Зборник радова Факултета техничких наука, Нови Сад

УДК: 004.9
ДОИ: https://doi.org/10.24867/27BE16Pavkovic

ДЕЦЕНТРАЛИЗОВАНА АПЛИКАЦИЈА ЗА БЕЗБЕДНО ДИСТРИБУИРАНО ЧУВАЊЕ ПОДАТАКА ПРИМЕНОМ БЛОКЧЕЈН ТЕХНОЛОГИЈЕ

DECENTRALIZED APPLICATION FOR SECURE DISTRIBUTED DATA STORING USING THE CONCEPTS OF BLOCKCHAIN TECHNOLOGY

Николина Павковић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Овај рад се бави развојем децентрализоване апликације за безбедно дистрибуирано чување података применом блокчејн технологије, односно развојем апликације која врши безбедно складиштење докумената. Анализом традиционалних централизованих решења за складиштење података примећено је да имају доста проблема са безбедношћу, скалабилношћу и доступношћу када се чува већа количина података. Задатак овог рада јесте да представи модерне технологије које помажу у превазилажењу наведених недостатака. Поред тога, описује имплеметацију једног од више могућих решења.*

Кључне речи: *блокчејн, Етеријум, паметни уговори, ИПФС*

Abstract – *This paper describes the development of a decentralized application for secure distributed data storing using the concepts of blockchain technology, or to be more specific, an application that performs secure document storing. By analyzing the traditional centralized data storing solutions, many problems concerning security, scalability and availability have been detected when storing large data. The purpose of this paper is to present modern technologies that can be used to overcome the mentioned shortcomings. Additionally, it describes the implementation of one of several possible solutions.*

Keywords: *blockchain, Ethereum, smart contracts, IPFS*

1. УВОД

Блокчејн (енгл. *Blockchain*) технологија у потпуности мења начин на који веб програмирање функционише и довела је до увођења нове парадигме под називом Веб 3.0 (енгл. *Web 3.0*).

Ова технологија стекла је велику популарност након увођења Биткоина (енгл. *Bitcoin*) 2009. године. Биткоин користи блокчејн искључиво као део система за плаћање, иако постоје многе друге области примена блокчејн технологије, као што су фунансије, пољопривреда, здравство, логистика, и тако даље.

У ери коју карактерише експоненцијални раст дигиталних података и све већа зависност од услуга у облаку, сигурно и ефикасно чување докумената постало је све важнија брига. Доба дигитализација радикално је изменило начин складиштења и приступања информацијама. Традиционални локални системи складиштења докумената све више нису довољни за управљање обимом и разноликошћу података које генерише савремени свет. Проблеми као што су губљење података, кварови хардвера, сајбер безбедносне претње подстакли су развој иновативних софтверских решења заснованих на блокчејну. Ова решења обећавају отпорност података, доступност и сигурност, често користећи дистрибуиране архитектуре складиштења као кључни елемент.

Циљ овог рада је да покаже како Етеријум (енгл. *Ethereum*) блокчејн платформа може бити искоришћена за развој решења у области децентрализованог и дистрибуираног складиштења података.

2. ТЕОРИЈСКЕ ОСНОВЕ

Како би објаснило на који начин Етеријум платформа која је коришћена за имплементација решења и како је дошло до њеног развоја, потребно је кренути од основних концепата на којима се она заснива.

2.1. Блокчејн

Блокчејн је вид имплементације дистрибуиране главне књиге која складишти трансакције и која не може бити измењена након што се трансакција верификује и дода у књигу. Свака трансакција је обезбеђена криптографским методама и валидирана од стране свако овлашћеног члана мреже коришћењем консензус алгоритма. Трансакција која није потврђена од стране свих чланова мреже се не додаје у базу података. Свака трансакција је део блока и сваки блок је везан за претходни у секвенцијалном редоследу стварајући ланац блокова. Трансакција се не може избрисати нити изменити, једини начин за измену је додавање нова трансакције у ланац блокова – блокчејн [1].

Постоји неколико типова блокчејна који се међусобно разликују по моделу пермисија у систему, који дефинише ко може да управља мрежом и да додаје нове блокове. Постоје јавни, приватни и хибридни блокчејн. У хибридни блокчејн спада конзорцијум [2].

НАПОМЕНА:

Овај рад проистекао је из мастер рада чији ментор је био др Душан Гајић, ванредни професор.

2.2. Паметни уговори

Паметни уговор је програм који се аутоматски извршава на блокчејну, када се испуне услови дефинисани уговором. Паметни уговори омогућавају да се трансакције и споразуми спорводе између различитих, анонимних страна, без потребе за централним органом, правним системом или неком трећом посредничком страном. Управо паметни уговори проширују функционалности блокчејна тако што пружа механизам којим је могуће дефинисати услове који, уколико су испуњени, резултују извршавањем трансакције. Паметне уговоре је 1994. године први предложио Ник Сабо [3].

Паметни уговор садржи тренутно стање, приватно складиште и извршни код. Стање уговора је складиштено на блокчејну и ажурира се сваки пут кад се активира и изврши паметни уговор. Једном кад се паметни уговор постави на мрежу, није га могуће накнадно изменити [3].

2.3. Етеријум

Етеријум је децентрализована блокчејн платформа заснована на П2П (енгл. *P2P – peer-to-peer*) мрежи, која омогућава безбедно извршавање и верификацију паметних уговора. Увођењем паметних уговора, Етеријум платформа је омогућила корисницима да врше трансакције, тргују крипто валутама, користе и чувају незамењиве токене, играју игрице, користе друштвене медије и још много тога [4].

Виталик Бутерин је креирао Етеријум пројекат као реакцију на недостатке Биткоина. Бутерин је 2013. објавио „Бели папир“ (енгл. *White paper*) Етеријума, са детаљима о паметним уговорима, непромењивим „ако-онда“ (енгл. *„if-then“*) исказима, који омогућавају развој децентрализованих апликација [5].

Етеријум је јавни блокчејн, представља ланац блокова са уграђеним рачунаром. У Етеријуму постоји један, канонски рачунар (познат као Етеријум Виртуелна Машина или EBM) чије стање сви на Етеријум мрежи прихватају као глобално главно стање. Сви учесници мреже (сваки Етеријум чвор) чувају копију стања овог рачунара. Поред тога, сваки учесник може послати захтев овом рачунару да изврши произвољно рачунање – трансакцију. Када се такав захтев пошаље, други учесници на мрежи проверавају, потврђују и извршавају трансакцију. Криптографски механизми обезбеђују да када трансакције буду верификоване као валидне и додате у ланац блокова, оне се не могу мењати касније [6].

Етер (енгл. *ether*) је домаћа крипто валута Етеријума, чија је сврха да пружи економски подстицај учесницима да верификују и изврше трансакције и обезбеде рачунарске ресурсе мрежи. Сваки учесник који емитује захтев за трансакцију мора понудити и одређену количину етера мрежи као накнаду и награду ономе ко на крају обави посао верификације трансакције, извршавања и чувања у ланцу блокова. Такође, накнаде спречавају злонамерне кориснике да намерно загушују мрежу захтевима за извршење бесконачних петљи. Деноминације етера су веи (енгл. *wei*) и гвеи (енгл. *gwei*) [7].

Етеријум налог је ентитет са етер балансом (стањем налога, „стањем рачуна“) који може да шаље трансакције на Етеријуму. Постоје два типа налога: налози у екстерном власништву и уговорни налози. Налози у екстерном власништву су они који могу бити контролисани од стране корисника. Уговорни налози су испоручени на мрежу као паметни уговори и контролисани су кодом тог уговора [8].

2.4. Децентрализоване апликације и Веб 3.0

Децентрализована апликације је апликације изграђена на децентрализованој мрежи која комбинује паметни уговор и кориснички интерфејс. Децентрализована апликација има позадински код смештен на П2П мрежи, за разлику од централизованих апликација чији се код извршава на централизованим серверима. Називају се децентрализованим јер се извршавају на јавној децентрализованој Етеријум платформи, на којој ниједан појединац, нити група нема контролу. Неке од предности развоја децентрализованих апликацију су да нема застоја, да је приватна јер корисници из реалног света не морају да открију свој идентитет како би интераговали са апликацијом, чува интегритет података јер су подаци који се складиште на блокчејну непромењиви и неоспорни [9].

Децентрализоване апликације су увеле децентрализацију са П2П протоколима у све аспекте веб апликација, као што су складиштење, размена порука, и тако даље. Тиме су преусмериле развој веб програмирања. Термин који се користи да опише нови правац у еволуцији веба јесте Веб 3, означавајући трећу верзију веба. Гевин Вуд је први предложио термин Веб 3, репрезентујући нову визију и фокус веб апликација: од централно поседованих и управљаних апликација до апликација изграђених на децентрализованим протоколима [9].

2.4. ИПФС

ИПФС (енгл. *IPFS – Inter Planetary File System*) је П2П дистрибуирани систем за складиштење, приступ и дељење датотека, веб сајтова, апликација и података. Стекао је популарност због револуционарног приступа складиштења података који представља алтернативу традиционалној клијент-сервер архитектури [10].

У ИПФС-у сваки део садржаја је идентификован јединственим хешом који се зове ЦИД (енгл. *CID – Content Identifier*). Садржај се чува и преузима на основу његовог хеша, а не његове локације (што је случај код традиционалних система), и то га чини тежим за цензурисање или манипулацију [10].

ИПФС има потенцијал да побољша скалабилност децентрализованих апликација на платформама као што је Етеријум. Интеграцијом са Етеријум паметним уговорима, ИПФС може да обезбеди сигурно и исплативо складиштење унутар крипто екосистема, побољшавајући перформансе Етеријума [10].

3. АРХИТЕКТУРА И НАМЕНА СИСТЕМА

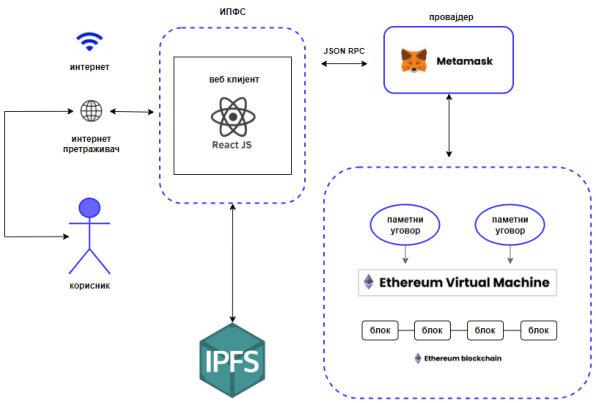
Намена система јесте да омогући корисницима да сачувају свој дигитални садржај на сигуран начин,

тако што корисник путем корисничког интерфејса постави документ који жели да сачува. Тада се креира позив ка ИПФС-у и чува се документ. Корисници такође имају могућност прегледа и брисања сачуваних докумената. Ради се о апликацији која има мали број функционалности и опција на корисничком интерфејсу. Једини вид аутентификације у систему јесте увезивање са крипто новчаником корисника, које је неопходно да би корисник могао да отпреми или обрише сачувана документа јер то у позадини изискује плаћање накнаде како би се трансакција извршила на Етеријуму.

Постоје два приступа приликом чувања фајлова на блокчејну. Документи могу да се чувају директно на ланцу, и могу да се чувају ван ланца. Оба начина имају своје предности и мане. Чување докумената директно на ланцу представља скуп начин чувања јер се подаци чувају унутар сваког блока у ланцу, међутим уколико дође до напада, подаци се могу вратити и искористити. Уколико се документи чувају ван ланца, на ланцу чувамо само мета податке. Сам садржај документа се не налази на ланцу, него на неком дистрибуираном складишту података што представља исплатив метод складиштења података.

Намена апликације јесте да покаже принцип чувања фајлова ван ланца, док се мета подаци чувају директно на блокчејну. Када се документ сачува на ИПФС, добије се ЦИД који представља идентификатор документа који омогућава његово лако добављање. Управо се тај ЦИД прослеђује паметном уговору и чува на ланцу. Уколико имамо сачуван ЦИД, увек можемо да приступимо документу на ИПФС-у.

Систем је развијен као децентрализована Веб 3.0 апликација, са одвојеним клијентским делом који комуницира са паметним уговорима испорученим на блокчејн, што је приказано на слици 1.



Слика 1. *Архитектура система*

Апликација не поседује серверску страну. Захваљујући томе, представља чист пример Веб 3.0 апликације која укључује клијентску страну која комуницира са паметним уговорима на блокчејну. Тиме што је избегнуто коришћење серверске стране, избегнуто је и ослањање на традиционалне системе по питању централизације. Када би постојао и сервер са којим веб клијент комуницира, постојала би и тачка која би чинила овај систем делимично централизованим.

4. ИМПЛЕМЕНТАЦИЈА СИСТЕМА

За имплементацију клијентске стране кориштен је Реакт.јс (енгл. *React.js*) радни оквир, заједно са веб3.јс (енгл. *web3.js*) скупом библиотека које омогућавају интеграцију са дигиталним новчаницима. На пример, као што је МетаМаск (енгл. *MetaMask*) новчаник уграђен у веб претраживач, а омогућава да корисници повежу свој Етеријум налог са налогом на систему и на тај омогући да корисници интерагују са паметним уговорима. МетаМаск је Етеријум провајдер (енгл. *provider*).

Поред клијентске апликације постоје и паметни уговори који су написани у програмском језику Солидити (енгл. *Solidity*). То је објектно оријентисан програмски језик, Тјуринг комплетан, специфично намењен за имплементацију паметних уговора. За развој и испоруку паметних уговора кориштен је радни оквир Трафл (енгл. *Truffle*). Приликом развоја апликације паметни уговори су за потребе тестирања испоручивани на тест мрежу Ганаш (енгл. *Ganache*), а касније на Сеполију (енгл. *Sepolia*). Тест мреже се користе јер би се у супротном за свако тестирање паметног уговора трошила права средства.

Како би се ступило у интеракцију са било којом блокчејн мрежом потребно је прикључити јој се. Покретање чвора захтева пристојан ниво техничког знања, стрпљења, процесорске снаге и меморије. То представља једну од најтежих баријера за усвајање блокчејна и коришћењем Инфуре та баријера је превазиђена. Инфура (енгл. *Infura*) представља скуп чворова, кластер. Може се посматрати као скуп алата који пружа своје услуге за интеграцију апликација са Етеријум мрежом, али и другим децентрализованим платформама попут ИПФС-а. Да би се користиле услуге Инфуре, све што је потребно јесте креирати налог на Инфура веб сајту и након тога верификовати имејл (енгл. *email*) адресу повезану са креираним налогом [11].

Апликација користи паметни уговор који садржи функције за чување, брисање и добављање докумената са ланца. На листингу 1 се може видети једна од претходно поменутих функција, функција за чување ЦИД-а на блокчејн. Функција прима 2 параметра, назив документа чији ЦИД чувамо и сам ЦИД тог документа. Пре него што се ЦИД сачува, прво се проверава да ли он већ постоји. Уколико постоји, неће бити поново додат. Да би клијентска страна могла да позива функције паметног уговора, неопходно је да има његов АБИ (енгл. *ABI – Application Binary Interface*) који је аутоматски генерисан приликом превођења (енгл. *compile*) кода. Паметни уговори писани су језицима високог нивоа. Приликом испоруке паметног уговора на блокчејн испоручује се бајт код који је резултат компајлирања, не изворни код. АБИ омогућава мапирање функција високог нивоа на бајт код и обрнуто, прецизно

описује називе функција, параметре фунцкија, повратне вредности.

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

contract File{
    mapping(string => string) public files;
    string[] public mapKeys;

...

    function saveCID(string memory filename, string memory
cid) external {
        require(bytes(files[cid]).length == 0, "File with
CID already exists");
        files[cid] = filename;
        mapKeys.push(cid);
    }
}
```

Листинг 1. *Функција за чување ЦИД-а*

АБИ уговора је смештен на клијентској страни и учитава се помоћу фунцкије приказане на листингу 2.

```
import contract from "@truffle/contract";

export const loadContract = async (name, provider) => {
  const res = await fetch(`/contracts/${name}.json`);
  const Artifact = await res.json();

  const _contract = contract(Artifact);
  _contract.setProvider(provider);

  const deployedContract = await _contract.deployed();

  return deployedContract;
};
```

Листинг 2. *Учитавање паметног уговора помоћу његовог АБИ-а*

Након што је паметни уговор учитан, обезбеђено је једноставно приступање методама уговора, тако да се методе позивају као обична функција објекта паметног уговора као да се ради о било ком објекту неког објектно оријентисаног језика.

5. ЗАКЉУЧАК

Појава Биткоина и блокчејна довела је до многих промена у свету финансија али и пољопривреде, медицине, туризма, логистике, спорта, па чак и уметности. Блокчејн технологија нуди револуционарне могућности за сигурно, непромењиво и трајно чување докумената. Због својих основних карактеристика, идеалан је за решавање проблема фалсификације и губитка података који су широко распрострањени у различитим областима.

Чување докумената на блокчејну има потенцијал да модернизује начин на који се информацију чувају и начин на који се њима управља. Сигурност, непромењивост и транспарентност које блокчејн пружа представљају велики напредак у односу на традиционалне методе чувања. Иако су изазови и даље присутни, у будућности се може очекивати да ће блокчејн технологија наставити да расте и мења начин на који се документи чувају и обрађују.

6. ЛИТЕРАТУРА

[1] S. Nevil, E. Rasure и M. Reeves, „*Distributed Ledger Technology (DLT): Definition and How It Works*,“ урл: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp [Последњи приступ: октобар 2023]

[2] The Crypto learn, „*Types of Blockchain — Clear classification,*“ урл: https://medium.com/coinmonks/types-of-blockchain-clear-classification-79c6bce26f00 [Последњи приступ: октобар 2023]

[3] J. Frankenfield, E. Rasure и S. Kvilhaug, „*What Are Smart Contracts on the Blockchain and How They Work,*“ урл: https://www.investopedia.com/terms/s/smart-contracts.asp [Последњи приступ: октобар 2023]

[4] C. Smith, „*Intro to Ethereum,*“ урл: https://ethereum.org/en/developers/docs/intro-to-ethereum/ [Последњи приступ октобар 2023]

[5] T. Copeland, „*A brief history of Ethereum,*“ урл: https://www.theblock.co/learn/245716/a-brief-history-of-ethereum [Последњи приступ октобар 2023]

[6] S. Tikhomirov, „*Ethereum: State of Knowledge and Research Perspectives,*“ у International Symposium on Foundations and Practice of Security, 2018.

[7] C. Smith, „*Intro to Ether,*“ урл: https://ethereum.org/en/developers/docs/intro-to-ether/ [Последњи приступ: октобар 2023]

[8] J. Cook, „*Ethereum Accounts,*“ урл: https://ethereum.org/en/developers/docs/accounts/ [Последњи приступ: октобар 2023]

[9] J. F. Vañó Francés, „*Blockhain DApps,*“ LAB University of Applied Sciences, 2022.

[10] Consensys, „*An Introduction to IPFS,*“ урл: https://medium.com/@Consensys/an-introduction-to-ipfs-9bba4860abd0 [Последњи приступ: октобар2023]

[11] Medium, „*What is Infura,*“ урл: https://medium.com/what-is-infura/what-is-infura-59dbdd778455 [Последњи приступ oktobar 2023]

Кратка биографија:

Николина Павковић рођена је у Сомбору 15. фебруара 2000. године. Факултет техничких наука у Новом Саду, студијски програм Рачунарство и аутоматика уписала је 2018. године. Након завршених основних студија, 2022. године, уписала је мастер академске студије из исте области.

контакт: pavkovicn@hotmail.com