Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.38
DOI: https://doi.org/10.24867/23BE12Kalocanj

ПЛАТФОРМА ЗА КУПОПРОДАЈУ НЕЗАМЕНЉИВИХ ТОКЕНА

PLATFORM FOR BUYING AND SELLING NON-FUNGIBLE TOKENS

Андреј Калочањ Мохачи, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Популарност blockchain технологија и незаменљивих токена, односно NFT, је током претходних неколико година знатно порасла. Услед тога су се појавили нови облици трговине и нова тржишта која се називају продавнице незаменљивих токена и омогућавају власницима да понуде своје токене под одређеним условима, а заинтересованим лицима да под тим условима купе токене. Примена паметних уговора омогућава кодификацију услова под којима се одвија купопродаја, а аутоматско извршавање тих уговора омогућава реализацију уговора односно уговорених одредби. У овом раду је представљено софтверско решење за купопродају незаменљивих токена под називом eArtRegister. Корисницима платформе дат је увид у одредбе паметних уговора на природном и програмском језику како би се боље информисали о правима и обавезама дефинисаним тим уговорима. У раду је приказана и евалуација ове платформе у односу на друга слична решења и дате су смернице за њено даље усавршавање.*

Кључне речи: *blockchain, NFT, паметни уговори*

Abstract – *The popularity of blockchain technologies and non-fungible tokens, NFTs, has increased significantly over the past few years. As a result, new forms of trade and new markets have emerged, which are called NFT marketplaces. These stores allow owners of NFTs to offer their tokens under certain conditions, and interested parties to buy tokens under those conditions. The application of smart contracts enables the codification of the conditions under which the purchase takes place, and the automatic execution of those contracts enables the realization of the contract, i.e. agreed provisions. This paper presents a software solution for buying and selling NFTs called eArtRegister. Users of this platform are able to preview smart contract provisions in natural language and programming language to better understand the rights and obligations defined by those contracts. The paper also shows the evaluation of this platform in relation to other similar solutions and provides guidelines for its further improvement.*

Keywords: *blockchain, NFT, smart contracts*

1. УВОД

Убрзани развој информационих технологија омогућио је да се помоћу сложених криптографских механизама створе услови за безбедно чување и размену података у небезбедном окружењу какав је Интернет. На тај начин је настао blockchain односно ланац блокова са подацима који истовремено пружају анонимност учесницима у трансакцијама, обезбеђују аутентичност и транспарентност података у тим трансакцијама.

Трансакцијама је најпре подржан промет новчаних средстава у такозваним криптовалутама, а на неким од blockchain платформи је убрзо затим подржано и коришћење паметних уговора чиме је омогућено да предмет трансакција буде извршавање програмског кода. Паметним уговорима је тако омогућено аутоматизовано управљање подацима или прометом новчаних средстава у складу са трансакцијама учесника који врше интеракцију са тим уговором.

Када се паметним уговорима представљају одредбе уговора у смислу облигационих односа, на тај начин се обезбеђује аутоматска примена и извршавање права и обавеза уговорних страна које из тог уговора произилазе. То је од посебног значаја за примену паметних уговора у купопродаји.

Помоћу ових уговора је могуће управљати подацима о власништву над такозваним токенима који могу бити заменљиви или незаменљиви [1]. Пример заменљивих токена су криптовалуте с обзиром на то је неку количину ових токена могуће заменити једнаком количином токена исте врсте. Незаменљиви токени представљају ствари које су јединствене и самим тим нису међусобно заменљиве.

У овом раду је приказано коришћење blockchain технологија за подршку купопродаји незаменљивих токена. Овим софтверским решењем се омогућава трговина дигиталним сликама, уз могућност увида у садржину паметних уговора у форми природног језика и програмског кода како би се олакшало разумевање права и обавеза купца и продавца.

Остатак овог рада је организован на следећи начин: у наредном одељку су анализирана сродна решења и технологије за купопродају незаменљивих токена, трећи одељак приказује метод израде платформе за купопродају незаменљивих токена eArtRegister, у четвртом одељку је представљен прототип платформе, пети одељак евалуира ефикасност ове платформе, а у шестом одељку су изнети закључци и дате су смернице за даље усавршавање прототипа.

НАПОМЕНА:

Овај рад је проистекао из мастер рада чији ментор је био др Марко Марковић, доцент.

2. СРОДНА ИСТРАЖИВАЊА

У овом одељку су анализирана сродна софтверска решења и технологије које омогућавају трговину незаменљивим токенима

OpenSea [2] је једна од највећих платформи за трговину незаменљивим токенима креираних по ERC-721 стандарду [3]. Платформа подржава више криптовалута од којих је Ethereum [4] подразумевана криптовалута. Безбедност трансакција на платформи је такође на високом нивоу, јер се при трговини власништво над токенима не преноси све док се продаја не реализује. Платформа задржава провизију у износу од 2,5% од сваке продаје.

Rarible [5] је такође једна од најпопуларнијих платформи за трговину незаменљивим токенима. За разлику од OpenSea платформе, Rarible подржава уплате у државним валутама, односно ако корисник поседује платну картицу омогућена му је куповина на овој платформи. Rarible је основао фондацију RARI [6] и креирао истоимену криптовалуту и дозволио њеним власницима право гласа у вези са будућим изменама на платформи. Платформа је испратила стандард за провизију према стваоцу NFT EIP-2981 [7].

Binance [8] је једна од највећих крипто-мењачница као и једна од највећих светских централизованих NFT тржишта, где је могуће прегледати понуду и трговати широким спектром артикала у играма, виртуелним земљиштем, уметничким делима и другим категоријама.

Crypto.com [9] је продавница незаменљивих токена и у потпуности је заснована на Crypto.org мрежи [10] која је потпуно децентрализована јавна blockchain [11] мрежа. Ова blockchain мрежа је дизајнирана да буде јавно добро које помаже у масовном усвајању blockchain технологије кроз разне случајеве коришћења, међу којима је и управљање незаменљивим токенима.

За идентификацију корисника и потписивање трансакција на blockchain мрежи користе се такозвани дигитални новчаници. Дигитални новчаник MetaMask [12] поседује релативно једноставан кориснички интерфејс и може се користити као додатак у веб прегледачима. MetaMask подржава Ethereum трансакције, док трансакције на другим платформама као што је Bitcoin [13] нису подржане.

За интеракцију *front-end* технологија са blockchain мрежом користе се посебне библиотеке које укључују и подршку за повезивање са дигиталним новчаницима. Тако се при изради корисничке апликације развијене у Angular радном оквиру [14] интеракција са MetaMask корисничким дигиталним новчаником може постићи употребом библиотеке web3.js [15] која уједно обезбеђује и комуникацију са blockchain мрежом.

Подршка за компајлирање паметних уговора за Node.js [16] окружење је доступна у оквиру пакета solc [17]. Овај сервис генерише bytecode и application binary interface (ABI) [18] на основу изворног кода паметног уговора. Поменути bytecode представља извршни кôд за Ethereum виртуелну машину EVM [19], а ABI је интерфејс преко којег је могућа интеракција са паметним уговором.

IPFS протокол [20] омогућава дистрибуирано складиштење датотека и пратећих метаподатака. С обзиром на то да blockchain мреже нису погодне за чување већих количина података, IPFS решава овај проблем на тај начин што се незаменљиви токени само референцирају на идентификаторе додељене датотекама при њиховом постављању на IPFS.

Програмски језик Solidity [21] омогућава имплементацију паметних уговора. Постављањем ових уговора на blockchain мрежу се омогућава аутоматско извршавање програмског кода који је у њима дефинисан. Solidity језик поседује доста сличности са савременим програмским језицима и представља најчешћи избор при изради паметних уговора за Ethereum платформу.

За потребе тестирања паметних уговора од великог значаја су тестне платформе на којима је могуће извршавати паметне уговоре без потребе за плаћањем провизија и без ризика од евентуалних финансијских губитака у случају грешака у програмском коду. Goerli Ethereum Testnet [22] је једна од највећих и најчешће коришћених тестних мрежа за Ethereum.

Паметни уговори су рачунарски програми који су смештени на blockchain мрежу и извршавају се на чворовима те мреже. Методе паметних уговора је могуће позивати путем трансакција чиме се врше промене стања уговора уз евентуалне новчане трансакције. Познавање интерфејса паметног уговора (ABI) је неопходан предуслов за позивање метода тог уговора [23]. Како су подаци на blockchain мрежи јавно доступни, тако су и информације о трансакцијама које су извршене над паметним уговорима транспарентне.

Стандард ERC-721 дефинише методе помоћу којих се обезбеђује управљање незаменљивим токенима. Овај стандард је заснован на оригиналном стандарду ERC-20 [24] који служи за креирање заменљивих токена, односно криптовалута.

3. МЕТОД

У овом одељку је описана имплементација платформе за купопродају незаменљивих токена. Наведени су функционални захтеви платформе, објашњена је структура паметних уговора које ова платформа користи и представљен је дизајн софтверског решења.

У систему постоје два типа учесника, нерегистровани корисник који има могућност претраживања и прегледања свих колекција незаменљивих токена, док регистровани корисници имају могућност креирања депозит уговора, уплате и исплате средстава са депозит уговора, креирања колекције токена, креирање токена за дигиталне слике, стављање токена на продају уз креирање купопродајног уговора (за продају у пуном износу, на рате или путем аукције) и куповине незаменљивих токена.

Депозит уговором се омогућава корисницима уплата средстава којима ће располагати на платформи eArtRegister и пријем средстава од продаје токена. Уплате на депозит уговор и повлачење средстава са овог уговора се врше уз помоћ MetaMask дигиталног новчаника.

Управљање незаменљивим токенима је реализовано по ERC-721 стандарду. Паметан уговор који обезбеђује управљање токенима имплементира интерфејс ERC721 који је дефинисан овим стандардом.

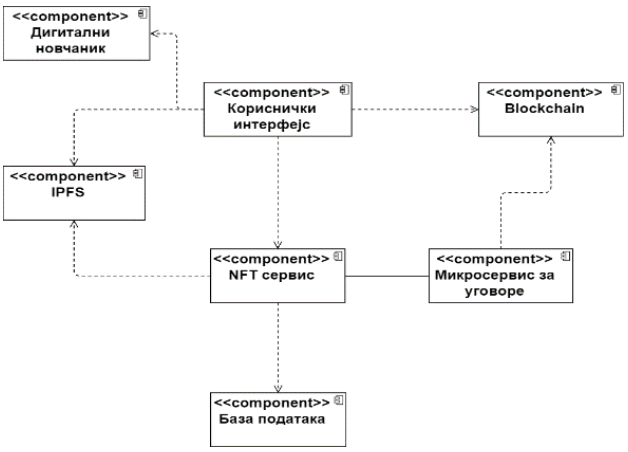
Овај стандард омогућава продавцу да купопродајном уговору додели права над токеном како би се у потпуности аутоматизовао пренос власништва у складу са уговореним одредбама.

На слици 1 приказан је дијаграм компоненти платформе eArtRegister. Компонента „Дигитални новчаник“ репрезентује кориснички дигитални новчаник који је неопходан да би корисник могао куповати, креирати или продавати незаменљиве токене путем ове платформе. „Кориснички интерфејс“ је *front-end* апликација преко које корисник врши интеракцију са платформом.

Компонента „NFT сервис“ обрађује захтеве са *front-end* апликације, стара се о перзистенцији података и комуницира са микросервисом за паметне уговоре. „IPFS“ је компонента за складиштење дигиталних слика, односно графичких датотека и пратећих датотека са метаподацима.

Компонента „Микросервис за уговоре“ генерише паметне уговоре и поставља их на blockchain. „База података“ представља складиште за податке о корисничким колекцијама токена и самим токенима који су предмет трговине на платформи.

Компонента „Blockchain“ репрезентује blockchain мрежу на којој се налазе креирани уговори и на којој се извршавају неопходне трансакције.

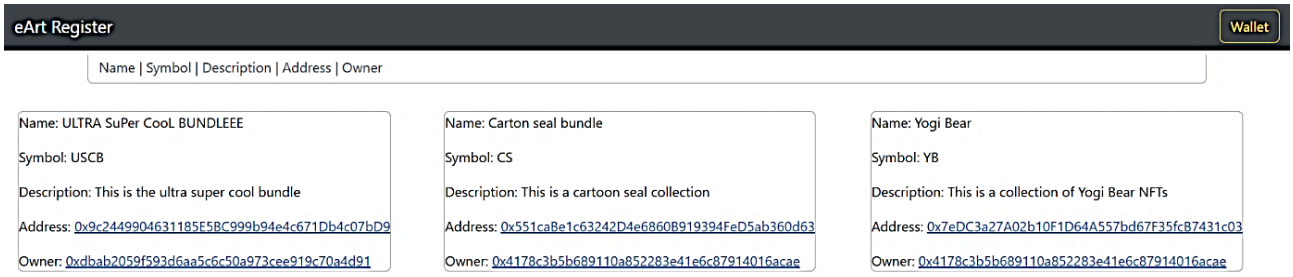


Слика 1. *Дијаграм компоненти*

4. РЕЗУЛТАТ

Према описаном методу развијено је прототипско решење за купопродају незаменљивих токена, односно платформа eArtRegister. Ово решење је имплементирано као веб апликација у којој је корисницима омогућено креирање сопствених колекција незаменљивих токена, стављање на продају и куповина токена. Депозит уговор и купопродајни уговор, који се користе у раду платформе, су доступни у текстуалном формату и у облику програмског кода, а њихова садржина се динамички генерише према одабраним условима купопродаје.

На слици 2 приказан је кориснички интерфејс платформе eArtRegister.



Слика 2. *Изглед корисничког интерфејса платформе eArtRegister*

5. ЕВАЛУАЦИЈА

У овом одељку је приказана евалуација платформе за купопродају незаменљивих токена. Анализирана је потрошња такозваног горива (енг. gas) потребног за извршавање трансакција у којима се власништво над незаменљивим токеном преноси са једног власника на другог. Количина утрошеног горива одговара ангажованим рачунарским ресурсима, па зато она представља значајан индикатор сложености и ефикасности имплементације паметног уговора. Поред тога, потрошња горива при извршавању трансакција директно утиче на накнаду која се обрачунава за иницирање ових трансакција.

Висина накнаде се израчунава као производ количине утрошеног горива и цене горива, при чему избор цене горива утиче на брзину извршавања трансакције [25].

Са сваке од анализираних платформи је прикупљен узорак од по пет трансакција у којима је извршен пренос власништва над незаменљивим токенима и упоређена је потрошња горива у тим трансакцијама.

Табела 1 даје преглед потрошње горива при преносу власништва над незаменљивим токенима за платформу eArtRegister и друге сродне платформе.

Табела 1. *Потрошња горива по платформама*

Платформа	Утрошено гориво		
	најнижа вредност	средња вредност	највиша вредност
eArtRegister	96443	108315,0	114852
OpenSea	189150	213172,0	617330
Rarible	108545	110174,6	110619
Binance	1617326	2841146,0	4280228
Crypto.com	120959	225572,0	360680

Из приказаних података се може закључити да је најнижа просечна потрошња горива на платформи eArtRegister и износи 108315 гаса. Највиша потрошња горива је забележена на Binance платформи и њена просечна вредност износи 2841146 гаса.

Без познавања тачне имплементације паметних уговора над којима су извршене ове трансакције није могуће дати прецизно тумачење ових резултата. С обзиром на то да потрошња горива зависи од комплексности операција које је потребно извршити овим трансакцијама, објашњење се може тражити како у сложености имплементације паметних уговора, тако и у оптимизованости њиховог програмског кода.

Платформа eArtRegister представља прототипску апликацију, те се може претпоставити да друге анализиране платформе, које постоје и развијају се дужи временски период, у својој имплементацији поседују захтевније операције како би се одговорило на изазове које поставља тржиште незаменљивих токена.

6. ЗАКЉУЧАК

У овом раду је приказано софтверско решење за купопродају незаменљивих токена. Објашњена је имплементација ове платформе и представљена је прототипска апликација eArtRegister.

Предност eArtRegister платформе је томе што она пружа корисницима могућност увида у одредбе паметних уговора на природном језику и на програмском језику, како би им се олакшало разумевање њихових права и обавеза.

Рад платформе је евалуиран уз поређење са другим сродним платформама у смислу потрошње горива. Платформа eArtRegister је показала најнижу просечну потрошњу горива у односу на остале платформе.

Даљим развојем ове платформе би требало обухватити подршку за друге типове дигиталних новчаника и друге blockchain платформе. Такође, корисницима би се могло омогућити да на платформи користе више од једног дигиталног новчаника.

7. ЛИТЕРАТУРА

[1] Knowledgehut, "NFT vs Cryptocurrency [Head-to-head Comparison]" https://www.knowledgehut.com/blog/blockchain/nft-vs-crypto (приступљено у фебруару 2023.)

[2] OpenSea, https://opensea.io/ (приступљено у фебруару 2023.)

[3] Ethereum, "ERC-721 Non-Fungible Token Standard" https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ (приступљено у фебруару 2023.)

[4] Ethereum, "What is ether (ETH)?" https://ethereum.org/en/eth/ (приступљено у фебруару 2023.)

[5] Rarible, https://rarible.com/ (приступљено у фебруару 2023.)

[6] RARI Foundation, https://rari.foundation/ (приступљено у фебруару 2023.)

[7] Medium, "Create NFT with Royalty (EIP-2981)" https://medium.com/@nufailismath15/create-nft-with-royalty-eip-2981-bf201105ab96 (приступљено у фебруару 2023.)

[8] Binance NFT, https://www.binance.com/en/nft/home/ (приступљено у фебруару 2023.)

[9] Crypto.com NFT, https://crypto.com/nft/ (приступљено у фебруару 2023.)

[10] Cryto.org, https://crypto.org/ (приступљено у фебруару 2023.)

[11] Investopedia, "Blockchain Facts: What Is It, How It Works, and How It Can Be Used", https://www.investopedia.com/terms/b/blockchain.asp (приступљено у фебруару 2023.)

[12] Metamask, https://metamask.io/ (приступљено у фебруару 2023.)

[13] Bitcoint, https://bitcoin.org/en/ (приступљено у фебруару 2023.)

[14] Angular, https://angular.io/ (приступљено у фебруару 2023.)

[15] Web3.js, https://web3js.readthedocs.io/en/v1.8.1/ (приступљено у фебруару 2023.)

[16] Nodejs, https://nodejs.org/en/ (приступљено у фебруару 2023.)

[17] https://www.npmjs.com/package/solc-js (приступљено у фебруару 2023.)

[18] Chainlink, "What Are ABI and Bytecode in Solidity?", https://blog.chain.link/what-are-abi-and-bytecode-in-solidity/ (приступљено у фебруару 2023.)

[19] Ethereum, "Ethereum Virtual Machine (EVM)", https://ethereum.org/en/developers/docs/evm/ (приступљено у фебруару 2023.)

[20] IPFS, https://ipfs.tech/ (приступљено у фебруару 2023.)

[21] Solidity, https://docs.soliditylang.org/en/v0.8.17/ (приступљено у фебруару 2023.)

[22] Goerli Testnet, https://goerli.net/ (приступљено у фебруару 2023.)

[23] QuickNode, "How to call another smart contract from your solidity code", https://www.quicknode.com/guides/smart-contract-development/how-to-call-another-smart-contract-from-your-solidity-code (приступљено у фебруару 2023.)

[24] Investopedia, "What Are ERC-20 Tokens on the Ethereum Network?", https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/ (приступљено у фебруару 2023.)

[25] Binance academy, "What Are Blockchain Transaction Fees", https://academy.binance.com/en/articles/what-are-blockchain-transaction-fees (приступљено у фебруару 2023.)

Кратка биографија:

Андреј Калочањ Мохачи је рођен 14.04.1997. у Кикинди где је стекао своје основно и средње образовање. Школске 2016/17 уписује основне академске студије на Факултету техничких наука, студијски програм Примењено софтверско инжењерство. На мастер академске студије Факултета техничких наука се уписује школске 2021/22. године на студијском програму Рачунарство и аутоматика.

контакт: andrej.km997@gmail.com