Зборник радова Факултета техничких наука, НовиСад

УДК: 4.75
ДОИ: https://doi.org/10.24867/34BE23Colovic

Развој од-краја-до краја шифрованог блокчејн протокола за преговоре и повраћај средстава након експлоатације на *Ethereum* мрежи

Development of an end-to-end encrypted blockchain protocol for negotiation and return of funds after an Ethereum network exploit

Алекса Чоловић, *Факултет техничких наука, Нови Сад*

Студијски програм – ПРИМЕЊЕНЕ РАЧУНАРСКЕ НАУКЕ И ИНФОРМАТИКА – ЕЛЕКТРОНСКО ПОСЛОВАЊЕ

Кратак садржај – *Овај рад представља RESET платформу децентрализовани Web3 протокол који омогућава сигурну, приватну и проверљиву комуникацију између компромитованих протокола и нападача. Рад описује архитектура система, коришћене технологије, имплементација паметних уговора и дизајн клијентске апликације.*

Кључне речи: *блокчејн, паметни уговори, Web3, Ethereum*

Abstract – *This paper presents RESET – a decentralized Web3 protocol enabling secure and verifiable post-exploit negotiations between hacked protocols and attackers. The paper describes system architecture, smart contract implementation and client application design.*

Keywords: *blockchain, smart contracts, Web3, Ethereum*

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

1. УВОД

Безбедност у децентрализованим финансијама (ДеФи) представља један од кључних изазова савремених блокчејн система. Упркос напретку у развоју паметних уговора и сигурносних механизама, хакерски напади на протоколе и даље су учестала појава, што доводи до значајних финансијских губитака. Према доступним подацима, само у 2022. години забележено је 231 великих сигурносних инцидената, са укупном штетом од око 3,7 милијарди долара [1]. Иако нападачи често нису мотивисани искључиво крађом, већ су спремни на преговоре и повраћај дела средстава у замену за избегавање правних последица, тренутни процес преговарања одвија се путем несигурних и неформалних канала, што отвара простор за манипулације и додатне ризике за нападаче.

RESET платформа решава овај проблем као децентрализовани *Web3* протокол који омогућава сигурну, приватну и проверљиву комуникацију између компромитованог протокола и нападача. Преговори се реализују путем енкриптованих порука чуваних на *Ethereum* мрежи, уз потпуну транспарентност трансакција. На тржишту тренутно не постоји познато решење које нуди сличан механизам, док се постојећи покушаји ослањају на *Web2* канале попут е-мејла или Телеграма, који не пружају гаранције приватности и интегритета. *RESET* уводи стандардизован процес без поверења за преговарање који је у потпуности на блокчејну, чиме се смањује ризик од манипулација и повећава вероватноћа постизања договора у безбедном окружењу.

Платформа омогућава власницима протокола да пријаве инцидент, дефинишу услове понуде за повраћај средстава, док нападачи могу да прихвате понуду или дају контрапонуду. Паметни уговори гарантују спровођење договорених услова без посредника, чиме се елиминише ризик од неиспуњених обавеза.

2. ПОЈАМ БЛОКЧЕЈН ТЕХНОЛОГИЈЕ

Блокчејн технологија је постала кључна основа за савремене дигиталне системе поверења, омогућавајући трансакције без посредника и централних ауторитета. Њена примена се посебно истиче у областима као што су финансије, управљање идентитетима и дигитална имовина, где су сигурност и транспарентност од пресудног значаја.

2.1. Дистрибуирани системи

Дистрибуирани систем чини скуп независних рачунарских елемената који кориснику делују као јединствена целина. Карактеришу га независност компоненти, њихова међусобна комуникација и кохерентност из угла корисника. У пракси, дистрибуирани системи често обухватају физички удаљене чворове ради веће доступности и отпорности на грешке.

2.2. Дистрибуирана главна књига

Дистрибуирана главна књига (енгл. *Distributed Ledger Technology* ДЛТ) представља специфичан тип дистрибуираног система без централног ауторитета, где учесници не морају веровати једни другима. Интегритет се обезбеђује криптографским механизмима и консензусним алгоритмима, што

омогућава децентрализацију, транспарентност и отпорност на манипулације. ДЛТ је основа за иновације попут ДеФи-а или НФТ-а.

2.3. Блокчејн

Блокчејн је најпознатија имплементација ДЛТ-а, заснована на линеарном ланцу криптографски повезаних блокова. Сваки блок садржи валидиране трансакције и хеш претходног блока, чиме се обезбеђује непроменљивост и сигурност података. Једном уписани подаци практично се не могу изменити без контроле над већином мреже, што блокчејн чини отпорним на цензуру и фалсификовање. Ова архитектура омогућава транспарентност и проверљивост, јер сви учесници могу независно верификовати историју трансакција. Први блокчејн систем, *Bitcoin* [2], уведен је 2009. године као одговор на потребу за децентрализованом дигиталном валутом, док је *Ethereum* проширио концепт увођењем паметних уговора, отварајући пут ка развоју комплексних децентрализованих апликација.

2.4. Алгоритми консензуса

Да би блокчејн мрежа функционисала без централног ауторитета, неопходно је да сви чворови постигну сагласност о валидности нових блокова. Овај процес обезбеђују консензусни алгоритми, међу којима су најпознатији *Proof of Work* [3] (*PoW*), *Proof of Stake* (*PoS*) [4] и њихове варијанте. *PoW* захтева решавање сложених криптографских задатака, чиме се гарантује сигурност уз високу потрошњу енергије, док *PoS* заснива избор валидатора на уложеним токенима, што смањује трошкове и повећава ефикасност. Поред ових, постоје и алгоритми попут *Practical Byzantine Fault Tolerance* [5], који се користе у приватним мрежама ради бржег постизања консензуса. Ови механизми чине основу децентрализације, јер спречавају манипулацију и обезбеђују интегритет података чак и у присуству злонамерних учесника.

3. ПАМЕТНИ УГОВОРИ

Паметни уговори представљају једну од најзначајнијих иновација у оквиру блокчејн технологије, јер омогућавају аутоматизовано, транспарентно и непроменљиво извршавање уговорних односа без посредника. Овај термин први је увео Ник Сабо [6]. За разлику од традиционалних уговора, који се ослањају на правне институције, судске механизме и поверење између страна, паметни уговори функционишу као програмски код имплементиран на блокчејну. Тиме се обезбеђује висок ниво сигурности, елиминација људске грешке и смањење трошкова трансакција. Њихова логика се извршава детерминистички, једном када су услови дефинисани и уговор постављен на мрежу, извршење је загарантовано без могућности произвољног мењања правила. Ова својства чине паметне уговоре погодним за окружења са ограниченим поверењем, јер се верификација заснива на криптографским механизмима и консензусним алгоритмима, а не на трећим странама.

Примена паметних уговора обухвата широк спектар области: од финансијских трансакција и управљања дигиталним идентитетима, преко аутоматизованих система плаћања и осигурања, до сложених пословних процеса у децентрализованим апликацијама. У ДеФи екосистему, паметни уговори омогућавају креирање протокола за позајмице, размену токена, стакинг и управљање ликвидношћу. Такође, паметни уговори у другим доменима подржавају токене засноване на стандардима (ЕРЦ-20, ЕРЦ-721), управљање власништвом над дигиталном имовином, па чак и имплементацију ДАО структура за колективно доношење одлука. Њихова непроменљивост и јавна проверљивост доприносе транспарентности, али истовремено намећу изазове у погледу флексибилности и скалабилности, јер свака грешка у коду може имати озбиљне последице. Управо због тога, развој паметних уговора захтева ригорозно тестирање, формалну верификацију и примену сигурносних образаца како би се обезбедила поузданост у реалним условима.

3.1. Писање паметних уговора

Писање паметних уговора подразумева дефинисање уговорних правила у облику програмског кода који се извршава на дистрибуираној блокчејн мрежи. За разлику од класичних апликација, код мора бити детерминистички, транспарентан и отпоран на манипулације, јер се извршава на великом броју независних чворова. Сваки чвор верификује резултат трансакције, а само идентични исходи бивају уписани у ланац блокова, чиме се обезбеђује интегритет и непоречивост извршења. Транспарентност се постиже јавном доступношћу изворног кода и историје трансакција, док се сигурност обезбеђује криптографским механизмима и консензусним алгоритмима. Због ових захтева, развој паметних уговора захтева пажљив дизајн, тестирање и примену безбедносних образаца, јер грешке могу имати директне финансијске последице. Правилно написан уговор представља основу поузданих и сигурних дигиталних трансакција у децентрализованом окружењу.

3.2. *Ethereum Virtual Machine EVM*

EVM [7] функционише као дистрибуирани глобални рачунар, где сваки чвор верификује и извршава код уговора, обезбеђујући сигурност и транспарентност. Паметни уговори се најчешће пишу у језику *Solidity*, а њихов код се извршава у изолованом виртуелном окружењу, чиме се спречава утицај на друге процесе. Писање директно у *EVM* бајткоду је непрактично, па се користе језици вишег нивоа. Поред *Solidity*-ја, користе се још и језици *Vyper* и *Yul*. *Ethereum* уводи концепт „гаса“ – свака операција има цену, што спречава злоупотребу ресурса и подстиче оптимизован код. Ови механизми чине *EVM* основом за поуздано и скалабилно извршавање паметних уговора.

4. *REACT*

React [8] је једна од најпопуларнијих *JavaScript* библиотека за развој модерних корисничких интерфејса, заснована на компонентном приступу и виртуелном ДОМ-у, што омогућава модуларност,

високе перформансе и једноставно одржавање кода. Његова декларативна природа и подршка за *JSX* синтаксу олакшавају развој интерактивних апликација, док *hook*-ови (попут *useState* и *useEffect*) поједностављују управљање стањима и асинхроним операцијама. Ове карактеристике чине *React* погодним за комплексне апликације, укључујући децентрализоване *Web3* системе.

4.1. Помоћне библиотеке

У контексту развоја децентрализованих апликација, *React* се често комбинује са библиотекама које проширују његову функционалност. *Ethers.js* омогућава директну интеракцију са *Ethereum* мрежом, управљање новчаницима, слање трансакција и позивање функција паметних уговора. *Wagmi*, заснован на *React*-у, додаје апстракције за повезивање крипто-новчаника као на пример *MetaMask*, управљање сесијама и праћење статуса трансакција, уз интеграцију са *React Query* библиотеком за кеширање и синхронизацију података. За рад са формама користи се *React Hook Form* библиотека, који обезбеђује ефикасну валидацију и минимално поновно исцртавање форме, што је кључно за перформансе. *SweetAlert2* библиотека доприноси побољшању корисничког искуства кроз приказ интерактивних обавештења и дијалога, посебно у критичним тачкама као што су потврде трансакција или обавештења о грешкама.

5. *SOLIDITY*

Solidity [9] је статички типизиран, објектно-оријентисан језик развијен за креирање паметних уговора на *Ethereum* мрежи. Синтакса је инспирисана *JavaScript*-ом, Ц++-ом и *Python*-ом, што олакшава учење и омогућава модуларност кроз наслеђивање, модификаторе и енкапсулацију. Паметни уговор се дефинише као скуп стања и функција, уз подршку за догађаје, грешке, структуре и енумерације. Сваки уговор почиње директивом *pragma* и кључном речи *contract*, а може да садржи променљиве стања, функције и контролне механизме. *Solidity* обезбеђује детерминистичко извршавање на *EVM*-у, при чему је правилно управљање меморијским контекстима (*storage, memory, calldata*) кључно за оптимизацију трошкова гаса и сигурност уговора. Захваљујући овим карактеристикама, *Solidity* је доминантан језик за развој децентрализованих апликација.

5.1. *OpenZeppelin* библиотека

OpenZeppelin [10] је стандардна библиотека отвореног кода која пружа аудитоване компоненте за развој сигурних паметних уговора u *Solidity*-ју. Садржи имплементације ЕРЦ стандарда, контролу приступа кроз *Ownable* и *AccessControl*, као и заштиту од напада попут *reentrancy*-ја помоћу *ReentrancyGuard*. Њена употреба значајно смањује ризик од грешака и убрзава развој ослањајући се на најбоље праксе индустрије.

6. ИМПЛЕМЕНТАЦИЈА *RESET* ПЛАТФОРМЕ

RESET платформа је пројектована као потпуно децентрализовано решење које елиминише потребу за централизованим серверима и базама података. Архитектура платформе обухвата три кључне компоненте: паметне уговоре који чувају пословну логику и податке, *The Graph* протокол за индексирање и претрагу информација са блокчејна, и клијентску апликацију која омогућава интеракцију корисника са системом. Овакав приступ обезбеђује сигурност, транспарентност и отпорност на манипулацију.

6.1. Паметни уговори *RESET* платформе

Језгро система чини скуп модуларних паметних уговора који управљају инцидентима, разменом порука, обрачуном накнада и емитовањем догађаја. Сваки уговор имплементира јасно дефинисане интерфејсе, што омогућава флексибилност и једноставну надоградњу без утицаја на друге компоненте. Као репрезентативан пример, *Incident.sol* паметни уговор користи се за: креирање нових понуда, њихово прихватање/одбијање, завршетак инцидента и емитовање пратећих догађаја, уз контролу приступа и заштиту од reentrancy напада.

6.2. *The Graph* и клијентска апликација

The Graph протокол омогућава ефикасно индексирање догађаја и приступ подацима путем *GraphQL* упита, чиме се елиминише потреба за централизованим серверским слојем. Клијентска апликација, развијена у *React*-у, интегрише *Ethers.js* и *Wagmi* библиотеке за комуникацију са блокчејном, док *React Query* и *SweetAlert2* библиотеке обезбеђују респонзивност и транспарентност интеракција. Ова комбинација омогућава директну, сигурну и децентрализовану комуникацију између корисника и паметних уговора.

7. ПРАКТИЧНА ДЕМОНСТРАЦИЈА

RESET платформа пружа једноставан и безбедан начин за решавање сајбер инцидената на блокчејну. Интеракција са платформом почиње идентификацијом улоге (протокол или нападач), након које корисник може да пријави инцидент или да започиње преговоре кроз креирање, прихватање или одбијање понуда. Све ове трансакције транспарентно су забележене на блокчејну. Вођење преговора се одвија путем енкриптованог канала унутар платформе, чиме се обезбеђује приватност и верификабилност процеса. Статус сваке акције прати интерактивна нотификација са директним линком ка *Etherscan*-у, што корисницима даје потпуну контролу и увид у ток преговора. Овакав приступ спаја децентрализацију, сигурност и интуитивно корисничко искуство.

8. ЗАКЉУЧАК

RESET платформа представља децентрализовано *Web3* решење за сигурну и проверљиву комуникацију између компромитованих протокола и нападача. Систем се ослања na *Ethereum* паметне уговоре писане у *Solidity*-ју, уз подршку *OpenZeppelin* библиотеке

чиме се обезбеђује безбедност. Архитектура укључује паметне уговоре, интеграцију са *The Grap*h протоколом за индексирање и *React* клијентску апликацију, омогућавајући транспарентне преговоре и енкриптовану размену порука. Демонстрација показује да *RESET* интегрише савремене *Web3* технологије у јединствено решење које смањује ризик и повећава поверење у ДеФи екосистему. Будући развој обухвата подршку за више токена, аутентификацију без поверења и оптимизацију индексирања, чиме се платформа припрема за скалабилну продукциону употребу.

9. ЛИТЕРАТУРА

[1] Chainalysis team, „Crypto Hacks Analisys.“ [Online] Доступно на: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/ (приступљено у новембру 2025.)

[2] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“, [Online] Доступно на: https://nakamotoinstitute.org/library/bitcoin/ (приступљено у новембру 2025.)

[3] Wikipedia, „Proof of Work”, [Online] Доступно на: https://en.wikipedia.org/wiki/Proof_of_work (приступљено у новембру 2025.)

[4] Wikipedia, „Proof of Stake”, [Online] Доступно на: https://en.wikipedia.org/wiki/Proof_of_stake (приступљено у новембру 2025.)

[5] GeeksForGeeks, „Practical Byzantine Fault Tolerance”, [Online] Доступно на: https://www.geeksforgeeks.org/computer-networks/practical-byzantine-fault-tolerancepbft/ (приступљено у новембру 2025.)

[6] Nick Szabo, „Smart Contracts: Building Blocks for Digital Markets“ [Online] Доступно на: https://nakamotoinstitute.org/library/smart-contracts-building-blocks-for-digital-markets/ (приступљено у новембру 2025.)

[7] Ethereum.org, „Ethereum Virtual Machine (EVM)“, [Online] Доступно на: https://ethereum.org/developers/docs/evm/ (приступљено у новембру 2025.)

Кратка биографија:

Алекса Чоловић рођен је 25.03.2000. у Новом Саду, где је стекао своје основно и средње образовање. Основне академске студије завршава 2023. године одбраном дипломског рада на тему „Систем за подршку здравог живота“ на Факултету техничких наука. Након чега наставља своје школовање на истом факултету, а мастер рад одбранио је 2025. године.

Контакт: colovic.aleksa11@gmail.com