Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/24BE11Raskovic

СИСТЕМ ЗА АУКЦИЈЕ НЕЗАМЕЊЉИВИХ ТОКЕНА

SYSTEM FOR AUCTIONS OF NON-FUNGIBLE TOKENS

Стеван Рашковић, *Факултет техничких наука, Нови Сад*

Област – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У овом раду је описан систем за једнодневне аукције незамењивих токена, чији су подаци смештени на блокчејну, на Ethereum мрежи. Описана је и примена замењивих токена као начина за гласање у оквиру децентрализоване независне организације. Поред тога, описани су основни концепти блокчејн технологије.*

Кључне речи: *блокчејн, паметни уговори, независне децентрализоване организације, незамењиви токени*

Abstract – *This paper presents a blockchain system on Ethereum that handles daily auctions of non-fungible tokens, with metadata being completely on-chain. Besides that, fungible tokens and their applications as voting tokens inside a decentralized autonomous organization are also presented. Additionally, the paper gives introduction to the fundamentals of blockchain technology.*

Keywords: *blockchain, smart contracts, decentralized autonomous organizations, non-fungible tokens*

1. УВОД

Велика мана централизованих система јесте то што постоји један ентитет који има контролу над читавим системом, а то захтева постојање поверења свих учесника у тај ентитет.

Блокчејн, као технологија која почива на децентрализацији, омогућава стварање система који су потпуно транспарентни, где сви учесници могу да виде шта се дешава у систему. На тај начин елиминише се централизовани ентитет ком је потребно веровати.

Овај рад бави се аукцијама и аутономним децентрализованим организацијама на *Ethereum* блокчејну. Као предмет аукције користе се незамењиви токени, чији се метаподаци, у потпуности налазе на блокчејну без централизованих компоненти. У раду је описана и примена замењивих токена као механизма за гласање у оквиру организације на блокчејну.

2. ТЕОРИЈСКЕ ОСНОВЕ

2.1. Блокчејн

Блокчејн у својој основи представља дистрибуирану базу података која може да складишти било које податке [1]. Блокчејн је децентрализован, што значи да не постоји централизовано место где се чувају подаци и диктирају њихове промене, већ се идентична копија базе налази на свим чворовима који чине блокчејн мрежу. Промене података одвијају се трансакцијама које се групишу у блокове, где се нови блок криптографским механизмима уланчава са претходним. Договор око тога како изгледа нови блок одвија се путем изабраног механизма консензуса [2]. Блокчејн користи криптографске механизме да обезбеди кориснике и податке. Једна битна карактеристика је да је историја непромењива, тако да нико на своју руку не може изменити трансакцију која се налази у неком блоку [3]. Такође, елиминише се потреба за постојањем централизованог ентитета коме сви морају веровати.

2.2. *Ethereum*

Ethereum је блокчејн мрежа замишљена као аутомат чије се стање мења трансакцијама. У *Ethereum* свету постоји један рачунар који се назива *Ethereum* виртуелна машина (*EVM*) и око чијег стања постоји консензус [4]. Сваки учесник у мрежи може да пошаље захтев за извршење трансакције чиме се мења стање и та промена се пропагира кроз целу мрежу.

Ether (ETH) је главни токен, односно криптовалута на *Ethereum* мрежи која се користи за слање трансакција или креирање паметних уговора.

Налози на *Ethereum* блокчејну су ентитети који граде стање мреже. Сваки има адресу, састављену од 20 бајтова. Постоје 2 типа налога, спољa контролисан (енг. *externally owned account*), кога контролише приватни кључ и који може да шаље трансакције, и налог паметног уговора који имају свој програмски код и не могу сами покретати трансакције.

2.3. Паметни уговори на *Ethereum* блокчејну

Паметни уговори (енг. *Smart Contracts*) су уговори између страна који се складиште на блокчејну и извршавају се када се испуне унапред дефинисани захтеви [5]. Као и све што се складишти на блокчејн мрежи, тако и паметни уговори имају особину да нико на своју руку не може да уради нешто што тај уговор не дозвољава. Паметни уговори су програми, тако да су сви услови репрезентовани програмским кодом. Битне погодности које нуде паметни уговори јесу елиминација треће стране којој је потребно веровати, елиминацију папира које је потребно потписивати и чувати, транспарентност и безбедност које доноси блокчејн технологија као и многе друге.

Паметни уговори на *Ethereum* мрежи јесу један тип налога и имају свој програмски код. *EVM* може да извршава програме написане у *EVM Bytecode*-у који је језик ниског нивоа и поседује скуп инструкција које програми могу да користе. Постоје и виши про-

---

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Горан Сладић, ред. проф.

грамски језици у којима је могуће писати паметне уговоре а чији код се може превести у *EVM Bytecode*. Један он најпопуларнијих је *Solidity*, објектно-оријентисан статички типизиран програмски језик.

2.4. Замењиви токени на *Ethereum* мрежи

Замењиви токени (енг. *Fungible Tokens*) су добра која нису јединствена и често су дељива [6]. Пример замењивог токена била би било која валута, на пример динар. Сваки динар има идентичну вредност, једну новчаницу од 100 динара је могуће заменити са две од 50 и вредност се не мења.

У *Ethereum* свету замењиви токени су стандардизовани *ERC-20* стандардом [7]. Стандард намеће интерфејс који треба да имплементирају паметни уговори који представљају овај тим токена. Такође стандард прописује и догађаје које је потребно забележити како би апликације које користе овај паметни уговор лакше могле да примете промене.

2.5. Незамењиви токени на *Ethereum* мрежи

Незамењиви токени (енг. *Non-Fungible Tokens, NFT*) су добра која су јединствена и сваки токен има своју вредност и особине које их међусобно разликују [8]. Типични примери овакве врсте токена су уметничка дела, јер свако је јединствено и заменом једног за другог не може се добити идентична ствар. Такође некретнине или личне карте би могле бити пример незамењивих токена. На *Ethereum* мрежи ови токени су представљени *ERC-721* стандардом [9]. Као и код замењивих токена, стандард прописује функције које је потребно имплементирати.

Метаподаци токена су такође стандардизовани. За складиштење метаподатака се могу користити различите опције, најчешће су то централизовани сервер (база података) или *IPFS*. Прва опција уводи један ентитет који у потпуности контролише податке и може да их промени на своју руку у било ком тренутку. *IPFS* гарантује непромењивост садржаја, али не постоји гаранција да ће фајлови увек бити доступни. Опција која ће се примењивати у овом раду је складиштење података на блокчејну - метаподаци се налазе у меморији паметног уговора. Предност овог приступа је то што су подаци увек доступни, међутим цена складиштење података и ограниченост простора могу бити проблем.

2.6. Независне децентрализоване организације

Независне децентрализоване организације (енг. *Decentralized Autonomous Organization, DAO*) су управљачке структуре без централног ентитета ком учесници морају да верују [10]. За имплементацију *DAO* структура користи се низ паметних уговора тако да су сва правила постављена кроз програмски код. За чланство се најчешће користе неки од претходно описаних токена. Идеја је да чланови заједно одлучују о томе у ком смеру се креће организација и на шта се троше средства која *DAO* поседује. Често се при имплементацији користи и *Timelock* уговор који има за циљ да одложи извршавање неког усвојеног предлога како би они који се са тим не слажу имали времена да је напусте пре примене тог предлога.

3. МОДЕЛ СИСТЕМА

Апликација којом се овај рад бави замишљена је као решење које је у потпуности независно од централизованих сервера, односно сва логика је реализована као скуп паметних уговора. Систем се састоји од *NFT* колекције која све податке чува на блокчејну. Колекција представља слике тзв. *смајлија* који имају следеће особине: позадина, лице, очи, уста, шешир и бркови. Свака особина има различите могуће вредности, од којих све вредности имају другачије вероватноће јављања.

Сваког дана креира се по један *NFT* и налази се на аукцији која траје 24 часа. Током тог периода било ко може да остави понуду. По истеку аукције, токен се пребацује победнику док *ETH* којим је плаћен токен пребацује на налог *DAO* организације. Истовремено се прави и нова аукција која траје 24 часа. Победник аукције такође добија и поене за гласање у вредности коју носи токен који је купљен. Број поена зависи од тога које вредности токен има за своје атрибуте - што су вредности ређе то токен носи више поена, који представљају гласове у оквиру организације. Онај ко оконча аукцију такође добија мали број гласачких поена, као накнаду за цену коју плати да би извршио ту трансакцију. Власник може своје поене да да на управљање некој другој страни.

У оквиру *DAO* организације било ко, чак и ако не поседује гласачке поене, може да поднесе предлог. Предлог се састоји од трансакција на блокчејну које могу бити или обичан пренос *ETH* токена, или позиви функција паметног уговора. Када се предлог постави, постоји одређен период пре него што крене гласање. Током тог периода могуће је извршити делегирање гласова, али било које увећање гласачких поена неће бити регистровано како би се спречила куповина гласова. Након периода гласања, уколико предлог прође, он поново мора да сачека одређен период пре него што се трансакције изврше како би било ко незадовољан исходом гласања могао да одреагује како жели, на пример да напусти организацију. Након тога, било ко може да покрене извршење трансакција.

Да би предлог прошао, мора да добије просту већину гласова, као и да је укупан број гласова довољно велик, односно да постови кворум.

4. ИМПЛЕМЕНТАЦИЈА

За имплементацију је употребљен *Solidity* програмски језик. Решење је развијано уз употребу *Hardhat* окружења за развој *Solidity* апликација које, поред осталог, даје могућност покретања локалног *EVM* блокчејна. Клијентски део апликације написан је употребом *Next.js* радног оквира и *Tailwind* библиотеке. За комуникацију са блокчејном употребљена је библиотека *ethers.js*. У наставку ће бити описан само део система на блокчејну.

4.1. Паметни уговор *SmileyAttribute*

Сваки од атрибута смајли токена имплементиран је по једном инстанцом *SmileyAttribute* паметног уговора. Уговор је описан *ISmileyAttribute* интерфејсом, који је приказан на листингу 1.

```
interface ISmileyAttribute {
    //returns name of the attributte
    function getAttributeName() external view returns (string
        memory);
    //retrives name of i-th value
    function getValueName(uint80 index) external view
returns    (string memory);
//returns SVG string of i-th value
    function getSVGData(uint80 index) external view returns
(string    memory);
    //"randomly" picks value taking weights into
consideration
    function pickRandomValue() external view returns
(uint80    value);
    //return how much points certain value worth
    function getPoints(uint80 index) external view returns
(uint256   value);
}
```

Листинг 1. *Интерфејс ISmileyAttribute*

За сваку могућу вредност атрибута чува се његов *SVG* опис, назив и учесталост јављања и број поена који носи. Функција *pickRandomValue* на случајан начин бира једну од могућих вредности и враћа њену нумеричку ознаку, док *getSVGData* за дату нумеричку ознаку враћа *SVG* код за ту вредност атрибута.

4.2. Паметни уговор *SmileyVotingToken*

SmileyVotingToken паметни уговор моделује гласачке поене у систему и заснован је на *ERC20* стандарду за замењиве токене.

За основне функционалности које прописује *ERC20* стандард, *SmileyVotingToken* користи имплементацију од стране *OpenZeppelin* библиотеке која покрива све захтеве из стандарда. Из ове библиотеке наслеђен је и *ERC20Votes* паметни уговор. Он има механизме за чување података о броју токена било које адресе за сваки блок на мрежи. У паметни уговор додата је и фунцкција *mint*. Улога ове функције је да креира нове токене за адресу која јој се проследи.

SmileyVotingToken уводи ограничење да се *mint* функција може позвати само од стране једне одабране адресе, која се касније може поставити на адресу паметног уговора који управља аукцијама како би само он могао да издаје нове токене.

4.3. Паметни уговор *SmileyNFT*

Како је овај уговор једна *NFT* колекција, за основне операције над токенима које прописује стандард као и код претходних уговора наслеђен је паметни уговор из *OpenZeppelin* библиотеке. За генерисање идентификатора токена користи се бројач.

Паметни уговор има листу *ISmileyAttribute* инстанци, по једну за сваки атрибут смајлија као и мапу где се за сваки токен чувају нумеричке ознаке вредности одговарајућих атрибута.

Функција *mint* приказана на листингу 2 служи за креирање новог токена и може је позвати само *minter* адреса, која је овом систему постављена на адресу паметног уговора који управља аукцијама. Приликом креирања новог токена бројач се увећава за један и тако се добија идентификатор новог токена. Затим се позива наслеђена *_mint* функција која ће генерисати токен и повезати га са новим власником. У оквиру *metadata* поља овог паметног уговора даље се додају вредности атрибута новонасталог токена, при чему вредности на псеудослучајан начин бирају *SmileyAttribute* инстанце на начин који је претходно описан. Процес се завршава објављивањем *SmileyMinted* догађаја.

```
function mint() public override minterOnly returns (uint256) {
    _tokenIds.increment();
    uint256 newItemId = _tokenIds.current();
    _mint(msg.sender, newItemId);
    for (uint16 i = 0; i < attributes.length; i++) {
        metadata[newItemId].push(attributes[i].pickRandomValue());
    }
    emit SmileyMinted(newItemId);
    return newItemId;
}
```

Листинг 2. *Функција mint SmileyNFT уговора*

Пошто токени треба да прате стандард и могу бити излистани на продавницама *NFT* токена, слике које ће се приказивати морају се из функције *tokenURI* паметног уговора вратити као *Base64* енкодоване. Употребом *abi.encodePacked* функције спајају се одговарајуће вредности за сваки атрибут, заједно са коренским *SVG* елементом. На крају се додају префикс за ознаку типа енкодованог *Base64* садржаја и врши енкодовање употребом екстерне библиотеке.

У функцији *tokenURI* на идентичан начин се генерише целокупан опис токена, који укључује име, опис, списак атрибута и њихових вредности као и генерисану *SVG* слику. Овакав опис се поново пакује као *Base64* енкодован садржај.

4.4. Паметни уговор *SmileyAuction*

SmileyAuction је паметни уговор који служи за управљање активном аукцијом, има привилегију да креира нове смајли токене и води рачуна о пристиглим понудама.

Паметни уговор поседује поља које означавају колико трају аукције, колики је минимални проценат повећања наредне понуде и слично. Ови параметри се могу конфигурисати од стране *DAO* организације.

Приликом креирања аукције генерише се нови токен у *SmileyNFT* паметном уговору, креира се нова аукција са тренутним вредностима за параметре аукције и објављује се догађај. Прва аукција мора бити покренута од стране адресе која је власник уговора, а покретање сваке наредне аукције је аутоматски након окончања претходне.

Уговор има функцију *completeAuctionAndStartNew* коју може позвати било ко, а која ће окончати тренутну аукцију, креирати нову и доделити адреси која је позвала функцију три поена за гласање. Ова функција позива друге две интерне функције, од којих је једна *_completeAuction* која садржи логику за окончање тренутне аукције. На почетку се врше провере да ли постоји тренутно активна аукција, да ли је аукција већ завршена, као и да ли је могуће завршити аукцију у датом тренутку. Уколико су услови испуњени аукција се означава завршеном. Уколико постоји нека понуда, смајли токен се пребацује на адресу која је оставила понуду, у супротном токен се пребацује *DAO* организацији. Уколико купац постоји,

њему се поред токена додају и гласачки поени а *ETH* токени којима је платио смајли се пребацују *DAO* организацији. На крају се у сваком случају емитује догађај за крај аукције.

4.5. Паметни уговори *SmileyGovernor* и *TimeLock*

DAO у оквиру система је, направљена уз ослонац на *OpenZeppelin* библиотеку. Имплементирана је са два паметна уговора: *SmileyGovernor* и *TimeLock*.

TimeLock паметни уговор само наслеђује *Timelock-Controller* из раније поменуте библиотеке. Улога овог паметног уговора јесте та да се након сваког успешног предлога трансакције које је потребно извршити додају у овај паметни уговор, затим се чека унапред дефинисан период а након тога је могуће извршити те трансакције. У овом систему трансакције ће моћи додавати само *SmileyGovernor*, а то ће радити након што неки предлог буде изгласан.

SmileyGovernor садржи логику везану за предлоге и гласање. Уговор користи друге паметне уговоре из *OpenZeppelin* библиотеке и повезује их у једну целину. *DAO* је у *OpenZeppelin* библиотеци реализован модуларно, где је основа апстрактни уговор *Governor* који садржи основу логику за додавање предлога и гласања и позива апстрактне функције које је потребно преклопити и реализовати жељену логику. У понуди су и други паметни уговори који имплементирају поједине апстрактне функције на начине које се најчешће користе у индустрији, тако да је могуће искористити вишеструко наслеђивање и на тај начин креирати целокупно решење. То је управо приступ који је употребљен у овом раду.

У наставку су дати описи паметних уговора који су наслеђени из *OpenZeppelin* библиоеке. *Governor-CountingSimple* служи за бројање гласова и нуди три врсте гласова: за, против и уздржан. *GovernorVotes-QuorumFraction* рачуна да ли је прикупљен довољан број гласова од укупног броја. *GovernorTimelock-Control* контролише *TimeLock* уговор, односно садржи логику која ће додати трансакције у *TimeLock* када се неки предлог изгласа. Такође може да мења и његове временске параметре.

5. ЗАКЉУЧАК

У овом раду описани су основне карактеристике и начин функционисања блокчејн технологије, уз акценат на *Ethereum* блокчејн. Иако је блокчејн првобитно кориштен за размену дигиталног новца, његова популарност и употреба непрестано се шире кроз многе друге сфере. Примене блокчејна расту непрекидно и у будућности ће свакако бити све више области у којима се примењује ова технологија.

Рад се фокусира на употребу замењивих и незамењивих токена на блокчејну и на управљачке структуре на блокчејну као што су независне децентрализоване организације. Употреба токена на блокчејну има многе примене, од креирања нових криптовалути, стварања дигиталних уметничких колекција па све до улазница за догађаје.

Организације на блокчејну елиминишу потребу за централизованим ентитетом ком остали учесници морају да верују и у потпуности елиминише потребу за поверењем. У раду је представљен и начин функционисања аукција на блокчејну.

Описана је употреба незамењивих токена у потпуности смештених на блокчејну. Предност оваквих токена лежи у томе што не постоји ризик да ће подаци нестати као што се дешавало раније са неким токенима који су метаподатке смештали на централизованим серверима. Овакав приступ има и своје мане, а једна од највећих јесте цена постављање података на блокчејн која може бити велика.

Рад може да послужи за упознавање са основним концептима *Ethereum* блокчејн технологије, као и начину функционисања замењивих и незамењивих токена и децентрализованих независних организација направљених употребом паметних уговора.

6. ЛИТЕРАТУРА

[1] https://www.forbes.com/advisor/investing/-cryptocurrency/what-is-blockchain/ (приступљено у марту 2023.)
[2] https://crypto.com/university/consensus-mechanisms-in-blockchain (приступљено у марту 2023.)
[3] https://101blockchains.com/introduction-to-blockchain-features (pristupljeno u martu 2023.)
[4] https://ethereum.org/en/developers/docs/intro-to-ethereum/ (приступљено у марту 2023.)
[5] https://www.ibm.com/topics/smart-contracts (приступљено у марту 2023.)
[6] https://cointelegraph.com/learn/fungible-vs-nonfungible-tokens-what-is-the-difference (приступљено у марту 2023.)
[7] https://eips.ethereum.org/EIPS/eip-20 (приступљено у марту 2023.)
[8] https://www.businessinsider.com/personal-finance/nft-meaning (приступљено у марту 2023.)
[9] https://eips.ethereum.org/EIPS/eip-721 (приступљено у марту 2023.)
[10] https://www.investopedia.com/tech/what-dao/ (приступљено у марту 2023.)

Кратка биографија:

Стеван Рашковић рођен је Руми 1996. године. Мастер рад на Факултету техничких наука из области Рачунарство и аутоматика – Електронско пословање одбранио је 2023. године.

контакт: lordsteva@gmail.com