УДК 004.056 https://doi.org/10.35546/kntu2078-4481.2022.2.10

І. В. СЕГЕДА
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0003-1958-4985
В. О. КОЦЮБА
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-9255-3029

ІНФОРМАЦІЙНА СИСТЕМА ОБЛІКУ РІВНЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ГАМАНЦІВ

В роботі розглянуті питання значимості електронної ролі комерції у сфері бізнес-діяльності і зростаючою потребою захисту учасників електронної комерції від шахрайських дій. Все більше злочинців намагаються використовувати цифрові ресурси, щоб приховати свою незаконну діяльність. Крім того, криптовалюти є чудовим способом відмивання коштів. Наявність відповідних заходів кібербезпеки може захистити нас від таких атак у майбутньому.

Найкращий спосіб захистити децентралізований світ від цих кібератак – це запровадити відповідні протоколи та методи криптографічної кібербезпеки. Одним з таких протоколів безпеки може слугувати система яка надасть доступ до рівня захищеності електронних гаманців користувачів децентралізованого світу.

В ході дослідження було проведено аналіз існуючих протоколів кібербезпеки на основі технології смарт-контрактів. Проведено аналіз та визначено переваги та недоліки наявних протоколів безпеки у сфері децентралізованих мереж. Обґрунтовано вибір засобів й технологій для створення інформаційної системи обліку рівня безпеки електронних гаманців за допомогою технології смарт-контрактів, основними складовими якої є збір даних про зловмисні атаки і крадіжки криптоактивів, подальше їх впровадження в базу, взаємодія і обмін даними з учасниками системи. Запропоновано програмну реалізацію та перелік використаних обчислювальних методів, засобів та моделей. Розроблено архітектуру системи. Спроектовано та описано процес розгортання системи та подано приклади взаємодії з нею. Розроблено користувацький інтерфейс для візуалізації роботи системи.

У спроектованій системі враховано інтерфейси роботи існуючих рішень, складовими яких є аудит смарт-контрактів, постійна підтримка впроваджених смарт-контрактів та захист даних за допомогою додаткового шару безпеки. Також, були використані всі переваги технології блокчейн, а саме підвищення довіри користувачів, безпека, прозорість і можливість відстеження даних разом з ефективністю. Результати роботи даної системи можуть бути використані та впроваджені різними великими компаніями у сфері децентралізованих фінансів. Створена інформаційна система є гнучкою в плані розширення і може бути використана як частина або основа для більш широко направлених програмних рішень у сфері кібербезпеки децентралізованих додатків.

Ключові слова: *блокчейн-технології, смарт-контракт, електронний гаманець, кібербезпека, криптоактиви.*

I. V. SEGEDA
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
ORCID: 0000-0003-1958-4985
V. O. KOTSIUBA
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
ORCID: 0000-0002-9255-3029

INFORMATION SYSTEM FOR RECORDING THE SECURITY LEVEL OF ELECTRONIC WALLETS

The paper examines the importance of the role of electronic commerce in the field of business activity and the growing need to protect participants in electronic commerce from fraudulent activities. More and more criminals are trying to use digital resources to hide their illegal activities. In addition, cryptocurrencies are a great way to launder money. Having appropriate cyber security measures in place can protect us from such attacks in the future.

The best way to protect the decentralized world from these cyberattacks is to implement appropriate cryptographic cybersecurity protocols and techniques. One of these security protocols can be a system that will provide access to the security level of electronic wallets of users of the decentralized world.

In the course of the study, an analysis of existing cyber security protocols based on smart contract technology was carried out. The analysis was carried out and the advantages and disadvantages of existing security protocols in the field of decentralized networks were determined. The choice of means and technologies for creating an information system for recording the level of security of electronic wallets using smart contract technology is substantiated, the main components of which are the collection of data on malicious attacks and theft of cryptoassets, their subsequent introduction into the database, interaction and data exchange with system participants. A software implementation and a list of used computing methods, tools and models are offered. The system architecture has been developed. The system deployment process is designed and described, and examples of interaction with it are presented. A user interface for visualizing the system's operation has been developed.

The designed system takes into account the work interfaces of existing solutions, the components of which are audit of smart contracts, permanent support of implemented smart contracts, and data protection with the help of an additional layer of security. Also, all the benefits of blockchain technology have been used, namely increased user trust, security, transparency and data traceability along with efficiency. The results of this system can be used and implemented by various large companies in the field of decentralized finance. The created information system is flexible in terms of expansion and can be used as a part or basis for more widely directed software solutions in the field of cyber security of decentralized applications.

Key words: *blockchain technologies, smart contract, electronic wallet, cyber security, crypto assets.*

Постановка проблеми

Криптовалюта міцно увійшла у повсякденне життя українців. В Україні легко завести криптогаманець, купити і обміняти криптовалюту чи розрахуватися нею за послуги і товари. За даними опитувань, близько 10% наших співвітчизників коли-небудь володіли криптоактивами. Потужні зміни платіжних звичок громадян у бік безготівкових розрахунків та електронних гаманців значно посилились після масштабних світових подій, пов'язаних із пандемією та військовою агресією РФ. Карантинні обмеження призвели до переходу на безконтактні платежі, збільшення проникнення електронних гаманців і ширшого використання автоматизації платежів B2B, P2P, A2A. Розвиток криптовалют і російське вторгнення співпали в часі і ми бачимо як через криптовалюти фінансують спротив, допомагають біженцям. Уряд України дозволив надати фінансову допомогу з використанням криптовалют, і Україні надійшло близько 100 млн. доларів США в такому форматі. [1; 2]. Але висока волатильність криптовалют і специфічні ризики на крипторинку вимагають уважного вивчення його особливостей.

Актуальність обраної тематики обґрунтована підвищенням значимості електронної ролі комерції у сфері бізнес-діяльності, а також зростаючою потребою захисту учасників електронної комерції від шахрайських дій. Найчастішою причиною злому програмних застосунків на технології блокчейн є намагання вкрасти криптоактиви користувачів. Це робиться шляхом шахрайства та введення в оману з подальшим розкраданням грошей й розмиванням їх в мережі. Наприклад, створення фішингових сайтів, котрі є копією реальних додатків, або ж розсилання спаму через різні месенджери з повідомленнями щодо отримання легкої винагороди, що так само є дуже привабливим для не досвідчених користувачів. Далі, завжди викрадені кошти прямують на електронні адреса шахраїв, котрі потім виводять їх через біржі та різні обмінники криптоактивів. Таким чином, виникає проблема в користуванні програмних додатків на технології блокчейн, а саме, як можливо убезпечити користувачів цих технологій від різних типів крадіжок. Одним зі способів розв'язання такої проблеми є створення інформаційної системи обліку електронних гаманців. Через те, що проблема стосується технології блокчейну, то створення такої системи потребує дотримання правил та консенсусу цієї технології, а отже створювана система буде розміщена у відкритому доступі для всіх користувачів на технології смарт-контрактів.

Аналіз останніх досліджень і публікацій

Одним із перспективних та сучасних напрямів в платіжній системі України в межах якого науковці на сьогодні зосереджують свої дослідження є цифровізація електронних платежів та перспективи розвитку системи електронних гаманців. Ці питання в своїх дослідженнях розглядають О.Д. Вовчак та Г.Є. Шпаргало [3], П.М. Куліков та Є.О. Полтавська, [4], Л.А. Некрасенко [5]. Дослідження окремих аспектів цієї проблеми висвітлено у працях таких науковців та дослідників, як Т.В. Мокієнко, Т.Б. Прийдак, Р.В. Ліпський, Т.І., Батракова [6] та інших. Проте постійні зміни в платіжному просторі України вимагають постійного аналізу стану криптовалюти, виявлення можливостей та ризику обігу електронних грошей, удосконалення і формування перспективних напрямів підвищення рівня їх надійності та продуктивності.

Формулювання мети дослідження

Саме актуальність питань, що порушуються у статті, дозволили сформулювати мету та окреслити коло завдань запропонованого дослідження.

Метою дослідження е створення інформаційної системи обліку рівня безпеки електронних гаманців за допомогою технології смарт-контрактів, основними складовими якої є збір даних про зловмисні атаки і крадіжки криптоактивів, подальше їх впровадження в базу, взаємодія і обмін даними з учасниками системи.

Основні задачі, які вирішуються для досягнення заявленої мети:

– проаналізувати наявні системи;

– обґрунтувати вибір засобів й технологій для створення інформаційної системи;

– розробити програмну реалізацію, архітектуру та перелік використаних обчислювальних методів, засобів, моделей інформаційної системи.

Викладення основного матеріалу

Технологія блокчейну має в собі негласні правила його користування та розробки на ньому. Наприклад, цифрову валюту на основі блокчейну можна створювати, передавати та зберігати поза контролем будь-якого уряду, фінансової установи чи особистого юриста, але кожна транзакція, з усім тим, записується в блокчейні та є публічною. Але, не тільки публічними транзакціями обмежується блокчейн, ця технологія загалом відкрита для всіх

охочих, особливо це стосується смарт-контрактів. Через активний розвиток технології “blockchain” «розумні контракти» замінили звичайні контракти. «Розумні контракти» (смарт-контракти) – це одне із застосувань блокчейну, яке викликає найбільший інтерес [7]. Смарт-контракт являє собою звичайний електронний гаманець, який додатково містить описану логіку взаємодії з ним. Завдяки смарт-контрактам блокчейн може відстежувати весь ланцюг роботи та перевіряти справжність виконаних методів, наприклад де і ким вони були створені, як і коли вони були викликані, які дані опрацювали або змінили. Це допомагає повністю виключити факт підробки даних, дізнатися їх походження і навіть перевірити відповідність виклику до транзакції. Отже, для розробки системи слід використати саме децентралізовану технологію смарт-контрактів.

Аналіз існуючих протоколів кібербезпеки на основі технології смарт-контрактів. З появою все нових програмних додатків на технології блокчейн, з’являється все більше нових типів інтерфейсів роботи з даними цієї технології, що зі свого боку провокує до появи нових вразливостей. Основними вразливостями є: втрата коштів та втрата персональних даних. Для уникнення таких проблем вже були розроблені безліч способів та методів їх вирішення. До них можна віднести, наприклад, попередній аудит смарт-контрактів, для пошуку його вразливостей якими можуть скористатися зловмисники, або використання оракулів для виклику методів смарт-контрактів. Також на даний час існують десятки додатків для покривання своїх електронних гаманців додатковим шаром безпеки, котрий контролює надсилання коштів. Програмні застосунки для збереження коштів в мережі блокчейн, наведено в табл. 1.

Таблиця 1

Програмні застосунки для збереження коштів в мережі блокчейн*

Програмний застосунок	Рішення що пропонуються
Hacken Аудит смарт-контрактів	Однин з найкращих організаторів проведення аудиту – широкої методичної перевірки та аналізу коду смарт-контракту, який використовується для взаємодії з криптовалютою або блокчейном
PolySwarm Екосистема виявлення загроз	Децентралізований ринок розвідки загроз, який став можливим завдяки смарт-контрактам Ethereum та технології блокчейн
Utrust Рішення для інтеграції платежів	Рішення для інтеграції платежів, яке дозволяє підприємствам електронної комерції приймати цифрові валюти як форму оплати
Shentu Chain Захищений блокчейн	Екосистема Shentu забезпечує наскрізні рішення безпеки для блокчейнів, децентралізованих додатків та інших критично важливих програмних додатків

*Зведено авторами: на основі [7-13]

Програмна реалізація інформаційної системи. Основною ціллю розробки є створення протоколу безпеки, який надалі може бути використаним як стандарт інформаційної системи обліку рівня безпеки електронних гаманців на основі блокчейнів типу EVM. Також, необхідно створити вебдодаток для демонстрації роботи смарт-контракту та взаємодії з ним. До складу архітектури розробленої інформаційної системи входять такі основні компоненти: – головний модуль системи; – модулі взаємодії для адміністрування системи; – модуль взаємодії для отримання/додавання даних до системи; – веб-версія системи для демонстрації роботи смарт-контракту.

Зазвичай для розробки програмних додатків або будь-яких інших систем типу Web 2.0 використовується архітектура клієнт-сервер. Необхідно зауважити, на відміну від програм типу Web 2.0, Web 3.0 усуває посередників. Немає централізованої бази даних, яка зберігає стан програми, і централізованого вебсервера, на якому розміщується логіка сервера (рис. 1).

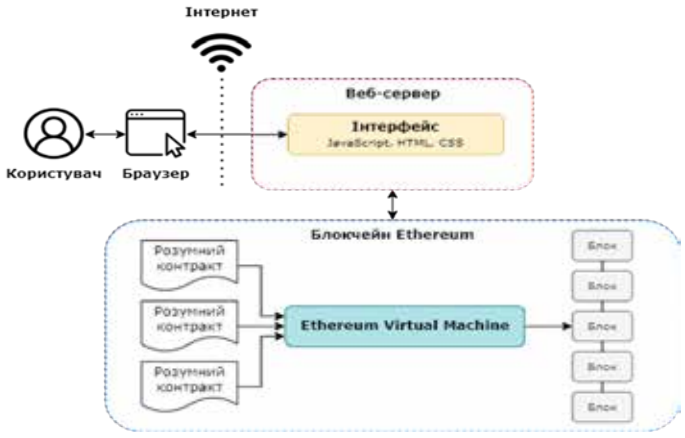

Рис. 1. Архітектура додатків типу Web 3.0

За такою архітектурою створені програми розміщуються на децентралізованому автоматі, яким керують анонімні вузли в Інтернеті. Під “автоматом” мається на увазі машина, яка підтримує певний стан програми та майбутні стани, дозволені на цій машині. Блокчейни – це автомати станів, які створені з певним станом генезису і мають дуже суворі правила (тобто консенсус), які визначають, як цей стан може змінитися. Що більше, жодна одиниця не контролює цей децентралізований автомат – її спільно тримають усі в мережі. Також, замість того, щоб контролювати серверне середовище, у Web 3.0 використовують розумні контракти, які визначають логіку додатків і реалізують їх на децентралізованому кінцевому автоматі. Це означає, що будь-яка людина, яка хоче створити додаток для блокчейну, розгортає свій код на цьому спільному кінцевому автоматі. Через те, що Ethereum – це децентралізована мережа, то кожен вузол в мережі Ethereum зберігає копію всіх станів на кінцевому автоматі Ethereum, включаючи код і дані, пов’язані з кожним розумним контрактом. Для взаємодії з даними та кодом у блокчейні, потрібно взаємодіяти з одним із його вузлів (рис. 2).

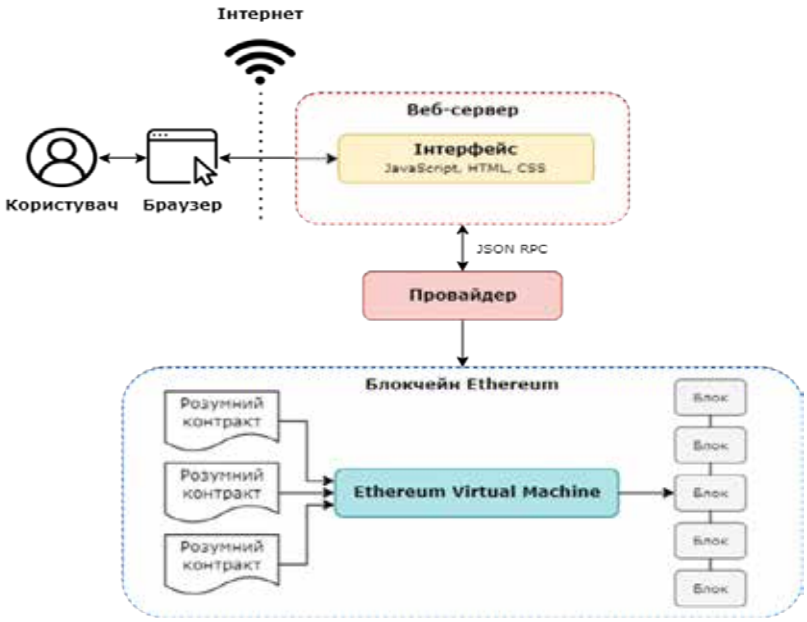

Рис. 2. Архітектура додатку типу Web 3.0 з використанням провайдеру

Це необхідно тому, що кожен вузол повинен транслювати запит транзакції на EVM (Ethereum Virtual Machine). Потім майнер виконає транзакцію і поширить результівну зміну стану на решту мережі. Щоб не встановлювати вузли блокчейну, слід використати загально доступні хмарні вузли, наприклад, які надає провайдер Infura (рисунок 2). Тоді веб-інтерфейс матиме змогу зв’язуватися зі смартконтрактами, а вони, зі свого боку, зможуть викликати функції. Кожен провайдер Ethereum реалізує специфікацію JSON-RPC. Це забезпечує єдиний набір методів, коли різні інтерфейсні програми хочуть взаємодіяти з блокчейном. JSON-RPC – це легкий протокол виклику віддалених процедур (RPC – Remote Procedure Call) без стану, який визначає кілька структур даних і правила їх обробки. Він не залежить від транспортного механізму, тому концепції можна використовувати в рамках одного процесу, через сокети, через HTTP або в багатьох різних середовищах обміну повідомленнями. Також, він використовує JSON як формат даних.

Схема зберігання даних в системі. Інформаційна система передбачає зберігання й обробку даних (дані про репортерів, їх типи, випадки та адреса шахраїв). Дані, зі свого боку, розташовані на блокчейні, а саме, на смарт-контракті, це дозволяє бути необмеженим в кількості збережених даних тому, що максимальний розмір сягає 2256 байт, це приблизно 1.1 · 1065 терабайт даних. Для реалізації запланованої логіки було спроектовано систему структур котра описує необхідні дані для зберігання в смарт-контракті. Схема продемонстрована на рис. 3. На схемі зображено 4 створені структури, їх поля, типи та зв’язки між ними. Структура ReporterType містить інформацію про тип репортера, його назву (name), множник винагороди (rewardFactor), а також статус привілейованості (privileged).

Структура Reporter, зі свого боку, описує дані самого репортера, наприклад, його ім’я (name), його адрес електронного гаманця (account), частота роботи (rate), його тип (reporterIdType) та баланс винагороди (balance).

Оскільки головною цілю смарт-контракту є збереження даних про адреси користувачів, використовується структура AddressInfo з такими полями, як ранг небезпеки адреси (rank), категорія правопорушення (category) та номер випадок до котрого ця адреса належить (caseId). Сама ж адреса зберігається як ключ до масиву даних

типу AddressInfo, що дозволяє отримувати дані за адресою швидше та надійніше, бо у такий спосіб для отримання даних використовується хеш-таблиці. Для зв'язування адрес спільних за одним випадком використовується структура Case. В ній наявні такі поля, як назва випадку (name), його категорія (category) та час коли він відбувся (timestamp). Також, додатково, було зображено схему з глобальними змінними контракту (ContractState), його подіями (Events), методами (Methods) та модифікаторами (Modifiers), тобто весь стан контракту (рис. 4).

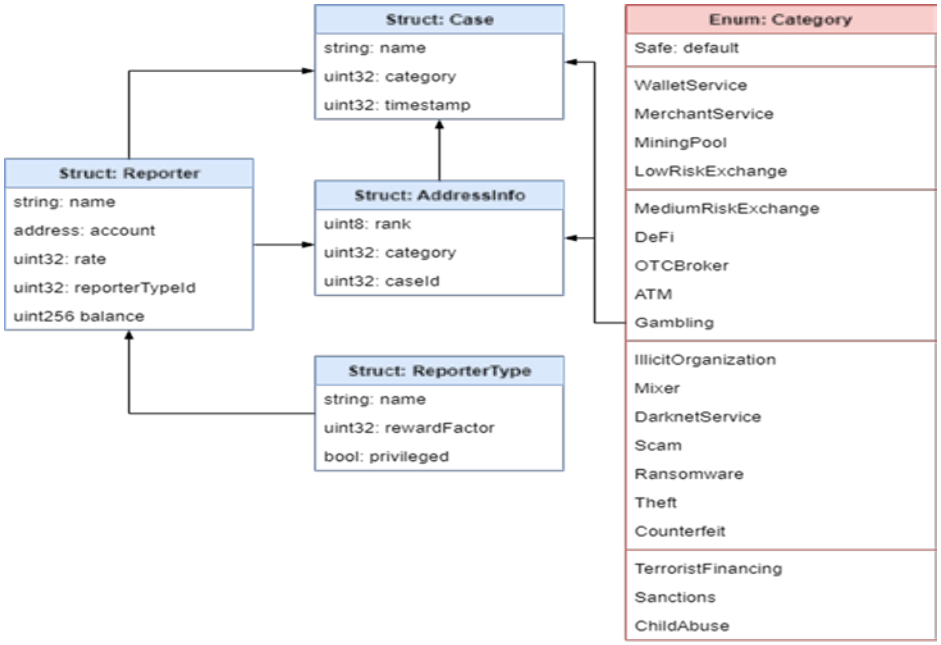

Рис. 3. Схема зв'язків між структурами даних

Слід зазначити, що модифікатори це спеціальні методи котрі реагують на певну умову і при її не виконанні повертають транзакцію. Також, окрім модифікаторів, існує ще один тип методів які називаються події. Зазвичай їх викликають коли відбувається певна зміна стану даних контракту, наприклад, коли вони змінюються, або додаються.

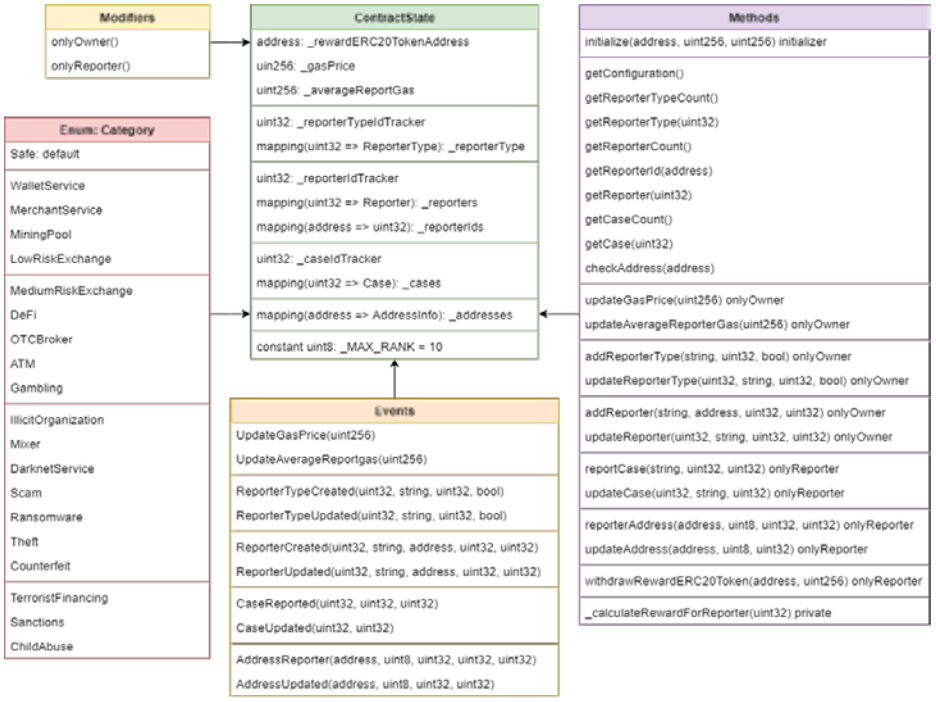

Рис. 4. Схема загального стану смарт-контракту

Після виклику цих методів буде записано до стану контракту додаткову інформацію котра описана в параметрах викликаної події. Внаслідок цього можна виконувати швидкий пошук даних, особливо використовуючи проіндексовані поля структур. Додатково, для поєднання електронних гаманців спільним випадком існує також перерахування Category, яке описує категорію за якою вони поєднуються. Категорії поділяються на декілька типів, це безпечні, з низьким, середнім, великим та високим ризиком. Низький ризик характерний для гаманців використаних в малих шахрайських обмінах, або, наприклад, при користуванні пулами майнерів, які згодом отримують винагороду на них. Середній рівень ризику описаний такими категоріями: великі шахрайські обміни, використання гаманців як криптовалютні банкомати, в азартних іграх, або децентралізованих додатках. За високим рівнем ризику мається на увазі використання гаманців в незаконних організаціях, на ринку даркнету, при крадіжках, підробці активів або для програм вимагачів. Гаманці котрі потрапляють в максимальний тип ризику – високий, використовуються в фінансуванні тероризму, в жорстокому поводженні з дітьми та порнографічними матеріалами, або мається в підсанкційних списках.

Адміністративні модулі смарт-контракту. При створені інтерфейсу інформаційної системи було додатково розроблено модуль для адміністративних функцій. Діаграма взаємодії даної структури з головним смарт-контрактом зображена на рис. 5. Вона поділяється на дві категорії смартконтрактів: для контролю доступу (Ownable) та для оновлення (TransperentProxy та ProxyAdmin). Найпоширенішою та основною формою контролю доступу є концепція «власності»: є обліковий запис, який володіє контрактом і може виконувати адміністративні завдання. Такий підхід цілком виправданий у випадку використання смарт-контрактів з одним користувачем-адміністратором. Контроль доступу дозволяє обмежити необхідний інтерфейс головного смарт-контракту та надати його для адміністратора. Для реалізації такої логіки було створено смарт-контракт Ownable, який також надає додатковий функціонал для: – отримання поточного власника контракту (owner); – передання власництва над контрактом іншому електронному гаманцю (transferOwnership); – видалення поточного власника (renounceOwnership). Також, створений інтерфейс був використаний як спосіб адміністрування смарт-контракту ProxyAdmin.

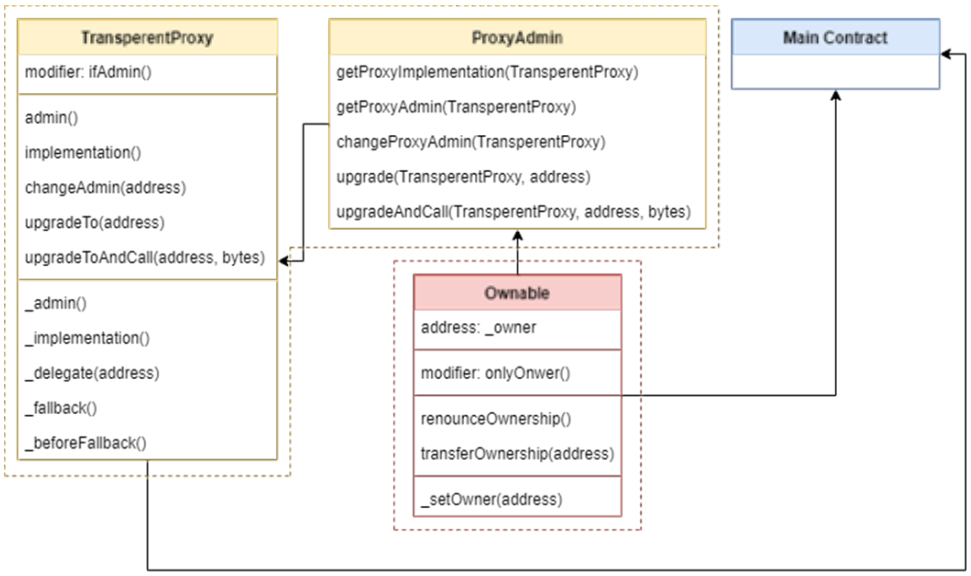

Рис. 5. Діаграма взаємодії адміністративних смарт-контрактів

Один з основних принципів EVM полягає в тому, що після того, як смартконтракт був розміщений на блокчейні, він не може бути змінений, а саме його інтерфейс. Натомість для оновлення смарт-контракту є можливим використання спеціального шаблону проксі.

Зазвичай, щоб оновити смарт-контракт необхідно було створити новий і розмістити вже його, але виникала проблема в втраті даних так, як для перезавантаження всіх даних зі старого контракту до нового необхідна велика сума коштів, щоб оплатити всі транзакції. Отже, за стандартизованим шаблоном проксі, було розроблено необхідну логіку. Його основна ідея полягає в тому, щоб використовувати проксі для оновлення. Перший контракт є простою обгорткою або «проксі», з яким користувачі взаємодіють безпосередньо і який відповідає за передачу транзакцій до/з другого контракту, який містить логіку. Ключова концепція, яку слід зрозуміти, полягає в тому, що логічний контракт можна замінити, тоді як проксі контракт або точку доступу ніколи не змінюють. Обидва контракти залишаються незмінними в тому сенсі, що їх код не можна змінити, але логічний контракт можна просто замінити іншим контрактом. Таким чином, проксі може вказувати на іншу реалізацію логіки, і програмне забезпечення таким чином «оновлюється» (рис. 6).

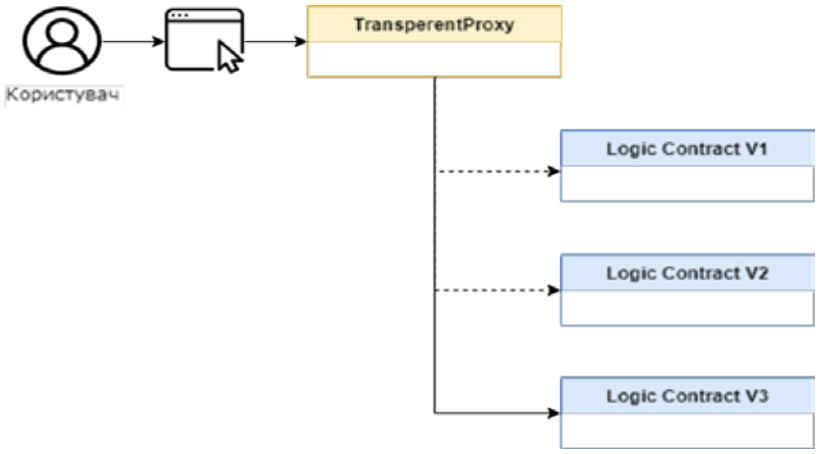

Рис. 6. Діаграма алгоритму оновлення смарт-контракту

На прикладі наведеному на рис. 6, за рахунок оновлення контракту реалізації проходить фактично їх заміна, з “Logic Contract V1” до “Logic Contract V2”, а потім і до “Logic Contract V3”. Тобто, в результаті користувач як використовував контракт TransperentProxy так надалі і використовує його без всіляких змін, а ось контракт з реалізацію був змінений два рази. Смарт-контракт з назвою TransperentProxy реалізує проксі-сервер, який може бути оновлений адміністратором. Щоб уникнути потенційних зіткнень селекторів проксі, цей контракт використовує прозорий шаблон проксі (TransperentProxy). Цей шаблон передбачає дві речі (рис. 7): – якщо будь-який обліковий запис без адміністратора викликає проксі-сервер (TransperentProxy), виклик буде передано до контракту реалізації (Logic Contract), навіть якщо цей виклик відповідає одній з адміністративних функцій, наданих самим проксі-сервером; – якщо адміністратор викликає проксі (ProxyAdmin), він може отримати доступ до адміністративних функцій, але його виклики ніколи не будуть передані до реалізації (Logic Contract). Якщо адміністратор спробує викликати функцію в реалізації (Logic Contract), вона вийде з ладу з повідомленням про помилку «адміністратор не може повернутися до цільового проксі».

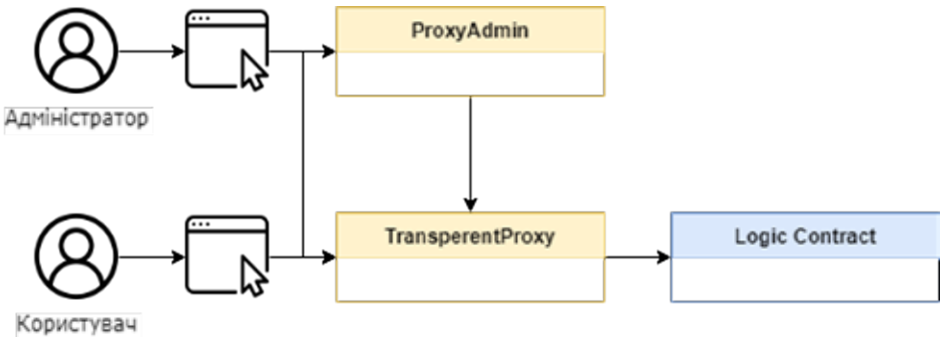

Рис. 7. Діаграма взаємодії різних користувачів з використанням шаблону проксі

Ці властивості означають, що обліковий запис адміністратора можна використовувати лише для адміністративних завдань, як, наприклад, оновлення проксі-сервера або зміна адміністратора, тому найкраще, якщо це буде виділений обліковий запис, який не використовується ні для чого іншого. Це дозволить уникнути проблем, викликаних раптовими помилками під час спроби викликати функцію з реалізації проксі. За шаблоном проксі слід, щоб виділений обліковий запис був екземпляром контракту ProxyAdmin. При налаштуванні таким чином, екземпляр контракту ProxyAdmin буде фактичним інтерфейсом адміністратора проксі-сервера TransperentProxy.

Архітектура веб-серверу. Для наочності використання створеної інформаційної системи було розроблено веб-додаток. Він розташований на веб-сервері, архітектура якого зображена на рис. 8.

Веб-сервер розроблений за методами Web 3.0, тому має декілька відмінностей від звичайних веб-серверів:

– наявність заздалегідь відомого інтерфейсу смарт-контракту, який описує всі методи взаємодії з ним;

– наявність екземпляра провайдеру, який, як було зазначено вище, надає можливість робити виклики впровадженого контракту на блокчейні Ethereum. Так, як використання смарт-контракту веде за собою втрату часу на додаткову обробку даних під час отримання та відправлення її на блокчейн, необхідно було зменшити витрати

часу в інших модулях додатка. Тому було використано бібліотеку NextJS з вбудованою бібліотекою ReactJS, яка слугує для розробки інтерфейсу. Головною перевагою використання саме цих технологій поміж інших це заощадження часу шляхом розбору інтерфейсу на різні підмодулі, такі як: компоненти, сторінки та шаблони.

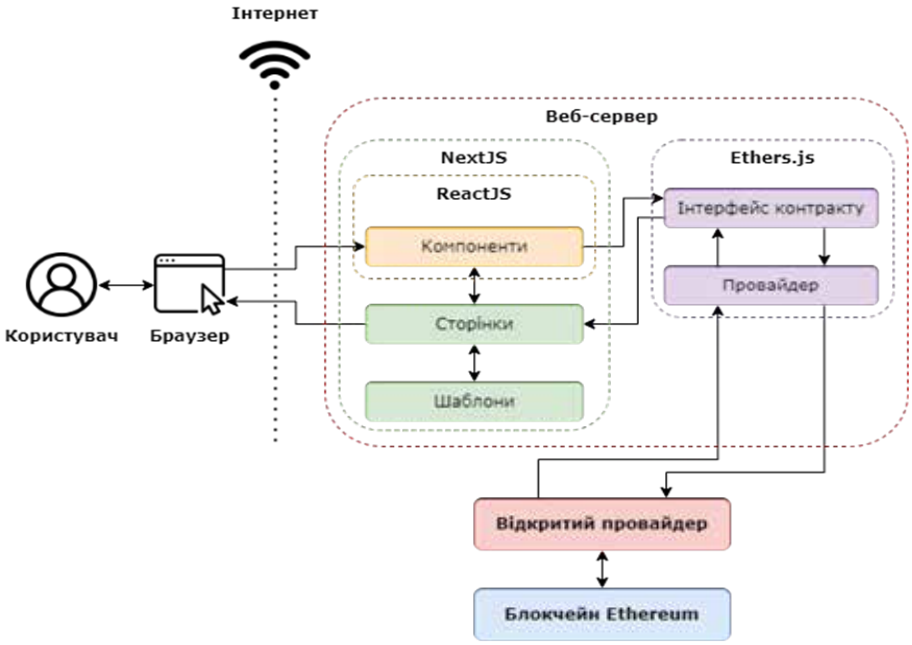

Рис. 8. Архітектура веб-серверу

Модуль компонентів відповідає за логіку обробки вхідних даних користувачів. Дані, зі свого боку, передаються далі до інтерфейсу контракту, котрий викликає потрібний його метод. Виклик проводиться через провайдера, результатом якого буде JSON об'єкт, який розбирається та оброблюється інтерфейсом контракту. Далі, готові дані використовуються для створення нової сторінки для користувача.

Використання веб-додатку. Після встановлення веб-додатку та початку його роботи згідно з командами описаними в інструкції, потрібно пройти за URL адресою зазначеною в консолі логування статусу виконання. Наприклад - це буде адреса: http://localhost:3003/. За цією адресою розташована головна сторінка веб-додатку (рис. 9).

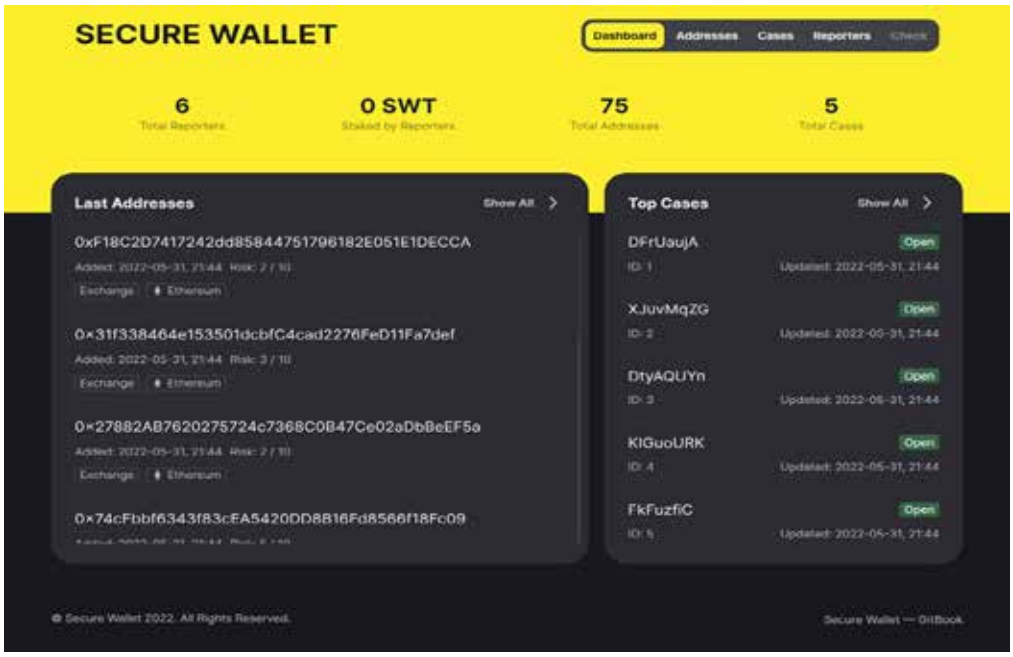

Рис. 9. Інтерфейс веб-додатку до розробленої інформаційної системи

На головній сторінці наявні такі дані як: загальна кількість репортерів, випадків та адрес, а також кількість токенів на балансі винагород репортерів. Додатково є вікна з адресами та випадками, що з'явилися останніми. Також, головна сторінка надає можливість перейти на інші сторінки за допомогою меню в правому верхньому куті, або перейти за додатковим посиланням в нижньому правому куті котре перенаправить користувача на сторінку з документацією веб-додатку реалізованою за допомогою платформи Github Gitbook.

Платформа написана за допомогою редактора вихідного коду Visual Studio Code. Для розробки системи використано технології: Solidity, HardHat, ethers.js, Git, Typescript, NextJS, HTML та CSS.

Висновки

1. Розроблена система дозволяє обмежити доступ до певних категорій електронних гаманців шляхом введення їх в базу даних яка спроектована за допомогою технології смарт-контракту.

2. Функціонал інформаційної системи розрахований на чотири категорії користувачів: адміністратор, видавець, дослідник та звичайний користувач. Кожен з них має свій інтерфейс для взаємодії с контрактом.

3. У створеній системі враховано інтерфейси роботи існуючих рішень, складовими яких є аудит смарт-контрактів, постійна підтримка впроваджених смарт-контрактів та захист даних за допомогою додаткового шару безпеки. Також, були використані всі переваги технології блокчейн, а саме підвищення довіри користувачів, безпека, прозорість і можливість відстеження даних разом з ефективністю.

4. Додатково, було створено веб-додаток для демонстрації функціонування розробленої системи. В ній надано можливість всім користувачам для перегляду даних, що існують в базі системи.

Створена інформаційна система є гнучкою в плані розширення і може бути використана як частина або основа для більш широко направлених програмних рішень у сфері кібербезпеки децентралізованих додатків. А результати роботи такої системи можуть бути використані та впроваджені різними великими компаніями у сфері децентралізованих фінансів та загалом у сфері кібербезпеки.

Список використаної літератури

1. Бедратенко О. Біткоїн і війна. Як Україні допомагають криптовалюти і чи зможе Росія скористатись "криптою", щоб обійти санкції. Голос Америки (VOA), 14.05.2022. URL: https://ukrainian.voanews.com/a/6571468.html (дата звернення: 11.09.2022).

2. Как криптовалюты помогают Украине и России во время войны: мнения экспертов. ФОКУС, URL: https://focus.ua/digital/508137-kak-kriptovalyuty-pomogayut-ukraine-i-rossii-vovremya-voyny-mneniya-ekspertov (дата звернення: 11.09.2022).

3. Вовчак О.Д, Шпаргало Г.Є. Платіжні системи: навч. посіб. К., Знання, 2008. 341 с.

4. Полтавська Є.О., Куліков П.М. Платіжні системи: навч. посіб. К., 2010. 219 с.

5. Некрасенко Л.А., Смолянська О.Ю. Сучасний стан та перспективи розвитку безготівкових платіжних інструментів в Україні. Вісник НТУ «ХПІ». 2014. 134 с.

6. Мокієнко Т.В., Прийдак Т.Б., Ліпський Р.В. Електронні гроші: сутність, класифікація та облікове вираження. Ефективна економіка. 2019. Вип. 6. DOI: 10.32702/2307-2105-2019.6.35

7. Smart Contract Audit. URL: https://coinmarketcap.com/ (дата звернення: 11.09.2022).

8. Hacken. Аудитор кибербезопасности WEB3 URL: https://hacken.io/ (дата звернення: 11.09.2022).

9. PolySwarm. URL:: https://polyswarm.io/(дата звернення: 11.09.2022).

10. Utrust. URL:https://utrust.com/ (дата звернення: 11.09.2022).

11. Utrust research.binance. URL: https://research.binance.com/en/projects/utrust (дата звернення: 11.09.2022).

12. Shentu. Shentu networks. URL: https://www.shentu.technology/ (дата звернення: 11.09.2022).

13. Shentu Whitepaper. URL: https://www.shentu.technology/whitepaper(дата звернення: 11.09.2022).

14. Сегеда І.В., Локотарев Є.О., Шаповал В.О. Реалізація використання блокчейн-технологій у енергетичному секторі. Вчені записки Таврійського національного університету імені В.І. Вернадського Серія: Економіка і управління Т. 30 (69). № 4, 2019, С. 160-165 DOI: https://doi.org/10.32838/2523-4803/69-4-51

References

1. Bedratenko O. Bitkoyn i voyna. Kak Ukraina mozhet pomoch' kriptovalyutam i kak Rossiya mozhet ispol'zovat' «kriptu», chtoby oboyti sanktsii.[Bitcoin and war. How Ukraine can help cryptocurrencies and how Russia can use "crypto" to circumvent sanctions] Golos Ameriki (VOA), Available at: https://ukrainian.voanews.com/a/6571468.html (accessed 11. September 2022).

2. Kak kriptovalyuty pomogayut Ukraine i Rossii vo vremya voyny: mneniya ekspertov [How cryptocurrencies help Ukraine and Russia during the war: expert opinions] FOKUS, Available at: https://focus.ua/digital/508137-kak-kriptovalyuty-pomogayut-ukraine-i-rossii-vovremya-voyny-mneniya-ekspertov (accessed 11 September 2022).

3. Vovchak, O.D. and Shpargalo G.E., Platizhni systemy [Payment systems], Znannia, Kyiv, Ukraine. 2008. 341 p.

4. Poltavska E.A. and Kulikov P.M. , Platizhni systemy [Payment systems], Kyiv, Ukraine. 2010. 219 p.

5. Nekrasenko L.A. and Smolyanska O.Yu. , “Current state and prospects of development of non-cash payment instruments in Ukraine”, Visnyk Natsional’noho tekhnichnoho universytetu «Kharkivs’kyy politekhnichnyy instytut», 2014. 134 p.

6. Mokijenko T.V., Pryjdak T.B., Lipsjkyj R.V. Elektronni ghroshi: sutnistj, klasyfikacija ta oblikove vyrazhennja [Electronic money: essence, classification and accounting expression]. Efektyvna ekonomika, vol. 6.2019.

7. Smart Contract Audit. 2022 Available at: https://coinmarketcap.com/ (accessed 11. September 2022).

8. Hacken. Cyber Security Auditor WEB3 WEB3 2022 Available at: https://hacken.io/ (accessed 11. September 2022).

9. PolySwarm NCT 2021.Available at: https://polyswarm.io/ (accessed 11. September 2022).

10. Utrust. 2022 Available at:https://utrust.com/ (accessed 11. September 2022).

11. Utrust . research.binance 2020. Available at: https://research.binance.com/en/projects/utrust (accessed 11. September 2022).

12. Shentu . Shentu networks. 2022Available at: https://www.shentu.technology/ (accessed 11. September 2022).

13. Shentu Whitepaper.2022. Available at: https://www.shentu.technology/whitepaper (accessed 11. September 2022).

14. Segeda I.V., Lokotarev Ye.O., Shapoval V.O. Vnedreniye razrabotki blokcheyn-tekhnologiy v energetike. [Implementation of blockchain technologies use in the energy sector] Vcheni zapiski Tavricheskogo natsional'nogo universiteta imeni V.I. Vernadskiy Seriya: Ekonomika i upravleniye T. 30 (69). 2019. № 4. S. 160-165. DOI: https://doi.org/10.32838/2523-4803/69-4-51.