подацима. Модерни систем треба да буде пацијент центричан, односно да пацијенту пружа потпуну контролу приступа сопственим здравственим информацијама, што нека од анализираних решења не нуде у својим тренутним верзијама.

6.7. Технолошко-софтверски алати и решења за развој и имплементацију компоненти предложеног модела

Вишеслојна архитектура предложеног модела дигиталног здравственог екосистема базираног на *blockchain* технологији захтева примену различитих технолошких решења и софтверских алата, како би се имплементирале планиране функционалности.

Предложени модел се састоји од следећих слојева (слика 19):



Слика 19. Слојеви развијеног модела

- Слој децентрализованог складишног простора. С обзиром да је складиштење великих количина података (као што су медицински подаци) директно у *blockchain* мрежи економски неисплативо, као решење за чување енкриптованих здравствених података пацијената и информација о пословним трансакцијама између стејкхолдера је изабран *IPFS* (енг. *Interplanetary File System*). *IPFS* је *peer-to-peer* дистрибуирани фајл систем, који омогућава рачунарима широм света да чувају и деле ускладиштене податке, формирајући на тај начин мрежу која је отпорна на отказе појединачних чворова, и одликује је велика пропусна моћ. Сваки фајл који се ускладишти у *IPFS* систему добија свој јединствени *CID*, који заправо представља хеш код израчунат на основу садржаја самог фајла, и помоћу њега се остварује и приступ. Сав саобраћај у оквиру *IPFS* мреже је јаван, укључујући и садржај ускладиштених фајлова. Да би се обезбедила приватност података, мора се применити одговарајући тип енкрипције.

- Слој комплементарне *cloud* базе података. С обзиром на транспарентност информација које се уписују у јавну *blockchain* мрежу, као и ограничену могућност складиштења у смислу обима уписаних података и трошкова извршавања трансакција у паметним уговорима, комплементарна *cloud* база чува метаподатке о корисничким налозима и документима који су ускладиштени у *IPFS* систему. За развијени модел је одабрана *MongoDB Atlas* база података, која је нерелациона, дистрибуирана, и карактеришу је велика пропусна моћ и флексибилне могућности индексирања и претраживања података. *MongoDB Atlas* подржава једноставно хоризонтално скалирање, односно дистрибуирање података на више сервера, што олакшава накнадно проширивање система. Висока доступност је обезбеђена путем реплицирања података на више физичких сервера, па и у случају отказивања неког од њих, подаци нису угрожени.
- *Blockchain* слој, који представља безбедну и транспарентну платформу у којој се чувају релевантне информације о налозима свих учесника дигиталног екосистема као и власништву над криптованим фајловима који су ускладиштени у *IPFS*-у. За имплементацију развијеног модела је изабрана *Ethereum* јавна *blockchain* мрежа, у коју су постављени паметни уговори који се извршавају у оквиру *EVM* виртуелне машине. Паметни уговори омогућавају управљање акцијама над подацима у *blockchain* мрежи и у њиховим променљивама стања се чувају записи о свим адресама налога и трансакцијама које они иницирају или прихватају, као и хеш кодови криптованих фајлова помоћу којих се може приступити подацима у *IPFS* систему.
- Слој система за енкрипцију и реенкрипцију података. Део развијеног модела који се односи на пружање услуга здравствене заштите је пацијент центричан, где је корисник власник сопствених података, и има могућност одређивања права приступа за друге заинтересоване стејкхолдере. Пре уписивања у *IPFS* систем, врши се асиметрична енкрипција помоћу *ECC* (енг. *Elliptic Curve Cryptography*) алгоритма, односно, здравствени подаци се енкриптују пацијентовим јавним кључем. Тако ускладиштеним подацима може приступити искључиво пацијент који је њихов власник, тако што ће они бити декриптовани помоћу његовог приватног кључа. Систем за реенкрипцију података врши декрипцију здравствених података пацијента и њихову поновну енкрипцију, на начин који обезбеђује приступ подацима заинтересованим стејкхолдерима којима је додељено право приступа. Исти принцип је примењен и у пословном делу модела, где се подаци о кореспонденцији укључених страна енкриптују њиховим јавним кључевима, тако да им само они могу приступати. Овај слој обезбеђује сигурност података ускладиштених у *blockchain*-у и *IPFS*-у.
- Кориснички слој. Овај слој обухвата све стејкхолдере дигиталног екосистема који обављају интеракцију са *Ethereum blockchain* мрежом и *IPFS* системом, односно врше упис, претраживање и приступ криптованим здравственим и пословним подацима. Приступ систему је реализован путем *Web3* децентрализоване апликације (*DApp*). Пацијенти приступају посебном делу апликације, где на једноставан и интуитиван начин могу да додељују права приступа здравственим подацима свим заинтересованим стејкхолдерима.

За израду децентрализоване апликације развијеног модела дигиталног здравственог екосистема заснованог на *blockchain*-у коришћене су следеће технологије и алати:

- *Remix IDE* – комплетан алат за писање и тестирање паметних уговора помоћу *Solidity* програмског језика, посебно развијеног за *Ethereum blockchain* мрежу.
- *Truffle*, као главна компонента *Truffle Suite* система за развој децентрализованих апликација, представља развојно окружење за аутоматизацију процеса компајлирања и мигрирања паметних уговора у *EVM* виртуелну машину, у којој се они извршавају у оквиру *Ethereum blockchain* мреже.
- *Ganache* – алат у оквиру *Truffle Suite*-а, који омогућава креирање приватне локалне *Ethereum blockchain* мреже, што олакшава процес развоја, постављања и тестирања децентрализованих апликација у контролисаном окружењу.
- *JavaScript* и *jQuery – frontend* корисничке апликације је израђен помоћу *JavaScript* програмског језика, уз коришћење *JQuery* радног оквира и *AJAX* функционалности.
- *Web3.js* – библиотека која нуди функције за повезивање *JavaScript* апликације са *Ethereum* налозима и паметним уговорима.
- *Node.js* – представља серверску *JavaScript* платформу, помоћу које је реализован *backend* корисничке апликације.
- *Express.js* – радни оквир који додатним могућностима проширује веб сервер функционалности *Node.js* платформе.
- *MetaMask* – интерфејс за повезивање *Ethereum* налога са *blockchain* мрежом, помоћу којег се управља трансакцијама у децентрализованој апликацији.
- *Visual Studio Code* – напредни едитор софтверског кода који може да се користи са готово свим актуелним програмским језицима. Олакшава развој софтвера функционалностима као што су: напредно отклањање грешака, обележавање кључних синтаксних наредби, интелигентно довршавање линија програмског кода итд.

6.8. Развој апликације модела дигиталног здравственог екосистема заснованог на *blockchain* технологији

За потребе дефинисаног модела дигиталног здравственог екосистема заснованог на *blockchain* технологији, развијена је децентрализована корисничка апликација – *BCHealth* (енг. *BlockChain HealthCare*), која се састоји из две главне компоненте:

1. здравствена компонента, која се односи на пружање услуга здравствене заштите, односно, на интеракцију пацијента с једне стране и лекара и установе у којој се пацијент тренутно прегледа, односно лечи, с друге стране. Ову компоненту користе лекари приликом прегледа пацијената и писања специјалистичких налаза. Овој компоненти припада и део апликације намењен пацијентима, у који се они пријављују ради увида у лични електронски здравствени картон, као и додељивања права приступа својим налазима и извештајима.

2. пословна компонента, која се односи на кореспонденцију између здравствених установа, фармацеутских кућа, добављача медицинске опреме итд., односно свих идентификованих стејкхолдера који учествују у пословању здравственог екосистема и имају потребу за коришћењем платформе која им омогућава чување историје пословних трансакција на безбедан начин.

Медицински подаци о пацијенту који се генеришу у здравственим установама, као и документа која настају као резултат пословне интеракције између институција у оквиру дигиталног здравственог екосистема, се складиште у дистрибуирани *IPFS* систем. *IPFS* платформа смешта ускладишене фајлове у чворове, а копија фајла се чува и у локалном чвору, који је иницирао слање. Сваки чвор након приступа жељеном фајлу прави и локалну копију истог. Уколико се фајл не преузима често, прилично агресиван механизам чишћења података (енг. *Garbage collection*), који је имплементиран у *IPFS* систем, ће обрисати кеширане фајлове из локалног чвора којима није приступано у скорије време. Да би се обезбедило трајно чување фајлова у чворовима, неопходно је фајлове закачити (енг. *Pinning*). Из наведеног разлога, здравствене установе, поред тога што су део *blockchain* мреже, у *BCHealth* систему имају улогу и *IPFS* чворова. Након слања фајлова са пацијентовим налазима односно пословном документацијом у *IPFS* систем, они бивају закачени у локалном чвору, чиме се обезбеђује трајно чување и кешираних копија података, што гарантује расположивост и већу брзину приступа.

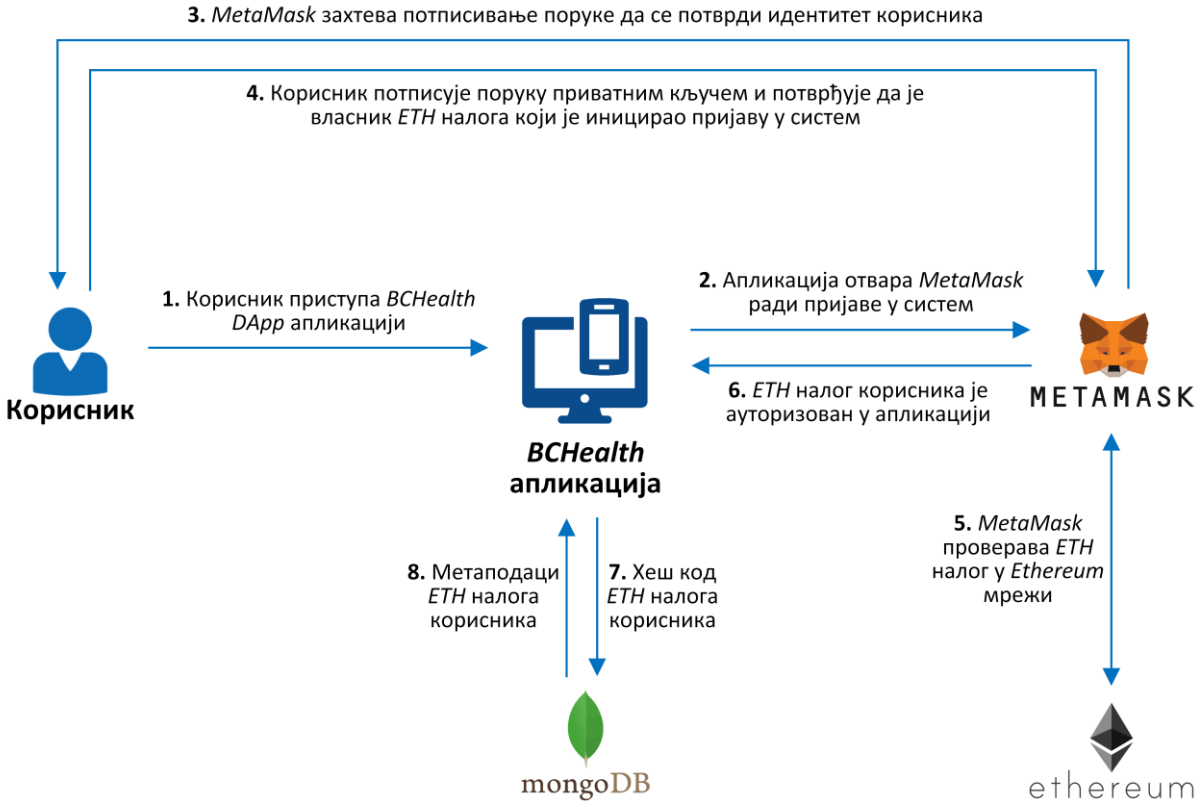
6.8.1. Пријава у *BCHealth* систем

Улазна тачка за *Web3* аутентификацију и могућност коришћења *Web3* децентрализоване апликације која се извршава на *Ethereum blockchain* мрежи јесте поседовање *Ethereum* налога, односно одговарајућег крипто новчаника, који садржи јавни и приватни кључ корисника. Како би се повезао крипто новчаник са *Web3* апликацијом, потребно је користити неки од софтверских додатака за интернет претраживаче који обезбеђују ту функционалност, како би се омогућила аутентификација корисника и приступ апликацији и паметним уговорима. *MetaMask* додатак за интернет претраживач инјектује *Web3* контекст у код веб странице, и омогућава потврђивање и потписивање трансакција садржаних у паметним уговорима, када год дође до њиховог иницирања у току коришћења апликације.

Приликом пријављивања у апликацију, систем проверава да ли је у интернет претраживачу инсталиран и активиран *MetaMask* додатак. Уколико додатак није детектован, претраживач врши преусмеравање на сајт за преузимање и инсталацију. Након успешне инсталације, корисник мора да се пријави у *MetaMask* помоћу свог постојећег *Ethereum* (*ETH*) налога односно јавне адресе крипто новчаника, или, уколико не поседује исти, да га креира.

Због специфичности здравственог сектора и токова података који се у њему одвијају, за имплементацију *BCHealth* апликације развијен је систем пријављивања који представља својеврсно хибридно решење између *Web3* аутентификације и класичних централизованих корисничких налога ускладиштених у одговарајућој бази података. Корисници се у *BCHealth* пријављују помоћу својих *Ethereum* налога, који у себи садрже јавни и приватни кључ. Приликом пријаве, паметни уговор шаље једноставну текстуалну поруку кориснику и захтева дигитални потпис исте. Потписивање поруке се врши

помоћу приватног кључа, и на тај начин корисник потврђује да је он заиста власник *Ethereum* налога који је иницирао пријаву у систем (слика 20).



Слика 20. Пријава у *BCHealth* систем

У промењивама стања у паметном уговору се од корисничких података чувају искључиво *ETH* адресе налога чиме се гарантује анонимност корисника, с обзиром на то да се информације складиште у јавној *blockchain* мрежи. У комплементарној *cloud* бази података се чувају преостале битне информације, које у случају корисничких налога, обухватају: име и презиме корисника, ЈМБГ, адресу, контакт телефон, имејл адресу итд. Сваки унос у колекцији корисника је повезан са одговарајућим *ETH* налогом који се чува у паметном уговору у *blockchain* мрежи.

У овако имплементираном решењу, не постоји систем лозинки за пријављивање корисника, јер се иста врши помоћу *Web3* аутентификације, односно валидација налога се обавља потписивањем поруке послате од стране паметног уговора помоћу приватног кључа. Овим је постигнуто да је *core* апликације, који је изграђен око паметних уговора, децентрализован, односно, паметни уговори се уз помоћ одговарајућих алата могу позивати и директно из *Ethereum blockchain* мреже, чак и у случају недоступности сајта са веб апликацијом.

6.8.2. Корисници *BCHealth* система

У *BCHealth* систему су идентификовани следећи типови корисника:

- Администратор система,
- Лекар,

- Пацијент,
- Финансијски службеник.

Здравствено регулаторно тело, као администратор целокупног система, је задужено за постављање паметних уговора на *blockchain* мрежу, као и за додавање у базу података свих здравствених установа, лекара и других стејкхолдера идентификованих у екосистему. На тај начин, сви корисници добијају своје *Ethereum* налоге, помоћу којих им је омогућено пријављивање у апликацију на *Ethereum blockchain* мрежи. Тип налога „финансијски службеник" обухвата немедицинско особље у идентификованим установама које користи пословни део апликације, који обухвата поручивање робе, фактурисање услуга, здравствено осигурање итд. У зависности од типа налога који свако од корисника поседује, приликом пријављивања у систем се учитава и приказује одговарајућа компонента апликације.

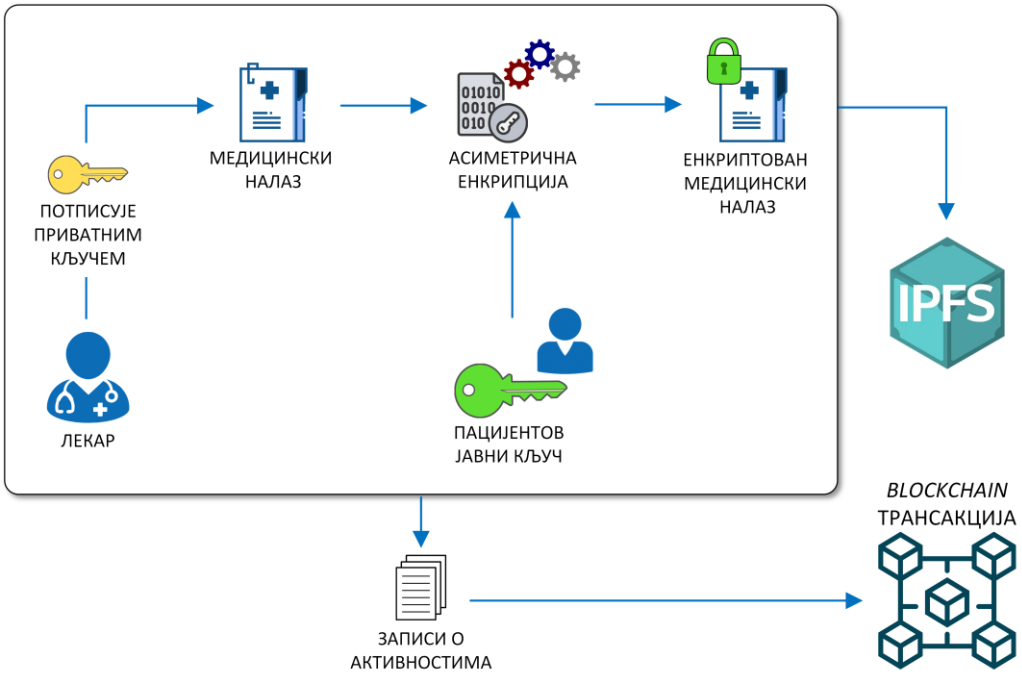
У променљивама стања паметних уговора који се извршавају на *blockchain*-у су мапиране, у оквиру хеш табела, *ETH* адресе болница, лекара, пацијената, односно, свих учесника у *BCHealth* систему. Паметни уговори чувају информације и о власништву над подацима у виду хеш кодова енкриптованих фајлова ускладиштених у *IPFS* систему, који су придружени припадајућим *ETH* налозима. Да би се очувала анонимност података у јавној *blockchain* мрежи, као и да би се количина података који се чувају у оквиру паметних уговора свела на минимум, додатне информације о налозима и ускладиштеним фајловима се чувају у комплементарној *MongoDB* бази података, где се као примарни кључ користе хеш кодови *ETH* налога.

6.8.3. *BCHealth* апликација – пружање услуга здравствене заштите

За адекватно лечење пацијената неопходна је потпуна историја њихових медицинских налаза. У развијеном моделу је искоришћена једна од најбитнијих карактеристика *IPFS* система – неизмењивост, јер се једном ускладиштени подаци могу само ажурирати додавањем нових верзија, без могућности брисања постојећих.

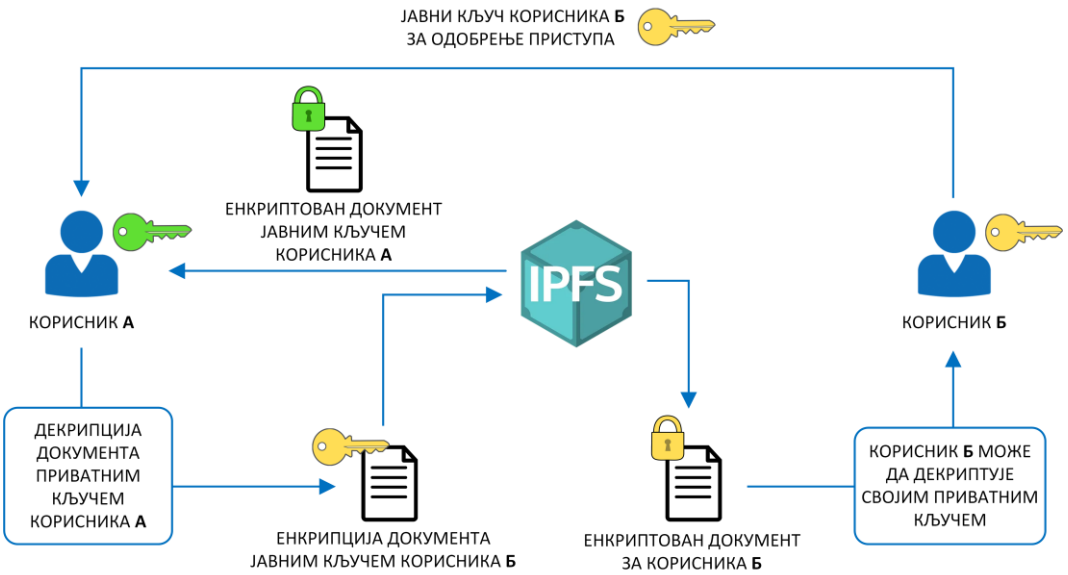
У компоненти *BCHealth* система која се односи на пружање услуга здравствене заштите, пацијент има потпуну контролу над приступом сопственим медицинским налазима. Он има могућност додељивања или укидања права приступа својим подацима, који су организовани у виду дигиталних здравствених картона. Једном ускладиштени, медицински налази су неизмењиви и не постоји могућност додавања нових информација у постојећи документ, већ само креирање нових. Пре слања у *IPFS* систем, здравствена установа енкриптује фајлове са налазима помоћу пацијентовог јавног кључа. Ово гарантује да је пацијент искључиви власник својих здравствених података, јер се они могу декриптовати само његовим приватним кључем.

Приликом уписивања медицинских налаза у *IPFS* систем, поред енкрипције помоћу пацијентовог јавног кључа, лекар дигитално потписује податке својим приватним кључем, чиме се избегава могућност нелегитимности извора и пружа погодност накнадних провера у ланцу одговорности (слика 21). Информације које се генеришу у току извршавања свих корака се бележе у *blockchain* трансакцијама.



Слика 21. Енкрипција медицинских налаза

Уколико нека болница, односно неко од припадајућег медицинског особља, жели да приступи одређеном налазу из пацијентовог дигиталног здравственог картона, то могу постићи тражењем захтева за приступ од пацијента. Након одобравања од стране пацијента, тражени медицински извештаји се енкриптују помоћу јавног кључа стране која је тражила приступ, уписују се у *IPFS* систем, и припадајући хеш код се бележи као трансакција у паметном уговору. Помоћу овог хеш кода, страна којој је одобрен приступ може да преузме одговарајући енкриптовани документ из *IPFS* система и декриптује га уз помоћ сопственог приватног кључа (слика 22). Дозвољен приступ може бити укинут од стране пацијента у било ком моменту.

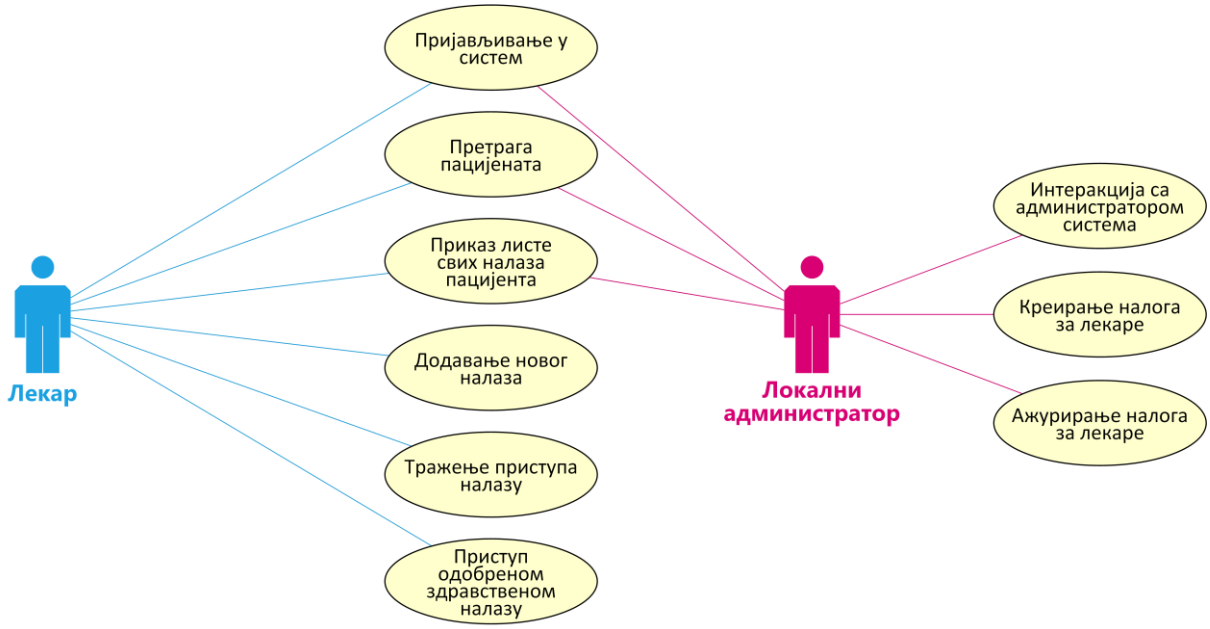


Слика 22. Реенкрипција документа

Овако пројектован пацијент-центрични приступ у развијеном моделу гарантује власништво над подацима, јер омогућава њихову сигурност, приватност, скалабилност и интегритет. *Blockchain* је искоришћен за неизмењиво бележење активности које се одвијају у систему, као што су:

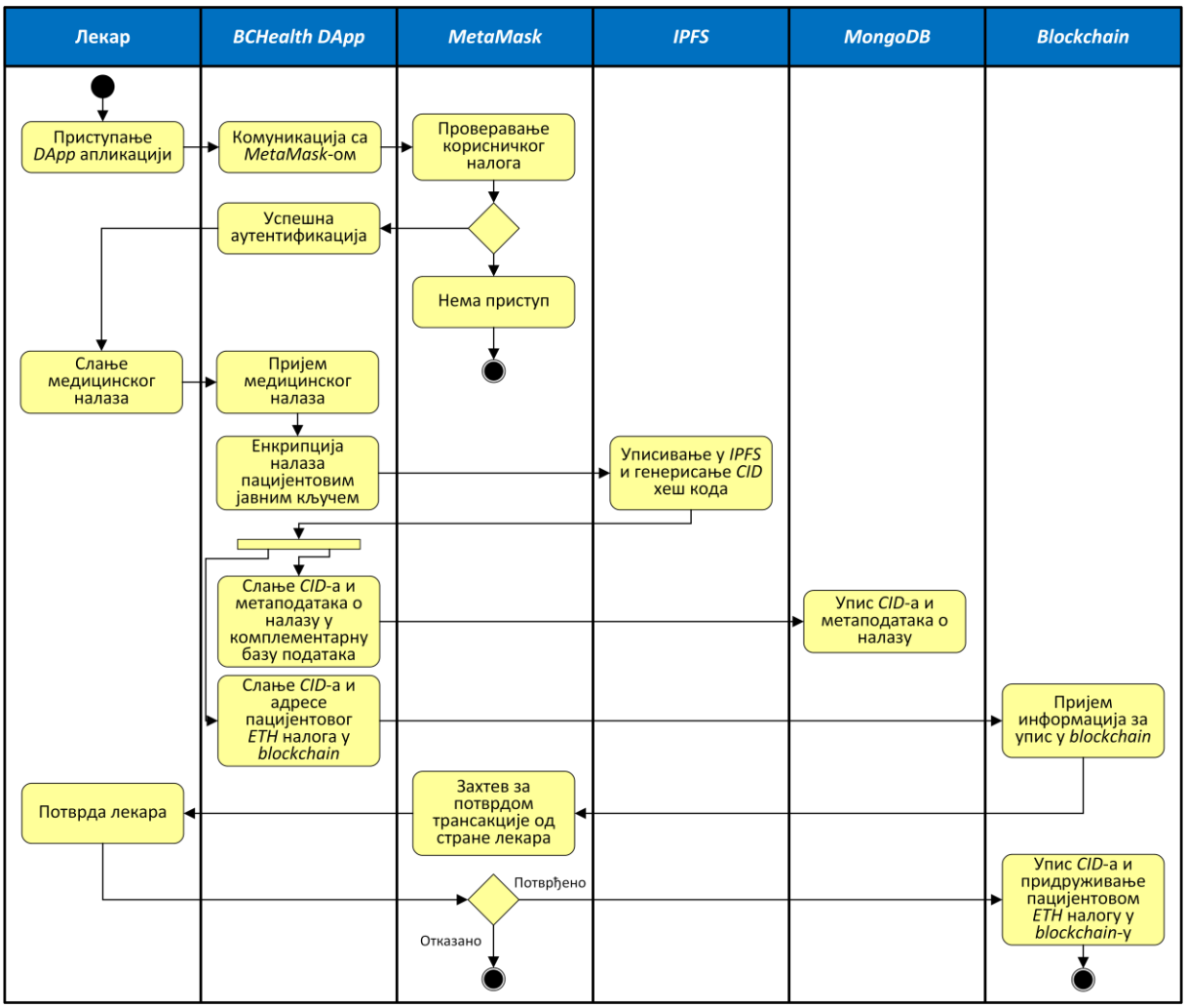
- лекар у здравственој установи креира медицински извештај за пацијента,
- пацијент приступа медицинским извештајима,
- пацијент одобрава или укида право приступа својим подацима за одређене заинтересоване учеснике система,
- заинтересована страна отвара пацијентове медицинске извештаје, за које јој је одобрен приступ.

На слици 23 су приказани случајеви коришћења *BCHealth* апликације у делу система који се односи на пружање здравствене заштите.



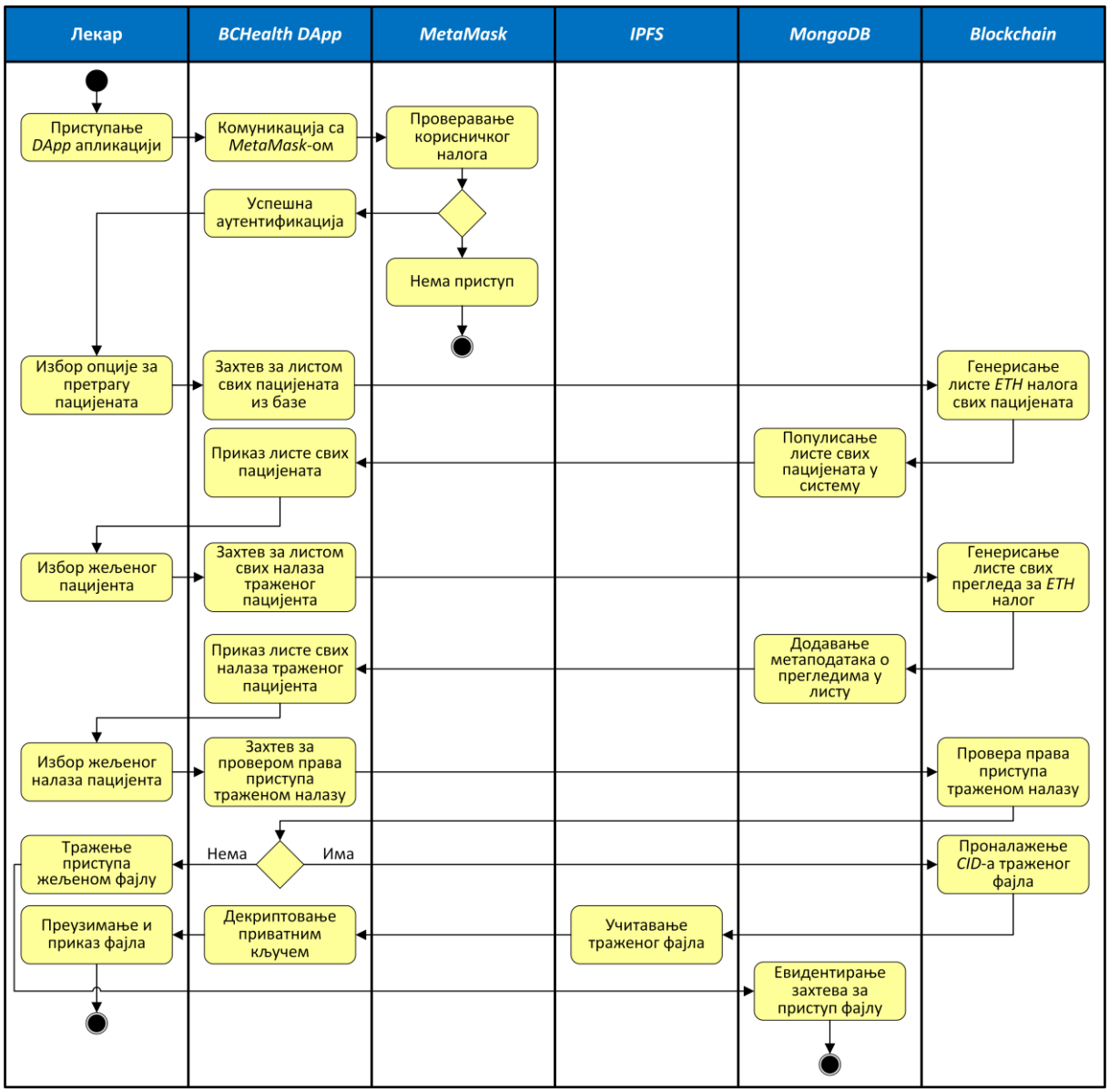
Слика 23. Модел случајева коришћења у компоненти апликације за пружање здравствене заштите

Дијаграм активности на слици 24 приказује интеракцију између компоненти система која се одиграва приликом генерисања и слања новог медицинског налаза у *BCHealth* базу. Надлежни лекар отвара *BCHealth DApp* апликацију и уз помоћ *MetaMask* интерфејса се ауторизује у систем. Након што је написан нови налаз за пацијента, он се шаље у *DApp* и енкриптује помоћу пацијентовог јавног кључа, након чега се складишти у *IPFS*. Као резултат, генерише се *CID* хеш код, који заправо представља локацију фајла у *IPFS* мрежи, и он се уписује у *Ethereum blockchain* у променљиву стања одговарајућег паметног уговора и придружује припадајућем налогу пацијента. Метаподаци о послатом фајлу се заједно са *CID* хеш кодом уписују у комплементарну *MongoDB* базу података.



Слика 24. Дијаграм активности за слање медицинског налаза у *IPFS* систем

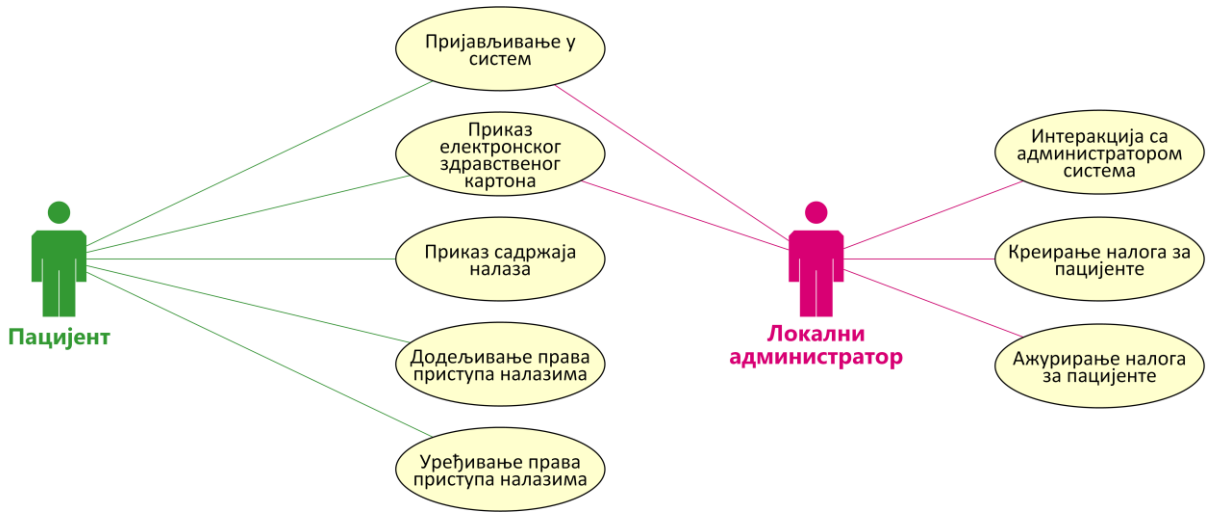
На слици 25 је приказан дијаграм активности за процес претраге листе пацијената и њихових припадајућих медицинских налаза, као и отварања жељеног извештаја. Лекар се логује у *BCHealth* апликацију и аутентификује својим налогом путем *MetaMask* интерфејса. Лекар затим бира приказ листе пацијената и њихових налаза и може да види основне податке. Избором одређеног налаза пацијента, у случају да му је приступ одобрен, лекар добија могућност да преузме и декриптује фајл својим приватним кључем, како би отворио садржај. У случају да му није одобрен приступ траженом налазу, он може да га затражи, што се евидентира и приказује на пацијентовој листи поднетих захтева за приступ здравственим подацима.



Слика 25. Дијаграм активности за приступ одређеном медицинском налазу пацијента

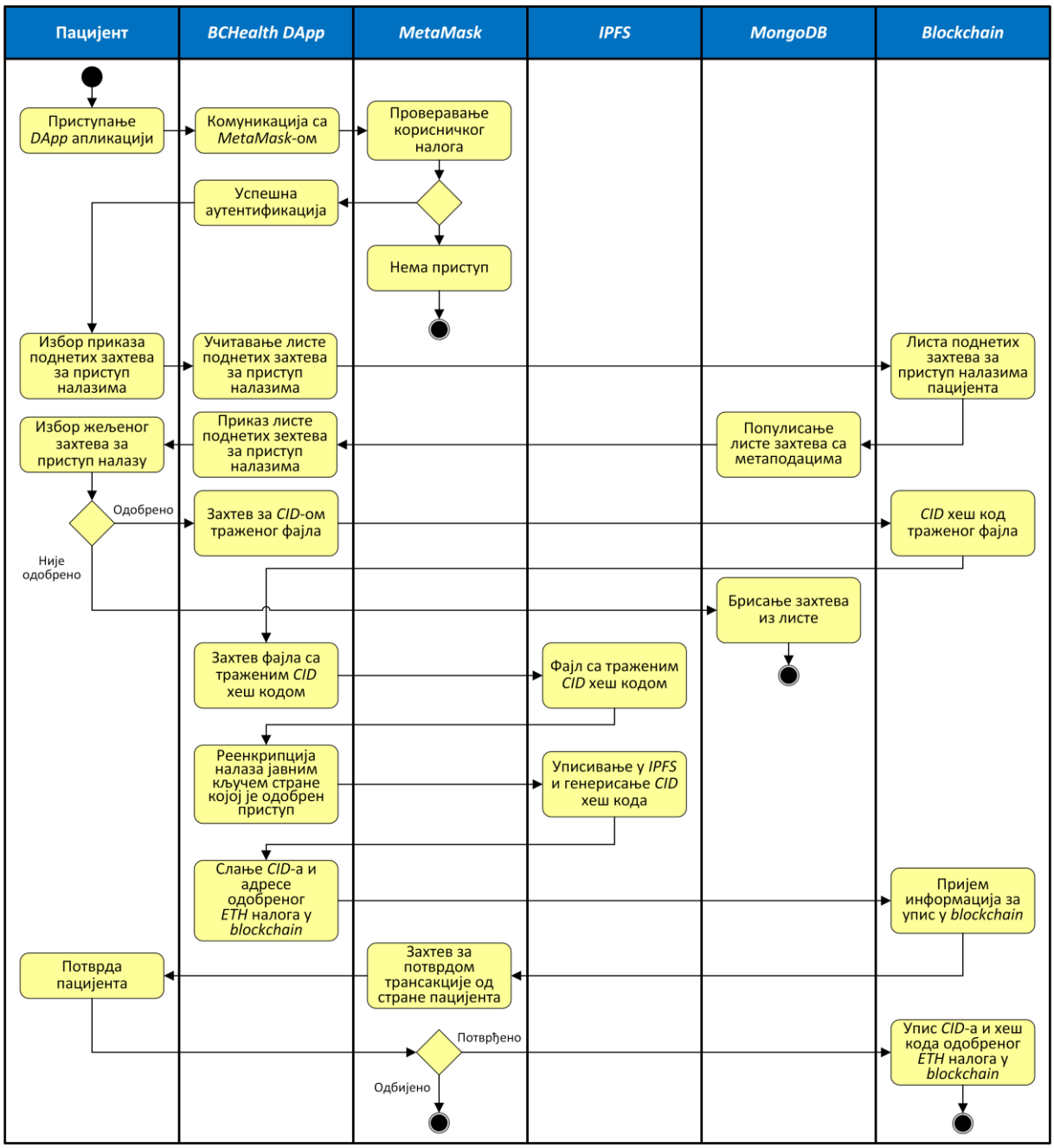
Део здравствене компоненте намењен пацијентима

Посебан део у оквиру здравствене компоненте *BCHealth* апликације пацијентима пружа увид у персоналне електронске здравствене картоне, као и могућност додељивања права приступа појединим налазима. На слици 26 је дат приказ дијаграма случајева коришћења учесника у делу здравствене компоненте апликације која је намењена пацијентима.



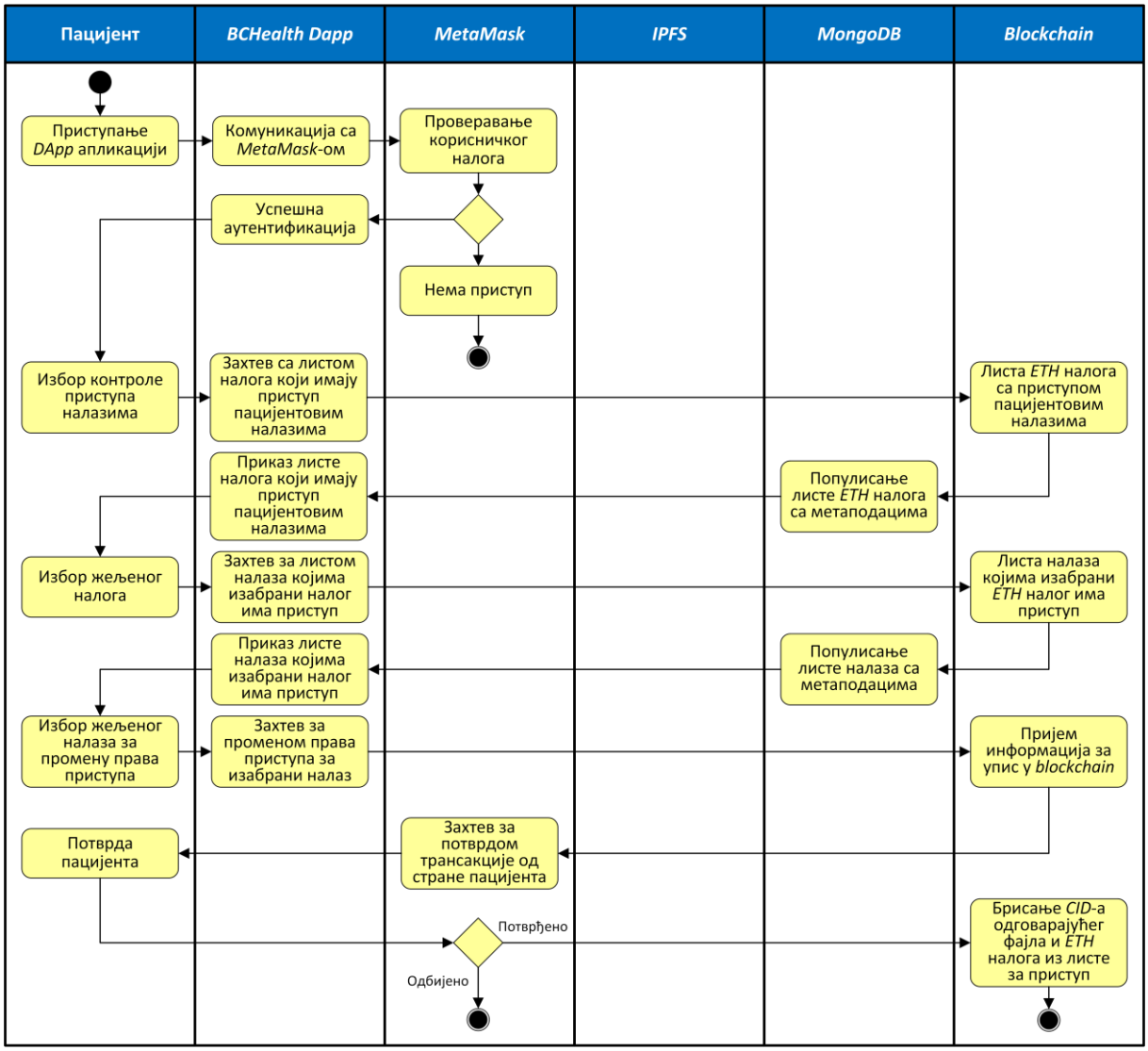
Слика 26. Дијаграм случајева коришћења у делу апликације намењеном пацијентима

Слика 27 приказује редослед активности приликом пацијентовог приступа систему и обраде листе поднетих захтева за приступ његовим здравственим налазима. Пацијент се логује у *BCHealth* апликацију и бира опцију за приказ поднетих захтева. У листи добија информацију ком здравственом налазу се тражи приступ, као и податке о лекару који је поднео захтев. Уколико пацијент одобри приступ налазу, одговарајући фајл се преузима из *IPFS* система и путем реенкрипције се енриптује јавним кључем подносиоца захтева за приступ. Новонастали фајл се шаље у *IPFS* систем, и *CID* хеш код који се генерише се уписује у *blockchain* и придружује *ETH* налогу којем је приступ одобрен.



Слика 27. Дијаграм активности за одобравање приступа медицинском налазу пацијента

Пацијент у сваком моменту може да врши измене приступа својим налазима. Избором функције контроле приступа, на одговарајућем екрану се приказује списак свих корисника система који имају право приступа одређеном документу. Пацијент може за сваки унос у листи да укине право приступа, или да га поново додели. Слика 28 приказује дијаграм активности за уређивање права приступа налазима пацијента.



Слика 28. Дијаграм активности за измену права приступа пацијентовом налазу

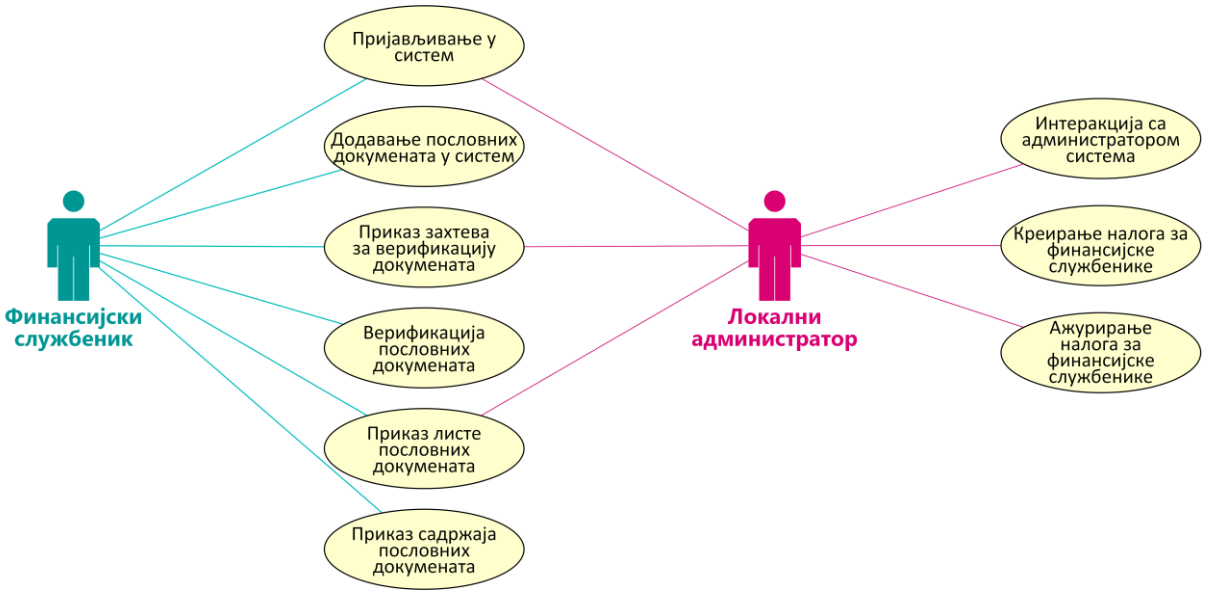
6.8.4. *BCHealth* апликација – пословна компонента

BCHealth апликација, поред описане компоненте која се односи на пружање услуга здравствене заштите, односно креирање и управљање медицинским налазима, нуди и функционалност верификације и безбедног архивирања докумената који се генеришу у активностима пословне интеракције стејкхолдера у дигиталном здравственом екосистему. Уговори, наруџбенице, фактуре и друга пословна документација захтевају складиштење на дуг временски рок, уз обезбеђење сигурности и неизмењивости једном уписаних информација, како би се спречио било који вид манипулације подацима и угрожавање пословања.

Подаци пословне кореспонденције стејкхолдера дигиталног екосистема се, аналогно примењеном алгоритму у здравственом делу *BCHealth* апликације, могу енкриптовати и складиштити у децентрализованом *IPFS* систему, уз чување приступних *CID* хеш кодова у промењивама стања *Ethereum blockchain* дигиталног регистра, односно одговарајућих паметних уговора. Као власници генерисаних и архивираних података се идентификују све стране које учествују у кореспонденцији и, захваљујући описаном начину

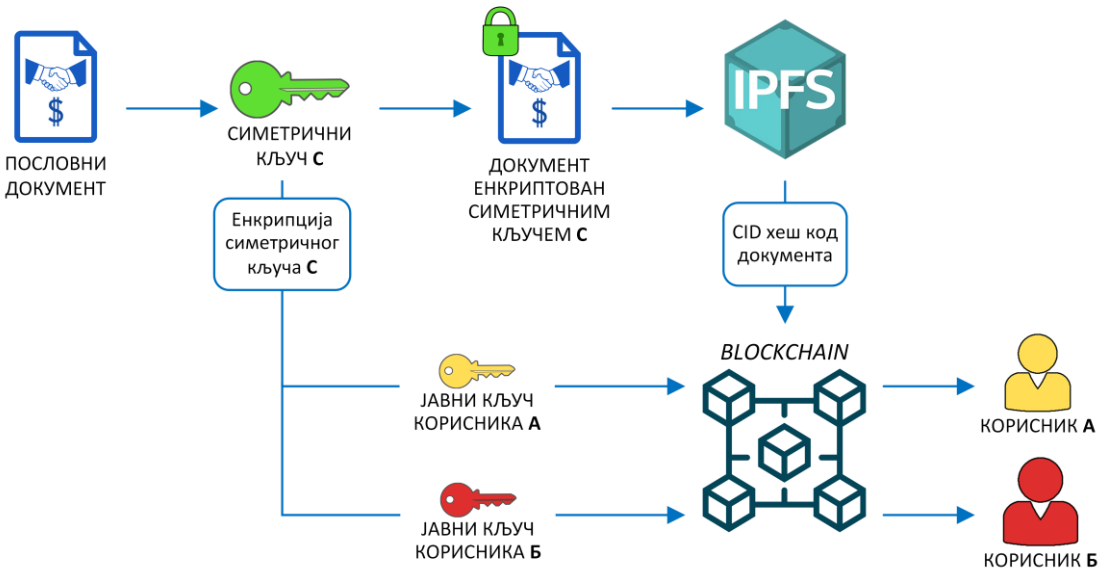
складиштења, само оне имају могућност отварања садржаја помоћу сопствених приватних кључева. Уколико се укаже потреба да се неком учеснику у дигиталном екосистему омогући приступ одређеном делу документације, то се може постићи реенкрипцијом одговарајућих фајлова, уз употребу јавног кључа заинтересоване стране.

У раду у пословној компоненти *BCHealth* апликације учествују, као представници својих матичних институција, финансијски службеници, који имају могућност да дигитално потписују фајлове са документацијом, који се затим безбедно складиште. За верификацију корисничких налога, као и неопходних одговарајућих *Ethereum* налога, задужен је администратор комплетног система, односно здравствено регулаторно тело, које врши проверу веродостојности идентификационих података корисника система. На слици 29 је дат приказ случајева коришћења учесника у пословном делу апликације *BCHealth*.



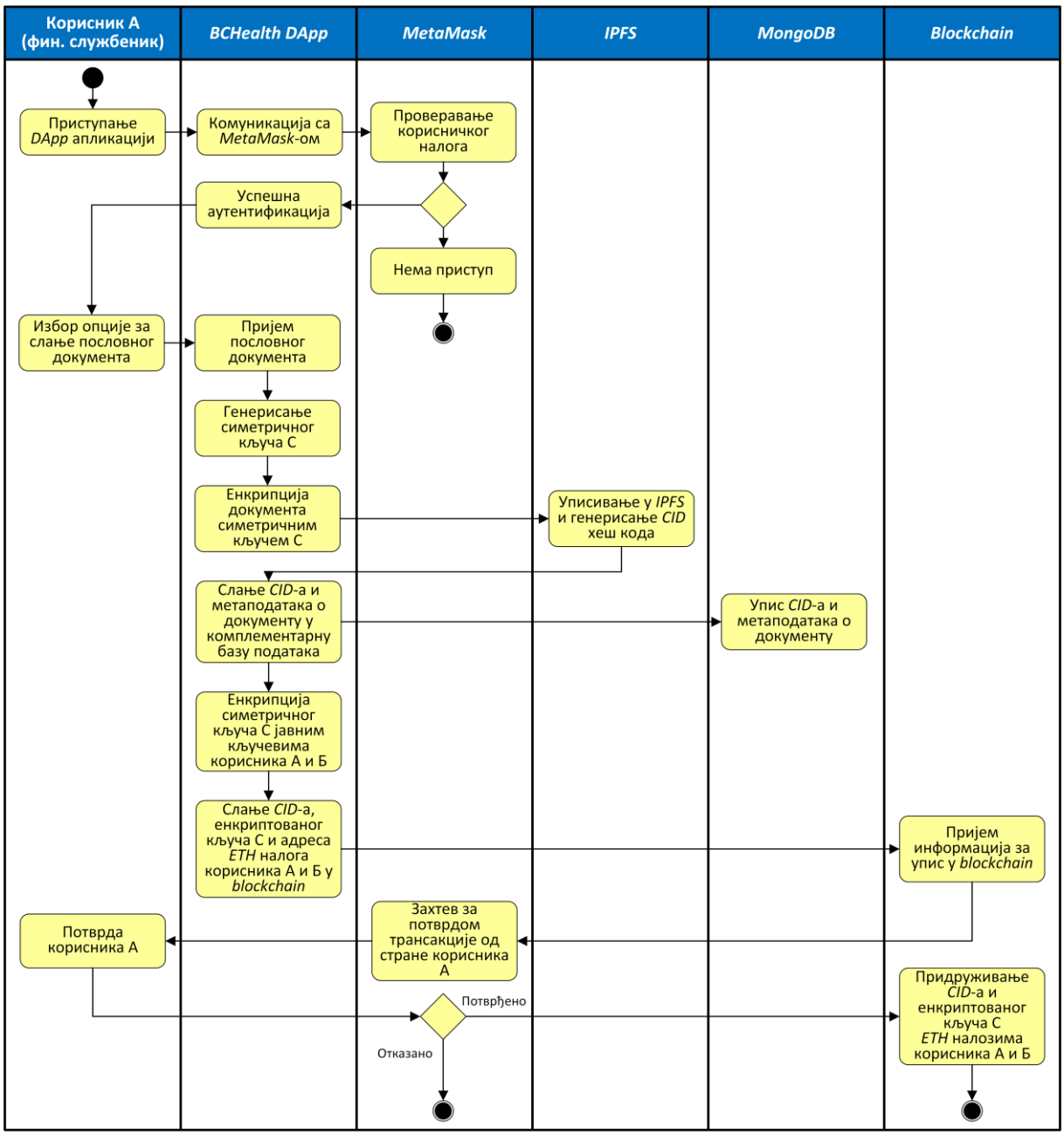
Слика 29. Дијаграм случајева коришћења у пословном делу апликације *BCHealth*

Документа која се генеришу у пословној кореспонденцији учесника дигиталног здравственог екосистема, поред енкрипције и складиштења у *IPFS*, морају да прођу процес верификације обе укључене стране. У случају да се ради о уговорима или споразумима који подразумевају већи број потписника документа, мора да буде омогућено бележење потписа односно верификација свих страна које су учесници. Управо из разлога могућег већег броја учесника односно потписника, за овај део апликације је изабрана комбинација симетричне и асиметричне енкрипције (слика 30). У оваквом случају, подаци се најпре енкриптују помоћу заједничког симетричног кључа за све стране. Како би се осигурало да само укључене стране могу приступити заштићеном садржају, систем енкриптује наведени симетрични кључ помоћу јавног кључа сваког од учесника засебно. На тај начин, укључени учесници могу својим приватним кључевима декриптовати симетрични кључ и помоћу њега приступити садржају одговарајућих заштићених докумената.



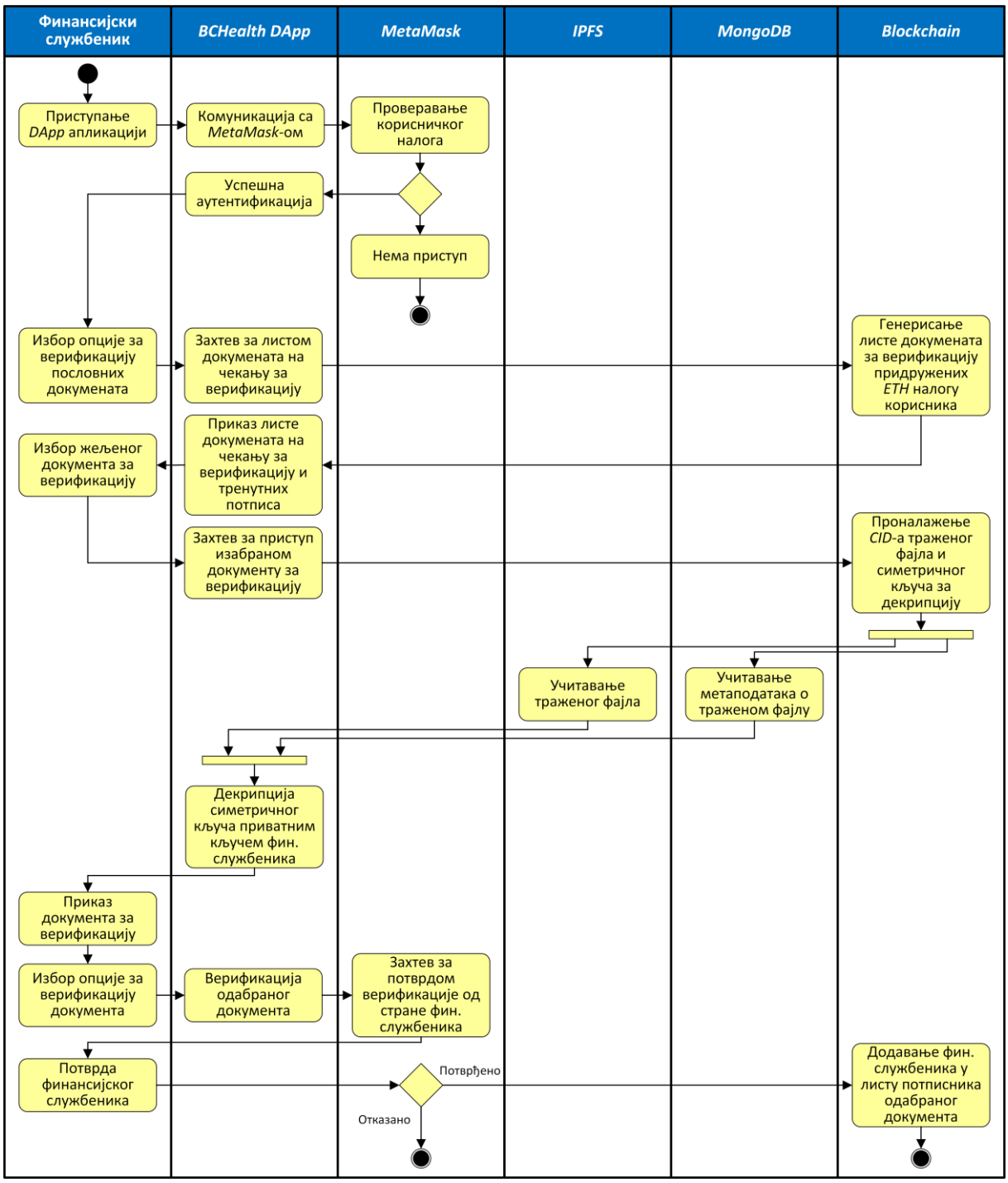
Слика 30. Комбинација симетричне и асиметричне енкрипције пословног документа

У *BCHealth* апликацији пословна документација се увози у виду генерисаних фајлова из посебних постојећих књиговодствених извора. Корисник А, који представља финансијског службеника своје матичне институције, се најпре пријављује у *BCHealth* систем помоћу сопственог *ETH* налога. Након успешне аутентификације, корисник А бира опцију за архивирање пословног документа. Учитани документ се енкриптује помоћу генерисаног симетричног кључа и шаље у *IPFS* систем на складиштење. У *MongoDB* базу се шаљу метаподаци о документу и *CID* хеш код генерисан од стране *IPFS* система. Симетрични кључ се енкриптује јавним кључевима корисника А и корисника Б, који представља другу страну укључену у пословну активност за коју је везан документ. Симетрични кључ, заједно са *CID* хеш кодом документа, се уписује у *blockchain* и придружује *ETH* налозима корисника А и Б. На овај начин, приступ симетричном кључу за декрипцију пословног документа ће имати само корисници А и Б, употребом сопствених приватних кључева. На слици 31 је приказан дијаграм активности који описује поступак слања и енкрипције пословног документа.



Слика 31. Дијаграм активности за складиштење пословног документа у *BCHealth* апликацији

Сваки од учесника пословне кореспонденције, након провере документа, верификује његов садржај и даје своју сагласност у виду својеврсног дигиталног потписа, који се бележи у *blockchain*-у и даје на увид преосталим странама. На крају процеса верификације свих страна које су учесници у пословној кореспонденцији везаној за одређени документ, добија се фајл који је енкриптован и безбедно ускладиштен у децентрализованом систему *IPFS*. У *blockchain*-у је уписана адреса за приступ фајлу, а симетрични кључ за отварање његовог садржаја је енкриптован јавним кључевима свих укључених учесника. Учесници помоћу својих приватних кључева могу приступити симетричном кључу а затим и траженом фајлу, а такође добити и потврду да су све преостале стране дигитално потписале односно верификовале садржај документа. На слици 32 је приказан дијаграм активности приликом верификације пословних докумената од стране финансијских службеника.



Слика 32. Дијаграм активности приликом верификације пословних докумената од стране финансијског службеника

7. ИМПЛЕМЕНТАЦИЈА РАЗВИЈЕНОГ МОДЕЛА

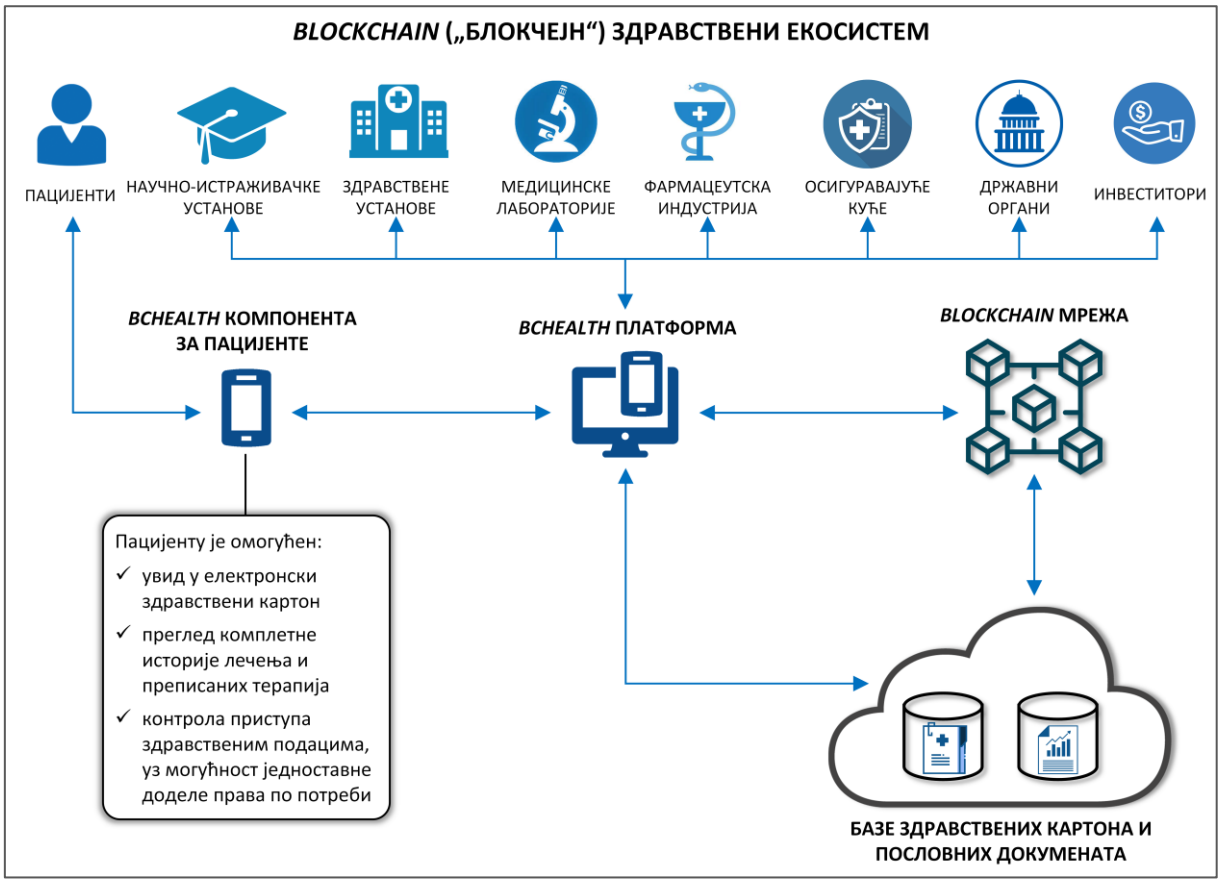
Процес имплементације предложеног модела истраживања пројектован је кроз следеће фазе:

- Пилот истраживање – анкета међу стејкхолдерима о познавању значаја дигиталног здравства, сајбер сигурности и *blockchain* технологије, са циљем процене потребе за развијањем сервиса дигиталног здравства базираног на *blockchain* технологији и уочавањем потенцијалних фактора значајних за имплементацију модела.
- Дизајнирање и израда софтверских решења за предложени модел дигиталног здравственог екосистема заснованог на *blockchain* технологији.
- Планирање имплементације развијеног модела у здравствену установу.
- Одабир здравствене установе у којој ће се спроводити имплементација развијеног модела.
- Практична примена софтверских решења из модела у изабраној здравственој установи и мониторинг процеса имплементације.

7.1. Пилот истраживање

У циљу процене заинтересованости, тј. потребе за увођењем новина у дигитално здравство, односно примене *blockchain*-а у функцији развијања сервиса дигиталног здравства базираног на овој технологији, спроведена је онлајн анкета путем *Google Forms* платформе у периоду од 03.01.2023. до 18.01.2023. Анкету је попунило 150 испитаника.

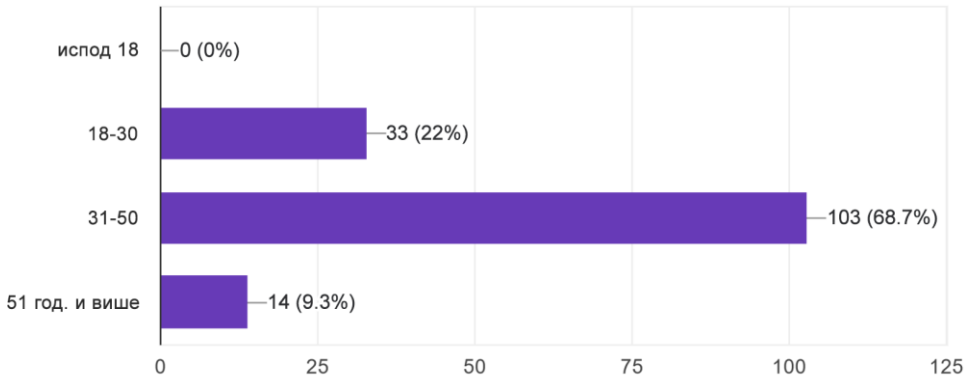
У уводу анкете је дат опис *blockchain* технологије у функцији дигиталног здравства, како би се испитаници детаљније упознали са значајем могуће примене у здравственом сектору, што је ради егзактнијег разумевања приказано и графички (слика 33). Представљени су идентификовани стејкхолдери здравственог сектора, ток информација између главних компоненти потенцијалног система, као и најважније функционалности које би пацијентима биле на располагању путем коришћења апликације базиране на *blockchain* технологији.



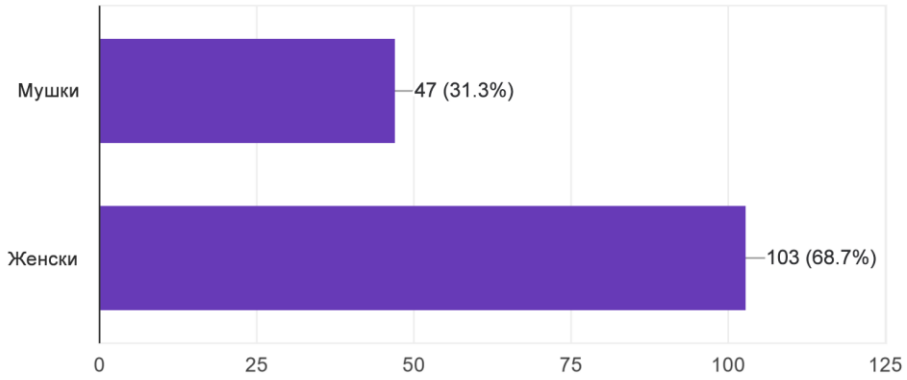
Слика 33. Слика која је дата анкетираним лицима у објашњењу значаја анкете

Графикони 1-32 приказују одговоре на свако од постављених питања у анкети у оквиру пилот истраживања.

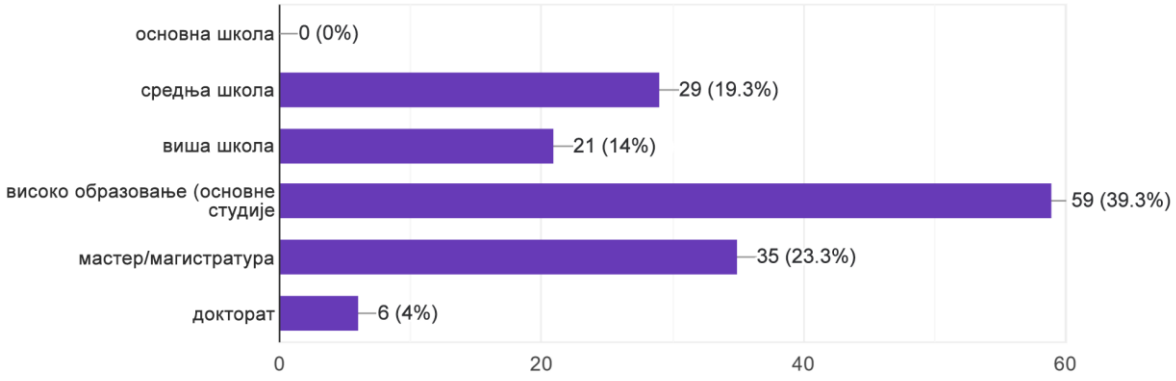
Графикон 1. Графички приказ одговора на питање: „Колико имате година?” 150 одговора



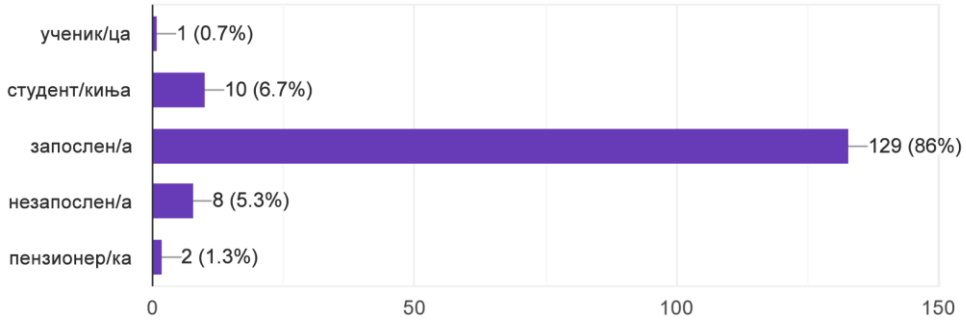
Графикон 2. Графички приказ одговора на питање: „Пол:” 150 одговора



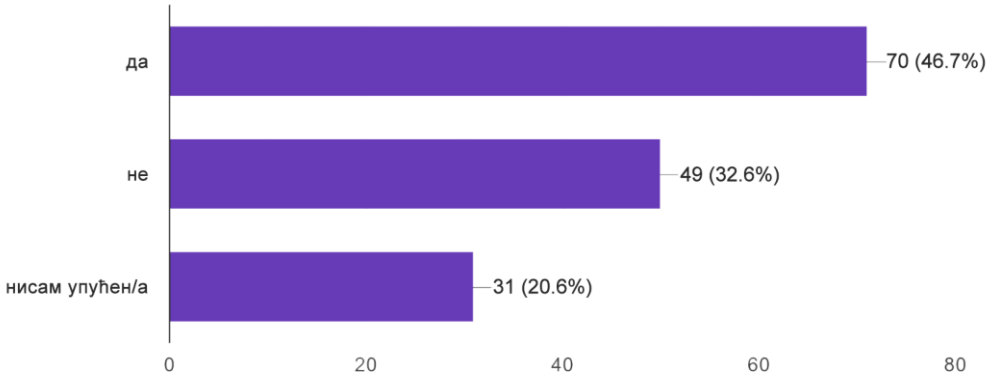
Графикон 3. Графички приказ одговора на питање: „Образовни ниво:” 150 одговора



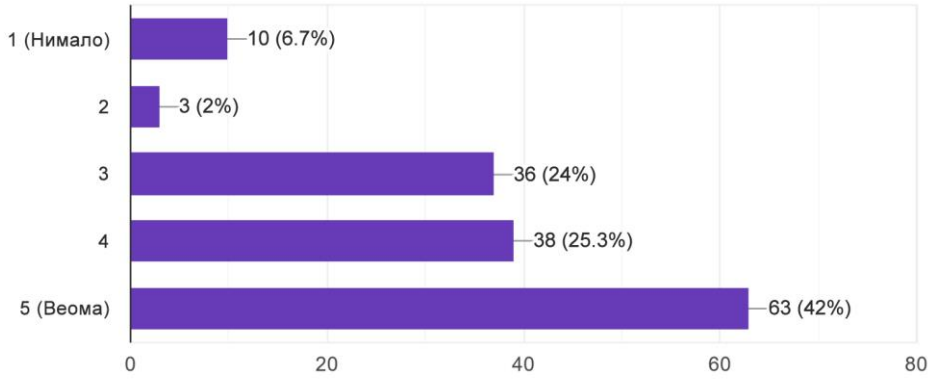
Графикон 4. Графички приказ одговора на питање: „Радни статус:” 150 одговора



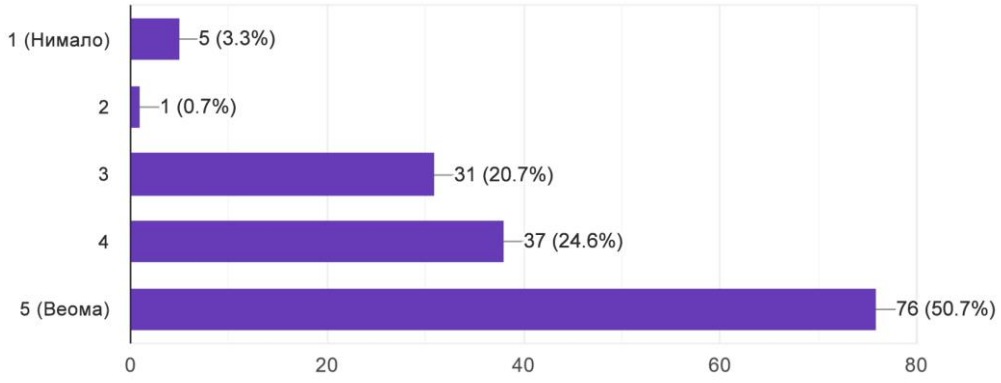
Графикон 5. Графички приказ одговора на питање: „Да ли користите неке од сервиса дигиталног здравства?” 150 одговора



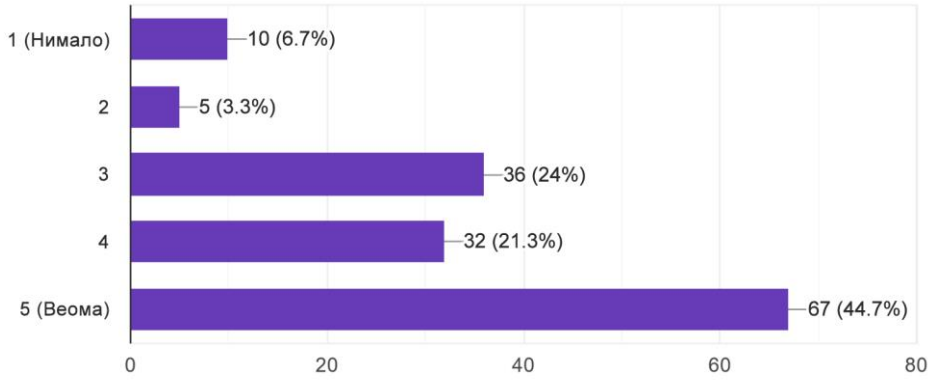
Графикон 6. Графички приказ одговора на питање: „На скали од 1 до 5 оцените у којој мери сматрате да је примена дигиталног здравства ефикаснија од традиционалног облика коришћења здравствених услуга:” 150 одговора



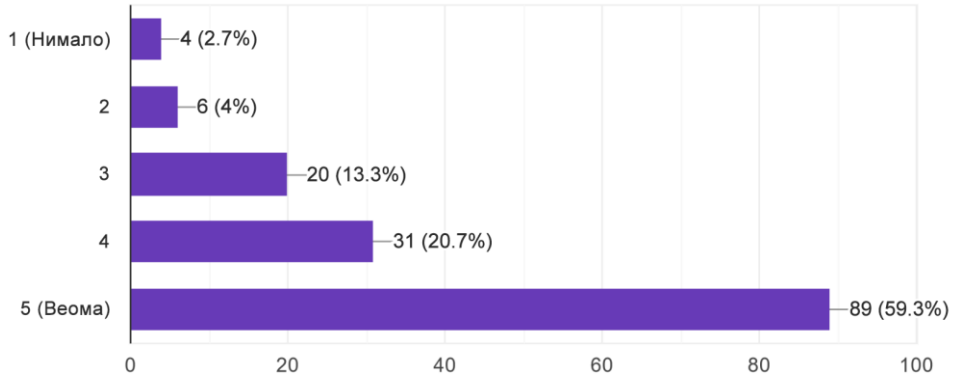
Графикон 7. Графички приказ одговора на питање: „Колико, по Вашем мишљењу, примена сервиса дигиталног здравства може да унапреди квалитет медицинских услуга?” 150 одговора



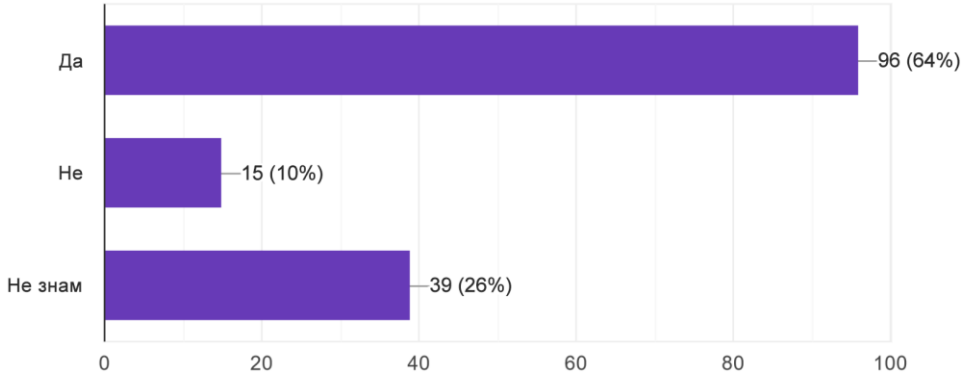
Графикон 8. Графички приказ одговора на питање: „На скали од 1 до 5 оцените у којој мери сматрате да услуге дигиталног здравства олакшавају Ваш медицински третман:” 150 одговора



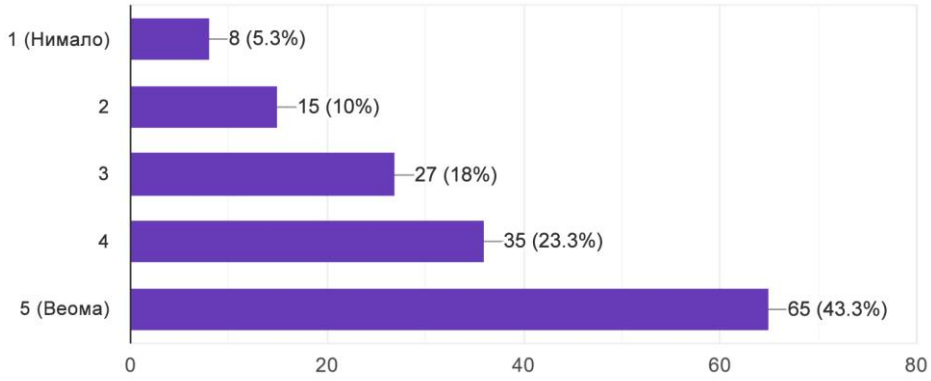
Графикон 9. Графички приказ одговора на питање: „На скали од 1 до 5 оцените у којој мери сматрате да бисте се могли прилагодити коришћењу сервиса дигиталног здравства:” 150 одговора



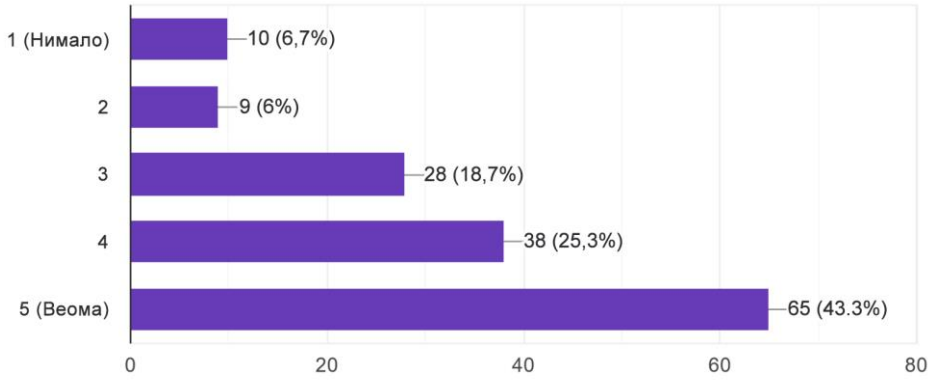
Графикон 10. Графички приказ одговора на питање: „Да ли неко из Вашег окружења користи сервисе дигиталног здравства (е-рецепт, дигиталне здравствене апликације,...)? 150 одговора



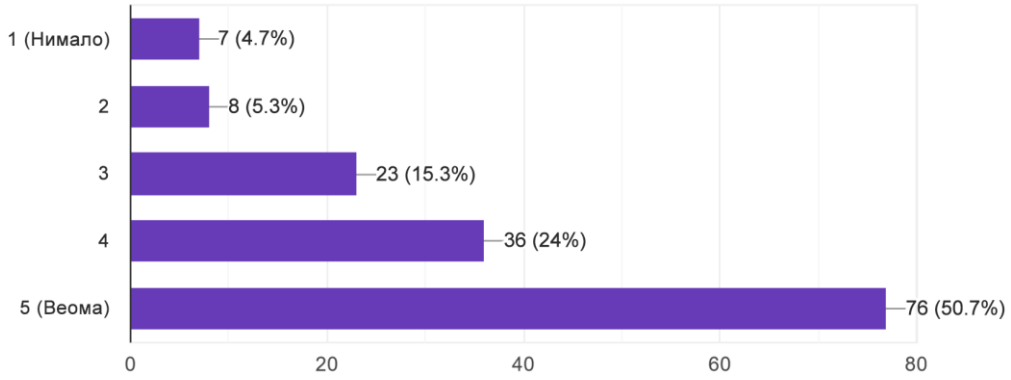
Графикон 11. Графички приказ одговора на питање: „У којој мери сматрате да се применом сервиса дигиталног здравства може постићи боља контрола Вашег здравља?” 150 одговора



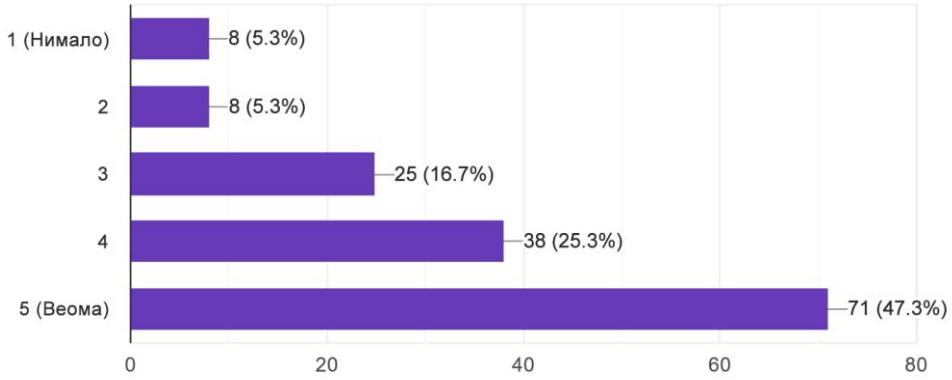
Графикон 12. Графички приказ одговора на питање: „Уколико неко из Вашег блиског окружења користи услуге дигиталног здравства, у којој мери ће Вас то подстаћи на њихову примену?” 150 одговора



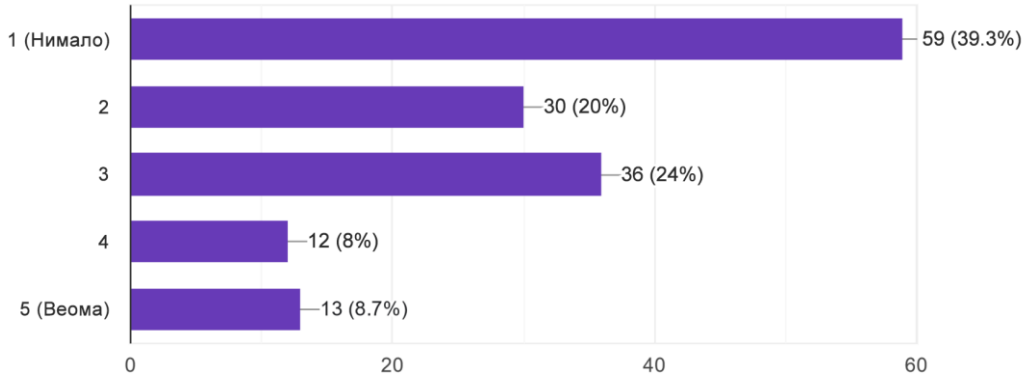
Графикон 13. Графички приказ одговора на питање: „У којој мери сматрате да примена сервиса дигиталног здравства подиже ниво здравствене културе целокупне популације?” 150 одговора



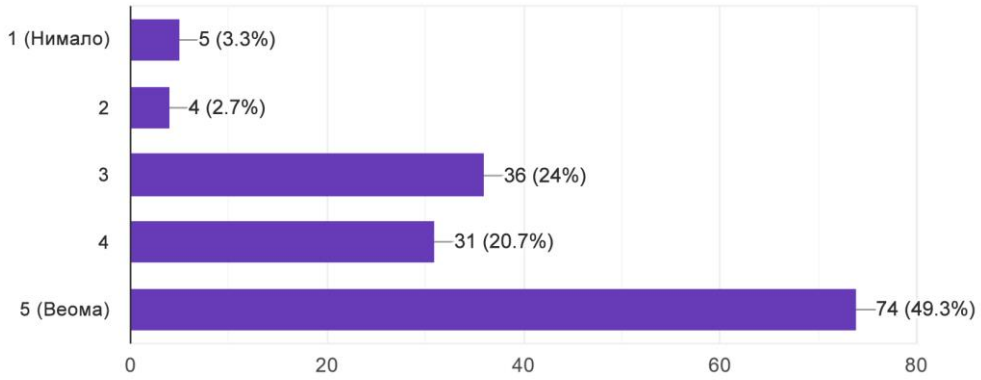
Графикон 14. Графички приказ одговора на питање: „У којој мери сматрате да поседујете довољно знања за употребу сервиса дигиталног здравства?” 150 одговора



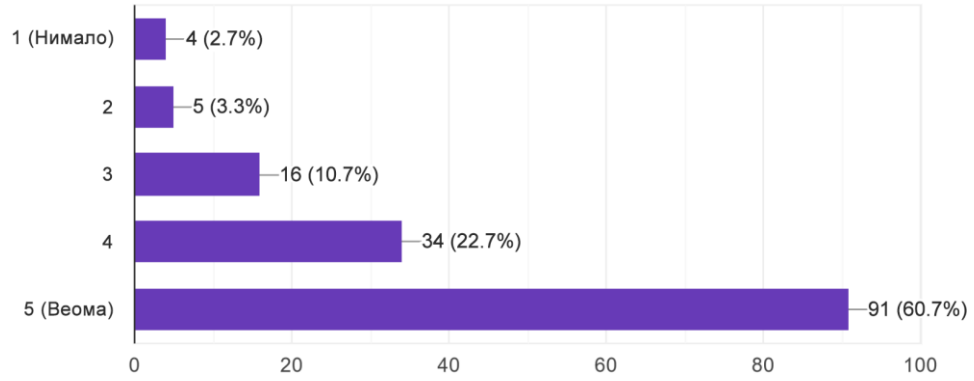
Графикон 15. Графички приказ одговора на питање: „У којој мери сматрате да је примена сервиса дигиталног здравства компликована за свакодневну примену?” 150 одговора



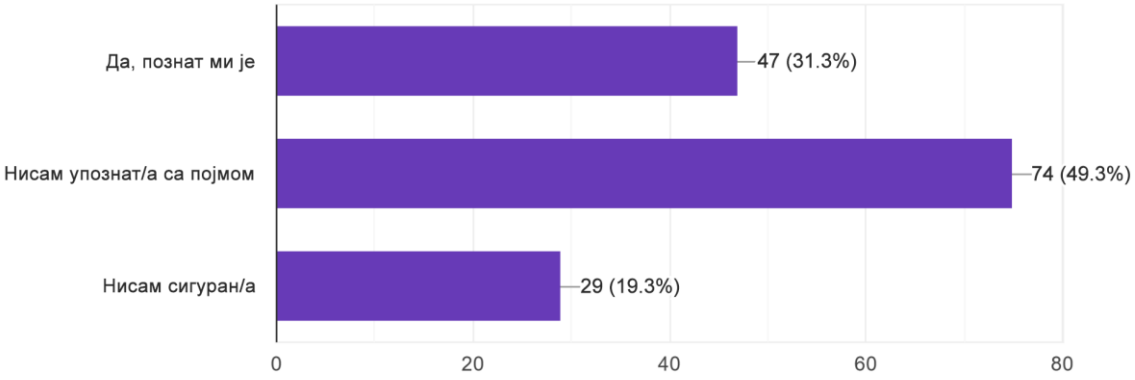
Графикон 16. Графички приказ одговора на питање: „У којој мери сматрате да дигитално здравство може да допринесе бољем приступу здравственој заштити?” 150 одговора



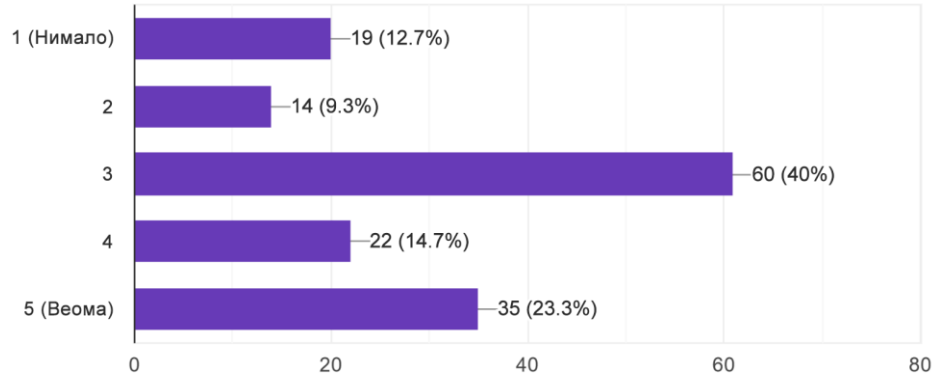
Графикон 17. Графички приказ одговора на питање: „Да ли, по Вашем мишљењу, примена дигиталног здравства може да олакша увид у Ваше целокупно здравствено стање када одлазите код лекара различитих специјалности?” 150 одговора



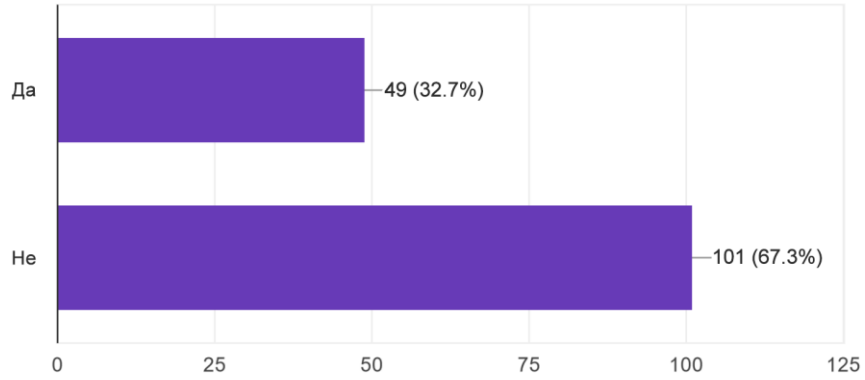
Графикон 18. Графички приказ одговора на питање: „Да ли Вам је познат појам блокчејн технологије и могућности њене примене?” 150 одговора



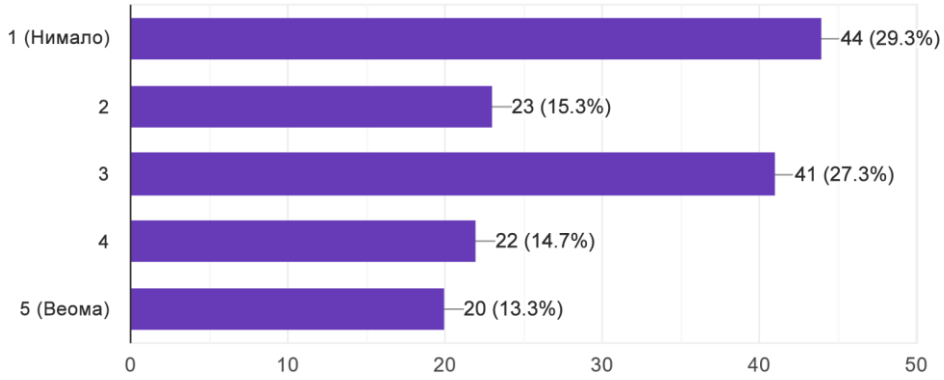
Графикон 19. Графички приказ одговора на питање: „Колико сматрате значајном блокчејн технологију за примену у здравственом сектору?” 150 одговора



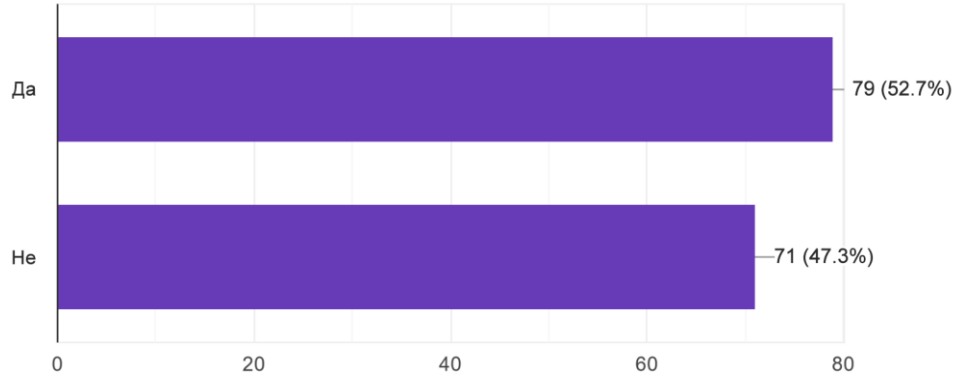
Графикон 20. Графички приказ одговора на питање: „Да ли сте упознати са трговином здравственим информацијама?” 150 одговора



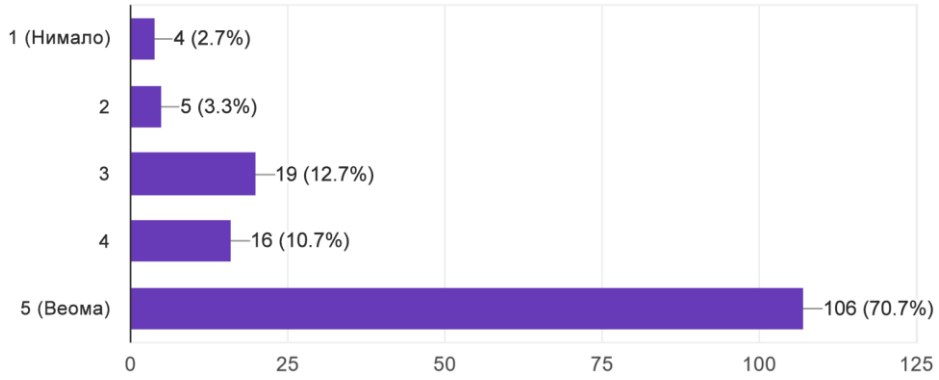
Графикон 21. Графички приказ одговора на питање: „Колико сте сигурни да Ваши подаци неће бити злоупотребљени када их делите са Вашим лекаром?” 150 одговора



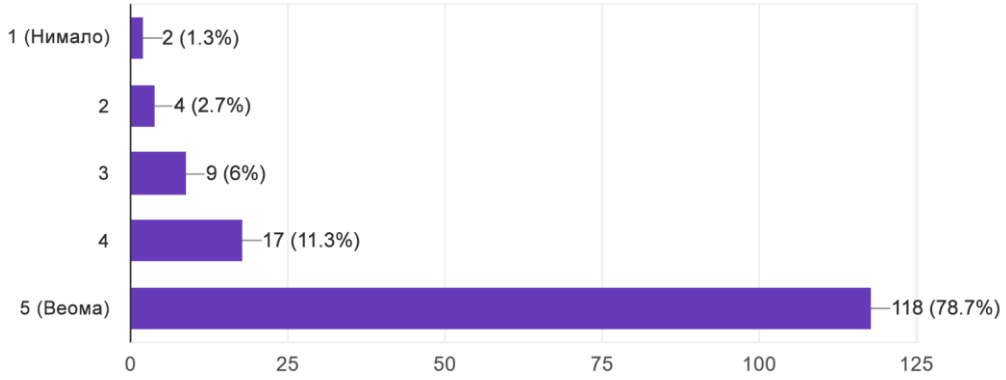
Графикон 22. Графички приказ одговора на питање: „Да ли сте сагласни да се Ваши медицински подаци користе и размењују између лекара, фармацеутских и научних институција?” 150 одговора



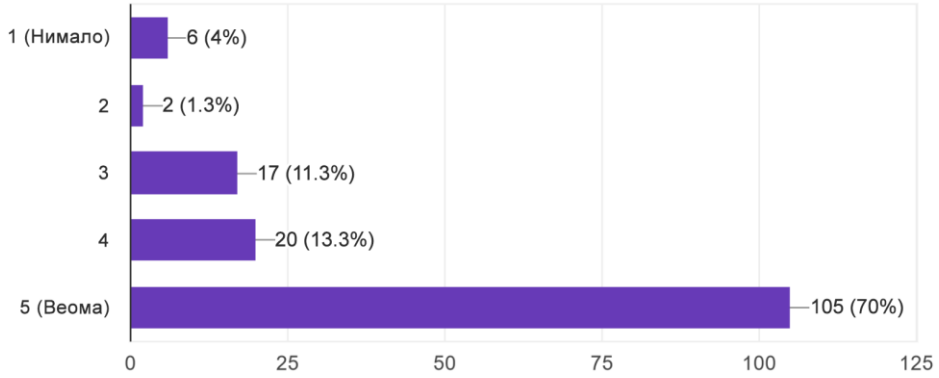
Графикон 23. Графички приказ одговора на питање: „Измерили сте крвни притисак код куће и проследили сте податак помоћу здравствене апликације Вашем лекару. Након неког периода схватите да је податак измењен. Колико је, по Вашем мишљењу, ситуација озбиљна?” 150 одговора



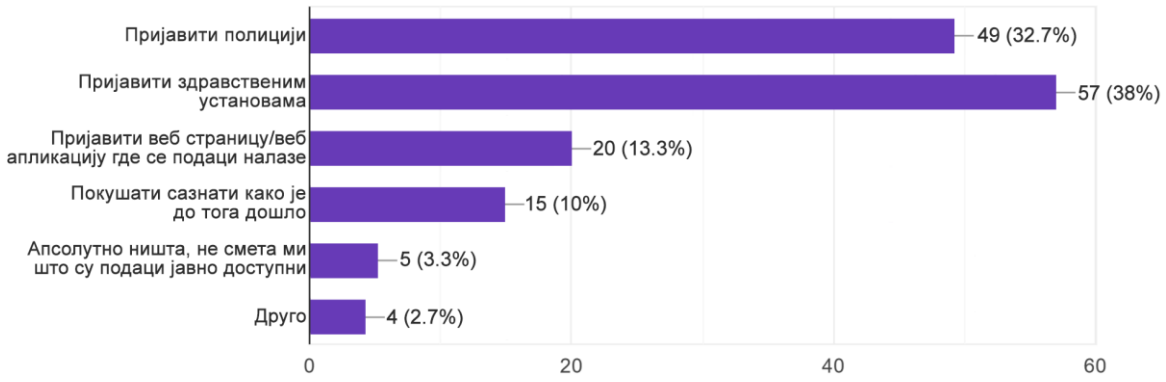
Графикон 24. Графички приказ одговора на питање: „Подаци са Вашим резултатима анализе крви су изманипулисани и измењени током слања из здравствене лабораторије лекару опште праксе. Колико је, по Вашем мишљењу, стање алармантно?” 150 одговора



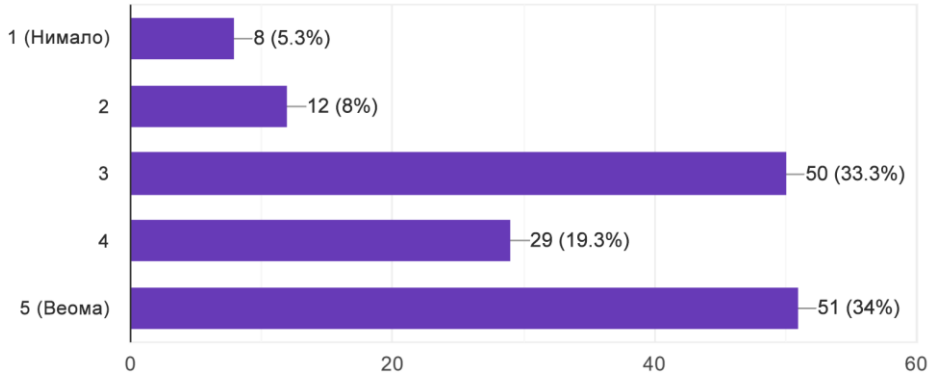
Графикон 25. Графички приказ одговора на питање: „Злонамерна особа (рачунарски „хакер”) напала је здравствени систем у којем се налазе и Ваши подаци, информације, анамнеза. Уколико би сви подаци били избрисани, оцените колико је ситуација ризична за даље лечење и здравствене услуге у будућности?” 150 одговора



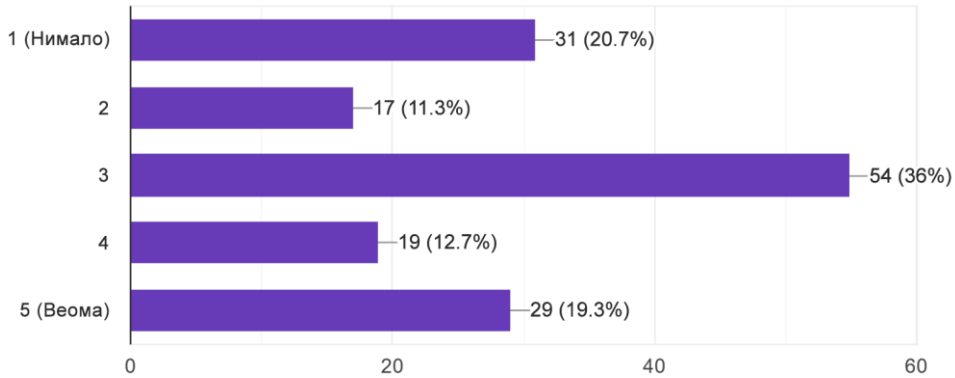
Графикон 26. Графички приказ одговора на питање: „Ваши здравствени подаци који се налазе у здравственом систему су из непознатог разлога пласирани у јавност и слободно су доступни на интернету. Шта ћете предузети? Одаберите један одговор који у највећој мери описује активност коју ћете предузети.” 150 одговора



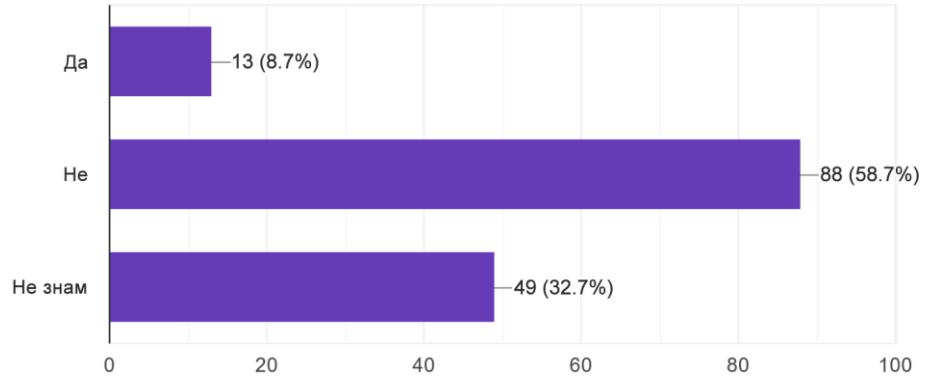
Графикон 27. Графички приказ одговора на питање: „У којој мери сматрате да ће се вршити фалсификовање здравствених пасоша?” 150 одговора



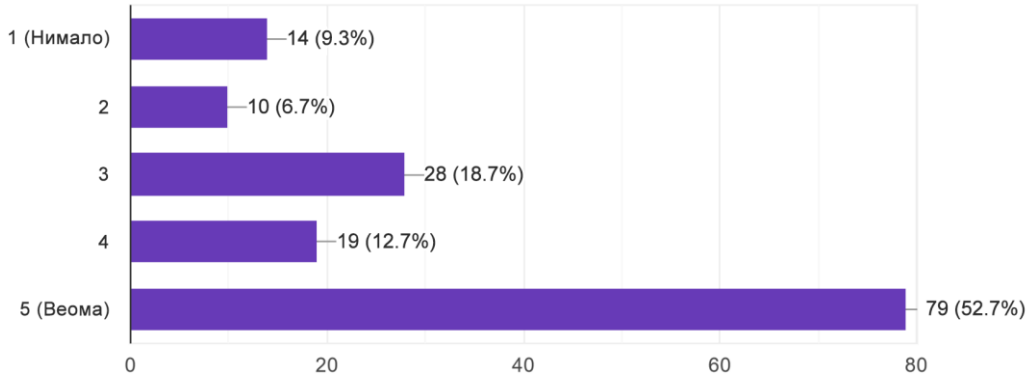
Графикон 28. Графички приказ одговора на питање: „У којој мери сматрате да су Ваши подаци сигурни када званичним организацијама које желе да провере Ваше здравствено стање (авио-компанија, гранична полиција,…) дајете на увид Ваш здравствени пасош?” 150 одговора



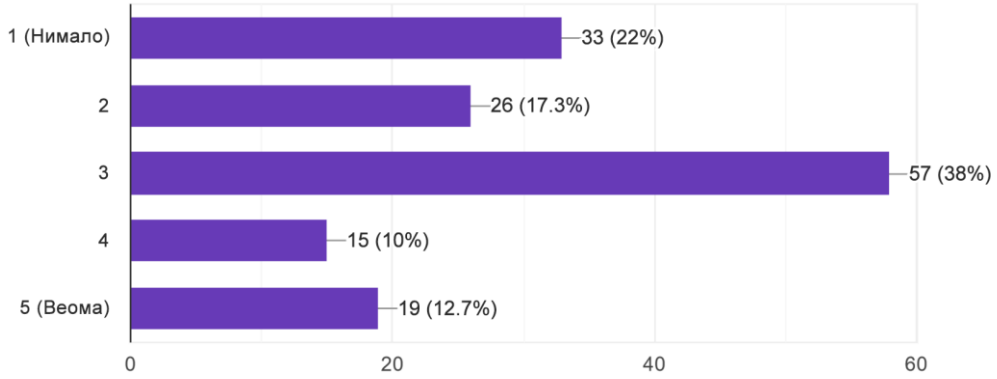
Графикон 29. Графички приказ одговора на питање: „Да ли бисте Ваше податке делили са медицинским установама помоћу здравствених апликација, иако знате да сервис/апликација није заштићена?” 150 одговора



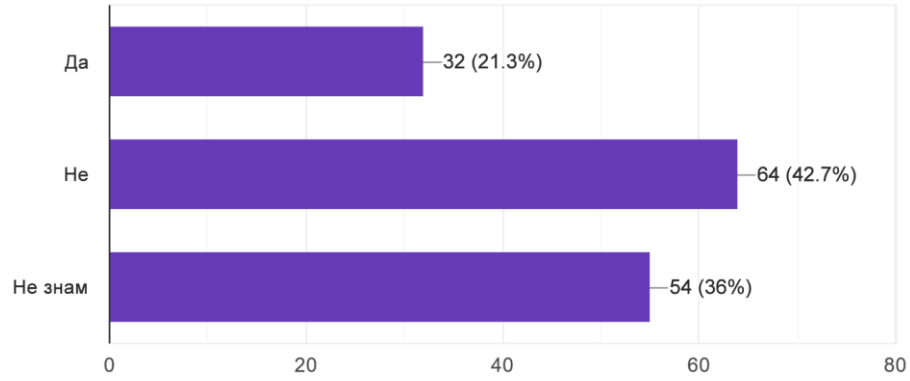
Графикон 30. Графички приказ одговора на питање: „На скали од 1 до 5 означите колико сматрате да је значајна сигурност Ваших електронских здравствених података?” 150 одговора



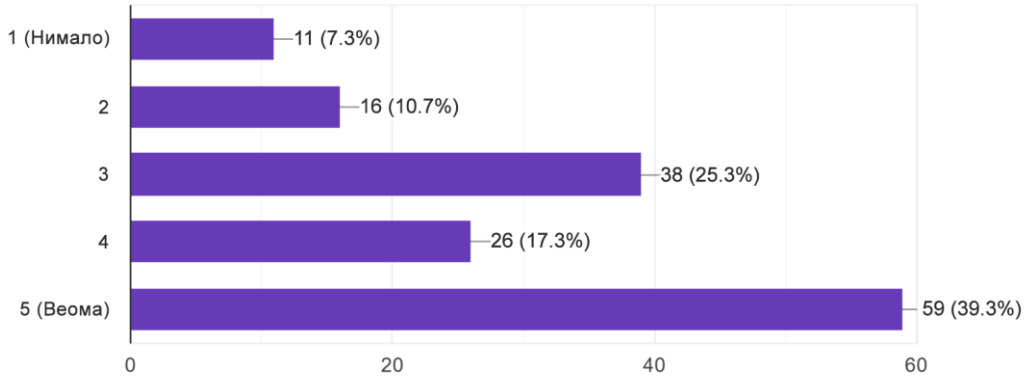
Графикон 31. Графички приказ одговора на питање: „На скали од 1 до 5, колико сматрате да су Ваши здравствени подаци електронски безбедно архивирани?” 150 одговора



Графикон 32. Графички приказ одговора на питање: „Да ли мислите да Вашим медицинским подацима приступају само особе које имају право приступа и које су ауторизоване?” 150 одговора



Графикон 33. Графички приказ одговора на питање: „У којој мери бисте били заинтересовани за примену сервиса базираних на дигиталној технологији у оквиру пружања здравствених услуга?” 150 одговора



Закључци који следе из спроведене анкете:

- Од шире јавности препозната је потреба за развојем дигиталног здравства, чиме се може обезбедити квалитетнији ниво медицинских услуга.
- Исказан је висок степен потребе за дигиталним здравством.
- Потенцијални корисници су већином припремљени за даље кораке дигитализације у сфери здравства, јер имају искуства са појединим услугама из домена е-здравства.
- Препозната је потреба за интегративном функционалношћу коју може да пружи даља дигитализација здравственог сектора, чиме се обезбеђује несметан проток здравствених података између здравствених установа у циљу кохерентног и интегрисаног приступа лечењу на основу увида у целокупне доступне здравствене податке.
- Идентификовано је релативно слабо познавање *blockchain* технологије али је уочен висок ниво свести о осетљивости здравствених података, односно препознат је

појам сајбер сигурности, јер корисници желе да се подаци деле између здравствених установа али уз максималну сигурност података.

7.2. Дизајнирање и израда софтверског решења за предложени модел дигиталног здравственог екосистема заснованог на *blockchain* технологији

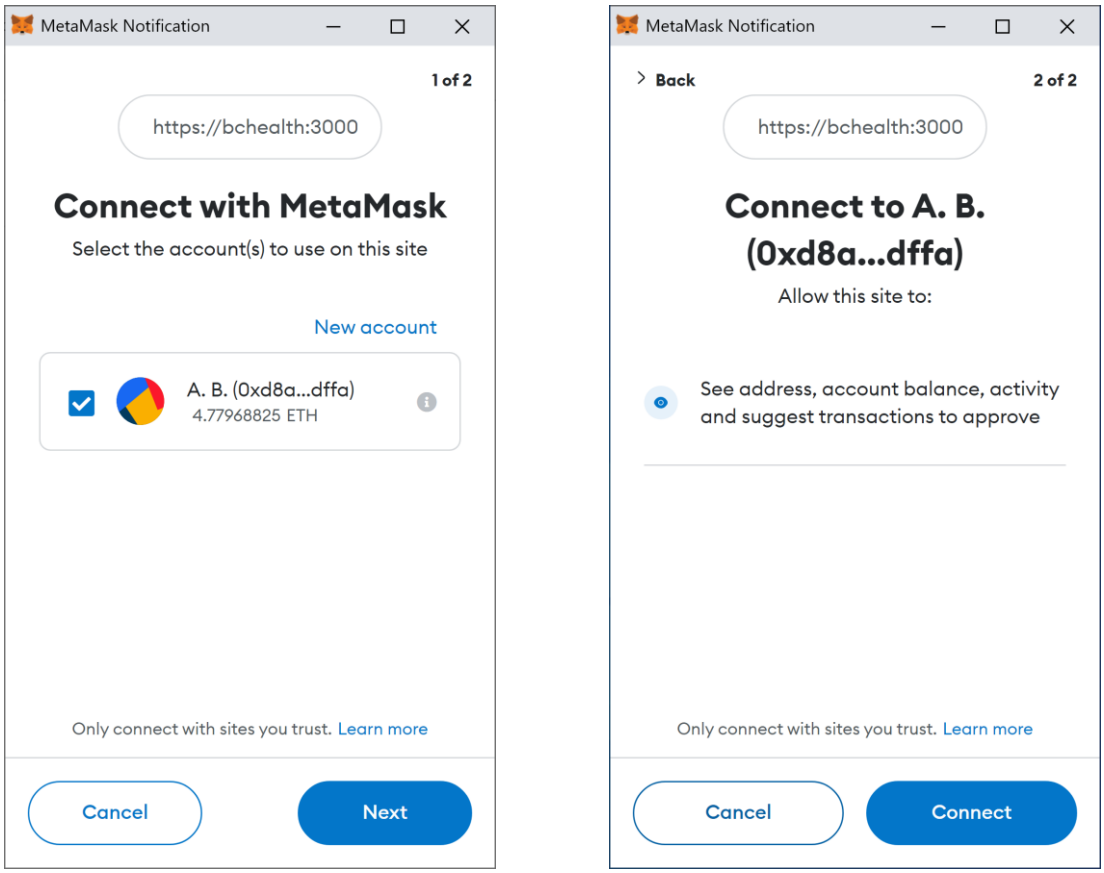
7.2.1. *BCHealth* апликација - здравствена компонента

Приступ децентрализованој веб апликацији се за лекаре и помоћно особље остварује путем стандардног интернет претраживача. На слици 34 је приказан почетни екран *BCHealth* апликације.

Слика 34. Почетни екран *BCHealth* апликације

Избором опције на екрану „Пријава у систем”, систем проверава да ли је на рачунару инсталиран *MetaMask* додатак за приступ корисниковом *ETH* налогу. У случају да *MetaMask* није детектован, корисник се преусмерава на интернет локацију на којој може да преузме поменути софтвер и инсталира га. Уколико корисник не поседује *ETH* налог, путем *MetaMask* софтвера он може бити креиран, међутим, приступ апликацији неће бити могућ све док администратор система не одобри исти.

У случају да је *MetaMask* инсталиран и корисник први пут приступа систему, неопходно је да се његов *ETH* налог повеже са *BCHealth* апликацијом. На слици 35 је приказан захтев *BCHealth* апликације за повезивање са *MetaMask ETH* налогом.

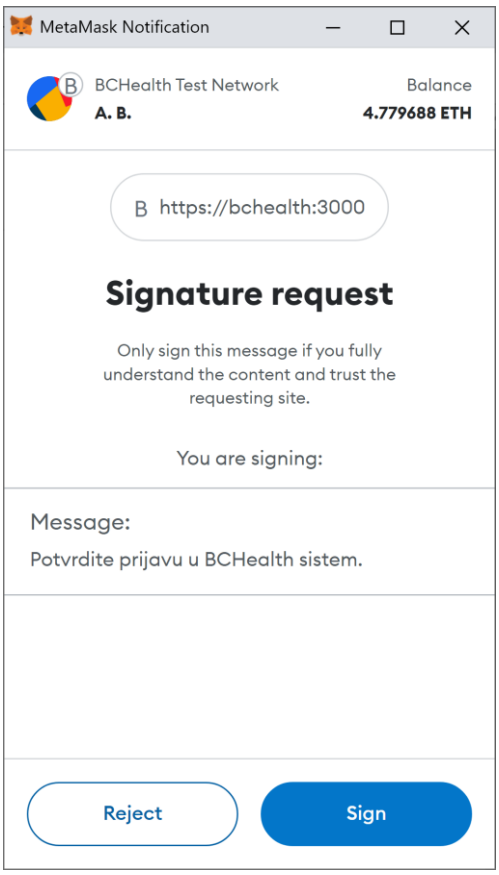


Слика 35. Повезивање децентрализоване апликације са *ETH* налогом корисника путем *MetaMask* интерфејса

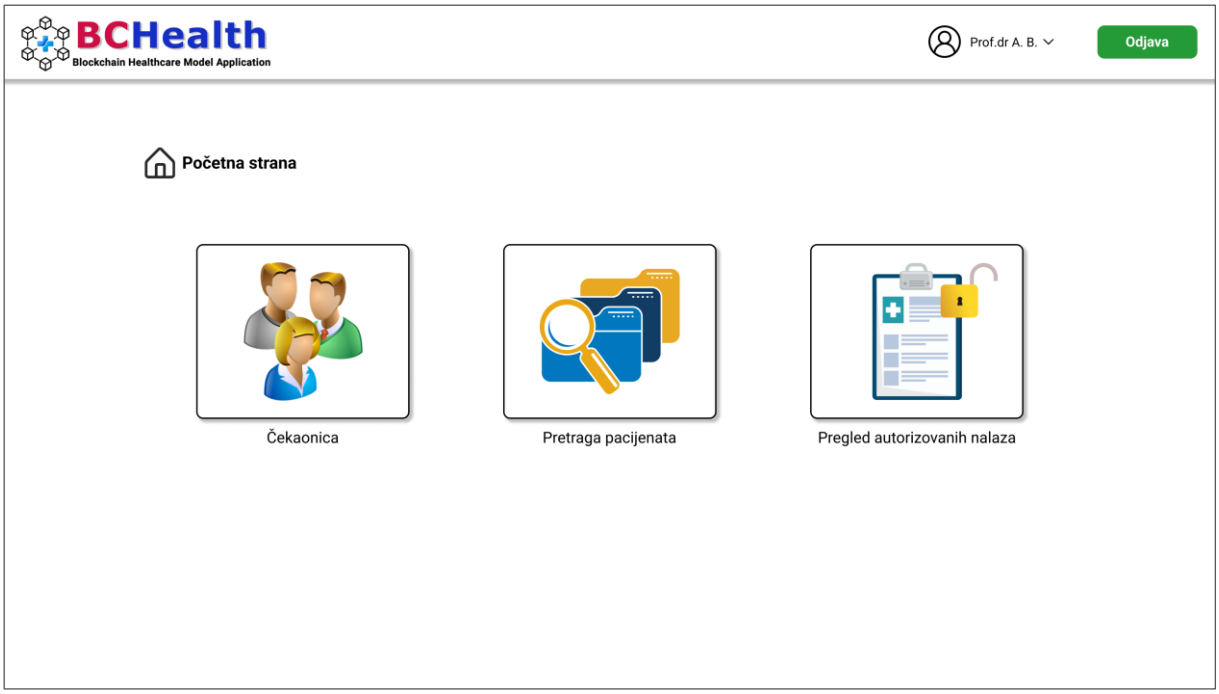
Након повезивања, *BCHealth* систем проверава да ли се налог налази у једној од мапираних хеш табела које одговарају идентификованим типовима корисника у систему. У случају да налог није пронађен, корисник добија информацију да процес активације још није завршен. Уколико је налог пронађен, да би процес пријављивања у систем био завршен, неопходна је *Web3* аутентификација, односно, корисник мора да докаже да је он заиста власник налога који је иницирао пријаву. Доказ власништва над налогом се постиже помоћу приватног кључа налога, кроз процес *Web3* личног потписивања. Систем шаље кориснику текстуалну поруку коју корисник треба да потпише својим приватним кључем. На основу потписа, одговарајућа *Web3* функција израчунава јавни кључ корисника и, уколико се он поклапа са јавним кључем налога који је иницирао пријаву, аутентификација је успешна и може се приступити коришћењу апликације. На слици 36 је приказан прозор *MetaMask* интерфејса са захтевом за потписивање поруке.

Након успешне пријаве у систем, у зависности од типа налога корисника, приказује се одговарајући почетни екран. Лекарима је од функција у апликацији на располагању (слика 37):

- чекаоница,
- претрага пацијената,
- преглед ауторизованих налаза.



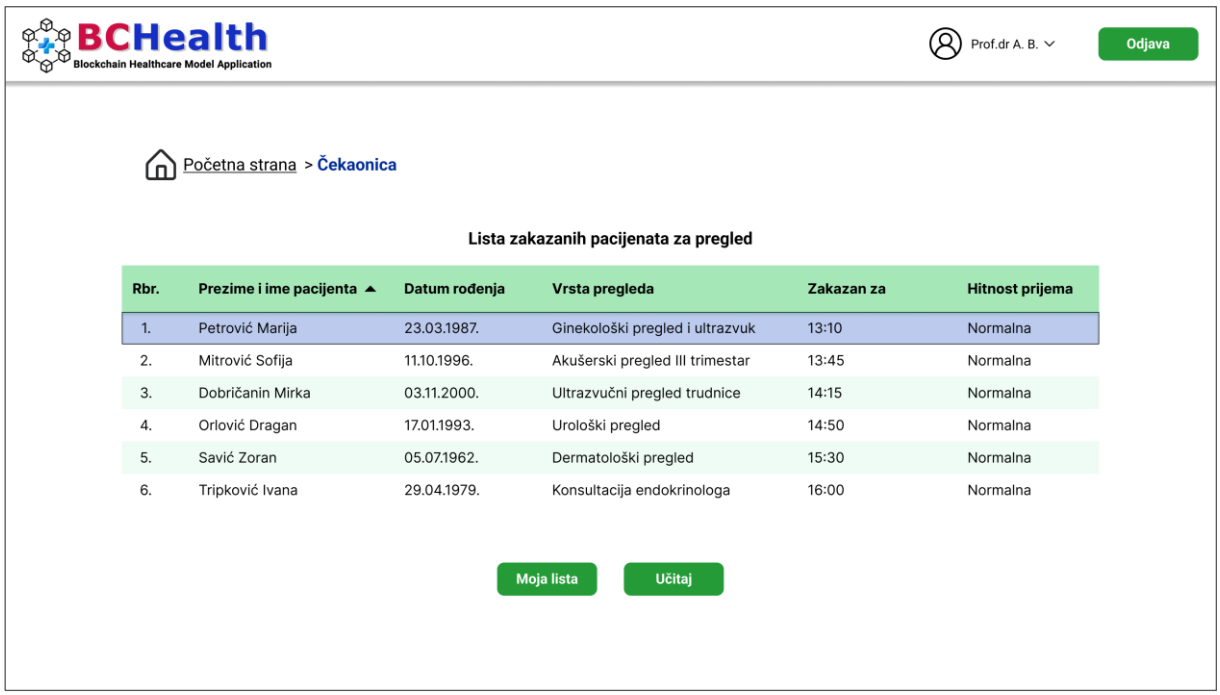
Слика 36. *MetaMask* прозор за лично потписивање поруке од стране корисника приликом пријаве у *BCHealth* систем



Слика 37. Почетни екран за корисника са типом налога „Лекар”

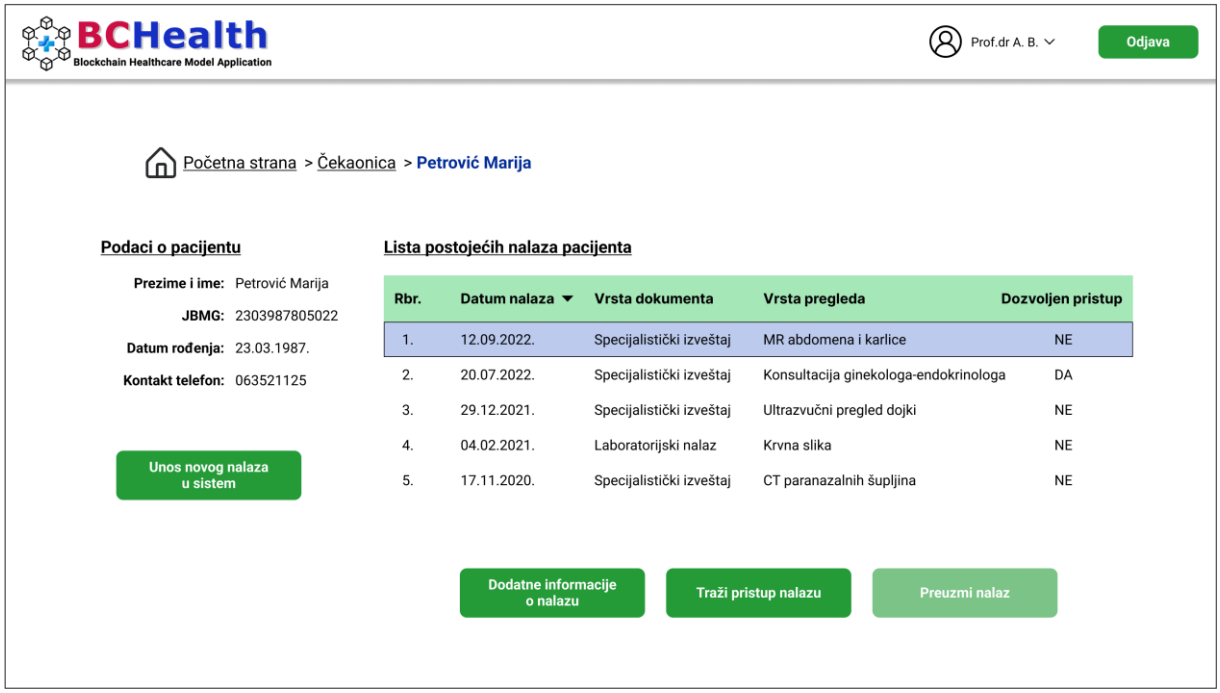
Чекаоница

Избором опције „Чекаоница”, на екрану се отвара списак пацијената који су прошли регистрацију на рецепцији поликлинике и чекају преглед код одговарајућег лекара на којег су упућени (слика 38). У листи су наведени сви пацијенти који чекају на преглед, а избором опције „Моја листа” се списак филтрира на приказ само пацијената који су заказани код тренутно пријављеног лекара у апликацији.



Слика 38. Списак пацијената који чекају преглед

Обележавањем пацијента у листи и одабиром опције „Учитај”, отвара се екран са детаљима о пацијенту и списком свих његових прегледа који су до сада забележени у *BCHealth* систему (слика 39).



Слика 39. Детаљи о пацијенту и његовим прегледима

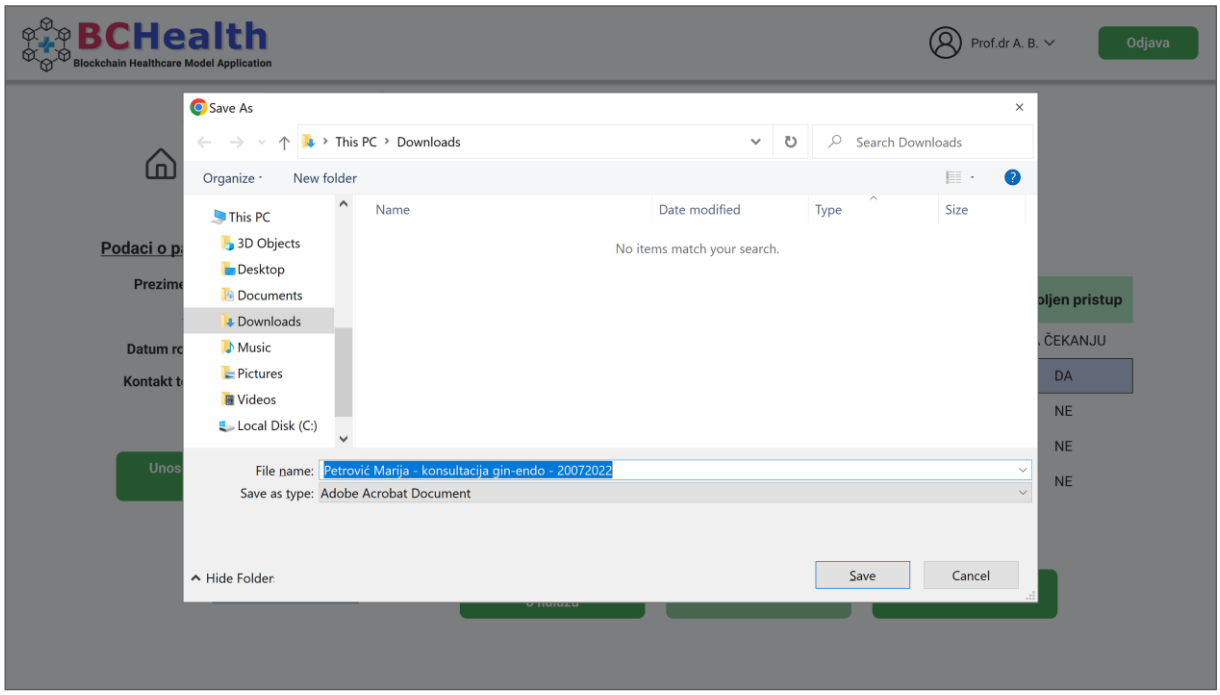
За сваки од ускладиштених налаза лекар може, избором одговарајуће опције на екрану, да добије детаљне информације о самом документу са налазом (слика 40).

Слика 40. Детаљи налаза забележеног у *BCHealth* систему

С обзиром на то да је једна од основних карактеристика развијеног модела пацијент центричност, приступ налазима у оквиру електронског здравственог картона је ограничен. Пацијент, као искључиви власник својих здравствених налаза, има могућност одређивања права приступа за поједине заинтересоване стране, које за то морају да упуте одговарајући захтев. У списку свих ускладиштених налаза је у посебној колони назначено да ли тренутно пријављени лекар има могућност приступа. За налазе којима приступ није дозвољен, лекар има могућност да га, избором одговарајуће опције, затражи, што ће бити евидентирано у корисничком налогу пацијента. Докле ког пацијент не одобри приступ, статус захтева ће бити „На чекању”, и налаз неће бити расположив за преузимање и приказ.

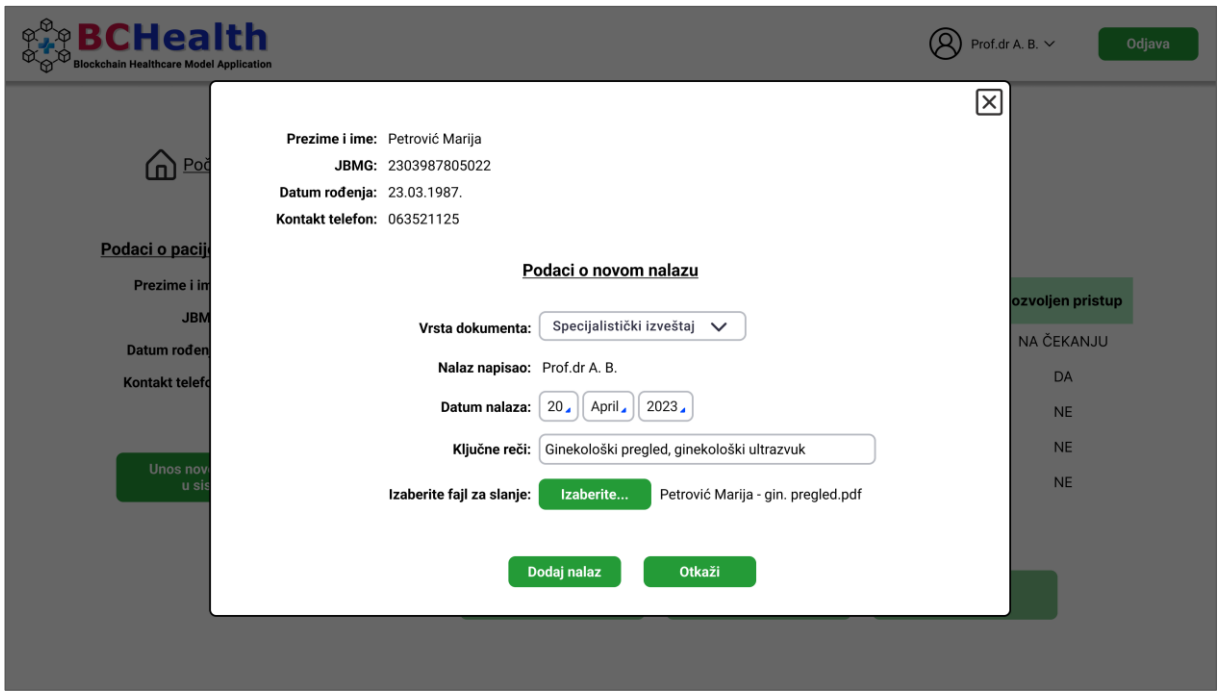
Налази, за које је одобрен приступ од стране пацијента, су енкриптовани у систему помоћу јавног кључа лекара. Избором опције „Преузми налаз”, налаз се декриптује

лекаровим приватним кључем и складишти на рачунар у стандардном PDF формату, након чега садржај документа постаје расположив за преглед (слика 41).



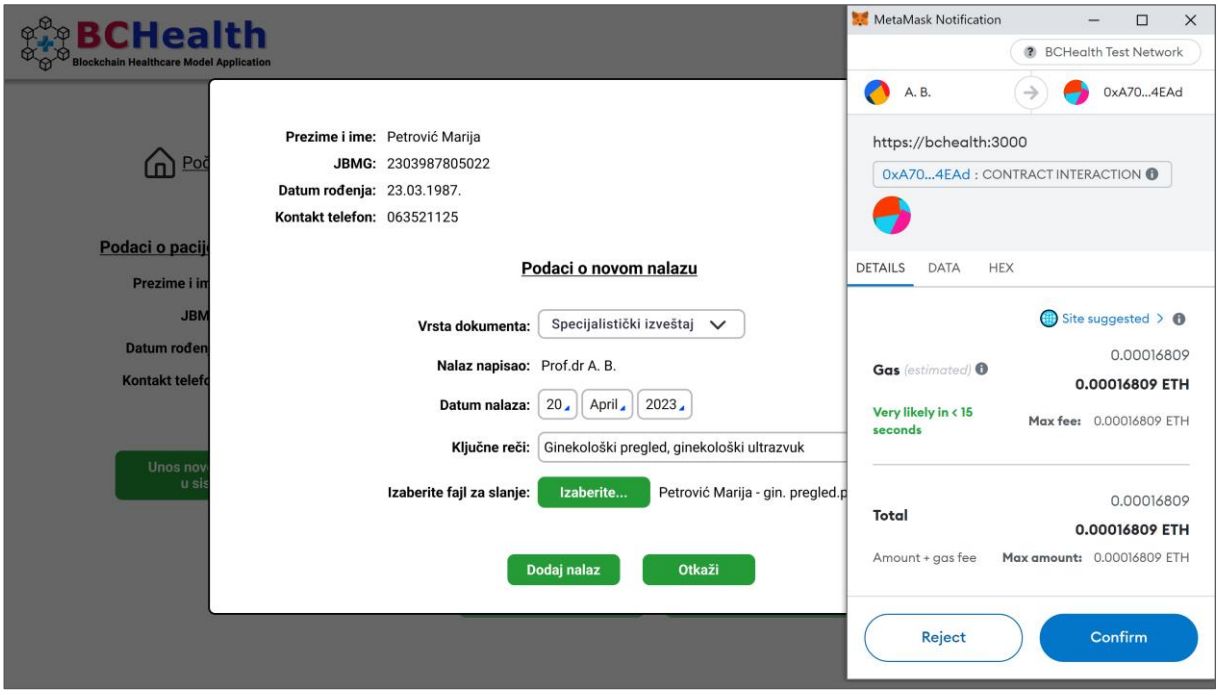
Слика 41. Преузимање налаза за који је дозвољен приступ

Након обављеног прегледа, лекар бира опцију „Унос новог налаза у систем”. На екрану се приказује прозор за унос детаља о прегледу у виду врсте документа, датума креирања и кључних речи, које могу олакшати накнадну претрагу налаза. На крају, потребно је из рачунара изабрати *PDF* документ са написаним налазом, који се жели ускладиштити у *blockchain*, у трајну и безбедну архиву (слика 42).



Слика 42. Унос новог налаза у *BCHealth* систем

Избором опције „Додај налаз”, отвара се *MetaMask* прозор за потврду трансакције уписивања података у *blockchain* мрежу. У прозору су приказане основне информације о самој трансакцији: *ETH* налог лекара који иницира трансакцију, *ETH* адреса паметног уговора чија ће одговарајућа функција бити извршена, као и висина износа гаса захтеваног за ту операцију (слика 43).

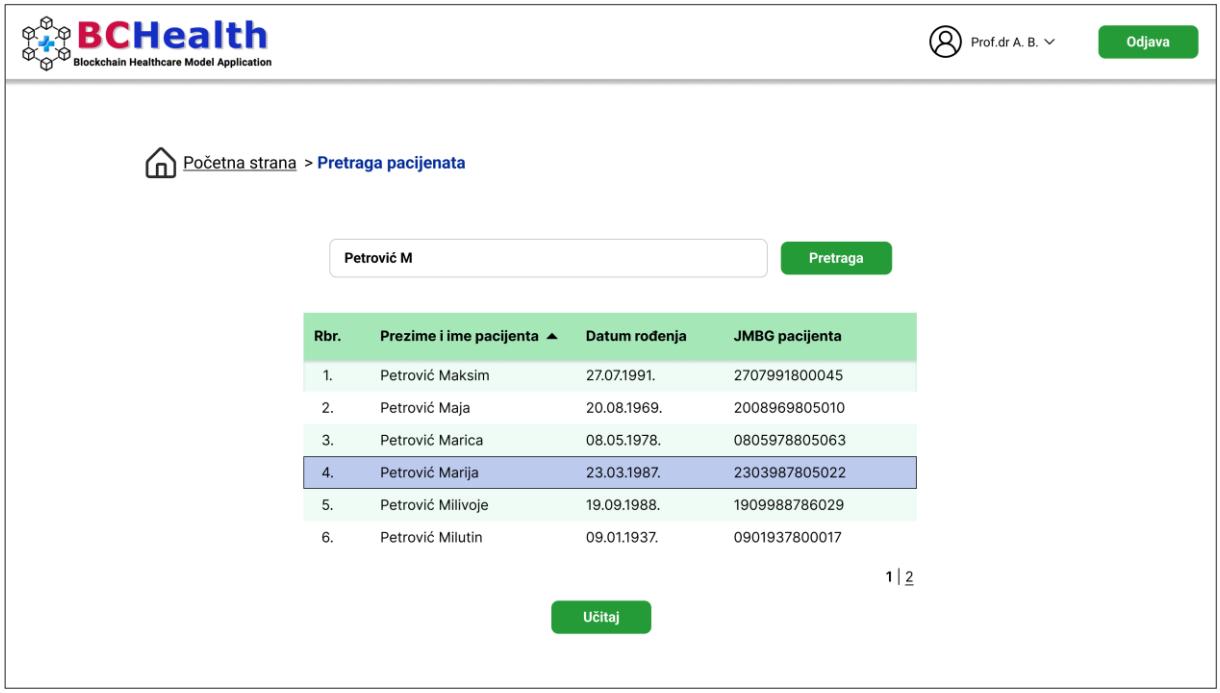


Слика 43. Ауторизација уписа новог налаза

Избором опције „*Confirm*”, ауторизује се трансакција, извршавају се потребне функције одговарајућег паметног уговора и изабрани документ се складишти у *BCHealth* платформу.

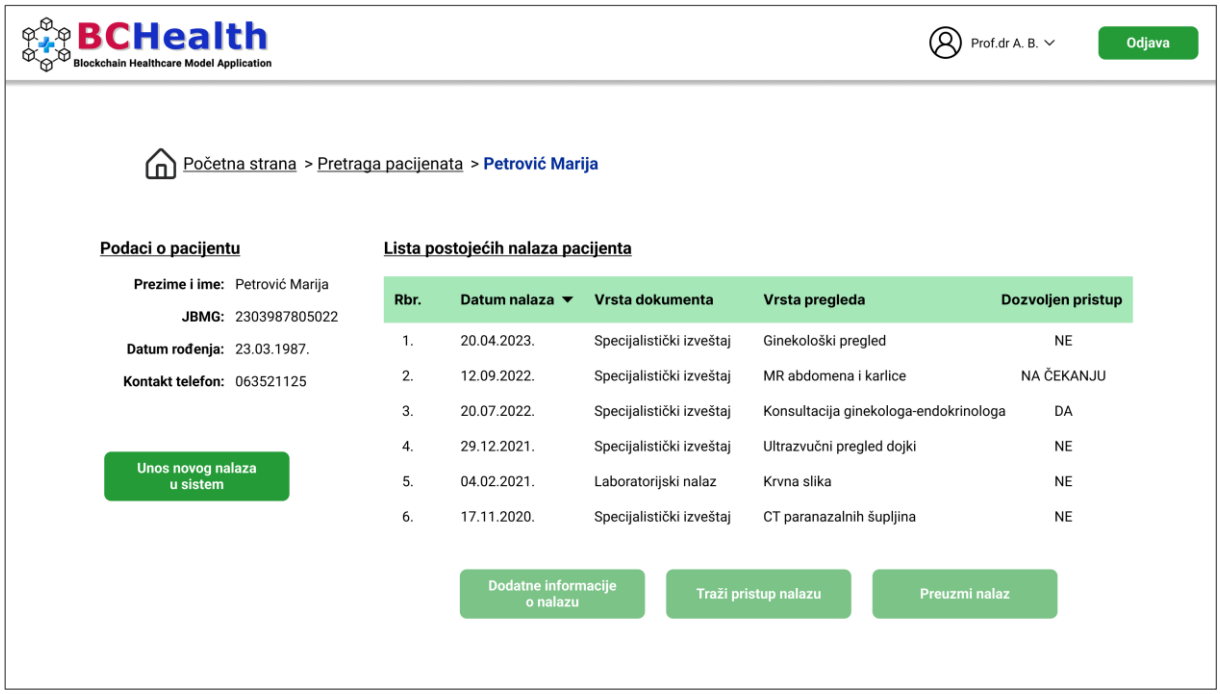
Претрага пацијената

Избором опције „Претрага пацијената” на почетном екрану апликације, отвара се одговарајућа компонента, у којој је могуће претраживати све пацијенте који су регистровани у *BCHealth* систему. Како би се филтрирали резултати из целокупне базе података, на располагању је стандардна форма за претрагу (слика 44).



Слика 44. Претрага базе пацијената у *BCHealth* систему

Учитавањем обележеног пацијента из резултата претраге, отвара се екран са детаљима о пацијенту. На екрану се приказују основни подаци о пацијенту као и о свим његовим налазима који су ускладиштени у систему (слика 45).



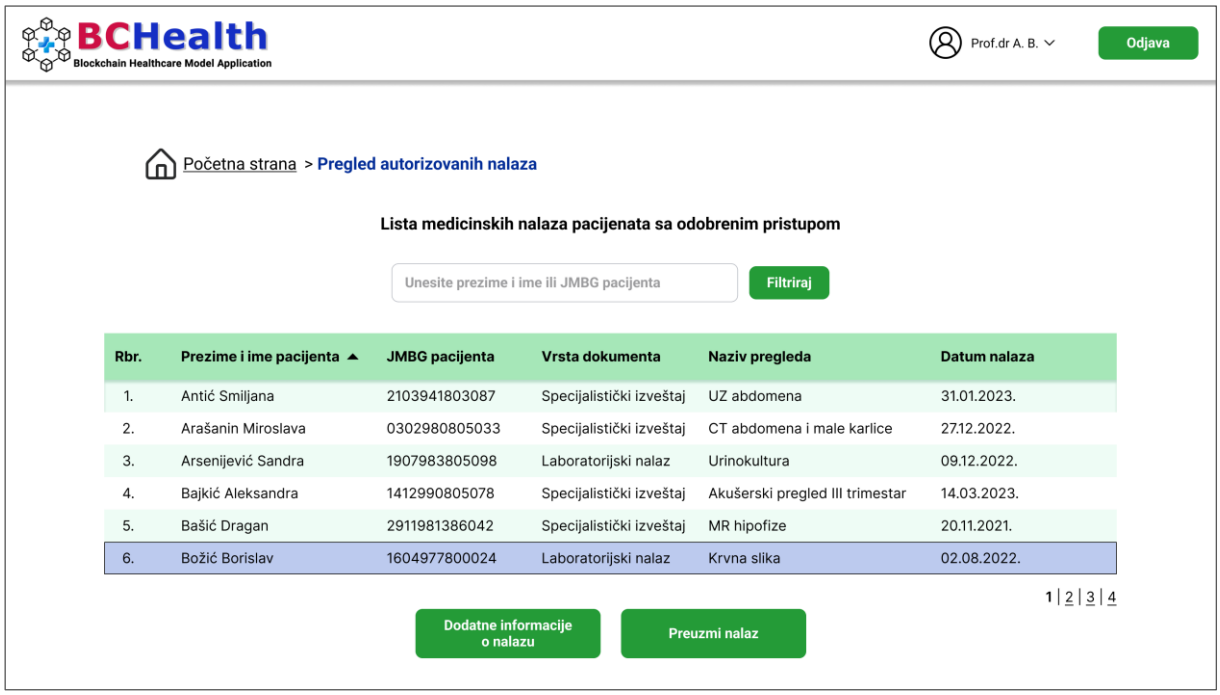
Слика 45. Детаљан приказ резултата претраге базе података пацијената

За сваки од уноса у листи се, поред детаља о самом налазу, може добити и информација о могућности отварања његовог садржаја односно, о тренутном статусу поднетог захтева за одобравање приступа од стране пацијента. Уколико приступ налазу није одобрен, лекар може да га затражи, а пацијент ће о томе бити адекватно информисан. Налази

којима је одобрен приступ се у овом делу апликације могу преузети на локални рачунар, након избора одговарајуће опције, која ће покренути декрипцију приватним кључем лекара пријављеног у систему и затим понудити могућност меморисања. У овом делу апликације је такође могуће приступити и опцији за додавање новог налаза у систем, уколико пацијент није прошао регистрацију на рецепцији, или се ради нпр. о хитном пријему.

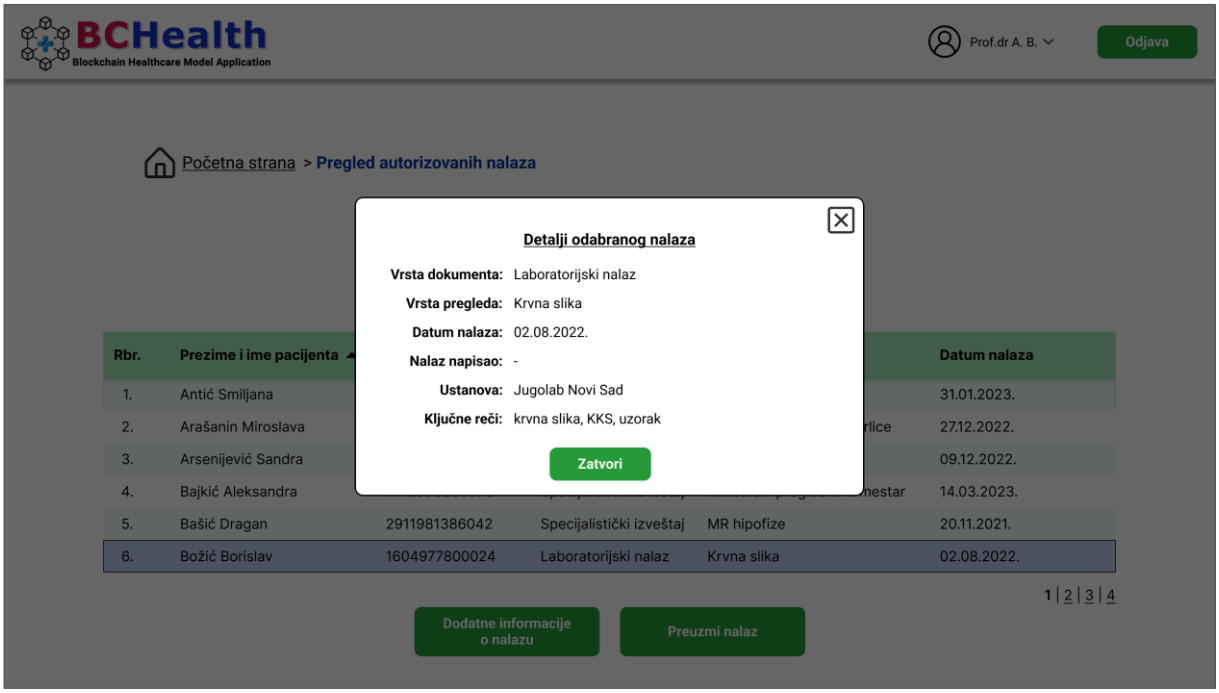
Преглед ауторизованих налаза

Последња од главних функционалности компоненте која се односи на пружање услуга здравствене заштите јесте „Преглед ауторизованих налаза", где су обједињени сви налази пацијената за које тренутно пријављени лекар има право приступа (слика 46).

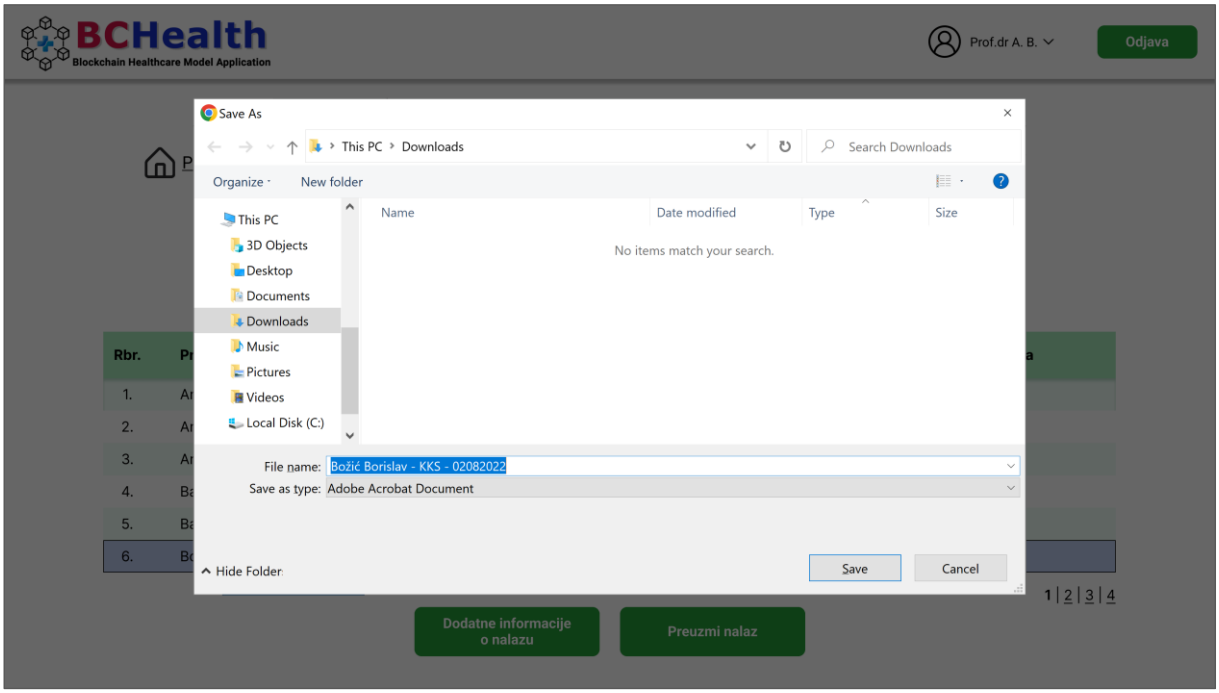


Слика 46. Листа свих налаза којима је одобрено право приступа

Целокупну листу је могуће филтрирати уобичајеним критеријумима за претрагу. Обележавањем жељеног уноса у листи, могу се добити додатне информације о налазу (слика 47). Избором опције „Преузми налаз", систем покреће декрипцију лекаровим приватним кључем, и као резултат се појављује стандардна форма за преузимање докумената у *PDF* формату на локални рачунар, након чега је налаз расположив за преглед (слика 48).



Слика 47. Детаљи налаза за који је одобрен приступ



Слика 48. Преузимање декриптованог документа на локални рачунар

7.2.2. Део здравствене компоненте намењен пацијентима

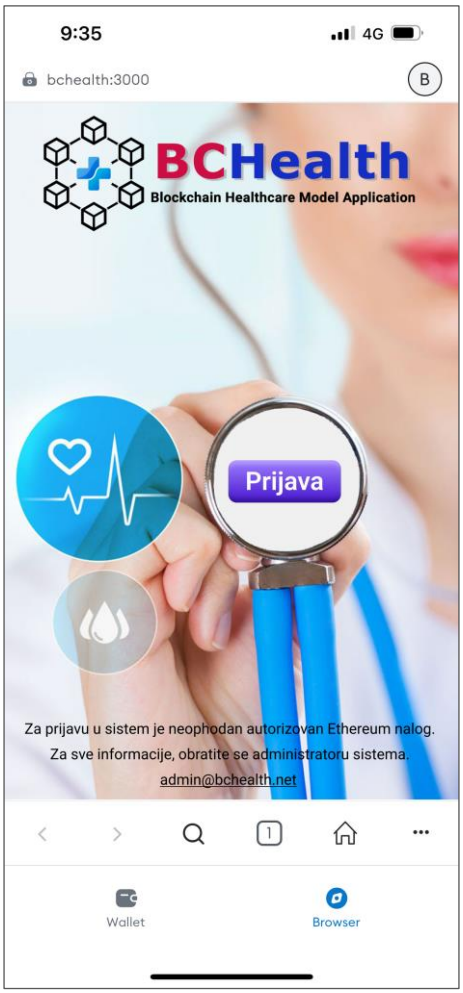
Пацијентима је на располагању посебан део у оквиру здравствене компоненте *BCHealth* апликације, у којем имају могућност да претражују налазе у оквиру свог електронског картона и додељују права приступа заинтересованим странама. Приказ на екрану је посебно прилагођен преносним уређајима (мобилни телефон, таблет), јер пацијенти углавном бирају овакав начин приступа због могућности интерактивне контроле над

својим подацима (нпр. када се налазе на прегледу у некој ординацији и желе да дозволе приступ неким својим претходним налазима).

На преносним уређајима приступ *Web3* децентрализованим апликацијама такође захтева присуство неког од софтвера са функционалношћу крипто новчаника, уз помоћ којег се може остварити веза са *blockchain* налогом корисника. Сам поступак приступа *Web3* апликацији је мало другачији, у смислу да се не могу користити уобичајени интернет претраживачи, већ искључиво специјализовани, који имају у себи уграђене компоненте за *Web3*.

За приступ *BCHealth* систему се и на мобилним уређајима користи *MetaMask* софтвер, за који мора бити инсталирана припадајућа апликација. *MetaMask Mobile* има у себи уграђен одговарајући интернет претраживач, тако да се приступ *BCHealth* апликацији, као и другим *Web3* страницама, одвија преко њега. Ради бољег корисничког искуства, приступ *BCHealth* апликацији је могуће иницирати и приступом из класичног интернет претраживача на телефону који ће затим, путем *„deep linking"* функционалности, отворити *MetaMask* претраживач и наставити са даљим радом.

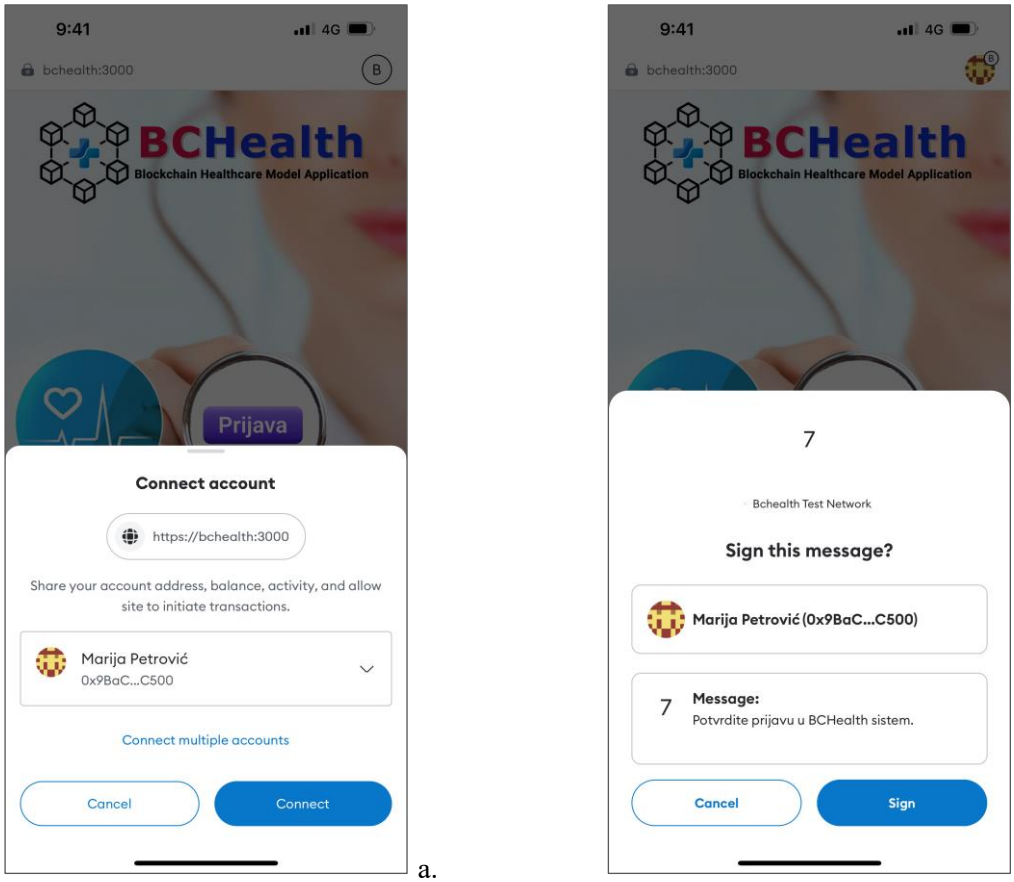
На слици 49 је дат приказ екрана за пријављивање, где је *BCHealth* апликацији приступљено из претраживача мобилне верзије *MetaMask* крипто софтвера.



Слика 49. Приказ екрана за пријављивање у *BCHealth* апликацију из *MetaMask Mobile* претраживача

Уколико на преносном уређају није инсталиран *MetaMask*, корисник ће бити преусмерен на страницу за преузимање поменутог софтвера. Након успешне инсталације, потребно је учитати лични *ETH* налог у *ETH* крипто новчаник. Као и код приступа са рачунара, код првог отварања апликације је најпре потребно повезати *MetaMask ETH* налог са *BCHealth* системом (слика 50а).

Након повезивања налога, активира се функција за пријављивање из одговарајућег паметног уговора, која проверава да ли је *ETH* налог, који покушава да приступи апликацији, регистрован у *blockchain* бази. Уколико је налогу дозвољена пријава, у оквиру *Web3* аутентификације у систем апликација шаље кориснику поруку на персонално потписивање (слика 50б).



а. б.

Слика 50. Повезивање *ETH* налога и пријављивање у *BCHealth* апликацију

Након успешне пријаве у систем, приказује се почетни екран са основним функционалностима које су на располагању пацијентима (слика 51):

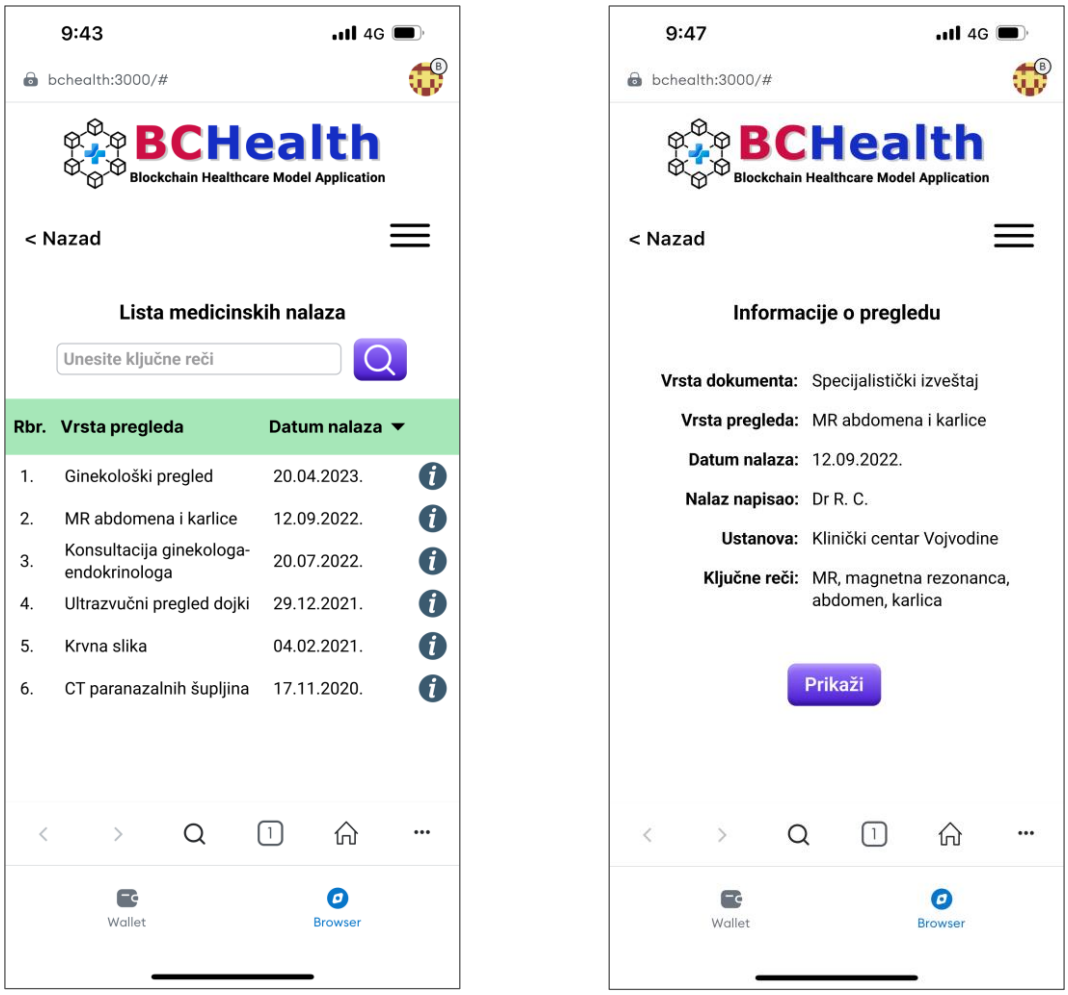
- моји налази,
- захтеви за приступ,
- контрола приступа.

Слика 51. Почетни екран компоненте *BCHealth* апликације намењене пацијентима

Моји налази

Избором прве опције на почетном екрану, пацијенти могу да добију увид у налазе који су ускладиштени у оквиру њиховог електронског здравственог картона (слика 52а). На располагању су стандардне опције сортирања приказа, као и филтрирање по кључним речима, које уносе лекари приликом додавања нових налаза у *BCHealth* систем.

За сваки од наведених уноса у листи, одабиром одговарајућег графичког симбола, могу се добити додатне информације о самом налазу које обухватају: врсту ускладиштеног документа, врсту и датум прегледа који је обављен, име лекара који је налаз написао, назив установе у којој је пружена здравствена услуга као и кључне речи, помоћу којих је могуће претраживати документе у електронском здравственом картону (слика 52б).



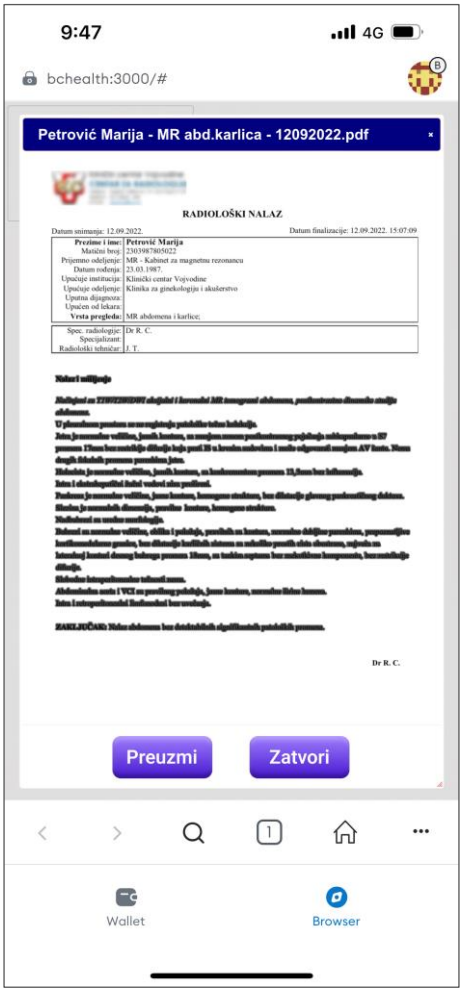
а. Листа свих налаза пацијента

б. Детаљне информације о налазу

Слика 52. Приказ екрана са листом свих налаза пацијента ускладиштених у електронском здравственом картону

Одабиром опције „Прикажи”, пацијент може да отвори садржај ускладиштеног документа (слика 53).

Приказани налаз може и да се преузме у локалну меморију преносног уређаја.



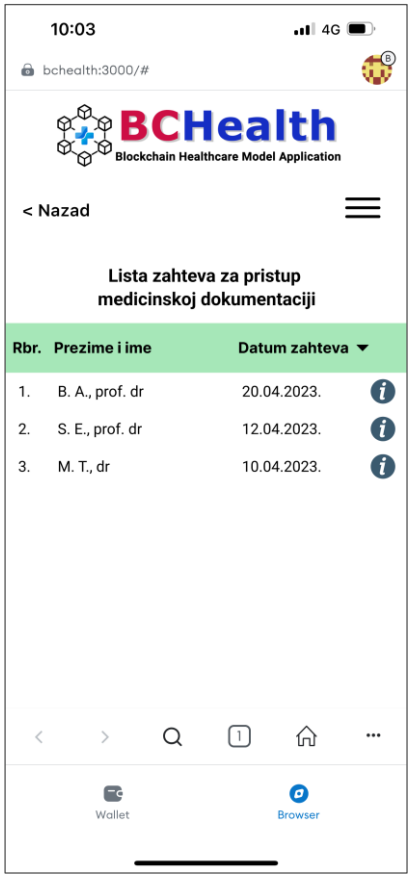
Слика 53. Приказ одабраног налаза

Захтеви за приступ

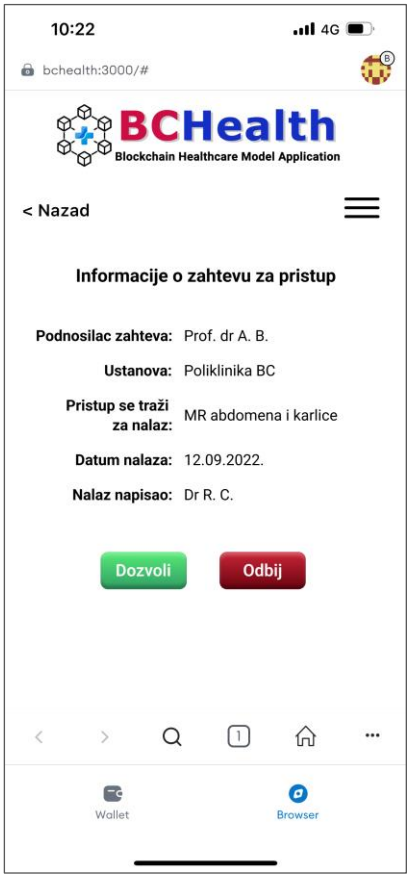
Наредна функционалност у делу апликације намењеном пацијентима јесте увид и обрада захтева за приступ њиховим здравственим подацима, а које су упутиле заинтересоване стране. Избором одговарајуће опције на почетном екрану, добија се приказ дат на слици 54а. У листи поднетих захтева наведени су име и презиме особе која је упутила захтев, уз евидентиран датум.

Избором графичког симбола за информације, добија се детаљан приказ информација о захтеву, који додатно обухвата и назив институције из које заинтересована страна тражи приступ, као и основне податке о самом предметном налазу (слика 54б).

За сваки захтев, пацијент има могућност да га прихвати и тиме дозволи заинтересованој страни приступ траженом здравственом налазу, или да га одбије, при чему ће бити послата одговарајућа нотификација. Избором опције „Дозволи”, отвара се *MetaMask* прозор са захтеваном ауторизацијом трансакције која треба да изврши функције из одговарајућег паметног уговора и упише нове вредности у *blockchain* мрежу (слика 55а). Уколико је извршавање трансакције успешно завршено, на екрану се добија одговарајућа информација, а предметни захтев се уклања из листе (слика 55б).

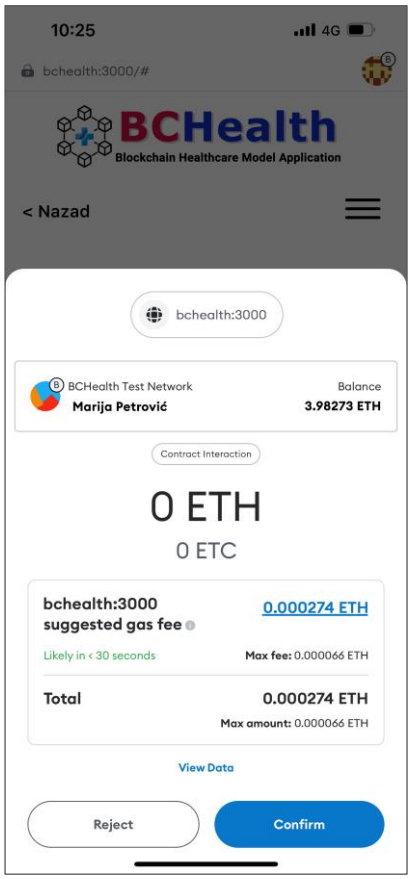


а.

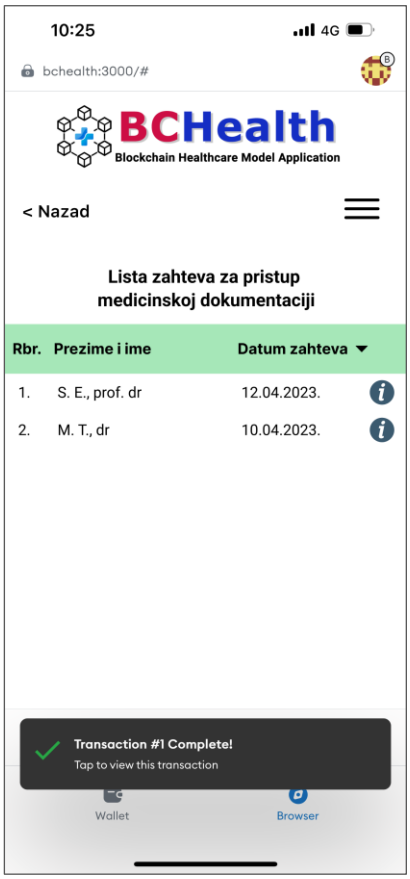


б.

Слика 54. Листа захтева за приступ подацима пацијента са детаљним приказом



а.



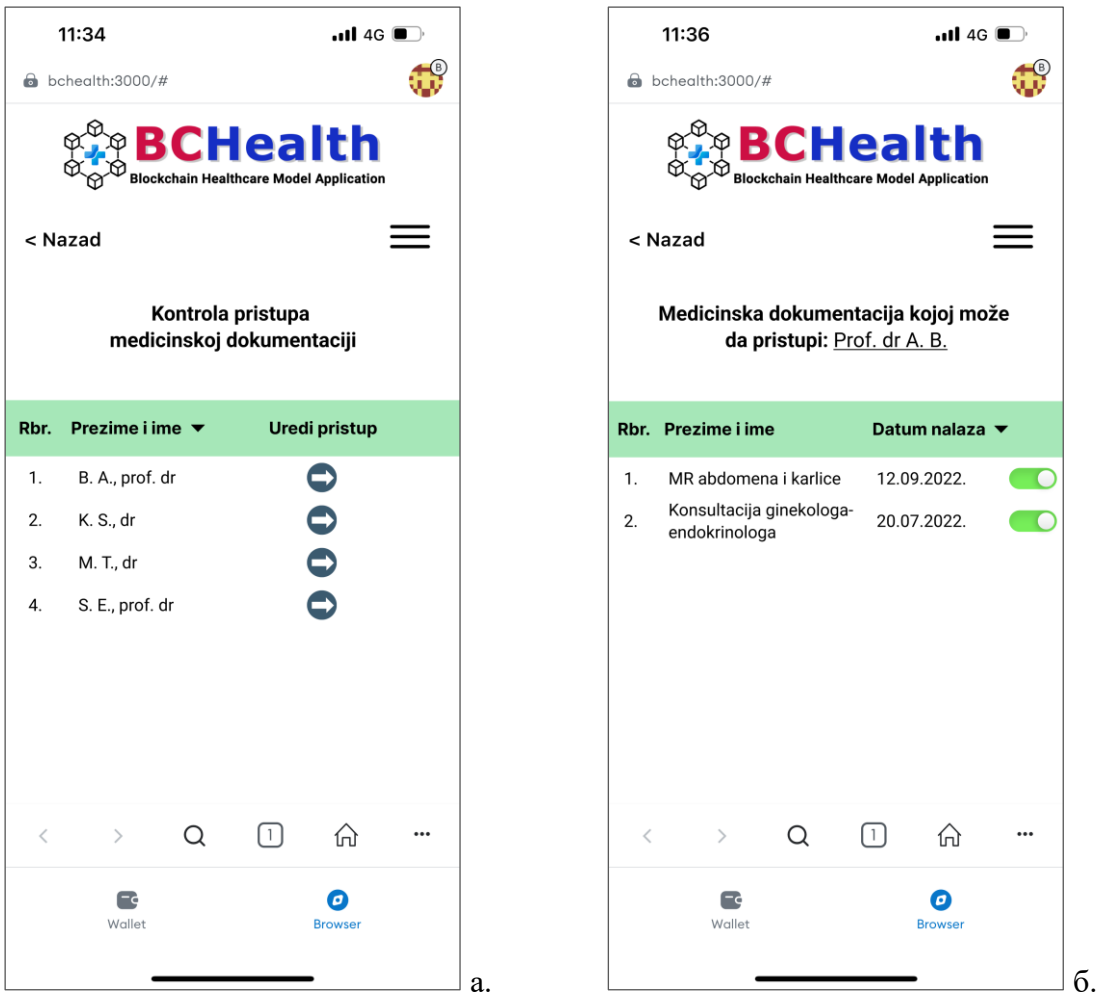
б.

Слика 55. Успешно извршавање *blockchain* трансакције

Контрола приступа

Последња функционалност дела апликације намењеног пацијентима је контрола приступа здравственим подацима. Ова опција нуди обједињени приказ додељених права приступа одређеним документима из електронског картона пацијента, као и могућност уређивања. У листи су побројани стејкхолдери којима је пацијент доделио могућност отварања садржаја својих здравствених налаза (слика 56а).

Избором одговарајућег графичког симбола уз име особе у листи чији приступ документима се жели уредити, отвара се екран са детаљима који садржи тачне називе и датуме прегледа којима је дозвољен приступ (слика 56б).

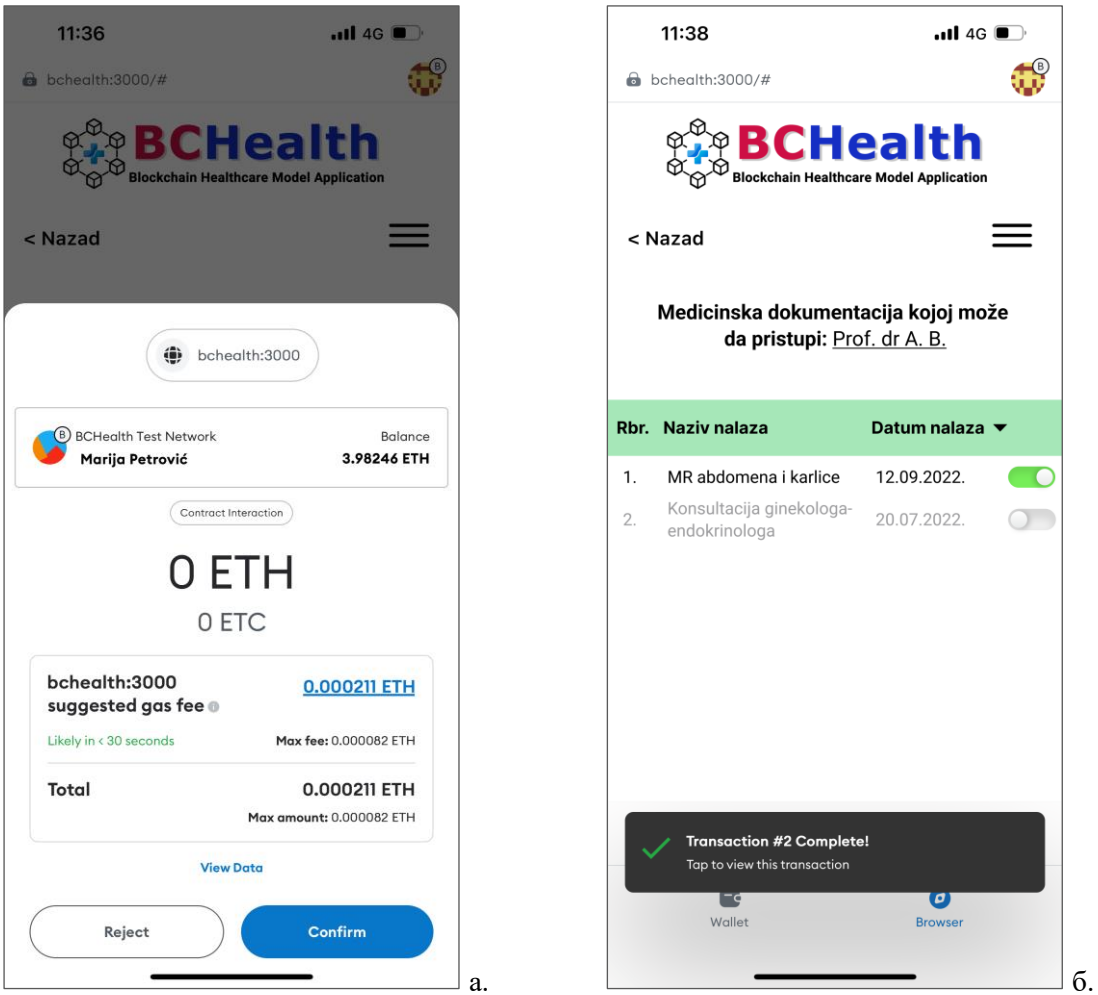


а. б.

Слика 56. Листа стејкхолдера којима је дат приступ документацији пацијента

Корисник има могућност да укине додељено право приступа избором графичке опције уз назив одговарајућег налаза. Уколико то уради, на екрану се приказује *MetaMask* прозор за ауторизацију неопходне трансакције, пошто се извршавањем ове функције мењају и променљиве стања одговарајућег паметног уговора у *blockchain* мрежи (слика 57а).

Уколико корисник потврди извршење *blockchain* трансакције, на екрану се добија одговарајућа нотификација, а уз име налаза за који је укинуто право приступа мења се стање графичког симбола (слика 57б).



а. б.

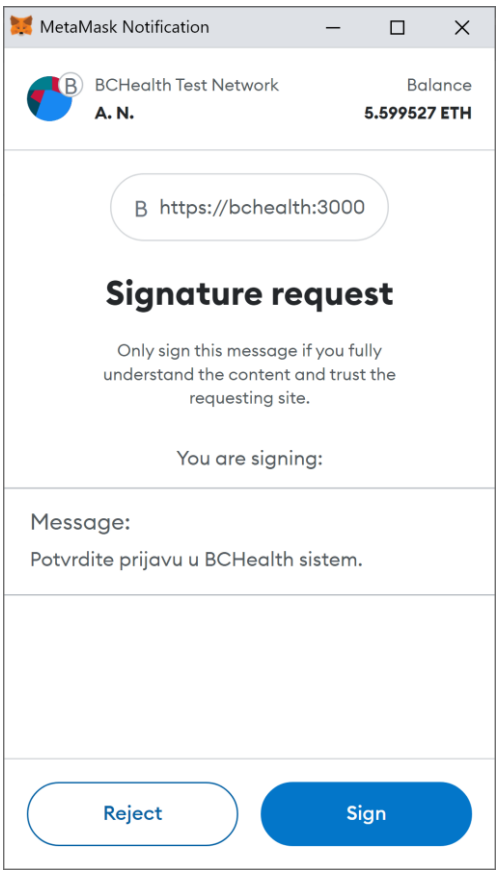
Слика 57. Ауторизација *blockchain* трансакције за измену права приступа пацијентовом налазу

7.2.3. *BCHealth* апликација – пословна компонента

Друга главна компонента *BCHealth* модела дигиталног здравственог екосистема јесте пословна кореспонденција између стејкхолдера. Финансијски службеници представљају тип корисника који испред своје установе обавља размену документације која се генерише као резултат пословних активности.

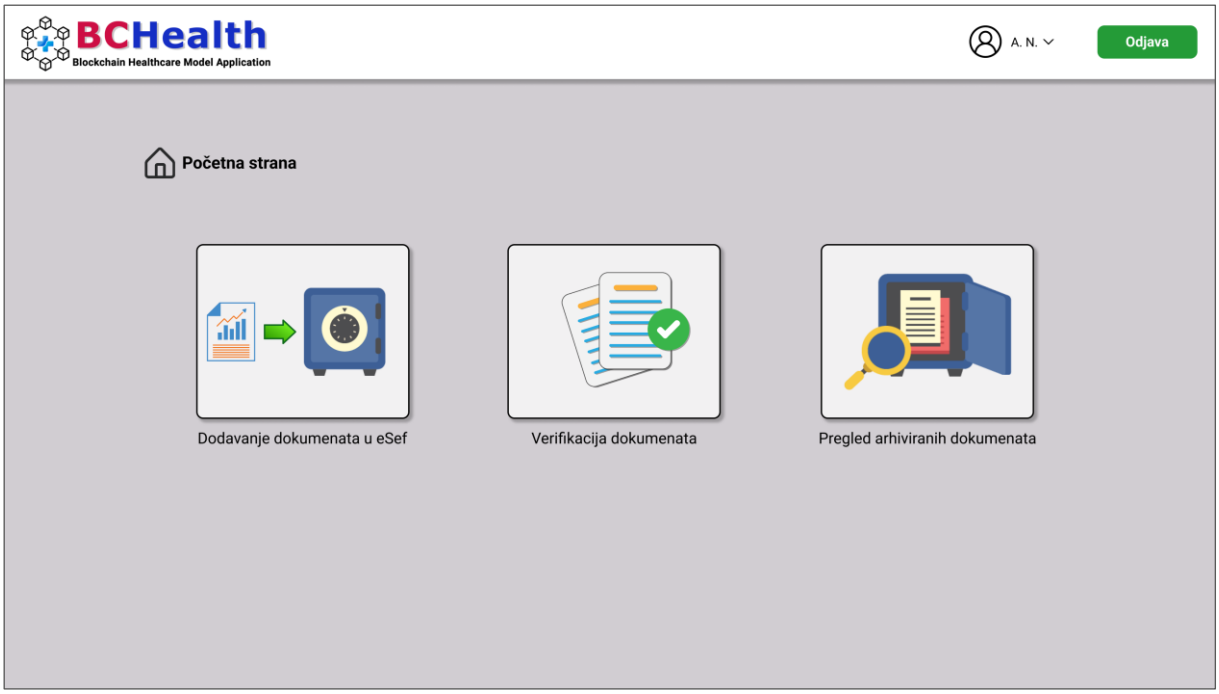
Пријава у систем за финансијског службеника је иста као и у здравственој компоненти апликације за корисника типа „Лекар”. Неопходно је да корисник поседује *Ethereum* налог као и *MetaMask* софтвер, помоћу којег ће се одвијати комуникација између крипто налога и паметних уговора *BCHealth* апликације, који су похрањени у *Ethereum blockchain* мрежи.

Избором опције „Пријава у систем” на главном екрану апликације (слика 34), отвара се *MetaMask* прозор за аутентификацију корисниковог *ETH* налога помоћу персоналног потписа (слика 58).



Слика 58. Потписивање поруке приликом пријаве финансијског службеника у систем

Након успешне пријаве, на екрану се приказује почетни екран за тип корисника „Финансијски службеник” (слика 59).



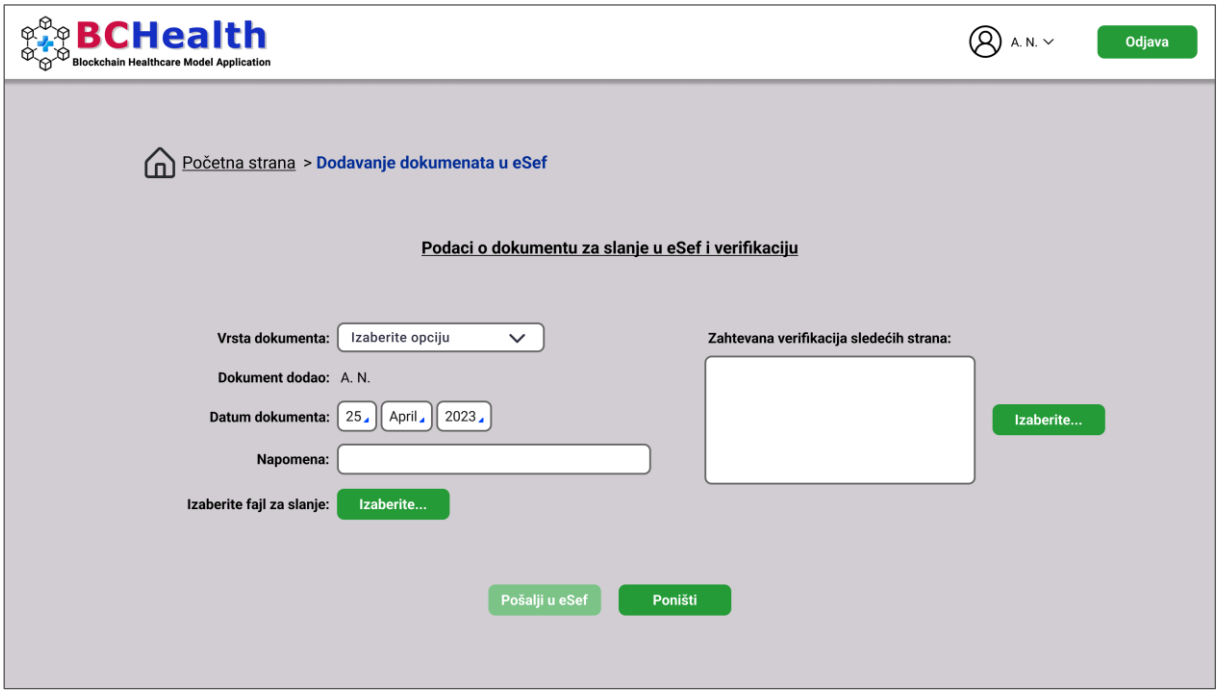
Слика 59. Почетни екран *BCHealth* апликације за финансијског службеника

На располагању су следеће главне функционалности:

- додавање докумената у еСеф,
- верификација докумената,
- преглед архивираних докумената.

Додавање докумената у еСеф

Избором опције „Додавање докумената у еСеф”, на екрану се отвара део апликације који омогућава складиштење пословних докумената у *BCHealth* систем (слика 60).



Слика 60. Изглед екрана за додавање нових пословних докумената у *BCHealth* систем

За унос пословних докумената, неопходно је попунити основне тражене податке као и изабрати сараднике који су учесници у конкретној пословној трансакцији, а чија ће се верификација у виду дигиталног потписа захтевати (слика 61).

Слика 61. Избор пословних контаката за верификацију документа

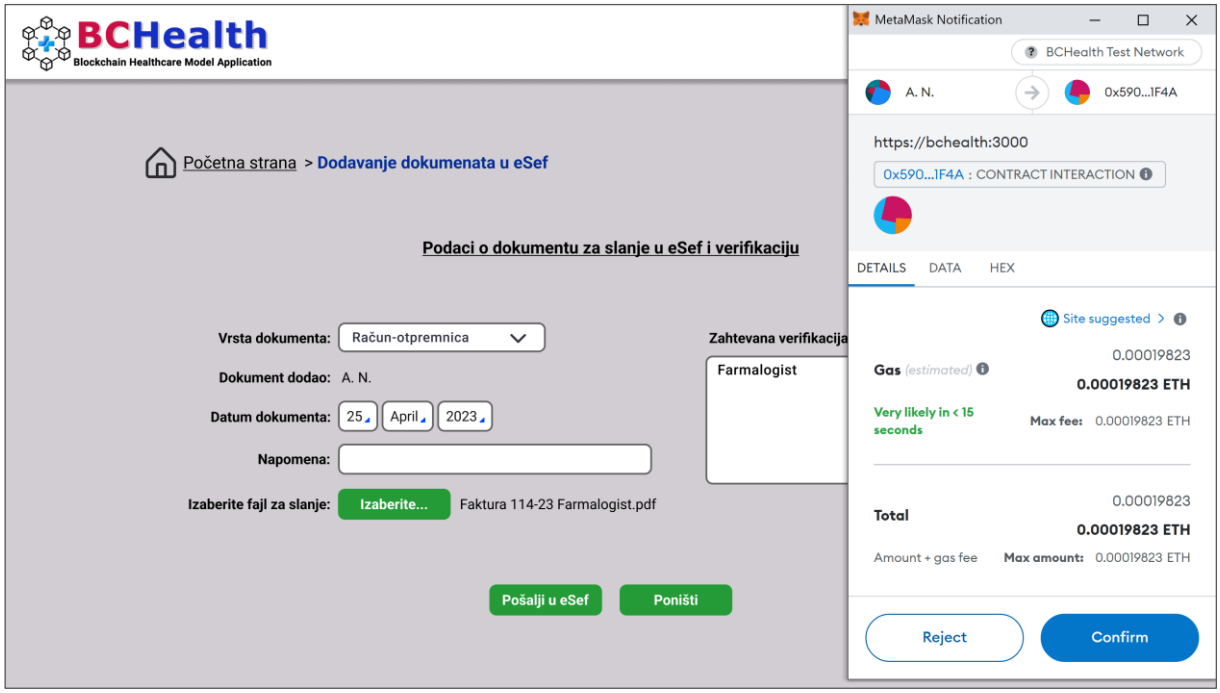
Након избора контаката, потребно је из локалне меморије рачунара одабрати пословни документ који се шаље у систем.

На слици 62 је приказан изглед попуњене форме за додавање пословног документа у систем.

Слика 62. Попуњена форма за додавање пословног документа у *BCHealth* систем

Након што су сва обавезна поља попуњена и изабран документ који се шаље, укључујући и контакте који ће морати да га верификују, опција „Пошаљи у еСеф" постаје активна, и документ се може ускладиштити у *BCHealth* систем. Избором опције за слање, иницира се комуникација са паметним уговором у *blockchain* мрежи, и приказује се одговарајући *MetaMask* прозор са информацијама о захтеваној трансакцији (слика 63).

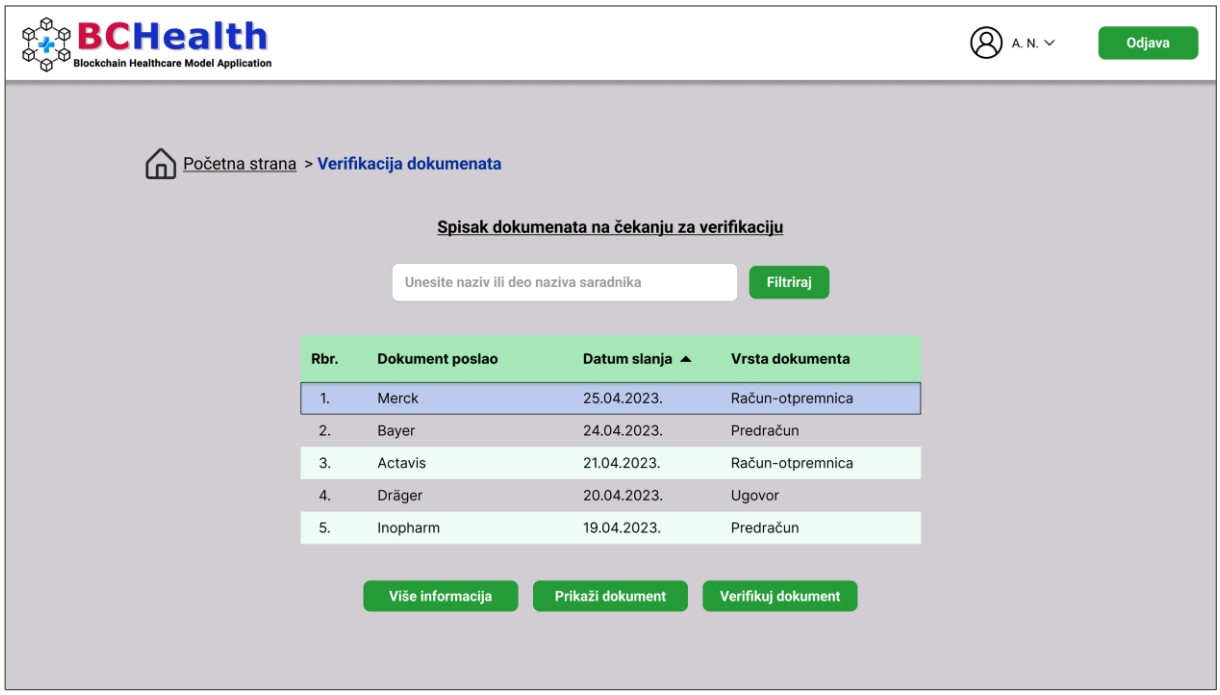
Након потврде извршења трансакције у *MetaMask* прозору, пословни документ се додаје у систем и аутоматски верификује од стране *ETH* налога који је покренуо слање, а у име установе којој припада. Садржај документа се криптографски заштићује, тако да само налог који је иницирао слање, као и налози клијената који су наведени као захтевани верификатори, могу да приступе његовом садржају.



Слика 63. *MetaMask* ауторизација уноса новог пословног документа у *BCHealth* систем

Верификација докумената

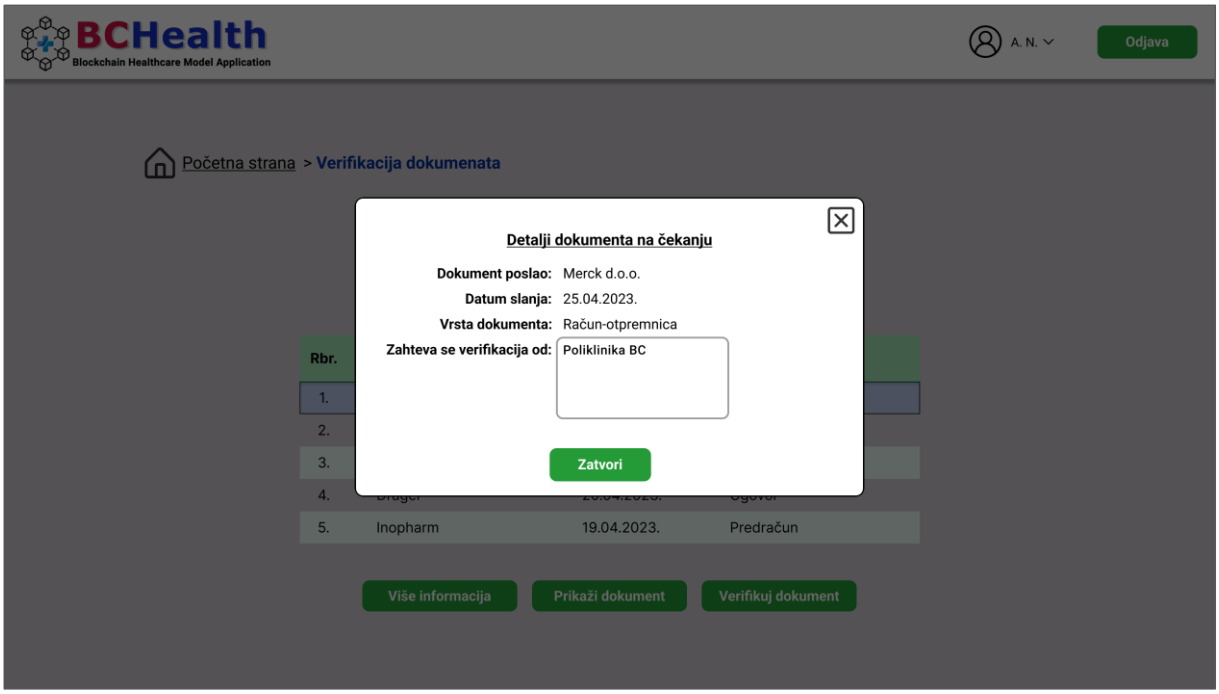
Избором опције „Верификација докумената” на главном екрану пословне компоненте *BCHealth* апликације, отвара се приказ дат на слици 64.



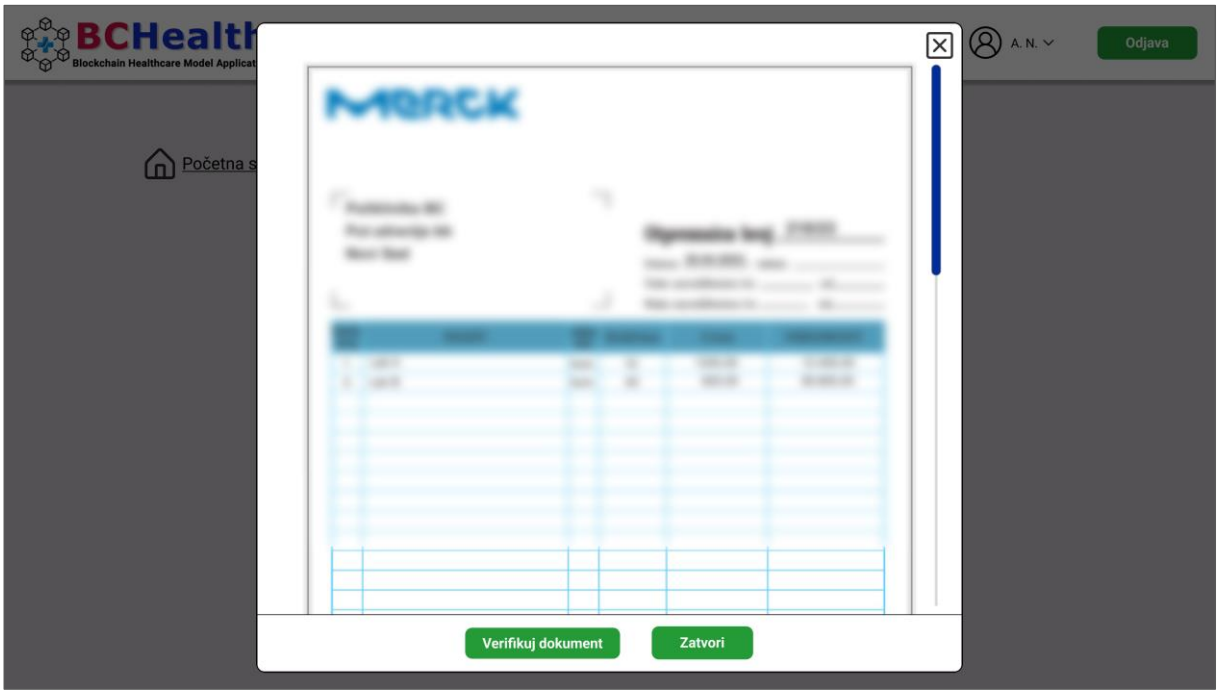
Слика 64. Верификација пословних докумената

У овој функцији апликације, на екрану се добија листа свих докумената који су од стране других учесника у екосистему послати установи на верификацију. На располагању су стандардне могућности филтрирања и сортирања приказа. Одабиром једног од

докумената из листе, могу се добити додатне информације о документу, које укључују и списак свих других учесника чија се верификација чека (слика 65), а може се и приказати садржај документа на екрану (слика 66).



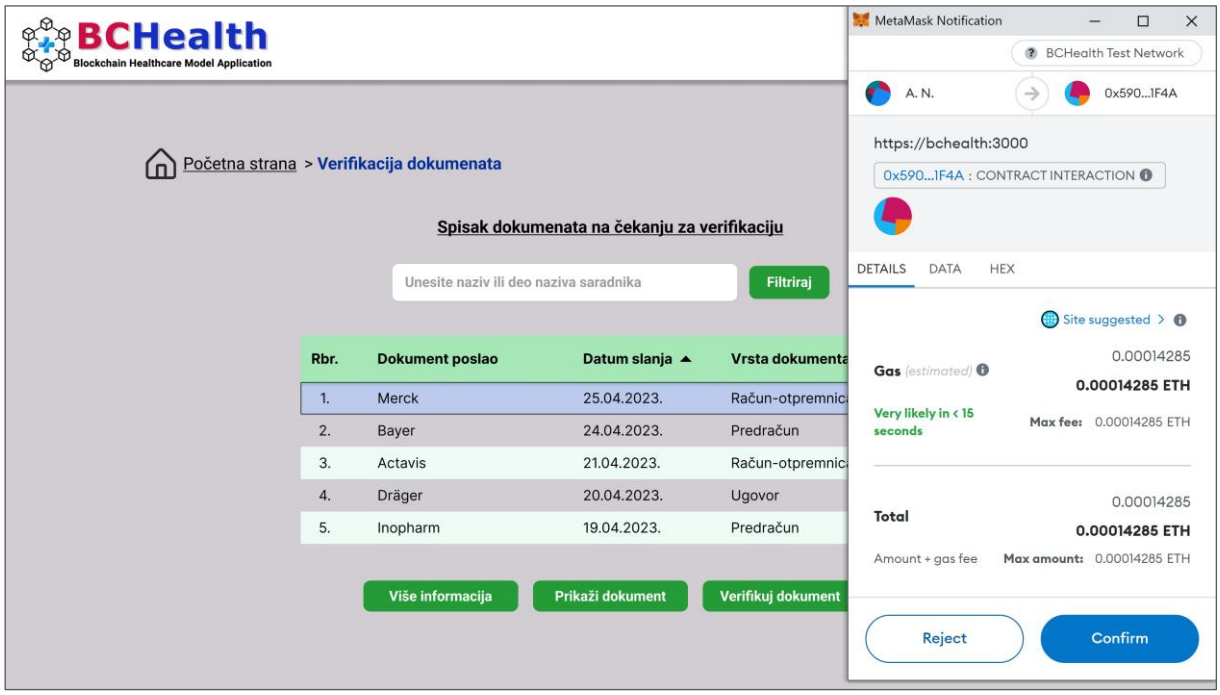
Слика 65. Приказ детаља документа који је на чекању за верификацију



Слика 66. Приказ документа који треба верификовати

Након увида у пословни документ и пратеће информације, финансијски службеник избором опције „Верификуј документ”, покреће функције одговарајућег паметног уговора и на екрану се приказује *MetaMask* прозор са упитом за извршавање трансакције. (слика 67). Након потврде, извршава се упис дигиталног потписа *ETH* налога

пријављеног финансијског службеника, чиме он потврђује веродостојност података у име своје матичне установе.



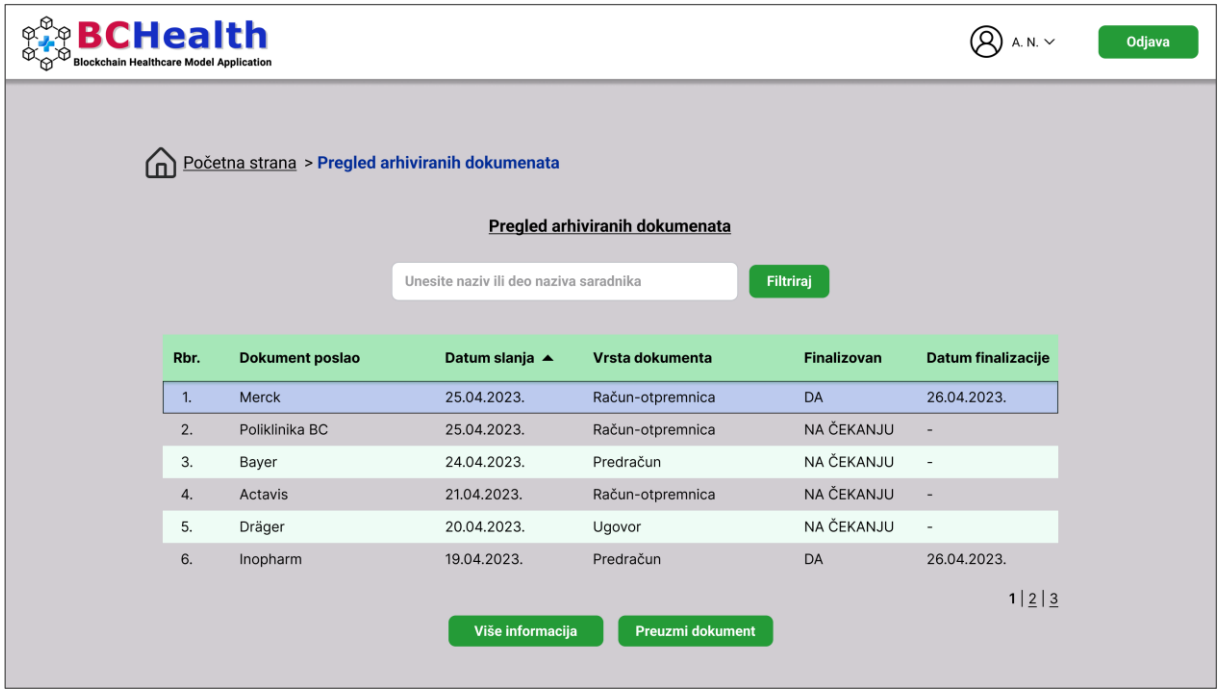
Слика 67. Потврда додавања дигиталног потписа у документ

Уколико су у пословној трансакцији биле укључене само две стране, односно, недостајао је један дигитални потпис, након извршења овог корака документ добија статус „финализован”, и брише се из листе чекања за верификацију.

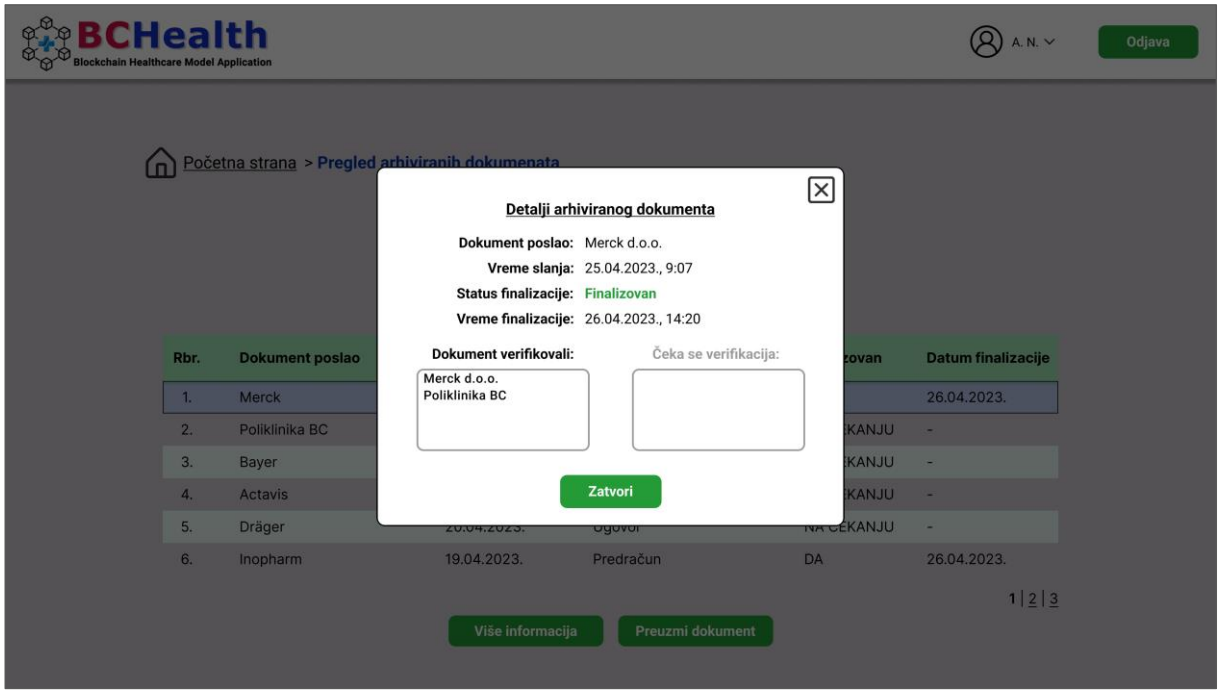
Преглед архивираних докумената

Избором одговарајуће опције на почетном екрану, финансијски службеник добија обједињен увид у сва пословна документа архивирана у *BCHealth* систему (слика 68). Путем табеларног приказа су дате информације о страни која је генерисала документ, датуму слања у систем, врсти документа као и тренутном статусу.

Избором опције „Више информација”, приказују се детаљи обележеног документа (слика 69). Уколико је верификован од стране свих захтеваних учесника пословне трансакције, документ добија статус „финализован”, а поље са недостајућим дигиталним потписима је празно.



Слика 68. Преглед архивираних докумената

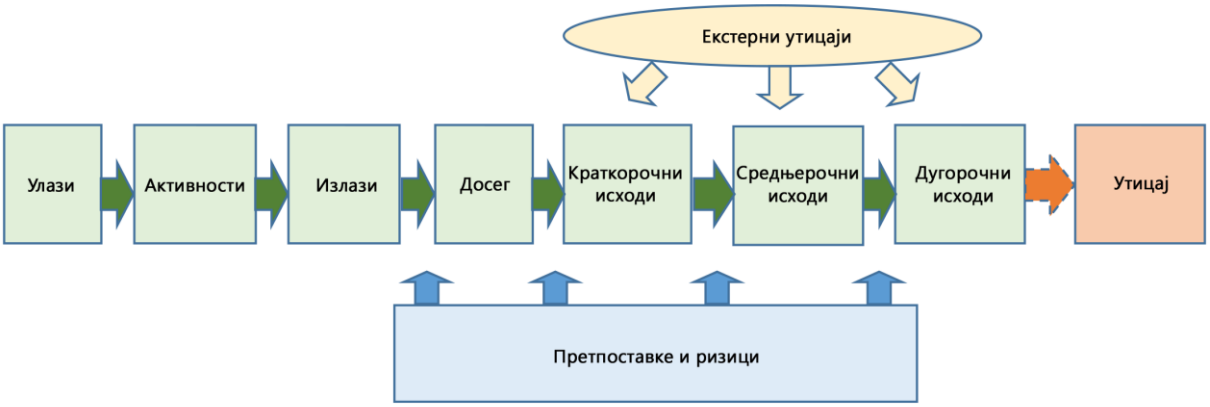


Слика 69. Детаљи одабраног архивираног документа

7.3. Планирање имплементације развијеног модела у здравствену установу

Логички модел који се користи у *„Evaluating new models of care: A guide for integrated care providers”* (Healthcare Improvement Scotland, 2017), приказан на слици 70, описује како се очекује да ће интервенција донети промену. У самом нацрту модела имплементације и евалуације дата је основна конструкција која мапира узрочне везе које

повезују ресурсе планиране за спровођење интервенције (инпути), са активностима које се планирају у току имплементације, резултатима, исходима и крајњем циљу (утицај) који се очекује да ће се постићи. Такође, експлицитно подразумева све имплицитне претпоставке о неопходним условима за успех, идентификује ризике и анализира спољне факторе који могу утицати на постизање жељених резултата.



Слика 70. Основне компоненте базичног модела имплементације нових технологија у сектору здравства (адаптирано из: Healthcare Improvement Scotland, 2017)

Активности: На основу спроведеног пилот истраживања изоловани су фактори од потенцијалног значаја за усвајање апликације базиране на *blockchain* технологији у здравственом сектору и они могу да допринесу усмеравању стратегије имплементације предложеног модела у одабрану здравствену установу. Као најзначајнији фактори издвајају се:

- Интегрисање здравствених података;
- Могућност размене здравствених информација између здравствених установа и лекара;
- Сигурност и заштита здравствених података;
- Поверење у систем контроле протока здравствених информација.

Обраћањем пажње на ове факторе може се постићи адекватнија имплементација модела.

Излази: Очекивани ефекти након имплементације модела су унапређено електронско пословање здравствене установе као и задовољство стејкхолдера функционисањем имплементираног модела.

Досег: Са аспекта евалуације модела, значајно је проценити његово функционисање након одређеног временског оквира примене и функционисања. Евалуација у овом истраживању је предвиђена након месец дана (краткорочни ефекти). У даљем току евалуације она се може спровести и након шест месеци (средњерочни ефекти) као и годину дана (дугорочни ефекти).

Претпоставке и ризици: Претпоставка је да ће постојати известан ниво отпора према примени нових технологија које су обухваћене овим моделом, што доводи у ризик процес имплементације модела, односно његово адекватно функционисање. Превазилажење ових ризика може се обезбедити проценом нефункционалности досадашњег начина пословања и указивањем свим стејкхолдерима на ниво значајности

очекиваних промена након имплементације модела, пре свега са аспекта сајбер сигурности.

Екстерни утицаји: Претпостављени спољни утицаји су ограничења која проистичу из нивоа опремљености и функционалности здравствене установе са аспекта ИКТ, јер је за несметано функционисање софтверских решења из модела потребан одређени ниво хардверске подршке.

7.4. Анализа стања електронског пословања у здравственој установи

Пре самог процеса имплементације развијеног модела у здравствену установу, неопходно је било спровести анализу актуелног стања електронског пословања.

У одабраној здравственој установи – Специјалистичкој поликлиници Новаков и сар. из Новог Сада – детаљно је анализирана употреба ИКТ и постојећих софтверских решења, процењен је ниво сајбер сигурности електронских података о пацијентима као и других аспеката електронског пословања установе.

Специјалистичка поликлиника Новаков и сар. основана је 2015. године у Новом Саду. Поља рада које покрива ова здравствена поликлиника су: гинекологија и акушерство, дерматологија, естетска медицина, интерна медицина, урологија и радиологија.

Тим стручњака који пружа здравствене услуге у Специјалистичкој поликлиници Новаков и сар. чине: 8 лекара специјалиста гинекологије и акушерства, 7 лекара специјалиста дерматологије, 8 лекара специјалиста интерне медицине (са ужим специјализацијама из ендокринологије, кардиологије, хематологије и гастроентерологије), 2 лекара специјалисте анестезиологије, 3 лекара специјалисте урологије, 1 лекар специјалиста радиологије и 2 лекара на специјализацији. Особље чине и 15 медицинских сестара-техничара као и 4 административна радника.

ИКТ инфраструктура која се користи у поликлиници обухвата уобичајене елементе у таквом типу установа у приватном сектору а то су:

- Стони рачунари реномираних произвођача, актуелних карактеристика и перформанси, који су распоређени у лекарским собама за преглед, административном одељењу као и рецепцији поликлинике.
- Рачунарска мрежа гигабитног режима рада, уз употребу савремене активне (*smart switch*) и адекватне пасивне мрежне опреме (одговарајуће *UTP* каблирање, разводни панели и комуникацијски ормани).
- Сервер, смештен у посебно намењеној просторији, који опслужује веб апликацију која се користи у поликлиници, а служи и као база података.
- Више преносивих уређаја као што су лаптопови, таблети итд.
- Ласерски штампачи и мултифункцијски уређаји са инкорпорираним скенерима, на којима се штампају налази пацијената и пословна документација.

Софтвер који се користи на пријемном шалтеру поликлинике и у административном одељењу има више функционалних целина, од којих је свакако најважнија она за заказивање прегледа.

Функција заказивања омогућава поједностављен избор термина за преглед код жељеног лекара, као и могућност измене времена и преузимање пацијената од стране других лекара, у случају изненадног одсуствовања. На располагању је прилагођен визуелни приказ свих заказаних прегледа по данима, лекарима, хитности пријема итд. Систем и графички упозорава уколико је дошло до преклапања термина или до превеликог броја прегледа заказаних у одређеном временском року код истог лекара.

Административно особље у посебном модулу апликације има могућност разних анализа пословања поликлинике, у смислу протока пацијената, остварених прихода, отказивања заказаних термина итд. Учинак се може пратити по разним критеријумима – по лекару, врсти прегледа или дијагностичке услуге, утрошку лекова и потрошног материјала, наплаћеним услугама итд. На располагању су и прилагођени статистички алати, чији резултати могу да се користе и у маркетиншке сврхе, како би се унапредило пословање у смислу квалитета пружених услуга, уз остваривање већег профита.

Посебан део апликације је посвећен интерној апотеци, где се прате залихе лекова, медицинских препарата и санитетског материјала, и благовремено се врше поручивања у оквиру књиговодственог дела софтвера, од стране особља задуженог за набавку. У оквиру функције апотеке, врши се и праћење стања инфективног отпада, и евидентира његово одлагање. Сви рачуни, отпремнице и књиговодствена документација се, поред електронског облика, чува и у папирној форми, сортирано у регистраторима.

Писање лекарских извештаја за сада није обухваћено поменутом апликацијом. Налази се куцају у *Word* текст процесору из *Microsoft Office* пакета, и снимају у базу на серверу података. Копије свих откуцаних лекарских извештаја се чувају и у папирном облику, у оквиру одговарајућих картотека.

Што се тиче безбедности података са хардверског аспекта, сервер је опремљен хард дисковима великог капацитета, који су организовани у одговарајуће *RAID* низове, обезбеђујући нормално функционисање у случајевима отказа, чак и више јединица истовремено. Сервер је стандардно опремљен *UPS* уређајем за непрекидно напајање, тако да је могућност оштећења датотека у случају варијација напона или нестанка струје сведена на минимум. Безбедносне копије података су раније вршене на сваке 2 недеље, али је после хаварије система то смањено на 48 часова.

Приступ апликацији се одвија путем интернет претраживача, уз имплементиране одговарајуће сигурносне сертификате. Апликација се користи искључиво у интранету, тако да је мрежни саобраћај према серверу, који долази изван локалне рачунарске мреже, блокиран.

7.5. Практична примена софтверских решења и мониторинг процеса имплементације

Апликација за пацијенте тестирана је у периоду 15.04.2023.–14.05.2023. док је пословна апликација тестирана у периоду 20.04.2023.–20.05.2023. Одабрано је различито временско започињање тестирања из разлога да истраживач може активно да учествује у примени датих софтверских решења у здравственој установи, јер се очекивало да ће

овакав иновативни приступ у функционисању здравствене установе имати одређене тешкоће на самом почетку тестирања апликација.

Сам процес практичне примене софтверских решења је пролазио кроз следеће фазе:

I Фаза иницијације,

II Фаза стабилизације,

III Фаза функционалне примене.

Фаза иницијације се односи на првих 7 дана примене датих софтверских решења. У том периоду пажљиво је инкорпорирана дата апликација. У примени апликације коришћени су тест подаци. У делу апликације који се односи на пружање здравствене заштите, подаци о пацијентима су били фиктивни, док је садржај лекарских извештаја графички замагљен. Лекари установе су представљани само иницијалима. У пословном делу апликације, тест податке су чиниле фиктивне фактуре и комуникациони подаци здравствене установе и стејкхолдера. Добављачи су представљани пуним називима, јер се ради о јавно доступним подацима, а сви су регистровани као субјекти који се баве дистрибуцијом медицинске опреме и уређаја, тако да одговарају тест окружењу. Разлог за овакав вид употребе података условљен је законом о заштити права пацијената, а свакако не утиче на исход, јер се ради о пробном тестирању софтвера.

Фаза стабилизације примене датих софтверских решења односи се на наредних 7 дана примене апликације. У овој фази рад на тестираним апликацијама достигао је стабилан ниво, уз перманентну контролу функционисања апликације од стране истраживача.

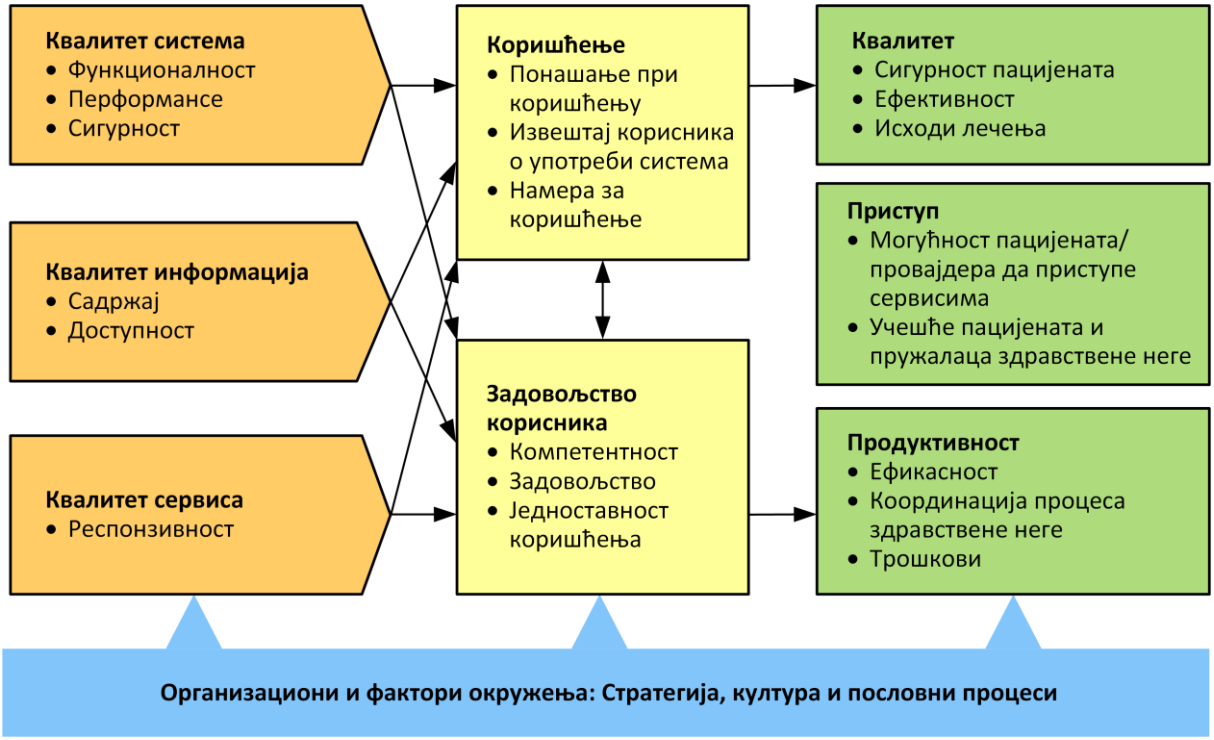
Фаза функционалне примене обухвата тест период функционисања апликације без активног учешћа истраживача. У овом истраживању, фаза функционалне примене је била ограничена на временски период од 14 дана.

8. ЕВАЛУАЦИЈА МОДЕЛА

Процес евалуације предложеног модела спроведен је кроз две фазе:

- евалуација имплементираног решења,
- идентификација кључних фактора који утичу на процес имплементације приказаног модела и мапирање узрочно-последичних веза од значаја за процес имплементације.

Основа за евалуацију модела представља комбинацију методологије и принципа који су предложени за сектор здравства – модела евалуације бенефита (енг. *Benefits evaluation model*) развијеног од стране Canada Health Infoway (2012), приказаног на слици 71 и модела имплементације нових технологија датог од стране Healthcare Improvement Scotland (2017) (слика 70).



Слика 71. Модел евалуације бенефита (адаптирано из: Canada Health Infoway, 2012)

На основу компоненти модела евалуације бенефита, дефинисани су кључни индикатори функционисања апликација који су праћени током и након имплементације модела и приказани су у табели 5.

У циљу евалуације, сачињени су структурирани интервју и скала процене према идентификованим кључним индикаторима перформанси (табела 5).

Евалуаторни интервју спроведен је након првих 14 дана тестирања апликације. Укупан број испитаника износио је 92, од чега су 22 испитаника били из реда медицинског особља (12 лекара специјалиста и 10 медицинских сестара/техничара) као и 70 пацијената/клијената.

Табела 5. Кључни индикатори перформанси имплементираног модела

Категорија и субкатегорија	Домен/субдомен бенефита	Индикатор
Квалитет система		
Функционалност	Општи квалитет	Структурирани интервју Скала процене
	Једноставност коришћења	
Перформансе	Интегративност	
	Поузданост	
Сигурност	Процена сигурности система	
Квалитет информација		
Садржај	Комплетност	Структурирани интервју Скала процене
	Прецизност	
Доступност	Брзина протока информација	
	Доступност информација	
	Формат и оквир информација	
Квалитет сервиса		
Респонзивност	Општи квалитет система	Структурирани интервју Скала процене
	Брзина овладавања системом	
	Ниво обучености	
	Ниво континуиране подршке	
Подаци о коришћењу	Процењени нивои употребе	
Намера коришћења	Ниво препоруке	
	Даља употреба система	
Задовољство корисника		
Корисничко искуство	Опште задовољство	Структурирани интервју Скала процене
	Значај за свакодневну праксу	
Лакоћа коришћења	Квалитет софтверских решења	
	Процена опсега рутинског коришћења	
	Предлог за унапређење	Отворен тип питања
Постигнути квалитет		
Сигурност пацијената	Процењени ниво сигурности	Структурирани интервју Скала процене
Приступање систему	Једноставност коришћења	
	Спремност прихватања нове технологије	
Утицај на квалитет услуге	Процена подизања нивоа квалитета	
Продуктивност		
Ефикасност	Процена ефикасности система	Структурирани интервју Скала процене
Координација процеса заштите	Процена нивоа координације	
Трошкови	Процена оправданости улагања	

Резултати интервјуа и анализа оцена на скали од 1 до 10 указују на висок степен процењеног квалитета апликације од стране корисника – медицинског особља и пацијената/клијената.

Просечне оцене употребе и перформанси апликације дате су у табели 6.

Табела 6. Просечне оцене употребе апликације за пацијенте (здравствени подаци)

Категорија	Медицинско особље		Пацијенти	
	x̄	SD	x̄	SD
Општи квалитет	9,00	0,75	9,20	1,37
Једноставност коришћења	8,50	1,01	8,86	1,67
Интеграција у свакодневну праксу	8,27	0,88	9,02	1,53
Поузданост	8,90	0,75	9,14	1,44
Процена сигурности система	9,09	0,68	9,23	1,39
Комплетност	8,90	0,88	9,13	1,51
Прецизност	8,86	0,79	9,08	1,63
Брзина пружања информација	8,59	1,22	9,30	1,34
Доступност када је потребна	9,04	0,78	9,41	1,30
Формат и оквир информација	9,22	0,75	9,38	1,31
Општи квалитет који систем пружа	9,40	0,73	9,51	0,84
Брзина овладавања системом	8,81	1,13	8,07	2,06
Ниво обучености	8,18	1,13	8,42	2,30
Ниво континуиране подршке	9,45	0,78	9,14	1,54
Ниво употребе	8,90	0,75	9,10	1,62
Ниво препоруке	9,36	0,65	9,20	1,49
Даља употреба система	9,31	0,71	9,28	1,37
Опште задовољство	9,04	0,80	9,14	1,45
Значај за свакодневну праксу	8,63	1,04	8,97	1,68
Квалитет софтверских решења	9,02	0,69	9,18	1,45
Процена опсега рутинског коришћења	8,09	1,37	8,89	1,82
Процењени ниво сигурности	9,22	0,61	9,24	1,47
Једноставност коришћења	8,40	1,43	9,0	0,92
Спремност прихватања	9,18	0,66	9,30	1,48
Процена подизања нивоа квалитета	9,22	0,58	9,40	1,37
Процена ефикасности система	9,13	0,56	9,08	1,57
Процена нивоа координације	9,22	0,81	9,41	0,81
Процена оправданости улагања	8,13	1,35	9,68	1,26

Подаци добијени интервјуом са анкетираним особама – корисницима (медицинско особље и пацијенти) указују на високо задовољство применом апликације.

Најчешћи одговори, у току интервјуа, на питања везана за примену апликације су:

- Нуди обједињени приказ здравствених података.
- Приступ подацима је једноставан и интуитиван.
- Пружа добар увид у ток лечења.
- Постигнут је висок ниво сигурности података.
- Препоручио/ла бих даљу употребу апликације.

С обзиром на одговоре у интервјуу и високе оцене на скали процене, може се извести закључак да постоји изражено задовољство употребом апликације, као и очекивани висок степен намере за даљу употребу и препоруку.

Предлози за унапређење се могу свести на следеће:

- Побољшати приказ ранијих епизода лечења.
- Инкорпорирати могућност заказивања.
- Омогућити повезивање са другим здравственим установама ради креирања јединственог и свеобухватног здравственог картона.

Евалуаторни интервју за пословну апликацију спроведен је након 14 дана од почетка тестирања апликације.

У циљу евалуације, сачињени су структурирани интервју и скала процене према идентификованим кључним индикаторима перформанси (табела 5).

Укупан број испитаника износио је 22 и њега сачињавају особе из менаџмента установе (3), фармацеутских компанија (5), добављача (11) и осигуравајућих кућа (3).

Резултати спроведеног интервјуа и процене на скали од 1 до 10 указују на високу оцену перформанси апликације као и њеног прихватања од стране корисника. Просечне оцене процене квалитета пословне апликације дате су у табели 7.

Табела 7. Просечне оцене квалитета пословне апликације

Категорија	$\bar{x}$	SD
Општи квалитет	9,27	0,76
Једноставност коришћења	9,13	0,88
Интеграција у свакодневну праксу	8,86	1,08
Поузданост	8,89	0,84
Процена сигурности система	9,18	0,58
Комплетност	9,09	0,62
Прецизност	8,86	0,71
Брзина пружања информација	8,68	0,89
Доступност када је потребна	9,14	0,56
Формат и оквир информација	8,95	0,96
Општи квалитет који систем пружа	9,18	0,63
Брзина овладавања системом	8,77	1,06
Ниво обучености	9,07	0,85
Ниво континуиране подршке	9,45	0,34
Ниво употребе	8,81	1,09
Ниво препоруке	9,54	0,50
Даља употреба система	9,59	0,79
Опште задовољство	9,72	0,55
Значај за свакодневну праксу	9,31	0,78
Квалитет софтверских решења	9,77	0,52

Категорија	x̄	SD
Процена опсега рутинског коришћења	9,13	1,20
Процењени ниво сигурности	9,76	0,42
Једноставност коришћења	9,21	1,24
Спремност прихватања	9,23	0,81
Процена подизања нивоа квалитета	8,95	1,36
Процена ефикасности система	9,18	0,73
Процена нивоа координације	8,86	1,03
Процена оправданости улагања	8,40	1,00

Подаци добијени интервјуом са анкетираним корисницима указују на високо задовољство применом апликације.

Најчешћи одговори на питања везана за примену апликације могу се сажети на истицање следећих карактеристика:

- једноставност примене,
- прегледна и функционална апликација,
- брз проток потребних информација,
- поверење и сигурност апликације.

С обзиром на одговоре у интервјуу и имајући у виду високе оцене на скали процене, може се закључити да постоји задовољство употребом апликације као и очекивани висок степен намере за даљу употребу и препоруку.

Препоруке које су дате могу се сумирати на:

- потребу за увођењем плаћања путем криптовалута,
- увођење листе где се уписује тип прописане терапије и потрошни материјал ради евиденције просечне потрошње по пацијенту, чиме се може предвидети набавка лекова и потрошног материјала, што је од значаја како за пословање здравствене установе тако и за целокупни систем здравствене заштите.

8.1. Идентификација фактора који утичу на прихватање апликација базираних на *blockchain* технологији и мапирање узрочно-последичних веза

У циљу даљег развијања модела дигиталног здравственог екосистема заснованог на *blockchain* технологији, неопходно је утврдити кључне факторе који доприносе процесу његове имплементације. Да би се проценили фактори као и њихов допринос усвајању развијеног модела, спроведено је истраживање након примене софтверских решења из модела. У истраживању су учествовали сви који су употребљавали апликацију током тестирања, 7 дана након завршетка пробног тестирања као и индивидуе које су особе које су тестирале апликацију навеле да су са њима поделиле искуство са тестирања апликације. Истраживање је спроведено применом анкетног упитника. Упитник је администриран путем *Google Forms* платформе и позив за попуњавање анкете прослеђен

је свима који су учествовали у тестирању, а који су даље проследили упитник особама са којима су поделили искуство са *blockchain* технологијом. Укупан број преузетих валидних упитника износио је 249.

8.1.1. Методологија

Подаци

У циљу прикупљања података креиран је упитник који се састојао из две целине. Први део упитника садржи информације о теми истраживања, мотивацији и циљевима за упознавање испитаника са ситуацијом, као и питања која се односе на демографске карактеристике испитаника. Други део је формиран од питања која репрезентују варијабле од процењеног значаја за прихватање ове технологије. Питања су дата у форми петостепене Ликертове скале, са одговорима „уопште се не слажем", „не слажем се", „нисам сигуран/а", „слажем се" и „потпуно се слажем", који одговарају нумеричким вредностима од 1, 2, 3, 4 и 5.

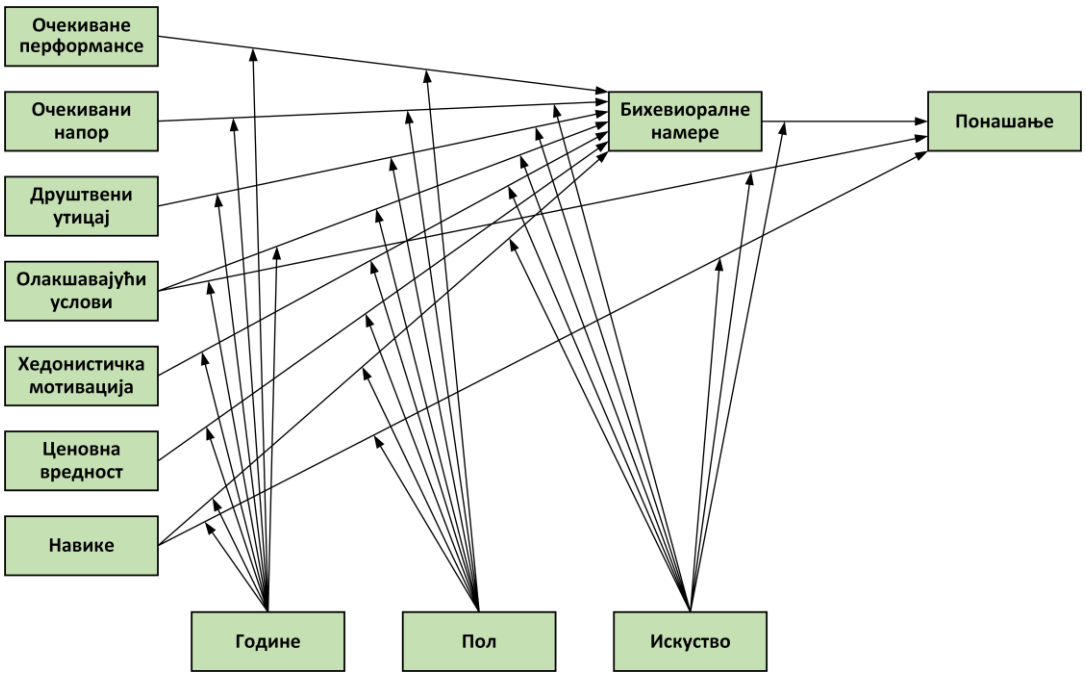
Дизајн упитника

Након првог дела упитника, који је садржао демографске податке – животно доба, пол, образовни и радни статус и улогу у здравственом систему, следи други део упитника, у чијем креирању се одабир варијабли базирао на теоријским конструктима који чине модел *TAM* (енг. *Technology Acceptance Model*), односно његових касније развијених модификација – *UTAUT* модела односно *UTAUT2* модела (енг. *Unified Theory of Acceptance and Use of Technology*).

UTAUT модел чине четири предикторска фактора за намере понашања корисника: очекиване перформансе, очекивани напор, социјални фактори и олакшавајући услови. Предиктор „Очекиване перформансе" обухвата: перципирану корисност, екстринзичку мотивацију, погодности за свакодневну употребу, релативну предност и очекивани исход, док очекивани радни напор обухвата перципирану једноставност употребе и сложеност. *UTAUT2* предвиђа да је употреба технологије од стране појединца исказана и са утицајем још три додатна конструкта, а то су (Venkatesh et al., 2012):

- Хедонистичка мотивација, која представља забавност или задовољство које проистиче из коришћења дате технологије, што је од великог значаја за прихватање и коришћење нових технолошких решења;
- Ценовна вредност, која се дефинише као компромис клијената између уочене користи у односу на новчана издвајања која продразумева њихово коришћење;
- Навика – конструкт који процењује у којој мери особе имају тенденцију да се понашају по навици.

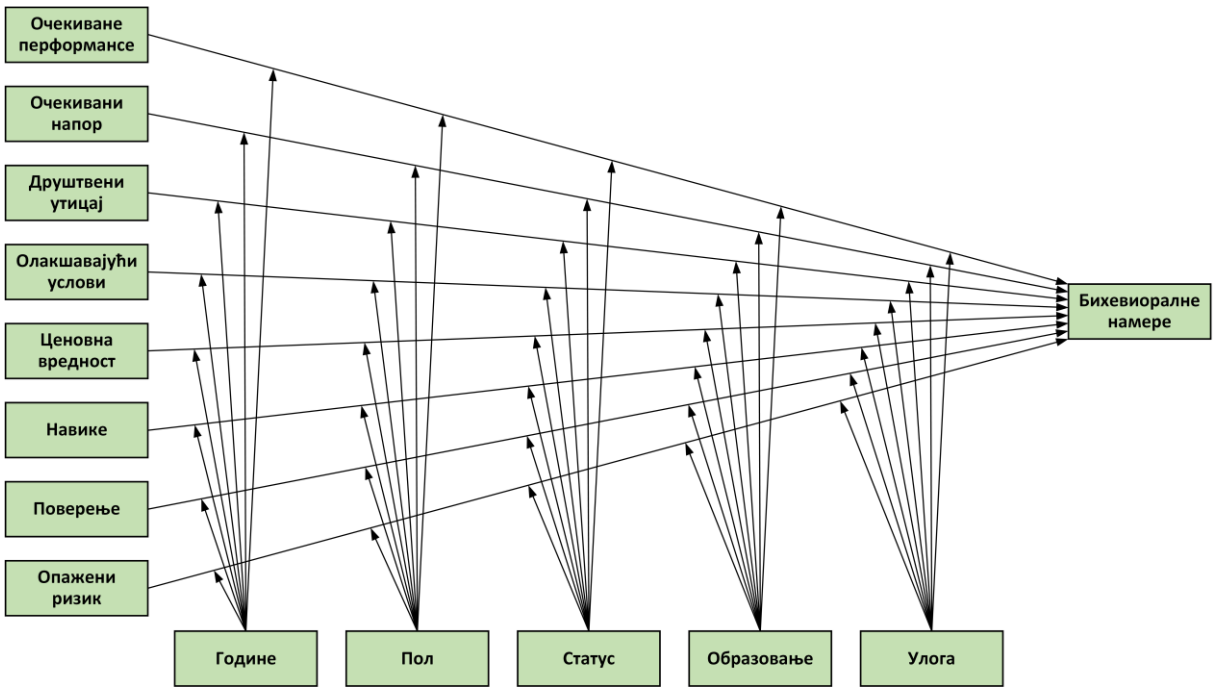
Графички приказ *UTAUT2* модела дат је на слици 72.



Слика 72. *UTAUT2* модел (адаптирано из: Venkatesh et al., 2012)

У сврху овог истраживања коришћен је модел који представља модификацију *UTAUT2* модела у којој је конструкт „Хедонистичка мотивација" замењен са конструктима „Опажени ризик" и „Поверење". Конструкте „Опажени ризик" и „Поверење" су предлагали Lee и сар. (2010), као модификацију оригиналног *UTAUT* модела. У бројним истраживањима је одавно уочено да опажени ризик има значајан утицај на понашање у дигиталном електронском пословању (Featherman & Pavlou, 2003; Zeithaml et al., 2006). Новија истраживања поново указују на значај опаженог ризика (Kettunen et al., 2018; Chao, 2019; Muktamarisa & Afiff, 2022; Jeon et al., 2020). Конструкт „Поверење" је дефинисан као ниво поверења корисника у технологију и представља део предности које се опажају у току коришћења технологије (El-Masri & Tarhini, 2017).

Приказани конструкти, који чине модификовани *UTAUT2* модел, који су разматрани у овом истраживању и за које се претпоставља да имају утицај на ниво усвајања и прихватања *blockchain* технологије у здравственом екосистему (бихевиоралне намере) су: очекиване перформансе, опажени ризик, друштвени утицај, очекивани учинак, ценовна вредност, олакшавајући услови, навике и поверење. Графички приказ овако модификованог *UTAUT2* модела дат је на слици 73.



Слика 73. Модификован *UTAUT2* модел

Наведени конструкти представљају независне варијабле док су модератор варијабле: животно доба, пол, образовни и радни статус и улога у здравственом систему.

Табела 8 садржи приказ питања из анкете везане за истраживање спремности примене *blockchain* технологије у здравственом сектору, према горе наведеним конструктима модификованог *UTAUT2* модела.

Табела 8. Распоред питања по конструктима из модификованог *UTAUT2* модела

Код	Ајтем
Очекиване перформансе	
PE1	Сматрам да би се применом апликације засноване на *blockchain* технологији постигло знатно унапређење функционисања здравственог сектора.
PE2	Увођење апликација у здравство је предуслов за квалитетније лечење и рад лекара и здравствене установе у целини.
PE3	Сматрам да је сигурније користити апликације засноване на *blockchain* технологији него традиционални начин лечења и организације процеса у здравственој установи.
PE4	Сматрам да би рад здравствене установе и лекара био ефикаснији и квалитетнији да постоји увид у целокупну документацију.
PE5	Третман пацијената је квалитетнији ако здравствена установа користи апликације засноване на *blockchain* технологији.
PE6	Сматрам да имплементација *blockchain* технологије нуди квалитетније услуге у здравственој установи.
PE7	Апликација заснована на *blockchain* технологији даје већу сигурност у раду здравствене установе и лекара.
PE8	По мом мишљењу, имплементација *blockchain* технологије резултира високим нивоом приватности личног здравственог картона, с обзиром на могућност приступања само од стране ауторизованих здравствених радника/органа.
PE9	*Blockchain* технологија обезбеђује да информације буду тачне, поуздане и једноставне за разумевање.

Код	Ајтем
PE10	Очекујем да подаци које размењујем са здравственом установом буду приватни и дељени само онима који имају право приступа.
PE11	Очекујем велику корист од примене *blockchain* технологије у здравству.
PE12	Апликација заснована на *blockchain* технологији је велики квалитативни искорак у сектору здравства.
Очекиван напор	
EE1	Сматрам да коришћење *blockchain* технологије знатно штеди време.
EE2	Сматрам да се коришћењем апликације за здравство засноване на *blockchain* технологији повећава безбедност података.
EE3	Коришћење апликације за здравство засноване на *blockchain* технологији је једноставно и практично.
Друштвени утицај	
SI1	Дељење здравствених информација има значај за побољшање начина лечења.
SI2	Намеравам да препоручим коришћење здравствених апликација заснованих на *blockchain* технологији својим пријатељима и породици.
Олакшавајући услови	
FC1	Применом *blockchain* технологије олакшана је онлајн размена информација.
FC2	Примена *blockchain* технологије резултира уштедом времена, како код пацијената тако и код осталих заинтересованих страна.
FC3	Применом *blockchain* технологије олакшава се рад здравствене установе.
FC4	Апликација заснована на *blockchain* технологији омогућава добру комуникацију медицинског особља и пацијената.
FC5	Приступ информацијама применом апликација заснованих на *blockchain* технологији је олакшан.
Ценовна вредност	
PV1	Улагање у апликације засноване на *blockchain* технологији представља оправдану инвестицију.
PV2	Спреман сам на додатне новчане издатке за апликације засноване на *blockchain* технологији.
Навике	
H1	Сматрам да је ефикасна и сигурна комуникација основ за квалитетније пружање услуга.
H2	Могућност дељења информација онлајн нуди велике предности у односу на традиционалне начине комуникације.
H3	Увек сам спреман да прихватам нова технолошка решења.
Поверење	
T1	*Blockchain* технологија повећава ниво поверења и сигурности.
T2	Осећам се сигурно када делим информације применом апликације засноване на *blockchain* технологији.
Опажени ризик	
PR1	Не осећам се сигурно да делим информације путем апликације засноване на *blockchain* технологији.
PR2	Подаци здравствене установе нису довољно сигурни при коришћењу апликације засноване на *blockchain* технологији.
PR3	Апликација заснована на *blockchain* технологији није функционална за примену у здравственој установи.
PR4	Информације које се деле путем примене апликације засноване на *blockchain* технологији у здравственој установи могу бити злоупотребљене.
PR5	Апликација заснована на *blockchain* технологији у здравственој установи је сложена за коришћење.
PR6	Важно ми је да подацима у здравственој установи може да приступа само ауторизовано особље контролом приступа.
PR7	Функционисање здравствене установе није безбедно уколико се комуникација одвија онлајн.

Код	Ајтем
PR8	Апликације засноване на *blockchain* технологији у здравственом сектору не смањују ризик од крађе података.
Бихевиоралне намере	
BI1	Спреман/на сам да и даље користим апликације за здравство засноване на *blockchain* технологији.
BI2	Сагласан/на сам да у апликацији заснованој на *blockchain* технологији чувам податке.
BI3	Сматрам да апликација заснована на *blockchain* технологији омогућује сигурну размену података у здравственом сектору.
BI4	Имам поверење у апликације засноване на *blockchain* технологији.
BI5	Намеравам да препоручим другима апликацију засновану на *blockchain* технологији.

8.2. Статистичка анализа мерног модела

Моделирање структурних једначина (енг. *Structural equation modeling – SEM*) је примењено да се испитају хипотезе. *SEM* представља статистичку технику која приказује посматране податке кроз структурне параметре које карактерише теоријски оквир (Khan et al., 2021).

Коришћењем коефицијента детерминације (*R-squared*), предиктивна тачност модела је одређена процесом који укључује квадратну корелацију између стварних и предвиђених вредности датог ендогеног конструкта. Овај коефицијент представља комбиновани утицај егзогене латентне варијабле на ендогену латентну варијаблу. Према Chin et al. (1988) вредности коефицијента веће од 0,67 су јаке, вредности од 0,33 до 0,67 су директне, оне од 0,19 до 0,33 су слабе, а оне испод 0,19 су искључене.

У циљу провере да ли мерни модел конструката има адекватну валидност и поузданост, примењена је анализа у два корака. *Chronbach's α* композитна поузданост (енг. *Composite Reliability – CR*) и просечна екстрахована варијанса (енг. *Average Variance Extracted – AVE*) употребљавају се за одређивање поузданости и ваљаности конструкција (Asadi et al., 2019).

Поузданост је процењена помоћу *Cronbach's α*, са вредношћу >0,7 за добру поузданост. Конвергентна валидност је прихватљива ако је факторско оптерећење за сваку конструктивну ставку >0,7, *CR* за сваку конструкцију је >0,7, а *AVE* за сваку конструкцију је >0,5. Дискриминаторна валидност је верификована ако је спољашње оптерећење сваке конструкције веће од било ког њеног унакрсног оптерећења на друге, и ако је квадратни корен *AVE* сваког конструкта већи од његових корелација са било којим другим (Wang et al., 2020).

Конфирматорна факторска анализа спроведена је у циљу провере да ли свака димензија испуњава стандарде за конвергентну валидност које су установили Fornell и Larcker (1981), а то су следећи:

- нормализовани фактори са оптерећењем >0,5 имају добру конвергентну валидност;
- латентне варијабле са *CR* од >0,6 (праг) имају одличну конзистентност;
- латентне варијабле са *AVE* од >0,5 имају погодну моћ објашњења.

Статистичка анализа изршена је применом *SmartPLS 4.0* софтверског алата.

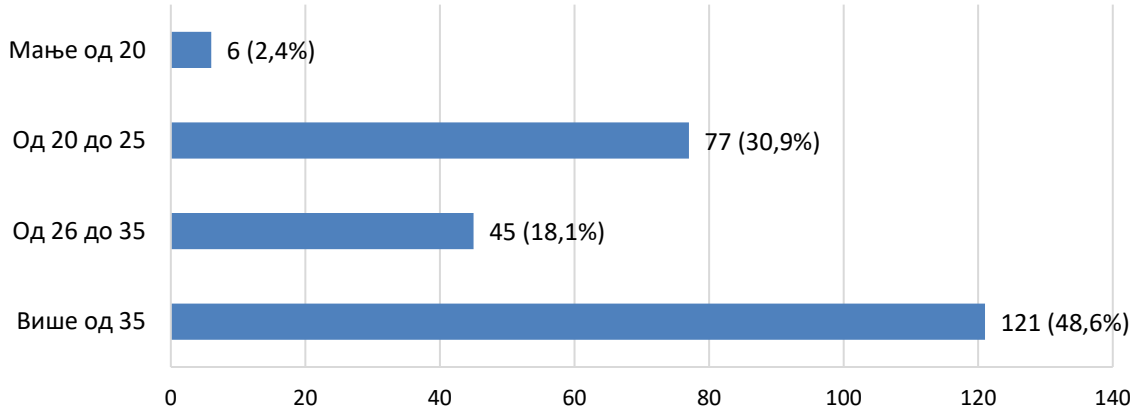
8.3. Резултати евалуације

Дескриптивни статистички подаци

Као што је наведено, анкетирано је укупно 249 испитаника. Испитаници/це се међусобно разликују по демографским подацима (старост, пол, радни статус, ниво образовања, улога у здравственом систему).

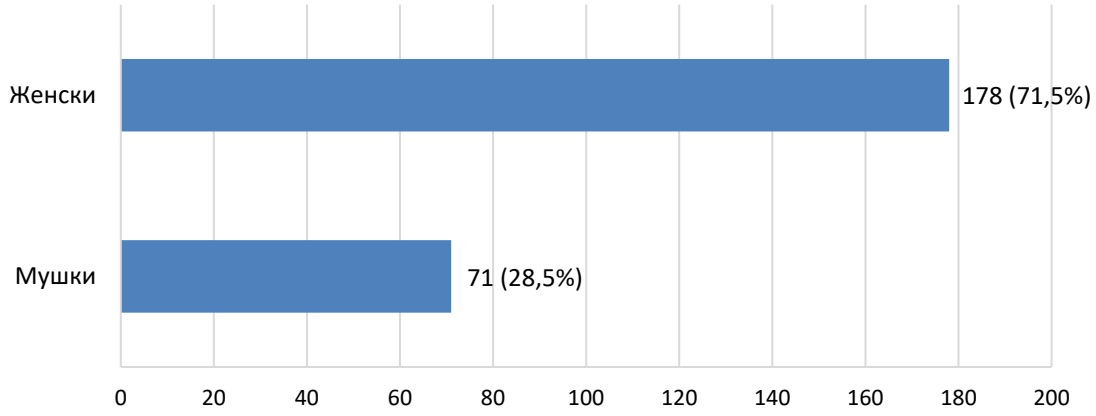
По питању животног узраста, највећи број испитаника/ца је старости преко 35 година, а затим следе испитаници/це узраста 20 до 25 година старости (графикон 34).

Графикон 34. Узорак испитаника по старости



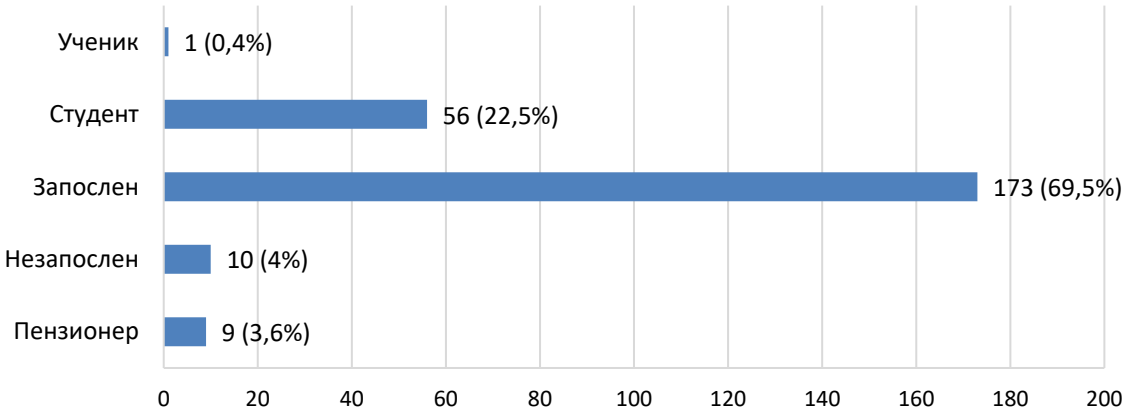
У истраживачкој анкети у већој мери су учествовали испитаници женског пола (графикон 35).

Графикон 35. Узорак испитаника по полу



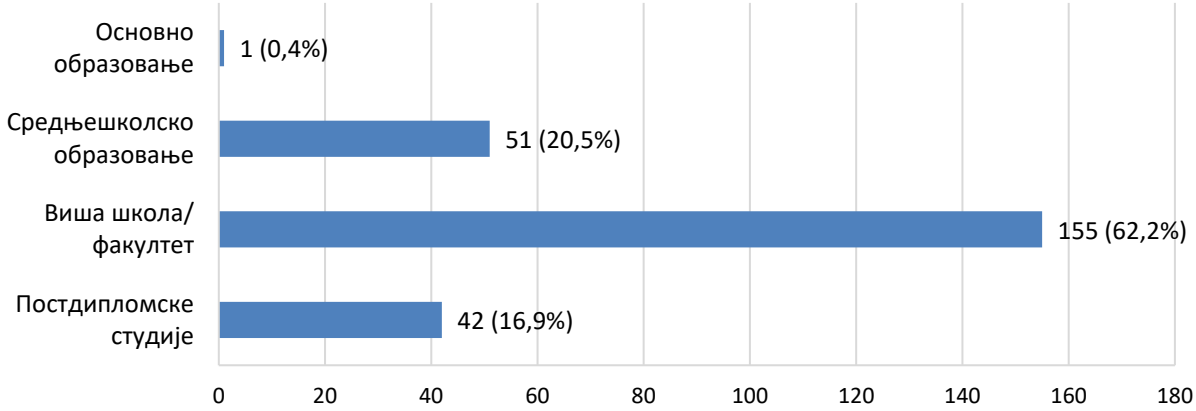
По питању радног статуса испитаника/ца, највећи број њих је запослен или студира. Осталим категоријама припада значајно мањи број испитаника (графикон 36).

Графикон 36. Узорак испитаника/ца према радном статусу



Највише је испитаника/ца који су завршили вишу школу или имају факултетско образовање, а мањи број њих има завршене постдипломске студије и средњешколско образовање (графикон 37).

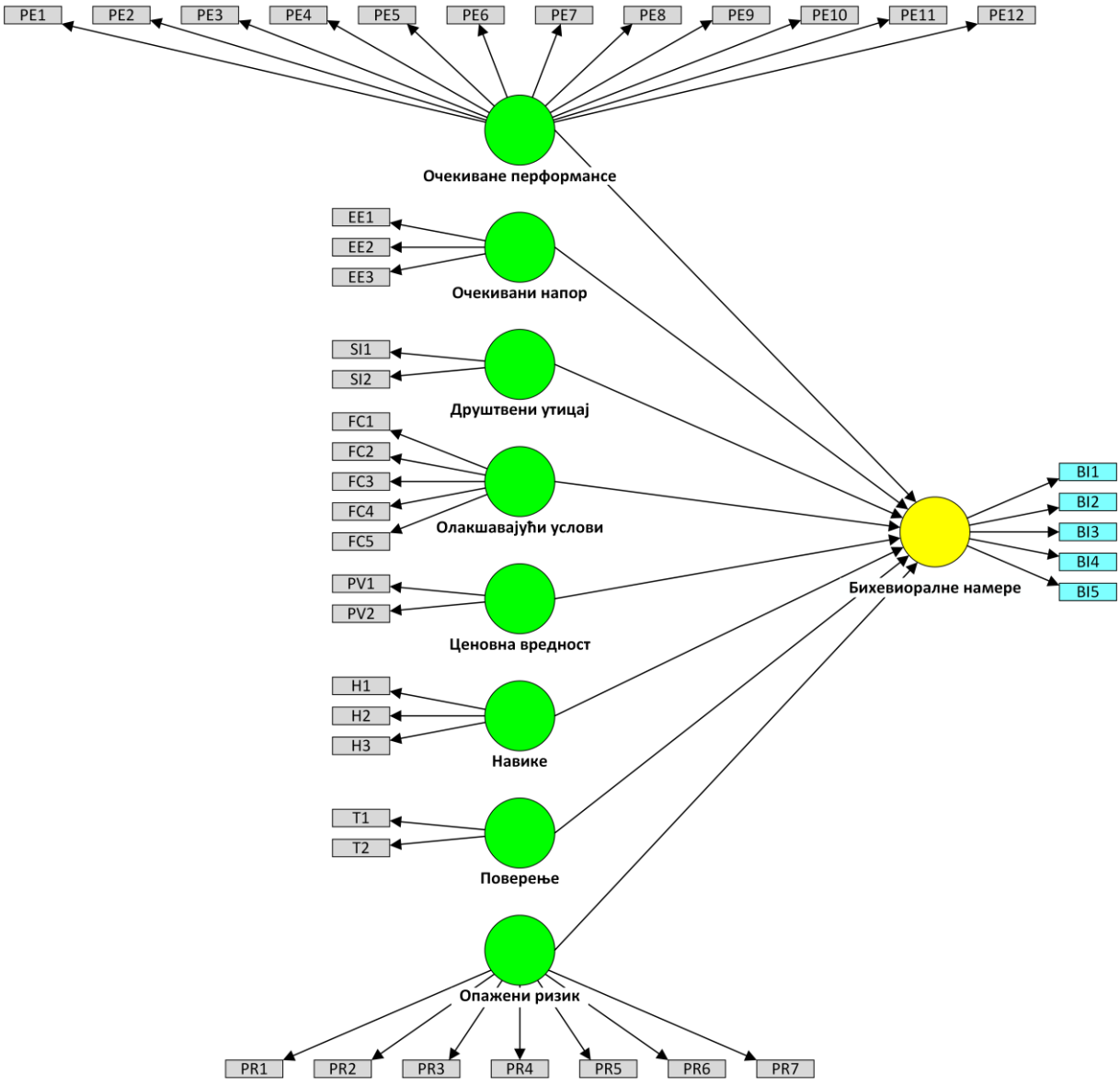
Графикон 37. Узорак испитаника/ца по образовном статусу



Према улози у систему здравствене заштите, највећи број њих има улогу пацијента, затим следе здравствени радници (медицинске сестре/техничари, фармацеути, лаборанти, лекари). Међу осталим, појављују се улоге: економисте, особља техничке службе, референата, ИТ стручњака, добављача итд. (графикон 38).

Графикон 38. Распоред испитаника/ца према улози у здравственом систему

На слици 74 приказан је модел мерења конструката из проширеног *UTAUT2* модела који представљају варијабле (очекиване перформансе, очекивани напор, друштвени утицај, олакшавајући услови, ценовна вредност, навике, поверење и опажени ризик) са својим ајтемима односно питањима. Зависна варијабла је „биохевиоралне намере", односно спремност корисника на коришћење *blockchain* технологије у дигиталном здравственом екосистему. Варијабле: старост, пол, статус, образовање и улога у здравственом систему представљају модератор варијабле.



Слика 74. Модел мерења испитиваних конструката

На основу приказаног модела су постављене следеће хипотезе:

X1: Процена очекиваног напора утиче на спремност корисника за коришћење *blockchain* технологије у здравственом сектору.

X2: Опажени ризик код корисника у здравственом сектору утиче на њихову спремност за коришћење *blockchain* технологије.

X3: Процењени друштвени утицај утиче на спремност корисника за коришћење *blockchain* технологије у здравственом сектору.

X4: Опажене очекиване перформансе утичу на спремност корисника за коришћење *blockchain* технологије у здравственом сектору.

X5: Процењена ценовна вредност утиче на спремност корисника за коришћење *blockchain* технологије у здравственом сектору.

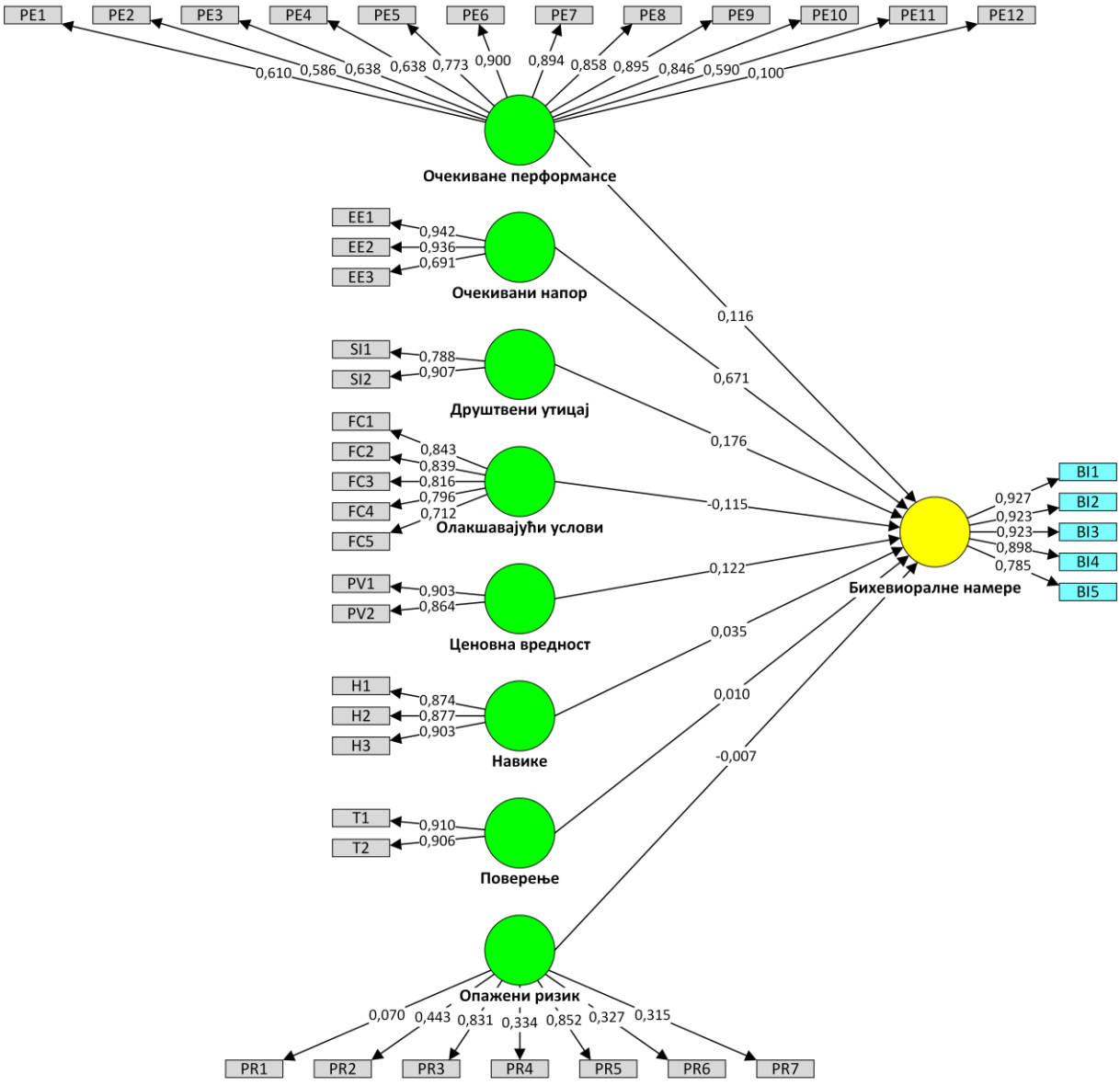
X6: Опажени олакшавајући услови утичу на спремност корисника да користе *blockchain* технологију имплементирану у оквиру здравственог система.

X7: Навике корисника имају утицај на спремност за коришћење *blockchain* технологије у здравственом сектору.

X8: Ниво поверења корисника има утицај на спремност за коришћење *blockchain* технологије у здравственом сектору.

Резултати

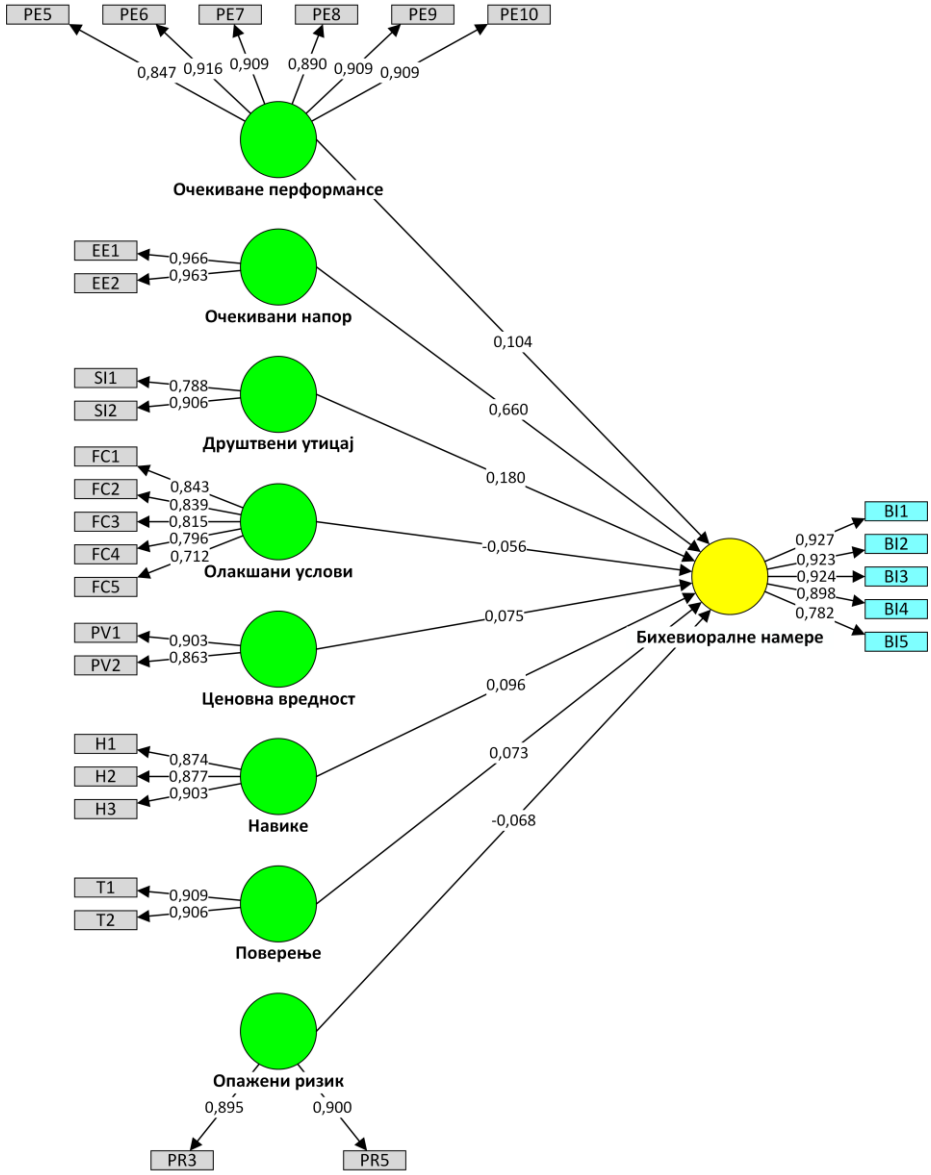
Применом *SmartPLS* софтвера, односно *PLS-SEM* алгоритма, евалуиран је мерни модел. Графички приказ спроведене анализе је дат на слици 75.



Слика 75. Резултат евалуације мерног модела применом *PLS-SEM* алгоритма

Детаљном анализом уочава се да поједина питања не мере добро кореспондентне конструкте, те су она елиминисана у циљу побољшања модела (ајтеми PE1, PE2, PE3, PE4, PE11, PE12, EE3, PR1, PR2, PR4, PR6, PR7).

Након њихове елиминације, преостали индикатори су основ за даљу статистичку анализу (слика 76).



Слика 76. Резултат примене *PLS-SEM* алгоритма након елиминације индикатора

Вредност *R-squared* од 0,918 указује да је модел добар, са високом предиктивном тачношћу, јер описује 91,8% варијансе зависне променљиве (табела 9).

Табела 9. Вредност *R-squared*

	R-squared	***Adjusted R-squared***
Бихевиоралне намере	0,918	0,907

У табели 10 је приказана оцена поузданости и валидности модела мерења испитиваних варијабли.

Табела 10. Оцена валидности модела мерења конструката

Варијабла	Индикатори	*Cronbach's α*	*Composite Reliability* (*CR*)	*Average Variance Extracted* (*AVE*)
Очекиване перформансе	PE5, PE6, PE7, PE8, PE9, PE10	0,942	0,966	0,815
Очекивани напор	EE1, EE2	0,913	0,965	0,929
Друштвени утицај	SI1, SI2	0,715	0,838	0,728
Олакшавајући услови	FC1, FC2, FC3, FC4, FC5	0,871	0,910	0,639
Ценовна вредност	PV1, PV2	0,731	0,867	0,778
Навике	H1, H2, H3	0,853	0,918	0,786
Поверење	T1, T2	0,796	0,909	0,828
Опажени ризик	PR3, PR5	0,768	0,899	0,810
Бихевиоралне намере	BI1, BI2, BI3, BI4, BI5	0,946	0,956	0,799

Вредност *Cronbach's α* је адекватна за све конструкте, што указује да су сва питања кохерентна и да адекватно мере конструкт којем су придружена. Вредности композитне поузданости (*CR*) су адекватне, као и вредности *AVE*.

Валидност је тестирана применом *Fornell-Larcker* критеријума. Табела 11 приказује матрицу корелација.

Табела 11. Оцена валидности модела – *Fornell-Larcker* критеријум

	Очекиване перформансе	Очекивани напор	Друштвени утицај	Олакшавајући услови	Ценовна вредност	Навике	Поверење	Опажени ризик	Бихевиоралне намере
Очекиване перформансе	0,897								
Очекивани напор	0,733	0,964							
Друштвени утицај	0,713	0,690	0,849						
Олакшавајући услови	0,733	0,690	0,654	0,803					
Ценовна вредност	0,633	0,695	0,707	0,568	0,883				
Навике	0,589	0,578	0,669	0,686	0,625	0,885			
Поверење	0,524	0,466	0,602	0,674	0,478	0,612	0,908		
Опажени ризик	0,577	0,626	0,662	0,685	0,512	0,801	0,573	0,898	
Бихевиоралне намере	0,777	0,920	0,789	0,704	0,755	0,658	0,561	0,643	0,893

Из табеле 12, која приказује тестирање хипотеза, закључује се да статистички значајан утицај на спремност примене *blockchain* технологије у здравственом сектору имају „Очекивани напор", „Друштвени утицај", „Ценовна вредност" и „Очекиване перформансе".

Табела 12. Тестирање хипотеза

Хипотеза	*Original sample (O)*	*Sample mean (M)*	*Standard deviation (STDEV)*	*T statistics (|O/STDEV|)*	*P values*
Очекиване перформансе → Бихевиоралне намере	0,116	0,119	0,058	2,002	0,045
Очекивани напор → Бихевиоралне намере	0,671	0,666	0,060	11,222	0,000
Друштвени утицај → Бихевиоралне намере	0,176	0,175	0,061	2,885	0,004
Олакшавајући услови → Бихевиоралне намере	-0,115	-0,110	0,062	1,863	0,063
Ценовна вредност → Бихевиоралне намере	0,122	0,121	0,044	2,807	0,005
Навике → Бихевиоралне намере	0,035	0,034	0,046	0,764	0,445
Поверење → Бихевиоралне намере	0,010	0,008	0,040	0,252	0,801
Опажени ризик → Бихевиоралне намере	-0,007	-0,003	0,046	0,151	0,880

Овакви резултати указују да на „Бихевиоралне намере" утичу „Очекивани напор", „Друштвени утицај", „Ценовна вредност" и „Очекиване перформансе", и да су заправо ови конструкти од највећег доприноса за спремност примене *blockchain* технолошких решења. У даљем раду и следственим истраживањима треба посветити пажњу управо овим конструктима. Промотивне стратегије треба базирати на истицању сигурности коју *blockchain* технологија пружа, оправданости улагања у развој апликација за здравство које се базирају на овој технологији као и указивању на утицај на повећање квалитета услуга и пословања у здравственом сектору применом *blockchain* технологије.

9. ЗАКЉУЧАК

У докторској дисертацији анализиран је проблем сајбер сигурности у области пословања здравственог система у дигиталном окружењу и предложен је модел дигиталног здравственог екосистема базиран на *blockchain* технологији. Приказана је исцрпна систематизација научне и стручне литературе из области *blockchain* технологије у здравственом сектору.

Главни циљ истраживања је предлог развоја модела дигиталног здравственог екосистема базираног на *blockchain* технологији. Предложени модел обухватио је кључне стејкхолдере дигиталног здравственог екосистема и размене података у пословним процесима, чија ће сигурност бити обезбеђена применом *blockchain* технологије. Сегментна анализа предложеног модела дигиталног здравственог екосисистема базираног на *blockchain* технологији издваја следеће карактеристике:

- *Core* модела представљају две базе података – здравствени картони пацијената и подаци о пословним трансакцијама које остварује здравствена установа са осталим стејкхолдерима у дигиталном здравственом екосистему.
- Модел подржава два нивоа интероперабилности података: пацијент-центричну и институционалну интероперабилност.
- У односу на пацијенте, формулација модела је пацијент-центрична, чиме се промовише квалитативно нови ниво интероперабилности података.
- Институционална интероперабилност података подржана је у предложеном моделу путем размене информација здравствене установе са осталим стејкхолдерима.
- Кључне трансакције података у предложеном моделу базирају се на примени *blockchain* технологије.
- Примена *blockchain* технологије у датом моделу омогућава управљање подацима и њихову верификацију без посредника, уз обезбеђење аутентичности, сталне доступности и проверљивости ускладиштених информација, као и постојање потпуне транспарентности.

Приказана су потенцијална техничка решења која су тестирана од стране кључних стејкхолдера у здравственом сектору у тест окружењу. За потребе дефинисаног модела дигиталног здравственог екосистема заснованог на *blockchain* технологији, развијена је децентрализована корисничка апликација – *BCHealth* (*BlockChain HealthCare*), која се састоји из две главне целине: здравствене компоненте, која се односи на подршку пружању услуга здравствене заштите и пословне компоненте, која обухвата кореспонденцију између здравствених установа, фармацеутских кућа, добављача медицинске опреме итд., односно свих идентификованих стејкхолдера који учествују у пословању здравственог екосистема и имају потребу за коришћењем платформе која им омогућава чување историје пословних трансакција на безбедан начин.

Примењена техничка решења, којима се обезбеђује функционисање предложеног модела, тестирана су и евалуирана у односу на квалитет система, квалитет информација, квалитет сервиса, коришћење система и задовољства корисника путем дефинисаних

одговарајућих кључних идентификатора перформанси. Анализа добијених резултата анкетирањем у пост-имплементационом периоду указује на високо задовољство применом предложених софтверско-техничких решења. Даљом анализом евалуаторних података идентификовани су кључни мотивациони фактори за усвајање *blockchain* технологије у сектору здравства и то су: очекивани напор, друштвени утицај, ценовна вредност и очекиване перформансе. Управо ови конструкти треба да представљају основ за промотивну стратегију примене *blockchain* технологије у сектору здравства Републике Србије.

Главна хипотеза која је тестирана у докторском раду и која гласи: „Развојем и применом модела дигиталног здравственог екосистема заснованог на *blockchain* технологији постиже се већа сигурност функционисања електронског пословања, проток и координација података, управљање подацима, интерабилност, кооперабилност стејкхолдера у здравственом сектору", као и посебне хипотезе у истраживању које су проистекле из главне истраживачке хипотезе су потврђене креирањем, имплементацијом, интеграцијом и евалуацијом предложеног модела.

Даљи развој предложеног модела може ићи у правцу омогућавања безбедних новчаних трансакција у оквирима апликација на којима се базира функционисање модела, било да се ради о трошковима лечења, било о новчаним токовима ланца набавке лекова, медицинских средстава и материјала; усмеравања складиштења и управљања подацима клиничких испитивања на безбедан и транспарентан начин (сваки корак тока клиничког испитивања снимљен на *blockchain*-у би омогућио олакшано праћење података и идентификовање грешака, верификацију идентитета пацијената и лекара, обезбеђујући максималну сигурност, јер би само овлашћени појединци имали приступ подацима клиничког испитивања); развој апликација за *IoMT*, креирајући безбедно окружење за *IoMT* уређаје који прате здравствено стање пацијената пружањем заштите од неовлашћеног приступа.

Кључни научни доприноси докторске дисертације се огледају у:

- Идентификацији проблема функционисања здравственог сектора са аспекта осетљивости здравствених података.
- Кохезивној теоријској концептуализацији проблематике сајбер сигурности у здравственом сектору.
- Предлогу методолошких корака у креирању модела дигиталног здравственог екосистема базираног на *blockchain* технологији.
- Предлогу модела дигиталног здравственог екосистема базираног на *blockchain* технологији.

Као стручни доприноси докторске дисертације издвајају се:

- Кохезиван приказ проблематике дигитализације здравственог сектора.
- Систематизован приказ и критички осврт на податке из научне и стручне литературе из области сајбер сигурности у здравственом сектору.
- Оригинална софтверско-техничка решења односно предлог апликација за здравствени сектор базираних на *blockchain* технологији.
- Могућност унапређења е-пословања здравствених установа применом *blockchain* технологије.

Резултати докторске дисертације дају могућност и ширих, друштвених импликација које се огледају у:

- Сагледавању проблематике функционисања здравственог сектора са аспекта сигурног протока информација.
- Креирању стратегија дигитализације здравственог сектора.
- Функционалном приступу имплементације *blockchain* технологије у здравствени сектор.
- Унапређењу процеса лечења заснованог на обједињеним здравственим информацијама о појединцу.
- Квалитативном помаку ка функционалном и унапређеном пословању, сарадњи и поверењу међу стејкхолдерима у дигиталном здравственом екосистему, пре свега базираном на сигурности протока података, како здравствених тако и података пословања здравствене установе.

ЛИТЕРАТУРА

[1] Abdelhak, M., Grostick, S., & Hanken, M. A. (2014). *Health information: Management of a strategic resource*. Philadelphia: Saunders.

[2] Aetsoft (n.d.). *Blockchain development for healthcare*. Available at: https://aetsoft.net/solutions/blockchain-healthcare/?gclid=Cj0KCQjwp86EBhD7ARIsAFkgakjYZgJbZag-kcYGs-k9hCl9j-FhnGXHPNqH8O_y4b-zjKV3LzMvk9caAq_SEALw_wcB

[3] Agarwal, R., Dugas, M., Gao, G. G., & Kannan, P. K. (2020). Emerging technologies and analytics for a new era of value-centered marketing in healthcare. *Journal of the Academy of Marketing Science*, *48*(1), 9–23. https://doi.org/10.1007/s11747-019-00692-4

[4] Ahamed, S. (2022, April 27). *10 Advantages and Disadvantages of Telemedicine*. DrCare247. Available at: https://www.drcare247.com/blog/telemedicine/10-advantages-and-disadvantages-of-telemedicine/

[5] Aich, S., Tripathy, S., Joo, M.-I., & Kim, H.-C. (2021). Critical Dimensions of Blockchain Technology Implementation in the Healthcare Industry: An Integrated Systems Management Approach. *Sustainability*, *13*(9), 5269. https://doi.org/10.3390/su13095269

[6] Algorand Developer Portal (n.d.) *Why Algorand?* Available at: https://developer.algorand.org/docs/get-started/basics/why_algorand

[7] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. *Journal of healthcare engineering*, *2019*, 7516035:1-7516035:15. https://doi.org/10.1155/2019/7516035

[8] Alkhushayni, S., Kengne, N., & Al-Zaleq, D. (2019). Blockchain Technology applied to Electronic Health Records. *Proceedings of 32nd International Conference on Computer Applications in Industry and Engineering*, *63*, 34-42. https://doi.org/10.29007/2x3r

[9] Arias, A. (2021, October 29). *5 Types of Healthcare Organizations and Their Medical Billing Practices*. NCG Medical. Available at: https://education.ncgmedical.com/blog/types-of-medical-organization

[10] Asadi, S., Abdullah, R., Safaei, M., & Nazir, S. (2019). An Integrated SEM-Neural Network Approach for Predicting Determinants of Adoption of Wearable Healthcare Devices. *Mobile Information Systems*, *2019*, 8026042:1-8026042:9. https://doi.org/10.1155/2019/8026042

[11] Ashbey, A. (2017, July 13). *Healthcare: The last frontier in e-commerce*. Forbes. Available at: https://www.forbes.com/sites/forbescommunicationscouncil/2017/07/03/healthcare-the-last-frontier-in-e-commerce/?sh=34df708f2130

[12] Asthana, S., Sheaff, R., Jones, R., & Chatterjee, A. (2020). eHealth technologies and the know-do gap: exploring the role of knowledge mobilisation. *Evidence & Policy*, *16*(4), 687-701. https://doi.org/10.1332/174426420X15808912803267

[13] Aunger, C. (2020, March 13). *'Chain' Reaction: The New Decade Will Bring Blockchain Piloting To Fruition In Healthcare And Beyond*. Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/03/13/chain-reaction-the-new-decade-will-bring-blockchain-piloting-to-fruition-in-healthcare-and-beyond/?sh=4a2933f450e1

[14] AuraQuantic (n.d.) *Industry 4.0 technologies*. Available at: https://www.auraquantic.com/technologies-intelligent-industry/

[15] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *Proceedings of 2nd International Conference on Open and Big Data (OBD)*, 25-30, https://doi.org/10.1109/OBD.2016.11

[16] Backlund, A. (2000). The definition of system. *Kybernetes*, *29*(4), 444–451. https://doi.org/10.1108/03684920010322055

[17] Bajwa, M. (2014). mHealth Security. *Pakistan Journal of Medical Sciences*, *30*(4), 904–907. https://doi.org/10.12669/pjms.304.5210

[18] Balestra, M. (2018). Telehealth and Legal Implications for Nurse Practitioners. *Journal for Nurse Practitioners*, *14*(1), 33–39. https://doi.org/10.1016/j.nurpra.2017.10.003

[19] Bali, S., Bali, V., Mohanty, R. P., & Gaur, D. (2022). Analysis of critical success factors for blockchain technology implementation in healthcare sector. *Benchmarking: An International Journal*, *30*(4), 1367-1399. https://doi.org/10.1108/BIJ-07-2021-0433

[20] Balingit, A. (2022, September 30). *Telemedicine: What to know*. MedicalNewsToday. Available at: https://www.medicalnewstoday.com/articles/telemedicine

[21] Barrett, M., Marron, J., Pillitteri, V. Y., Boyens, J., Quinn, S., Witte, G., & Feldman, L. (2020). Approaches for Federal Agencies to Use the Cybersecurity Framework. Gaithersburg (MD): National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8170-upd

[22] Birch, P. (2018, January 26). *New Business Models For The Emerging Consumer-Driven On-Demand Healthcare Economy*. Health IT Outcomes. Available at: https://www.healthitoutcomes.com/doc/new-business-models-for-the-emerging-consumer-driven-on-demand-healthcare-economy-0001

[23] Bjelica, A. (2020). *Razvoj inovativnog modela komunikacije u elektronskom poslovanju zdravstvenih ustanova* (doktorska disertacija). Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, Srbija.

[24] Bjelica, A., Bjelica, D., Despotović-Zrakić, M., & Labus, A. (2021). Model for digital healthcare ecosystem based on blockchain technology: a pilot study. *E-Business Technologies Conference Proceedings*, *1*(1), 146–147. https://ebt.rs/journals/index.php/conf-proc/article/view/57

[25] Bocas, J. (2022, Jan 31). *Main Challenges in Digital Healthcare Innovation*. LinkedIn. Available at: https://www.linkedin.com/pulse/main-challenges-digital-healthcare-innovation-jo%C3%A3o-bocas

[26] Bonuccelli, G. (2022, April 6). *All You Need to Know about Cloud Security Services.* Parallels. Available at: https://www.parallels.com/blogs/ras/cloud-security-services/

[27] Briscoe, G., & De Wilde, P. (2006). Digital Ecosystems: Evolving Service-Oriented Architectures. *Proceedings of 1st International Conference on Bio-Inspired models of Network, Information and Computing Systems (BIONETICS)*. 1-6. http://dx.doi.org/10.1109/BIMNICS.2006.361817

[28] Broadband Commission (2018). *The Promise of Digital Health: Addressing Non-communicable Diseases to Accelerate Universal Health Coverage in LMICs*. https://www.novartisfoundation.org/sites/arctic_novartisfoundation/files/2020-11/2018-the-promise-of-digital-health-full-report.pdf

[29] Bromberger, J., Ilg, J., & Miranda, A. M. (2022, March 15). *The mainstreaming of additive manufacturing*. McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/the-mainstreaming-of-additive-manufacturing

[30] Brush, K. (n.d). *Digital Ecosystem*. TechTarget. Available at: https://www.techtarget.com/searchcio/definition/digital-ecosystem

[31] Buchberger, C. (2021, Jul 15). *An Introduction to Industry 4.0*. EMnify. Available at: https://www.emnify.com/blog/industry-4-0

[32] Burke, T. (2018). The Essential Diversity of Blockchain Nodes. *IEEE Blockchain Initiative Briefs*. Available at: https://blockchain.ieee.org/technicalbriefs/december-2018/the-essential-diversity-of-blockchain-nodes

[33] BusinessWire (2020, April 21). *Outlook on the Worldwide Telemedicine Industry to 2027 - by Component, Delivery Model, Technology, Application, Type, End Use, Region and Segment Forecasts – ResearchAndMarkets.com*. Available at: https://www.businesswire.com/news/home/20200421005471/en/Outlook-on-the-Worldwide-Telemedicine-Industry-to-2027---by-Component-Delivery-Model-Technology-Application-Type-End-Use-Region-and-Segment-Forecasts---ResearchAndMarkets.com

[34] Bygstad, B., & Dulsrud, A. (2020). Digital Ecosystems as a Unit of Scientific Analysis. A Sociological Investigation. *Proceedings of the Annual Hawaii International Conference on System Sciences (HICSS)*. https://doi.org/10.24251/HICSS.2020.698

[35] Canada Health Infoway (2012, April). *Canada Health Infoway Benefits Evaluation Indicators - Techical Report, Version 2.0.* Toronto-Montreal-Halifax-Vancouver: Canada Health Infoway in collaboration with University of Victoria. Available at: https://www.infoway-inforoute.ca/en/component/edocman/450-benefits-evaluation-indicators-technical-report-version-2-0/view-document?Itemid=0

[36] Canorea, E. (2022, August 30). *How is Blockchain Improving Internet of Things?* Plain Concepts. Available at: https://www.plainconcepts.com/blockchain-iot/

[37] Cassetto, O. (2023, February 1). *Cybersecurity Threats: Everything you Need to Know.* Exabeam. Available at: https://www.exabeam.com/information-security/cyber-security-threat/

[38] Chanchaichujit, J., Tan, A., Meng, F., & Eaimkhong, S. (2019). Blockchain Technology in Healthcare. In *Healthcare 4.0* (pp. 37-62). Palgrave Pivot. https://doi.org/10.1007/978-981-13-8114-0_3

[39] Chao, C. M. (2019). Factors Determining the Behavioral Intention to Use Mobile Learning: An Application and Extension of the UTAUT Model. *Frontiers in Psychology, 10*, 1652. https://doi.org/10.3389/fpsyg.2019.01652

[40] Chatterjee, S. (2020, March 25). *Successful digital ecosystems depend on cloud services*. TechTarget. Available at: https://searchcio.techtarget.com/feature/Successful-digital-ecosystems-depend-on-cloud-services

[41] Chigrinetc, A. (2019, Jan 15). *C2B in Healthcare: Why the patient is now in charge*. Healthcare Business Leaders. Available at: https://www.healthcarebusinessleaders.com/post/c2b-in-healthcare-why-the-patient-is-now-in-charge

[42] Chin, J. P., Diehl, V. A., & Norman, K. L. (1988). Development of an instrument measuring user satisfaction of the human-computer interface. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 213-218. https://doi.org/10.1145/57167.57203

[43] Chukwu, E., & Garg, L. (2020). A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access, 8*, 21196-21214. https://doi.org/10.1109/ACCESS.2020.2969881

[44] CIS Consulting (n.d.). *Converting From Paper To Electronic Medical Records*. Available at: https://www.cisc-llc.com/blog/electronic-medical-record-implementation

[45] CISA (2019, Nov 14). *What is Cybersecurity?* Cybersecurity & Infrastructure Security Agency. Available at: https://www.cisa.gov/uscert/ncas/tips/ST04-001

[46] Clancy, R. (2022, Nov 25). *All You Need to Know About Network Security, Firewalls, and VPNs*. EC-Council University. Available at: https://www.eccu.edu/blog/cybersecurity/network-security-firewalls-vpns/

[47] Cointelegraph (n.d.). *What is Ethereum and how does it work?* Available at: https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum-a-beginners-guide-to-eth-cryptocurrency

[48] Collier, J. (2018, September 12). *mHealth: What is it, and how can it help us?* Medical News Today. Available at: https://www.medicalnewstoday.com/articles/322865

[49] Coté, M. (2020). *The Business Bottleneck*. O'Reilly Media Company.

[50] Cottrell, E., Whitlock, E., Kato, E., Uhl, S., Belinson, S., Chang, C., Hoomans, T., Meltzer, D., Noorani, H., Robinson, K., Schoelles, K., Motu'apuaka, M., Anderson, J., Paynter, R., & Guise, J. M. (2014). *Defining the Benefits of Stakeholder Engagement in Systematic Reviews*. Agency for Healthcare Research and Quality (US).

[51] Cowie, M. R., Bax, J., Bruining, N., Cleland, J. G., Koehler, F., Malik, M., Pinto, F., van der Velde, E., & Vardas, P. (2016). e-Health: a position statement of the European Society of Cardiology. *European Heart Journal*, *37*(1), 63–66. https://doi.org/10.1093/eurheartj/ehv416

[52] Credihealth (2023, January 31). *Digital Healthcare Ecosystem - The Beginning of New Healthcare Era*. Available at: https://www.credihealth.com/blog/digital-healthcare-ecosystem-the-beginning-of-new-healthcare-era

[53] Cryptopedia Staff (2022, March 30). *Algorand (ALGO): A Blockchain Breakthrough in Speed and Efficiency*. Cryptopedia. Available at: https://www.gemini.com/cryptopedia/what-is-algorand-cryptocurrency-blockchain

[54] Cybalt (n.d.). Industry 4.0 Cyber Security Challenges – How real it is? Cybalt Inc. https://www.cybalt.com/docs/default-source/white_papers/cybalt-white-paper---industry-4.0-cyber-security-challenges---how-real-it-is.pdf

[55] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society*, *39*, 283-297. https://doi.org/10.1016/j.scs.2018.02.014

[56] Daley, S., & Whitfield, B. (2022, September 01). *What is Blockchain?* Built In. Available at: https://builtin.com/blockchain

[57] Davenport, T. H., Hongsermeier, T. M., & Mc Cord, K. A. (2018, December 13). *Using AI to Improve Electronic Health Records*. Harvard Business Review. Available at: https://hbr.org/2018/12/using-ai-to-improve-electronic-health-records

[58] de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

[59] Deetjen, U., Biesdorf, S., Giuliani, G., & Oberhänsli, W. (2020). Unleashing the power of digital health through ecosystems. McKinsey & Company. https://www.mckinsey.com/ch/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Switzerland/Digital%20Health/McK-Whitepaper-Unleashing_the_power_of_digital_health_through_ecosystems.pdf

[60] Denoo, L., & Yli-Renko, H. (2019). Entrepreneurship in a New Digital Industry: The Emergence and Growth of Mobile Health. In R. Baierl, J. Behrens & A. Brem (Eds.), *Digital Entrepreneurship* (pp. 79-98). Springer International Publishing, https://doi.org/10.1007/978-3-030-20138-8_4

[61] Derecha, V. (n.d.) *Distributed Ledger Frameworks Comparison: Corda vs Hyperledger Fabric*. ELEKS. Available at: https://labs.eleks.com/2021/04/distributed-ledger-frameworks-comparison-corda-vs-hyperledger-fabric.html

[62] Dicianno, B. E., Parmanto, B., Fairman, A. D., Crytzer, T. M., Yu, D. X., Pramana, G., Coughenour, D., & Petrazzi, A. A. (2015). Perspectives on the evolution of mobile (mHealth) technologies and application to rehabilitation. *Physical therapy*, *95*(3), 397–405. https://doi.org/10.2522/ptj.20130534

[63] Domnisch, N. (2022, Apr 25). *Digital Healthcare Ecosystems Are Changing Healthcare As We Know It*. Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2022/04/25/digital-healthcare-ecosystems-are-changing-healthcare-as-we-know-it

[64] E-commercetoolbox (n.d.). *e-Commerce transaction models (x2x)*. Available at: https://e-commercetoolbox.webnode.be/a1-introduction-to-e-commerce/e-business-models/a4-e-commerce-models/

[65] Elgendy, N., & Elragal, A. (2014). Big Data Analytics: A Literature Review Paper. In P. Perner (Eds.), *Advances in Data Mining. Applications and Theoretical Aspects*. *ICDM*

2014, Lecture Notes in Computer Science (vol. 8557, pp. 214-227). Springer, Cham. https://doi.org/10.1007/978-3-319-08976-8_16

[66] El-Masri, M., & Tarhini, A. (2017). Factors affecting the adoption of elearning systems in Qatar and USA: Extending the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2). *Educational Technology Research and Development*, *65*(3), 743-763. https://doi.org/10.1007/s11423-016-9508-8

[67] ESA Automation (2020, Jul 02). Additive Manufacturing in Industry 4.0. Available at: https://www.esa-automation.com/en/additive-manufacturing-in-industry-4-0/

[68] European Parliament (2015). *eHealth – Technology for health*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/551324/EPRS_BRI(2015)551324_EN.pdf

[69] Evans, B. J. (2017). Power to the People: Data Citizens in the Age of Precision Medicine. *Vanderbilt journal of entertainment and technology law*, *19*(2), 243–265. Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol19/iss2/2

[70] eVisit (2018, January 23). *The State of Telemedicine 2018*. Available at: https://evisit.com/the-state-of-telemedicine-2018

[71] Eysenbach, G. (2000). Consumer health informatics. *BMJ: British Medical Journal*, *320*(7251), 1713-1716. https://www.bmj.com/content/320/7251/1713

[72] Eysenbach, G. (2001). What is e-health? *Journal of Medical Internet Research*, *3*(2), e20. https://doi.org/10.2196/jmir.3.2.e20

[73] Featherman, M. S., & Pavlou, P. A. (2003). Predicting E-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474. http://dx.doi.org/10.1016/S1071-5819(03)00111-3

[74] Ferreira, P. L., Tavares, A. I., Quintal, C., & Santana, P. (2018). EU health systems classification: a new proposal from EURO-HEALTHY. *BMC Health Services Research*, *18*(1), 511. https://doi.org/10.1186/s12913-018-3323-3

[75] Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., Castillo, A. P., Ducom, J. C., Topol, E. J., & Steinhubl, S. R. (2016). Privacy and security in the era of digital health: what should translational researchers know and do about it? *American Journal of Translational Research*, *8*(3), 1560–1580. www.ajtr.org /ISSN:1943-8141/AJTR0020863

[76] Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382-388. http://dx.doi.org/10.2307/3150980

[77] Frankenfield, J. (2022, September 30). *Cloud Security: Definition, How Cloud Computing Works, and Safety*. Investopedia. Available at: https://www.investopedia.com/terms/c/cloud-security.asp

[78] Frankenfield, J. (2023, May 31) *What Does Proof-of-Stake (PoS) Mean in Crypto?* Investopedia. Available at: https://www.investopedia.com/terms/p/proof-stake-pos.asp

[79] Fürstenau, D., Auschra, C., Klein, S., & Gersch, M. (2019). A process perspective on platform design and management: evidence from a digital platform in health care. *Electronic Markets*, *29*(4), 581-596. https://doi.org/10.1007/s12525-018-0323-4

[80] Gaggioli, A. (2018). Blockchain Technology: Living in a Decentralized Everything. *Cyberpsychology, Behavior, and Social Networking*, *21*(1), 65-66. https://doi.org/10.1089/cyber.2017.29097.csi

[81] Garg, I. (2020, February 26). *How the Global Development Community will Shape the Future of Blockchain in Health Care*. Blockmanity. Available at: https://blockmanity.com/news/feature/how-the-global-development-community-will-shape-the-future-of-blockchain-in-health-care/

[82] Geroni, D. (2021, January 27). *Top 5 Benefits of Blockchain Technology*. 101 Blockchains. Available at: https://101blockchains.com/benefits-of-blockchain-technology

[83] Ghiro, L., Restuccia, F., D'oro, S., Basagni, S., Melodia, T., Maccari, L., & Cigno, R. L. (2021). What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things. *ArXiv*. https://doi.org/10.48550/arXiv.2102.03750

[84] Giansanti, D. (2021). Cybersecurity and the Digital-Health: The Challenge of This Millennium. *Healthcare*, *9*(1), 62. https://doi.org/10.3390/healthcare9010062

[85] Giansanti, D., & Monoscalco, L. (2021). The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists. *mHealth*, *7*(28). https://doi.org/10.21037/mhealth.2020.01.08

[86] Gilchrist, A. (2016). *Industry 4.0: The Industrial Internet of Things.* Apress. https://doi.org/10.1007/978-1-4842-2047-4

[87] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal, 16*, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

[88] Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. *Frontiers in Blockchain*, *4*, 616779:1-616779:11. http://dx.doi.org/10.3389/fbloc.2021.616779

[89] Görlitz, R. (2014). *Patient-centered Coordination in Healthcare Service Networks* (Doctoral dissertation). Karlsruhe Institute of Technology.

[90] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

[91] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences-A scoping review. *International journal of medical informatics*, *134*, 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040

[92] Healthcare Improvement Scotland (2017). *Evaluating new models of care: A guide for integrated care providers*. Available at: https://ihub.scot/media/1267/20170815-evaluation-guide-draft-v1.pdf

[93] HealthIT (2021). *Electronic Health Information Exchange by Office-based Physicians*. Available at: https://www.healthit.gov/data/quickstats/electronic-health-information-exchange-office-based-physicians

[94] Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2019). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87-98. https://doi.org/10.1007/s12525-019-00377-4

[95] Holmes, R. (2022, Sept 07). *Cybersecurity vs. Information Security: Is There A Difference?* Bitsight. Available at: https://www.bitsight.com/blog/cybersecurity-vs-information-security

[96] Iberdrola (n.d.). *eHealth, when technology becomes the key to social well-being*. Available at: https://www.iberdrola.com/innovation/ehealth

[97] Ibrahim, A., Kadir, T. A. A., & Kamaludin, A. (2020). Industry 4.0: Eyeing The Future via Simulation. *IOP Conference Series: Materials Science and Engineering*, *769*(1), 012001. https://doi.org/10.1088/1757-899X/769/1/012001

[98] Integrated Health Systems: Definition & Types (2021, May 6). Available at: https://study.com/academy/lesson/integrated-health-systems-definition-types.html

[99] Isakovic, M., Cijan, J., Sedlar, U., Volk, M., & Bester, J. (2015). The Role of mHealth Applications in Societal and Social Challenges of the Future. *12th International Conference on Information Technology – New Generations*, 561-566. https://dx.doi.org/10.1109/ITNG.2015.94

[100] iSPIRT (2020, Jul 4). *Health Information Flows (HIFs) – Technology Specifications*. Available at: https://ispirt.in/depa-hif/

[101] Istepanian, R. S., & Lacal, J. C. (2003). Emerging Mobile Communication Technologies for Health: Some Imperative Notes on m-health. *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, *2*, 1414-1416. https://doi.org/10.1109/IEMBS.2003.1279581

[102] Javaid, M., Haleem, A., Singh, R.P., & Suman, R. (2021). Artificial Intelligence Applications for Industry 4.0: A Literature-Based Study. *Journal of Industrial Integration and Management*, *7*(1), 83-111. https://dx.doi.org/10.1142/S2424862221300040

[103] Jeon, H. M., Sung, H. J., & Kim, H. Y. (2020). Customers' acceptance intention of self-service technology of restaurant industry: expanding UTAUT with perceived risk and innovativeness. *Service Business*, *14*(4), 533–551. https://doi.org/10.1007/s11628-020-00425-6

[104] Jovanović, S., Milovanović, S., Mandić, J. & Jovović, S. (2015). Health care systems. *Engrami*, *37*(1), 75-82. https://dx.doi.org/10.5937/engrami1501075J

[105] Kaur, A. (2021, Sep 27). *Digital Transformation in Healthcare: Trends, Challenges & Solutions*. Net Solutions. Available at: https://www.netsolutions.com/insights/digital-transformation-in-healthcare/

[106] KBK Communications (Feb 5, 2020). *The 5 Advantages of eCommerce in Healthcare*. Available at: https://www.kbkcommunications.com/blog/the-5-advantages-of-ecommerce-in-healthcare

[107] Kelley, K. (2023, Jan 30). *What is Cybersecurity and Why It is Important?* Simplilearn. Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

[108] Kettunen, E., Kemppainen, T., Lievonen, M., Makkonen, M., Frank, L., & Kari, T. (2018). Ideal Types of Online Shoppers: A Qualitative Analysis of Online Shopping Behavior. In P. Kourouthanassis, P. Markopoulos, A. Pateli, N. Pouloudi, A. Pucihar, & J. V. D. Cunha (Eds.), *MCIS 2018: 12th Mediterranean Conference on Information Systems* (pp. 1-16). MCIS. https://aisel.aisnet.org/mcis2018/30

[109] Khan, M. I., Saleh, M. A., & Quazi, A. (2021). Social Media Adoption by Health Professionals: A TAM-Based Study. *Informatics*, *8*(1), 6. https://doi.org/10.3390/informatics8010006

[110] Khanna, R., & Yen, T. (2014). Computerized Physician Order Entry: Promise, Perils, and Experience. *The Neurohospitalist*, *4*(1), 26–33. https://doi.org/10.1177/1941874413495701

[111] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, *9*(9), 1736. http://dx.doi.org/10.3390/app9091736

[112] Kissi, J., Dai, B., Owusu-Marfo, J., Asare, I., Opuni, M., & Clemency, B. (2018). A Review of Information Security Policies and Procedures for Healthcare Services. *Canadian Journal of Applied Science and Technology*, *6*(2), 812-819.

[113] Kneck, Å., Flink, M., Frykholm, O., Kirsebom, M., & Ekstedt, M. (2019). The Information Flow in a Healthcare Organisation with Integrated Units. *International journal of integrated care*, *19*(3), 20. https://doi.org/10.5334/ijic.4192

[114] Koch, M., Krohmer, D., Naab, M, Rost, D., & Trapp, M. (2022). A matter of definition: Criteria for digital ecosystems. *Digital Business*, *2*(2), 100027. https://doi.org/10.1016/j.digbus.2022.100027

[115] Koeppe, D. (2020). Towards Guidelines for Medical Professionals to Ensure Cybersecurity in Digital Health Care. In M. Christen, B. Gordijn & Loi, M. (Eds.) *The Ethics of Cybersecurity* (pp. 331-345). Springer Cham. https://doi.org/10.1007/978-3-030-29053-5

[116] Kozarkiewicz, A. (2020). General and Specific: The Impact of Digital Transformation on Project Processes and Management Methods. *Foundations of Management*, *12*(1), 237-248. https://doi.org/10.2478/fman-2020-0018

[117] Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. *SAGE Open*, *11*(3). http://dx.doi.org/10.1177/21582440211047576

[118] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48. https://doi.org/10.1016/j.cosrev.2019.05.002

[119] Landi, H. (2022, Feb 1). *Healthcare data breaches hit all-time high in 2021, impacting 45M people*. Health Tech. Available at: https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

[120] Laoyan, S. (2022, Oct 24). *6 ways digital transformation can improve your business*. Asana. Available at: https://asana.com/resources/what-is-digital-transformation

[121] Lee, J.-H., Kim, S. W., & Song, C. H. (2010). The Effects of Trust and Perceived Risk on Users' Acceptance of ICT Services. KAIST College of Business Working Paper Series No. 2010-007. http://dx.doi.org/10.2139/ssrn.1703213

[122] Lee, S. M., Lee, D., & Schniederjans, M. J. (2011). Supply chain innovation and organizational performance in the healthcare industry. *International Journal of Operations & Production Management, 31*(11), 1193-1214. http://dx.doi.org/10.1108/01443571111178493

[123] Lennon, M. R., Bouamrane, M. M., Devlin, A. M., O'Connor, S., O'Donnell, C., Chetty, U., Agbakoba, R., Bikker, A., Grieve, E., Finch, T., Watson, N., Wyke, S., & Mair, F. S. (2017). Readiness for Delivering Digital Health at Scale: Lessons From a Longitudinal Qualitative Evaluation of a National Digital Health Innovation Program in the United Kingdom. *Journal of medical Internet research*, *19*(2), e42. https://doi.org/10.2196/jmir.6900

[124] Levi, S. D., & Lipton, A. B. (2018, May 26). *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*. Harvard Law School Forum on Corporate Governance. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations

[125] Li, W., Badr, Y., & Biennier, F. (2012). Digital ecosystems: Challenges and prospects. *Proceedings of the International Conference on Management of Emergent Digital EcoSystems*, 117-122. https://doi.org/10.1145/2457276.2457297

[126] Ludwick, D. A., & Doucette, J. (2009). Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. *International journal of medical informatics*, *78*(1), 22–31. https://doi.org/10.1016/j.ijmedinf.2008.06.005

[127] Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics, 35*(8), 2337-2354. https://doi.org/10.1016/j.tele.2018.10.004

[128] Manteghinejad, A., & Javanmard, S. H. (2021). Challenges and opportunities of digital health in a post-COVID19 world. *Journal of Research in Medical Sciences*, *26*(11). https://doi.org/10.4103/jrms.jrms_1255_20

[129] Manu, M. R., Musthafa, N., Balamurugan, B., & Chauhan, R. (2020). Blockchain Components and Concept. In P. Raj, K. Saini, & C. Surianarayanan (Eds.), *Blockchain Technology and Applications (1st Edition)* (pp. 21-49). Auerbach Publications. https://doi.org/10.1201/9781003081487

[130] Marcos-Pablos, S., García-Holgado, A., & García-Peñalvo, F. J. (2019). Modelling the business structure of a digital health ecosystem. In M. Á. Conde-González, F. J. Rodríguez-Sedano, C. Fernández-Llamas, & F. J. García-Peñalvo (Eds.), *TEEM'19 Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality*, 838-845. ACM Association for Computing Machinery. https://doi.org/10.1145/3362789.3362949

[131] Marini, M. G. (2019). *Languages of Care in Narrative Medicine. Words, Space and Time in the Healthcare Ecosystem*. Springer Cham. https://doi.org/10.1007/978-3-319-94727-3

[132] Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk management and healthcare policy*, *4*, 47–55. https://doi.org/10.2147/RMHP.S12985

[133] Meyers, T., & Tone, J. (2022, October 27). *Prioritizing Cybersecurity to Enable Better Health Outcomes.* G2xchange Health. Available at: https://health.g2xchange.com/prioritizing-cybersecurity-to-enable-better-health-outcomes/

[134] Moro-Visconti, R. (2021, October 23). The Valuation of e-Health and Telemedicine Startups. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4132488

[135] Muktamarisa, S., & Afiff, A. Z. (2022). Customers' acceptance intention of self-service technology in casual dining restaurant: Expanding UTAUT with perceived risk and perceived vulnerability. *Proceedings of the 6th International Conference on Family Business and Entrepreneurship, 3*(1), 392-401. http://dx.doi.org/10.33021/icfbe.v3i1.3802

[136] Mummadi, S. R., & Mishra, R. (2018). Effectiveness of provider price display in computerized physician order entry (CPOE) on healthcare quality: a systematic review. *Journal of the American Medical Informatics Association: JAMIA*, *25*(9), 1228–1239. https://doi.org/10.1093/jamia/ocy076

[137] Murphy, W. H., & Wilson, G. A. (2022). Dynamic capabilities and stakeholder theory explanation of superior performance among award-winning hospitals. *International Journal of Healthcare Management*, *15*(3), 211-219. https://doi.org/10.1080/20479700.2020.1870356

[138] Musharraf, M. (2022, October 25). *What is the Blockchain Trilemma?* Ledger Academy. Available at: https://www.ledger.com/academy/what-is-the-blockchain-trilemma

[139] Newton, D. (2018, June 05). *What is Corda?* Corda.net. Available at: https://corda.net/blog/what-is-corda

[140] Nguyen, A. (2022, June 10). *What is Layer 0, Layer 1, Layer 2, Layer 3?* CoinCu. Available at: https://news.coincu.com/97393-what-is-layer-0-layer-1-layer-2-layer-3

[141] Nicolai, B., Tallarico, S., Pellegrini, L., Gastaldi, L., Vella, G., & Lazzini, S. (2022). Blockchain for electronic medical record: assessing stakeholders' readiness for successful blockchain adoption in health-care. *Measuring Business Excellence*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/MBE-12-2021-0155

[142] Nilsen, P., Seing, I., Ericsson, C., Birken, S. A., & Schildmeijer, K. (2020). Characteristics of successful changes in health care organizations: an interview study with physicians, registered nurses and assistant nurses. *BMC Health Services Research*, *20*(1), 147. https://doi.org/10.1186/s12913-020-4999-8

[143] Nivarthi, C., & Akhilesh, K. (2020). Cybercare – Role of Cyber Security in Healthcare Industry. In K. Akhilesh & D. Möller (Eds.), *Smart Technologies* (pp. 291-304). Springer. http://dx.doi.org/10.1007/978-981-13-7139-4_22

[144] Nowak, M. (2021, July 28). *Internal & External Stakeholders in a Health Care Sector*. Linkedin. Available at: https://www.linkedin.com/pulse/internal-external-stakeholders-health-care-sector-monika-nowak

[145] O'Brien, C. (2022, Jun 07). *What is Digital Transformation? A Guide for Businesses.* Digital Marketing Institute. Available at: https://digitalmarketinginstitute.com/blog/digital-transformation-business-guide

[146] O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. M. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, *113*, 653-658. https://doi.org/10.1016/j.procs.2017.08.329

[147] Obradović, M. (2009). Modeli e-health komunikacije u zdravstvenom sistemu. *Infoteh-Jahorina*, *8*, E-VI-4, 747-750.

[148] Olden, P. (2019). *Management of Healthcare Organizations: An Introduction, Third Edition*. Health Administration Press.

[149] 101 Blockchains (2021, February 16). *The Ultimate Corda Tutorial 2022*. Available at: https://101blockchains.com/corda-tutorial

[150] Ozturan, M., Atasu, I., & Soydan, H. (2019). Assessment of Blockchain Technology Readiness Level of Banking Industry: Case of Turkey. *International Journal of Business Marketing and Management*, *4*(12), pp. 1-13. http://www.ijbmm.com/paper/Dec2019/2115167856.pdf

[151] Pandey, K. (2022, September 19). *What Are the Different Layers of Blockchain Technology?* Jumpstart. Available at: https://www.jumpstartmag.com/what-are-the-different-layers-of-blockchain-technology

[152] Papanicolas, I., Kringos, D., Klazinga, N. S., & Smith, P. C. (2013). Health system performance comparison: new directions in research and policy. *Health policy*, *112*(1-2), 1–3. https://doi.org/10.1016/j.healthpol.2013.07.018

[153] Park, Y. T. (2016). Emerging New Era of Mobile Health Technologies. *Healthcare informatics research*, *22*(4), 253–254. https://doi.org/10.4258/hir.2016.22.4.253

[154] Paul, P., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). Blockchain Technology and Its Types – A Short Review. *International Journal of Applied Science and Engineering (IJASE)*, *9*(2), 189-200. https://ssrn.com/abstract=4050933

[155] Paul, S., Riffat, M., Yasir, A., Mahim, M. N., Sharnali, B. Y., Naheen, I. T., Rahman, A., & Kulkarni, A. (2021). Industry 4.0 Applications for Medical/Healthcare Services. *Journal of Sensor and Actuator Networks*. *10*(3), 43. https://doi.org/10.3390/jsan10030043

[156] Porterfield, A., Engelbert, K., & Coustasse, A. (2014). Electronic Prescribing: Improving the Efficiency and Accuracy of Prescribing in the Ambulatory Care Setting. *Perspectives in Health Information Management*, *11*(Spring), 1g.

[157] Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37–43. https://doi.org/10.1038/s41591-018-0272-7

[158] Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., & Labus, A. (2015). *Elektronsko poslovanje.* Beograd: Fakultet organizacionih nauka

[159] Refat, K. (2022, October 25). *8 Applications of blockchain technology in business*. BlogAcademy. Available at: https://www.blogacademy.tech/en/applications-blockchain-technology/

[160] Reiff, N. (2022, October 15). Algorand (ALGO). Investopedia. Available at: https://www.investopedia.com/algorand-algo-definition-5217725

[161] Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing*, *16*(1), 69-73. https://doi.org/10.1109/MIC.2012.14

[162] Rennock, M. J. W., Cohn, A., & Butcher, J. R. (2018, February/March). *Blockchain Technology and Regulatory Investigations*. Thomson Reuters. https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf

[163] Ribeiro, J. (2021, Feb 2). *A (very) Brief Introduction to AI in the Industry 4.0*. Medium. Available at: https://medium.com/tech-cult-heartbeat/a-very-brief-introduction-to-ai-in-the-industry-4-0-14e6f4b46cd1

[164] Riggi, J. (n.d.). *The importance of cybersecurity in protecting patient safety*. AHA Center for Health Innovation. Available at: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

[165] Rockwern, B., Johnson, D., Snyder Sulmasy, L., & Medical Informatics Committee and Ethics, Professionalism and Human Rights Committee of the American College of Physicians (2021). Health Information Privacy, Protection, and Use in the Expanding Digital Health Ecosystem: A Position Paper of the American College of Physicians. *Annals of internal medicine*, *174*(7), 994–998. https://doi.org/10.7326/M20-7639

[166] Rodić Trmčić, B. (2018). *Razvoj modela mobilnog zdravstva zasnovanog na wearable computing-u* (doktorska disertacija). Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, Srbija.

[167] Rodrigues, J. J. P. C., Compte, S. S., & de la Torra-Diez, I. (2016). *e-Health Systems*. Elsevier. https://doi.org/10.1016/B978-1-78548-091-1.50013-0

[168] Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics*, *71*, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012

[169] Roland Berger Strategy Consultants (2015). *The digital transformation of industry*. BDI. https://www.rolandberger.com/publications/publication_pdf/roland_berger_digital_transformation_of_industry_20150315.pdf

[170] Ruotsalainen, P., & Blobel, B. (2019). Digital pHealth - Problems and Solutions for Ethics, Trust and Privacy. *Studies in health technology and informatics*, *261*, 31–46. https://doi.org/10.3233/978-1-61499-975-1-31

[171] Ruotsalainen, P., & Blobel, B. (2022). Transformed Health Ecosystems-Challenges for Security, Privacy, and Trust. *Frontiers in medicine*, *9*, 827253. https://doi.org/10.3389/fmed.2022.827253

[172] Sanchini, V., & Marelli, L. (2020). Data Protection and Ethical Issues in European P5 eHealth. In: G. Pravettoni & S. Triberti (Eds.) *P5 eHealth: An Agenda for the Health*

Technologies of the Future (pp. 173-189). Springer, Cham. https://doi.org/10.1007/978-3-030-27994-3_10

[173] Sanghyun, P., & Kyungho, L. (2014). Advanced Approach to Information Security Management System Model for Industrial Control System. *The Scientific World Journal*, *vol. 2014*, Article ID 348305. https://doi.org/10.1155/2014/348305

[174] Sarwal, R., Prasad, U. R., Gopal, K. M., Kalal, S., Kaur, D., Kumar, A., Regy, P. V., & Sharma, J. (2021). *Investment Opportunities in India's Healthcare Sector*. NITI Aayog. https://doi.org/10.31219/osf.io/rtup2

[175] Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. *12*(2), 53-74. https://doi.org/10.15394/jdfsl.2017.1476

[176] Schwertner, K. (2021). The Impact of Digital Transformation on Business: A Detailed Review. In J. Metselaar (Ed.), *Strategic Management in the Age of Digital Transformation* (pp. 1-29). Proud Pen. https://doi.org/10.51432/978-1-8381524-3-7_1

[177] Schwab, K., (2016, Jan 14). *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[178] Scott, R. E., & Mars, M. (2013). Principles and Framework for eHealth Strategy Development. *Journal of Medical Internet Research*, *15*(7), e155. https://doi.org/10.2196%2Fjmir.2250

[179] Serbanati, L. D., Ricci, F. L., Mercurio, G, & Vasilateanu, A. (2011). Steps towards a digital health ecosystem. *Journal of Biomedical Informatics*, *44*(4), 621-636. https://doi.org/10.1016/j.jbi.2011.02.011

[180] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, *7*, 147782-147795. https://doi.org/10.1109/ACCESS.2019.294637

[181] Sharma, S. (2021). Co-creational leadership capability for driving health-care service innovation. *Measuring Business Excellence*, *25*(4), 434-451. https://doi.org/10.1108/MBE-11-2019-0117

[182] Shred-it (2022, January 28). *Cybercrime Attacks: 9 Effective Ways to Stop It.* Stericycle, Inc. Available at: https://www.shredit.sg/en-sg/blog/cybersecurity/nine-ways-to-stop-cyber-attacks

[183] Simplilearn (2022, Nov 11). *Cyber Security vs. Information Security: The Supreme Guide to Cyber Protection Policies*. Available at: https://www.simplilearn.com/information-security-vs-cyber-security-article

[184] Sinhasane, S. (2020, October 12). *Digital Healthcare Ecosystem: The New Era of Medical Care*. Mobisoft Discover Mobility. Available at: https://mobisoftinfotech.com/resources/blog/digital-healthcare-ecosystem-the-new-era-of-medical-care/

[185] Smith, C. (2022). *Proof-of-stake (PoS)*. Ethereum.org. Available at: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[186] Smith, J. (2018, Aug 21). *What is IIoT (Industrial IoT)?* dotCMS. Available at: https://www.dotcms.com/blog/post/what-is-iiot-industrial-iot-

[187] Spiewak, M. (2022, July 26). *Choose a perfect blockchain platform – the must-know blockchain platform list*. Crustlab. Available at: https://crustlab.com/blog/choose-perfect-blockchain-platform-must-know-blockchain-platforms-list/

[188] Steinhubl, S. R., Muse, E. D., & Topol, E. J. (2015). The emerging field of mobile health. *Science Translational Medicine, 7*(283). https://doi.org/10.1126%2Fscitranslmed.aaa3487

[189] Sulmasy, L. S., López, A. M., Horwitch, C. A., & American College of Physicians Ethics, Professionalism and Human Rights Committee (2017). Ethical Implications of the Electronic Health Record: In the Service of the Patient. *Journal of general internal medicine*, *32*(8), 935–939. https://doi.org/10.1007/s11606-017-4030-1

[190] Tabim, V. M., Ayala, N. F., & Frank, A. G. (2021). Implementing Vertical Integration in the Industry 4.0 Journey: Which Factors Influence the Process of Information Systems Adoption?. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10220-x

[191] Tagarev, T., Sharkov, G., & Stoianov, N. (2017). Cyber Security and Resilience of Modern Societies: A Research Management Architecture. *Information & Security: An International Journal*, *38*, 93-108. https://doi.org/10.11610/isij.3807

[192] Takyar, A. (n.d.). *Blockchain use cases*. LeewayHertz. Available at: https://www.leewayhertz.com/blockchain-use-cases

[193] Taylor, H. (2023, April 23). What Are Cyber Threats and How to Safeguard Your Data. Prey Project. Available at: https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them

[194] TIGA Healthcare Technologies (n.d.). *What Is Digital Healthcare Ecosystem?* Available at: https://www.tigahealth.com/what-is-digital-healthcare-ecosystem

[195] Tokkozhina, U., Lucia Martins, A., & Ferreira, J. C. (2022). Uncovering dimensions of the impact of blockchain technology in supply chain management. *Operations Management Research*, 1–27. https://doi.org/10.1007/s12063-022-00273-9

[196] Tsaramirsis, G., Kantaros, A., Al-Darraji, I., Piromalis, D., Apostolopoulos, C., Pavlopoulou, A., Alrammal, M., Ismail, Z., Buhari, S. M., Stojmenovic, M., Tamimi, H., Randhawa, P., Patel, A., & Alrammal, M. (2022). A Modern Approach towards an Industry 4.0 Model: From Driving Technologies to Management. *Journal of Sensors*, *2022*, 5023011. https://doi.org/10.1155/2022/5023011

[197] Tulchinsky, T. H., & Varavikova, E. A. (2015). *The New Public Health* (3rd ed.). Academic Press. https://doi.org/10.1016/C2010-0-68514-2

[198] Uddin, M., Memon, M. S., Memon, I., Halepoto, I. A., Memon, J., Abdelhaq, M. & Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. *Computers, Materials and Continua*. *68*(2). 2377-2397. http://dx.doi.org/10.32604/cmc.2021.015354

[199] Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A Glimpse. *Procedia Manufacturing*, *20*, 233–238. https://doi.org/10.1016/j.promfg.2018.02.034

[200] Valdez-de-Leon, O. (2019). How to Develop a Digital Ecosystem: a Practical Framework. *Technology Innovation Management Review*, *9*(8), 43-54. http://doi.org/10.22215/timreview/1260

[201] Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1533

[202] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

[203] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

[204] Waldman, A. E. (2018). Privacy as Trust: Information Privacy for an Information Age. Cambridge University Press.

[205] Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *International Journal of Information Management*, *50*, 387-394. https://doi.org/10.1016/j.ijinfomgt.2019.09.002

[206] Wanitcharakkhakul, L., & Rotchanakitumnuai, S. (2017). Blockchain Technology Acceptance in Electronic Medical Record System. *Proceedings of International Conference on Electronic Business*. https://aisel.aisnet.org/iceb2017/7

[207] Weallans, S. (2018, Sep 4). *IIoT And Industry 4.0: The Basics You Need to Know*. Fierce Electronics. Available at: https://www.fierceelectronics.com/components/iiot-and-industry-4-0-basics-you-need-to-know

[208] Wegrzyn, K. E., & Wang, E. (2021, August 19). *Types of Blockchain: Public, Private, or Something in Between*. Foley. Available at: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

[209] White, G. B., Fisch, E. A., & Pooch, U. W. (2017). *Computer system and network security*. CRC press.

[210] Witte, A. K. (2020). A Review on Digital Healthcare Ecosystem Structure: Identifying Elements and Characteristics. *Proceedings of Pacific Asia Conference on Information Systems*, *228*. Available at: https://aisel.aisnet.org/pacis2020/228

[211] World Health Organization (2000). The World Health Report 2000 – Health Systems: Improving Performance. World Health Organization. https://apps.who.int/iris/handle/10665/42281

[212] World Health Organization and International Telecommunication Union (2012). *National eHealth Strategy Toolkit.* World Health Organization and International Telecommunication Union. https://apps.who.int/iris/handle/10665/75211

[213] World Health Organization (2018). Continuity and coordination of care: A practice brief to support implementation of the WHO Framework on integrated people-centred health services. World Health Organization. https://apps.who.int/iris/handle/10665/274628

[214] World Health Organization (2019). WHO Guideline: recommendations on digital interventions for health system strengthening. World Health Organization. https://apps.who.int/iris/handle/10665/311980

[215] [x]cube LABS (2022, Jan 28). *How Blockchain will benefit the Healthcare Industry in 2022 and Beyond*. Available at: https://www.xcubelabs.com/blog/how-blockchain-will-benefit-the-healthcare-industry-in-2022-and-beyond/

[216] Yoon, H. J. (2019). Blockchain Technology and Healthcare. *Healthcare informatics research*, *25*(2), 59–60. https://doi.org/10.4258/hir.2019.25.2.59

[217] Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. *Nature biomedical engineering*, *2*(10), 719–731. https://doi.org/10.1038/s41551-018-0305-z

[218] Zangiacomi, A., Pessot, E., Fornasiero, R., Bertetti, M., & Sacco, M. (2020). Moving towards digitalization: a multiple case study in manufacturing. *Production Planning & Control*, *31*(2-3), 143-157. https://doi.org/10.1080/09537287.2019.1631468

[219] Zeithaml, V. A., Bitner, M. J., & Gremler, D. D. (2006). *Services marketing: integrating customer focus across the firm* (4th ed.). McGraw-Hill Irwin.

[220] Zhao, J., Feng, Q., Wu, P., Lupu, R. A., Wilke, R. A., Wells, Q. S., Denny, J. C., & Wei, W. Q. (2019). Learning from Longitudinal Data in Electronic Health Record and Genetic Data to Improve Cardiovascular Event Prediction. *Scientific Reports*, *9*(1), 717. https://doi.org/10.1038/s41598-018-36745-x

[221] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., & Imran, M. A. (2020). An Overview on Smart Contracts: Challenges, Advances and Platforms. *Future Generation Computer Systems*, *105*, 475-491. https://doi.org/10.1016/j.future.2019.12.019

[222] Zonneveld, N., Driessen, N., Stüssgen, R. A. J., & Minkman, M. M. N. (2018). Values of Integrated Care: A Systematic Review. *International Journal of Integrated Care*, *18*(4), 9. https://doi.org/10.5334/ijic.4172

СПИСАК СЛИКА

СПИСАК ГРАФИКОНА

СПИСАК ТАБЕЛА

БИОГРАФИЈА

Даниел Бјелица рођен је 04.09.1978. године у Новом Саду, где је завршио основну школу и гимназију општег смера. Вишу пословну школу у Новом Саду, смер Информациони системи, завршио је 2003. године. На интегрисаним студијама из области Индустријског инжењерства и менаџмента, модул Информационо-управљачки и комуникациони системи, дипломирао је 2006. године на Факултету техничких наука Универзитета у Новом Саду. На истом факултету је 2019. године завршио и мастер студије на смеру Инжењерство информационих система. Докторске студије на Факултету организационих наука Универзитета у Београду уписује 2020. године, на студијском програму Информациони системи и квантитативни менаџмент, модул Електронско пословање.

Од 1997. до 2000. године радио је на Природно-математичком факултету у Новом Саду, Департман за математику и информатику, као систем администратор рачунског центра, задужен за одржавање примарног доменског контролера, као и имејл, *FTP* и веб сервера Департмана.

Од 2001. до 2002. године радио је у *Scenic Pro* д.о.о. Нови Сад, као руководилац одељења сервиса и техничке подршке за *brandname* рачунаре и опрему.

Од 2003. до 2010. године радио је у *BNL Systems* д.о.о. Нови Сад, као администратор рачунарских мрежа, укључен у пројектовање мрежних модела и конфигурисање и одржавање активне мрежне опреме.

Од 2013. године запослен је у Центру за радиологију Клиничког центра Војводине, као ИТ инжењер задужен за одржавање *RIS* и *PACS* радиолошких информационих система. Учествује у бројним радиолошким истраживачким пројектима као стручни сарадник из ИТ области.

ИЗЈАВА О АУТОРСТВУ

Име и презиме аутора: Даниел Бјелица

Број индекса: 5024/2020

Изјављујем

да је докторска дисертација под насловом:

„Модел дигиталног здравственог екосистема заснован на *blockchain* технологији”

- 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 ауторска права и користио интелектуалну својину других лица.

У Београду, 11.09.2023. **Потпис аутора**

_____

ИЗЈАВА О ИСТОВЕТНОСТИ ШТАМПАНЕ И ЕЛЕКТРОНСКЕ ВЕРЗИЈЕ ДОКТОРСКОГ РАДА

Име и презиме аутора:	Даниел Бјелица
Број индекса:	5024/2020
Студијски програм:	Информациони системи и квантитативни менаџмент
Наслов рада:	**Модел дигиталног здравственог екосистема заснован на *blockchain* технологији**
Ментор:	Проф. др Александра Лабус

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао ради похрањења 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.

У Београду, 11.09.2023. **Потпис аутора**

_____

ИЗЈАВА О КОРИШЋЕЊУ

Овлашћујем Универзитетску библиотеку "Светозар Марковић" да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Модел дигиталног здравственог екосистема заснован на *blockchain* технологији

која је моје ауторско дело.

Дисертацију са свим прилозима предао 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.

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)

У Београду, 11.09.2023. **Потпис аутора**

_____