Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/26BE25Kljestan

ДЕЦЕНТРАЛИЗОВАНИ СОФТВЕРСКИ СИСТЕМ ЗА ЗАШТИТУ ДИГИТАЛНОГ САДРЖАЈА ПРИМЈЕНОМ КОНЦЕПАТА BLOCKCHAIN ТЕХНОЛОГИЈЕ

DECENTRALIZED SOFTWARE SYSTEM FOR SECURING DIGITAL ASSETS USING THE CONCEPTS OF BLOCKCHAIN TECHNOLOGY

Марија Кљештан, *Факултет техничких наука, Нови Сад*

Област – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У овом раду описана је имплементација децентрализованог система који омогућава корисницима да обезбиједе свој дигитални садржај креирајући незамјенљиви токен на Ethereum платформи, а чији метаподаци су смјештени на IPFS дистрибуираном систему. Поред тога, описани су основни концепти blockchain технологије.*

Кључне ријечи: *децентрализовани системи, блокчејн, Ethereum, незамјенљиви токени*

Abstract – *This paper describes the implementation of a decentralizes system that allows users to secure their digital content by creating NFT on Ethereum blockchain, which metadata is stored on IPFS. Also, this paper gives introduction to the fundamentals of distributed systems and blockchain technology.*

Keywords: *decentralized systems, blockchain, Ethereum, non-fungible tokens*

1. УВОД

Blockchain технологија стекла је велику популарност након увођења биткоина 2009. године. Још од тада, много корисника посматра блокчејн технологију искључиво из перспективе биткоина и система плаћања.

Међутим, *blockchain* као дистрибуирана дијељена главна књига, која обезбјеђује интегритет и непромјенљивост сачуваних података, без учешћа посредничких страна, нашла је широку примјену како у области финансија, пољопривреде, здравства, туризма, образовања и сличних области, тако и у умјетности, гдје су од посебне важности незамјенљиви токени [1].

Овај рад бави се безбједним чувањем и утврђивањем власништва дигиталог садржаја. Чување се врши на *IPFS* дистрибуираном систему, а историја власништва је трајно сачувана на *Ethereum blockchain*-у употребом незамјенљивих токена. У раду су детаљно описане теоријске основе свих концепата примијењених у имплементацији система.

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

2. ТЕОРИЈСКЕ ОСНОВЕ

2.1. Blockchain

Blockchain је дистрибуирана, дијељена главна књига (енг. *ledger*) која складишти трансакције и која не може бити измијењена након што се трансакција верификује и дода у књигу [1]. Трансакције се групишу у блокове, при чему је свака трансакција обезбјеђена криптографским методама и валидирана од стране сваког овлашћеног члана мреже, коришћењем консензус алгоритама, тј. скупа правила за валидацију. Трансакција коју нису потврдили сви чланови мреже се не додаје у базу података. Свака трансакција је везана за претходну трансакцију у секвенцијалном редослиједу, стварајући ланац трансакција, односно блокова. Трансакција се не може избрисати или измијенити, једини начин за измјену је додавање друге трансакције у ланац. Осим тога, у *blockchain* системима елиминише се потреба за постојањем централизованог ентитета, који имају контролу над цијелим системом и којем сви морају вјеровати [2].

2.2. Ethereum

Ethereum представља децентрализовани систем који покреће рачунар под називом *Ethereum* Виртуелна Машина (*EVM*). Свако ко учествује у *Ethereum* мрежи (сваки *Ethereum* чвор) чува копију стања овог рачунара. Поред тога, сваки учесник може да емитује захтјев да овај рачунар изврши произвољно израчунавање. Кад год се такав захтјев емитује, други учесници на мрежи верификују, потврђују и извршавају прорачун. Ово извршење изазива промјену стања у *EVM*-у, која се пропагира кроз цијелу мрежу. Захтјеви за израчунавање се називају захтјеви за трансакције, а евиденција о свим трансакцијама и тренутном стању *EVM*-а се чува на *blockchain*-у [3].

Сваки рачунар (чвор) у мрежи мора да се сложи око додавања сваког новог блока у ланац. Чворови осигуравају да сви који ступају у интеракцију са *blockchain*-ом имају исте податке. Како би се ово постигло, *Ethereum* користи *Proof of Stake* (*PoS*) консензус механизам [4].

Ether (*Eth*) је криптовалута која се користи на *Ethereum* мрежи.

Ethereum стање састоји се од објеката који се зову налози. Налог представља мапирање између адресе и стања налога. То је ентитет који посједује *Ether* (*Eth*)

биланс и стога може да обавља трансакције на *Ethereum* мрежи. Постоје 2 типа налога - налози који су контролисани од стране корисника и налози паметних уговора [5].

2.3. Паметни уговори

Увођењем паметних уговора, *Ethereum* платформа је омогућила корисницима да поред обављања трансакција и трговања криптовалутама, користе и чувају незамјенљиве токен, креирају децентрализоване апликације и још много тога због чега се *Ethereum* сматра представником 3. генерације веба [3].

Паметни уговори су рачунарски програми који се чувају на *blockchain*-у и извршавају се на *Ethereum* виртуелној машини. Сваки паметни уговор се састоји од кода који специфицира унапријед одређене услове који, када се испуне, покрећу њихово извршавање. Покретањем на децентрализованој платформи, умјесто на централизованом серверу, паметни уговори омогућавају да више страна дођу до заједничког резултата на прецизан, благовремен и безбједан начин, без учешћа централног администратора [6].

Паметни уговори се углавном пишу у програмским језицима високог нивоа, од којих је најпопуларнији *Solidity*. С обзиром на чињеницу да *EVM* може да извршава програме написане у језицима ниског нивоа, паметни уговори писани у језицима вишег нивоа преводе се у *EVM Bytecode* који посједује посебан скуп инструкција за интерпретирање кода паметних уговора.

2.4 Незамјенљиви токени

Попут физичког новца, криптовалуте су обично замјенљиве, што значи да се њима може трговати и да се могу размјењивати једна за другу. Такође, могу се дијелити на мање фракције.

Незамјенљиви токени (енг. *Non-Fungible Token, NFT*) мијењају крипто парадигму чинећи сваки токен јединственим и незамјенљивим, односно чинећи немогућим да један незамјенљив токен буде „једнак“ другом токену. Они су дигитална репрезентација средстава и могу се упоредити са дигиталним пасошима, јер сваки токен садржи јединствени, непреносиви идентитет који га разликује од других токена. Осим тога, ови токени су недјељиви, односно не могу се подијелити на мање фракције [7].

NFT-ови су направљени у складу са стандардом *ERC*-721 (*Ethereum Request for Comment*#721), који диктира како се власништво токена преноси, методе за валидацију трансакција и како апликације рукују безбједним трансферима токена [7].

Поменути стандард се односи и на метаподатке токена. Када је ријеч о складиштењу метаподатака, они се попут самог токена, могу складиштити на *blockchain*-у. Међутим, у том случају долази до проблема перформанси и складиштења података *blockchain* система. Због тога се метаподаци чешће складиште ван *blockchain*-а (енг. *offchain*) на централизованим серверима или дистрибуираним системима, као што је *IPFS*, који је кориштен и у овом раду [8].

2.5 Децентрализоване апликације и *Web* 3.0

Децентрализована апликација (*DApp*) је апликација изграђена на децентрализованој мрежи, која комбинује паметне уговоре и кориснички интерфејс [9].

Децентрализована апликација има свој позадински код, у виду паметних уговора, који се извршавају на децентрализованој мрежи, насупрот традиционалним апликацијама, у којима се позадински код извршава на централизованим серверима.

DApp може да има клијентску страну написану на било ком језику (као и у случају централизоване апликације) која упућује позиве свом позадинском дијелу.

Уводећи децентрализацију у све аспекте веб апликација, као што су складиштење, размјена порука и слично, децентрализоване апликације су преусмјериле развој веба. Термин који се користи да опише нови правац у еволуцији веба јесте *web3*, означавајући при томе трећу "верзију" веба [6].

2.6 *IPFS*

IPFS (енг. *Inter Planetary File System*) је *peer-to-peer* (*P2P*) дистрибуирани систем за складиштење, приступ и дијељење датотека, вебсајтова, апликација и података [8].

Кључна разлика између централизованог и децентрализованог веба је у томе како се подаци идентификују и преузимају. У централизованом вебу, корисници зависе од поузданих ентитета који чувају њихове податке и приступају им помоћу јединствених локатора ресурса (*URL*-ова) заснованих на локацији.

Насупрот томе, *IPFS* мрежа користи систем адресирања садржаја, гдје сам садржај има кључну улогу у омогућавању корисницима да пронађу оно што траже. У *IPFS*-у, сваки дио садржаја је идентификован јединственим хешом који се зове *CID* (*Content Identifier*). То значи да се садржај чува и преузима на основу његовог хеша, а не његове локације, што га чини много тежим за цензурисање или манипулацију.

3. МОДЕЛ СИСТЕМА

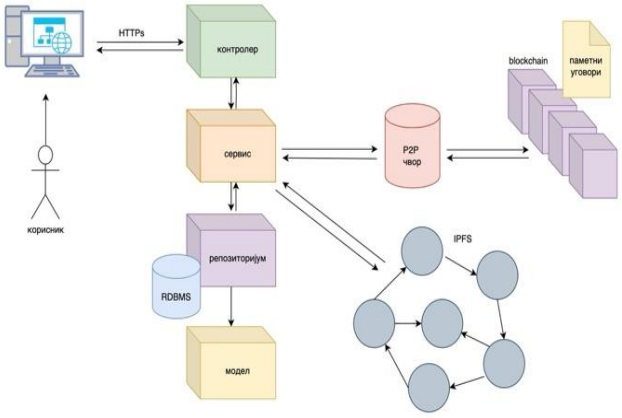
Намјена система којим се бави овај рад јесте да омогући корисницима да сачувају свој дигитални садржај од вриједности на сигуран начин, тако што корисник путем корисничког интерфејса унесе свој дигитални садржај у облику датотеке, која се чува на дистрибуираном систему, а затим се креира *NFT* позивом паметног уговора који се извршава на *blockchain* мрежи, као и да корисник има преглед својих *NFT*-ова везаних за одређени дигитални новчаник.

Систем је развијен као децентрализована веб апликација, са одвојеним клијентским и серверским дијелом, а дијаграм њене архитектуре представљен је на сл. 1.

Клијентска страна представља апликацију која се извршава у прегледачу (енг. *browser*). Серверску страну чини монолитна апликација која се састоји од модула, тако да подржава вишеслојну архитектуру.

Ова апликација комуницира са *IPFS* мрежом, ради складиштења датотека које је корисник унио, као и са ентитетима *blockchain* мреже, како би позивала функције паметног уговора за креирање и добављање корисникових *NFT*-ова.

Иако садржи елементе који су карактеристични за традиционалне веб апликације, функционалности које су од суштинског значаја као што су складиштење дигиталног садржаја и управљање *NFT*-овима, имплементиране су примјеном принципа *blockchain* технологије и дистрибуираних система, чиме се ова апликација може сматрати децентрализованим софтверским рјешењем.



Слика 1. *Дијаграм архитектуре система*

4. ИМПЛЕМЕНТАЦИЈА

За имплементацију клијентске стране кориштена је *React.js* библиотека, заједно са *ether.js* скупом библиотека које омогућавају интеграцију са дигиталним крипто новчаницима, као што је *MetaMask*, новчаник уграђен у веб претраживач, а омогућава да корисници повежу свој *Ethereum* налог са налогом на систему и на тај начин уз пар корака креирају нове *NFT*-ове.

Серверску страну апликације чине паметни уговори који су писани у *Solidity* програмском језику, који представља објектно оријентисани програмски језик, специфично намијењен за имплементацију паметних уговора. За развој и поставку паметних уговора на *Ethereum* мрежу коришћен је *Truffle* радни оквир. Паметни уговори су уз помоћ овог окружења постављени на *Sepolia* тестну *Ethereum* мрежу.

За складиштење докумената и *NFT* метаподатака кориштен је *IPFS* чиме је обезбјеђено *offchain* складиштење података, које доприноси очувању ефикасности и перформанси *blockchain* мреже. Комуникација са *IPFS* и блокчејн мрежом врши се преко монолитне веб апликације имплементиране у *Golang* програмском језику.

4.1 Повезивање са blockchain мрежом

Како би могле да користе услуге *Ethereum* платформе, децентрализоване апликације морају да се повежу на *peer-to-peer* мрежу, што може довести до успореног развоја апликације још у почетној фази развоја. Када би се покретао нови чвор у мрежи, његова синхронизација са *Ethereum blockchain*-ом би могла потрајати сатима, па чак и данима.

Ове проблеме рјешава *Infura* сервис, платформа која нуди инфраструктуру и алате потребне за брже, лакше и ефикасније повезивање децентрализованих апликација са *Ethereum* мрежом. Употребом тих алата, развојни тимови не морају да брину о синхронизацији или сложеном конфигурисању чворова како би се повезали на *Ethereum* мрежу.

Ethereum API који пружа *Infura* нуди инстант приступ *Ethereum blockchain* мрежи преко *WebSocket*-а и *HTTPS*-а, што представља једну од највећих предности употребе овакве платформе.

Поред главне *Ethereum* мреже (енг. *Mainnet*), постоје и тестне мреже. Ове мреже користе углавном развојни тимови приликом имплементације паметних уговора, како би их тестирали у окружењу сличном продукционом, прије постављања на главну мрежу.

Sepolia мрежа је препоручена подразумијевана тестна мрежа за развој апликација и кориштена је приликом имплементације овог система.

4.2 Паметни уговор NFT

За поставку овог паметног уговора на *Sepolia* тестну мрежу, кориштен је *Truffle* радни оквир, који омогућава бржи развој и поставку паметних уговора.

С обзиром да се ради о *NFT* колекцији, за основне операције над токенима које су прописане стандардом, наслијеђени су паметни уговори из *OpenZeppelin* библиотеке, што се може видјети на листингу 1.

```
contract NFT is ERC721URIStorage, Ownable {
    using Counters for Counters.Counter;
    Counters.Counter private _tokenIds;
    constructor() ERC721("NFT", "NFT collection") {}

    function mintNFT(address recipient, string memory tokenURI)
    public onlyOwner
    returns (uint256)
    {
        _tokenIds.increment();
        uint256 newItemId = _tokenIds.current();
        _mint(recipient, newItemId);
        _setTokenURI(newItemId, tokenURI);
        return newItemId;
    }
}
```

Листинг 1. *Функција за генерисање NFT-а*

Функција *mintNFT* представљена на листингу 1 служи за креирање новог токена и има 2 параметра. Први

параметар је *Ethereum* адреса налога који је иницирао трансакцију за креирање токена, а други параметар представља адресу метаподатака *NFT*-а, смјештених на *IPFS*-у. Приликом креирања токена, користи се бројач који се инкрементира за 1, а затим се позива *_mint* функција која генерише токен у власништву корисника са прослијеђеном адресом. Затим се новокреирани токен повезује за адресом метаподатака позивом функције *_setTokenURI*.

4.3 Интеграција са крипто новчаником

MetaMask је дигитални крипто новчаник који представља интерфејс за интеракцију са чворовима *blockchain* мреже. Подразумијевано се повезује на *Infura* чвор, али се може повезати и на чвор који је покренут локално.

Приликом иницирања трансакције за креирање *NFT*-а, апликацији је потребна адреса корисниковог *Ethereum* налога, како би се одредило у чијем власништву је креирани токен на *Ethereum* мрежи. Најбезбједнији, и за корисника најједноставнији, начин добављања његове адресе јесте увезивање апликације са *MetaMask* новчаником корисника.

JavaScript библиотека која омогућава интеграцију децентрализованих апликација са *Ethereum* мрежом јесте *Ether.js*. Ова библиотека омогућава и интеграцију апликација са крипто новчаницима. На листингу 2 представљен је дио кода из клијентске апликације који врши добављање тренутног биланса корисниковог налога.

```
function connectToMetaMaskBtnHandler() {
      if (window.ethereum) {
            window.ethereum
            .request({ method: "eth_requestAccounts" })
            .then((res) => {
                  accountChangeHandler(res[0])
            });
      } else {
            alert(" please, install metamask extension!!");
      }
}
const getbalance = (address) => {
      window.ethereum
      .request({
            method: "eth_getBalance",
            params: [address, "latest"]
      })
      .then((balance) => {
            setdata({
                  Balance: ethers.utils.formatEther(balance),
            });
      });
};
```

Листинг 2. *Интеграција са MetaMask новчаником*

5. ЗАКЉУЧАК

Blockchain технологија представља радикалан и нови, а притом безбједан и транспарентан начин обављања свих врста трансакција преко интернета, свима доступног медија за пренос података. Појава *bitcoin*-а и *blockchain*-а довела је до многих промјена у свијету финансија, али и пољопривреде, медицине, туризма, логистике, спорта, па чак и умјетности.

NFT-ови, или незамјењиви токени, представљају токене засноване на *blockchain* технологији, који омогућавају дигиталну репрезентацију физичких или дигиталних средстава. Ова релативно нова технологија пружа могућност праћења власништва над имовином и провјере њене аутентичности, омогућавајући већу транспарентност. Као резултат тога, имовином се може релативно лако трговати, а процес преноса власништва је неупоредиво бржи због изостанка посредничких страна.

Овај рад се бавио примјеном концепата *blockchain* технологије и незамјењивих токена за рјешавање проблема безбједног и ефикасног чувања дигиталних средстава корисника. Поред *blockchain*-а, кориштена је и сродна технологија заснована на концептима дистриубуираних система - *IPFS*.

Рад може да послужи као основа за упознавање са концептима *blockchain* технологије, незамјењивих токена, децентрализованих апликација изграђених на *Ethereum* платформи, али и система попут *IPFS*-а.

6. ЛИТЕРАТУРА

[1] H. Natarajan, S. Krause, H. Gradstein, „*Distributed Ledger Technology and Blockchain*“, *FinTech Note*, 2017.

[2] R. Shaan, „*Blockchains: The technology of transactions*“ , Towards Data Science, 2018.

[3] D. Vujicic, D. Jagodic, S. Randic, *„Blockchain technology, bitcoin, and Ethereum: A brief overview“, 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1-6, 2018.

[4] J. Wi, „*Blockchain without Waste: Proof-of-Stake*“, The Review of Financial Studies, т. 34, бр. 3, pp. 1156-1190, 2021.

[5] https://ethereum.org/en/developers/docs/nodes-and-clients/ (приступљено у септембру 2023.)

[6] V. Buterin, „*A next-generation smart contract and decentralized application platform*“, white paper, т. 3, бр. 37, 2014.

[7] R. Sharma, „*Non-Fungible Token (NFT): What It Means and How It Works*“, 2023.

[8] J. Benet, „*IPFS - Content Addressed, Versioned, P2P File System*“, Cornell University, 2014.

[9] https://ethereum.org/en/developers/docs/dapps/ (приступљено у септембру 2023)

Кратка биографија:

Марија Кљештан рођена је у Лозници 1999. године. Мастер рад на Факултету техничких наука из области Рачунарство и аутоматика – Примењене рачунарске науке и информатика одбранила је 2023. године.

контакт: marijakljestan@gmail.com