Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/23BE11Maksimovic

РАЗВОЈ ДЕЦЕНТРАЛИЗОВАНОГ ИНФОРМАЦИОНОГ СИСТЕМА ЗА УПРАВЉАЊЕ ТРАНСАКЦИЈАМА НЕЗАМЕЊИВИХ ТОКЕНА

DEVELOPMENT OF A DECENTRALIZED INFORMATION SYSTEM FOR THE NFT TRANSACTION MANAGEMENT

Владислав Максимовић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду описан је информациони систем који омогућава размену дигиталних средстава у виду незамењивих токена. Као платформа за подршку овој апликацији је изабрана Ethereum блокчејн платформа. Приказано решење користи блокчејн као део свог система како би омогућио децентрализовану размену дигиталних средстава. У раду су ради бољег разумевања самог проблема и његовог решења приказани основи децентрализације, блокчејна као и основи технологија коришћених за израду информационог система.*

Кључне речи: *Базе података, дистрибуирани информациони системи, блокчејн, незамењиви токени*

Abstract – *This thesis describes an information system which implements the exchange of digital assets in the form of NFTs. The Ethereum blockchain has been chosen as the platform to support this application. The presented solution uses blockchain as part of its system to enable the decentralized exchange of digital assets. In order to better understand the problem itself and its solution, the thesis presents the basics of decentralization, blockchain and basics of technology used to create an information system.*

Keywords: *Databases, distributed information systems, blockchain, NFT*

1. УВОД

У овом раду описан је информациони систем са фокусом решавања проблема децентрализоване размене незамењивих токена (енгл. NFT). Другим речима, циљ платформе јесте то да се омогући децентрализовано место на коме корисници, односно власници незамењивих токена, могу да размењују своје токене са другим учесницима платформе кроз интерактивни интерфејс клијентске апликације самог информационог система.

Тема која је обрађена у овом раду покушава да реши проблем једноставне размене дигиталних средстава у виду незамењивих токена кроз једну платформу. Намера је да се уз што једноставније кораке приступи платформи и обави размена средстава.

Постоји неколико мотива за изградњу децентрализованог информационог система за размену незамењивих токена. Први од њих јесте безбедност која се огледа у томе да децентрализовани системи могу пружити већу сигурност од централизованих система јер се не ослањају на једну тачку квара за разлику од централизованих система. То је изразито битно за незамењиве токене који су често вредни и могу бити мета нападача.

Још један од мотива јесте и отпор цензури. Децентрализовани системи су отпорни на цензуру јер немају један ентитет који их контролише. То значи да се незамењиви токени не могу произвољно уклонити или не могу бити блокирани за трговину на платформи. Поред отпора цензури још један од мотива јесте и истинско власништво средстава. То се односи на то да децентрализовани системи омогућавају право власништво над незамењивим токенима јер се чувају у децентрализованој књизи коју не контролише ниједан ентитет. Другим речима, то значи да власнику токена не може бити одузето власништво над токенем без његовог првобитног пристанка на то.

Још неки од мотива за изградњу децентрализованог информационог система за размену незамењивих токена су и интероперабилност и транспарентност. Интероперабилност се односи на то да децентрализовани системи могу олакшати размену токена између различитих платформи и протокола, што олакшава куповину и продају токена на широком спектру платформи. С друге стране, транспарентност се односи на то да децентрализовани системи пружају транспарентност јер се све трансакције евидентирају у јавној књизи. На тај начин су омогућене транспарентност и одговорност на тржишту незамењивих токена.

Све у свему, децентрализовани информациони системи за размену незамењивих токена нуде бројне предности, укључујући повећану безбедност, отпорност на цензуру, право власништво, интероперабилност и транспарентност што представља довољан број мотива и разлога за изградњу једног таквог информационог система [1].

2. БЛОКЧЕЈН, ПАМЕТНИ УГОВОРИ И НЕЗАМЕЊИВИ ТОКЕНИ

Пре неколико година, термин блокчејна био је само израз који се користио у компјутерским наукама и односио се на чување и структурирање података. Данас, блокчејн се сматра револуцијом, не само у крипто индустрији или индустрији новца, већ и у будућности технологије, бизниса и света уопште.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Душан Гајић, ванр. проф.

Принципи блокчејна, иако делују компликовано, почивају на неким једноставним основама које није толико тешко разумети. Блокчејн је заправо врста базе података. Прва кључна разлика између типичне базе података и блокчејна је начин на који су подаци структурирани. Блокчејн не групише информације у табеле, већ у блокове. Дакле, блок се може посматрати као једна јединица базе података која садржи одређене информације.

Ако се узме у посматрање тренутно један од најпопуларнијих блокчејнова или ти Биткоинов блокчејн, може се приметити да је он база података која чува све трансакције Биткоина икада направљених и да му је то једина функција. Ултимативни циљ овог блокчејна јесте да свака трансакција буде верификована, исправна и забележена. Блок можете једноставно замислити као виртуелно парче папира које садржи информације о трансакцијама на мрежи. Један блок у ланцу Биткоина садржи информације о више од 500 трансакција. Информације се односе на то ко је послао биткоин, коме, колико, хеш блока (који се може сматрати јединственим идентификатором, отиском прста који је различит за сваки блок), као и хеш претходног блока. Баш зато што сваки блок садржи свој хеш, али и хеш претходног блока, сви блокови се надовезују један на други и креирају тако ланац или ти популарно блокчејн (енгл. Blockchain) [2] [3] [7].

Оно што гарантује безбедност мрежи је то што је блокчејн мрежа равноправних корисника (енгл. peer-to-peer) или популарно П2П (енгл. P2P). Блокчејн користи мрежу равноправних корисника како би вршио верификације на безбеднији начин. За разлику од сервера који су суштински гомила моћних компјутера у власништву једне компаније, на једном месту, П2П мрежа коју користи блокчејн састављена је од независних рачунара који се налазе широм света. У серверској архитектури, сви подаци се налазе на једном месту односно на серверу. Рачунари морају да приступе серверу како би приступили подацима. У П2П архитектури, сервер не постоји, већ су сви подаци дељени, дистрибуирани међу независним рачунарима који својим постојањем креирају мрежу.

Иако можда делује да је Виталик Бутерн као оснивач Етхереума оснивач и проналазач паметних уговора, то заправо није тако. Паметне уговоре и њихову дефиницију и појам је увео Ник Шабо још 1994. године. Тада је Ник утврдио да је паметни уговор (енгл. Smart contract) рачунарски програм или протокол трансакције који је намењен за аутоматско извршавање, контролу или документовање догађаја и радњи у складу са условима уговора или споразума. Циљеви паметних уговора су смањење потребе за посредницима од поверења, трошкова арбитраже и губитака од преваре, као и смањење злонамерних и случајних изузетака. Паметни уговори се обично повезују са криптовалутама, а паметни уговори које је увео Етхереум генерално се сматрају основним блоком за децентрализоване финансије (енгл. DeFi) и NFT апликације. Другим речима, паметни уговори су програми који се налазе у оквиру децентрализованих блокова и извршавају се у складу са покренутим упутствима. Паметни уговор делује на сличан начин као традиционални споразум, али негира потребу за учешћем треће стране. Паметни уговори су способни да аутоматски иницирају своје команде, чиме се елиминише учешће регулаторног тела. Као последица непроменљиве карактеристике блокчејна, паметни уговори се развијају на начин који се разликује од традиционалног софтвера. Када се једном примени на блокчејн, паметни уговор се не може модификовати или ажурирати за безбедносне пропусте, чиме се охрабрују програмери да примене јаке безбедносне стратегије пре примене како би избегли потенцијалну експлоатацију у каснијем тренутку.

Постоји неколико корака које програмери могу предузети како би осигурали безбедност и сигурност њихових паметних уговора. Прво, важно је пажљиво планирати и дизајнирати уговор пре него што се напише било који код. Ово укључује јасно прецизирање захтева и циљева уговора и идентификацију свих потенцијалних ризика или рањивости. Затим је од суштинског значаја темељно тестирање уговора пре објављивања на блокчејн. Ово може укључивати писање јединичних тестова како би се осигурало да појединачне компоненте уговора функционишу исправно, као и извођење ручног тестирања како би се проверило целокупно понашање уговора. Такође је важно користити безбедне праксе кодирања приликом писања уговора [4]. Ово може укључивати праћење утврђених најбољих пракси и коришћење сигурносних библиотека и оквира, као и избегавање уобичајених безбедносних замки као што су несигурно генерисање случајних бројева и непроверени унос.

У економији, замењивост се односи на својство робе и добара. На пример злато, оно је замењиво. Кило злата у златним полугама исто је вредно као и кило злата у златним новчићима истоветне чистоће. Десет долара је десет долара, без обзира да ли долази у облику једне новчанице или у четири кованице по два и по долара. Незамењивост се односи на чињеницу да је посреди податак који „живи” на блокчејну и јединствен је. Ова јединственост се изражава тиме што постоји „оригинал” и самим тим је погодан за бележење разних облика власништва, идентитета, права. Незамењиви токен је могуће купити или продати, „заменити” га (у значењу замене добара) за нешто друго. Али два незамењива токена нису међусобно замењива, као два биткоина, на пример. Ако вам неко да једну новчаницу од десет динара, а ви неком трећем дате једну новчаницу од десет динара, то је исто, осим ако нека од тих новчаница није поцепана или уништена. Али ако вам неко да токен који доказује да је тај неко власник тог токена, а ви њему дате токен који доказује да сте ви власник неког трећег токена, размена се догодила, али не и замена, јер свако одлази са својим јединственим токеном, на коме је паметни уговор. Незамењиви токен је ништа више од паметног уговора на ERC-721 токену [8].

3. КОРИШЋЕНЕ ТЕХНОЛОГИЈЕ И АЛАТИ

Један од основа за изградњу једног оваквог информационог система је Хардхат који представља вредан алат за Етхереум програмере који желе да поједноставе свој развојни процес и осигурају квалитет својих паметних уговора [2] [5]. Он је пројекат отвореног кода и може се лако инсталирати и конфигурисати на било ком систему који подржава Node.JS.

Са својим уграђеним функцијама за тестирање и примену, модуларном архитектуром и снажном подршком заједнице, Хардхат је моћно развојно окружење за изградњу и примену Етхереум паметних уговора [6]. Да би се ти паметни уговорили написали на Етхереуму, коришћен је програмски језик Солидити. Солидити је програмски језик за писање паметних уговора на Етхереум мрежи. Он је објектно оријентисан језик високог нивоа са синтаксом сличном оној у Јава Скрипту. Солидити је дизајниран да буде лак за писање и читање, а истовремено је довољно изражајан и моћан да имплементира сложену логику и уговоре. Како би се све то приказало и како би се омогућила интеракција преко корисничког интерфејса, коришћен је оквир за развој клијентских апликација под називом Next.JS. Оно што је спојило паметни уговор са клијентском апликацијом јесте TheGraph који представља софтвер отвореног кода који се користи за прикупљање, обраду и складиштење података из различитих блокчејн апликација како би се олакшало проналажење информација [6]. Поред тога, један од алата преко ког се поједностављује коришћене апликације јесте и Metamask који представља бестплатну екстензију за веб претраживач и мобилну апликацију која омогућава корисницима да чувају и замењују криптовалуте, комуницирају са Етхереумом и хостују децентрализоване апликације.

4. РЕШЕЊЕ

Архитектура система је декомпонована на три модула. Сваки од модула има своју сврху и намену у читавом систему. Први модул је клијентска апликација изграђена на оквиру за развој клијентских апликација са називом Нехт (енгл. Next.JS). Корисник платформе користи клијентску апликацију кроз интерактивни интерфејс, након чега се клијентска апликација обраћа другом модулу, односно Граф (енгл. TheGraph) пројекту који је задужен да чува и складишти догађаје (енгл. Events) које трећи модул, односно Хардхат пројекат објављује, у оквиру њега је и изграђен паметни уговор система који се налази на блокчејну.

5. ЗАКЉУЧАК

Децентрализовани информациони систем за размену незамењивих токена описан у овом раду је развијен и успешно извршаван на Етхереум платформи. Имплементацијом овог система омогућена је безбеднија, отпорнија на цензуру, са правим правом на власништво размена незамењивих токена при чему је омогућена и интероперабилност, као и транспарентност кроз блокчејн. Потенцијална унапређења могу бити вођена у више смерова, први и конкретан би могао да буде повећање ефикасности потрошње гаса. Неопходно је анализирати један део система, односно конкретно паметни уговор и видети сваку функцију и измерити колико гаса троши свака од њих, те потом идентификовати проблематичне и онда пробати извршити оптимизацију потрошње. Наредно унапређење може бити оријентисано ка анализи безбедности и сигурности паметног уговора, где је потребно савладати принципе и оквире добрих пракси у Солидитију са којима сте имали прилику да се упознате у претходним поглављима, а након тога извршити детаљну проверу тренутног паметног уговора и покушати наћи рањивости и одмах након тога решења која спречавају те рањивости, чиме би се повећала безбедност и сигурност паметног уговора, а тако и самог информационог система. Наравно, једно од унапређења може бити и повећање броја функционалности које пружа сама платформа.

6. ЛИТЕРАТУРА

[1] Душан Гајић, *Материјали са предмета Паралелни и дистрибуирани алгоритми и структуре података*, доступно на: http://www.acs.uns.ac.rs/sr/node/237/4468699, последњи приступ јул 2022.

[2] *Ethereum Documentation*, доступно на https://ethereum.org/en/developers/docs/, последњи приступ децембар 2022.

[3] Виталик Бутерин, *The Meaning of Decentralization*, доступно на: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274, последњи приступ новембар 2022.

[4] *Solidity Patterns*, доступно на: https://fravoll.github.io/solidity-patterns/, последњи приступ децембар 2022.

[5] *Hardhat Documentation*, доступно на: https://hardhat.org/docs, последњи приступ септембар 2022.

[6] *TheGraph*, доступно на: https://thegraph.com/, последњи приступ новембар 2022.

[7] *Ecd*, доступно на: https://ecd.rs/, последњи приступ август 2022

[8] *Ethereum Improvement Proposals*, доступно на: https://eips.ethereum.org/EIPS/eip-721, последњи приступ јануар 2023

Кратка биографија:

Владислав Максимовић, рођен је 3. јула 1998. Факултет техничких наука у Новом Саду, студијски програм Рачунарство и аутоматика, уписао је 2017. год. Дипломирао је 2021. год., а потом уписао мастер академске студије из исте области.

контакт: maksimovic98vladislav@gmail.com