https://doi.org/10.31891/2219-9365-2025-81-11
УДК 004.75:656.13.05:004.056.5

БАНДУРКА Олена
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0002-8059-1861
o.i.bandurra@ukr.net
РОМАНІВ Роман
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
roma.romaniv2013@gmail.com
СВИНЧУК Ольга
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0001-9032-6335
7011990@ukr.net

АРХІТЕКТУРА РОЗПОДІЛЕНОЇ ФУНКЦІОНАЛЬНО СТІЙКОЇ СИСТЕМИ МОНІТОРИНГУ ТРАНСПОРТНИХ ЗАСОБІВ НА БАЗІ БЛОКЧЕЙН-ТЕХНОЛОГІЇ

Стаття присвячена дослідженню методів забезпечення функціональної стійкості розподілених інформаційних систем моніторингу руху транспортних засобів із застосуванням блокчейн-технології. З огляду на стрімкий розвиток інтелектуальних транспортних систем та зростаючі вимоги до їхньої надійності, забезпечення безперервного функціонування таких систем є критично важливим для безпеки та ефективності дорожнього руху. Зокрема, основними викликами для таких систем залишаються стійкість до апаратних та програмних збоїв, адаптація до динамічних змін у транспортній інфраструктурі, захист від кібератак, а також забезпечення цілісності та достовірності даних.

Метою дослідження є розробка архітектури розподілених систем на базі блокчейну, здатних протистояти збоям, кібератакам та динамічним змінам навантаження. Основний акцент зроблено на інтеграції децентралізованих механізмів консенсусу, смарт-контрактів та алгоритмів автоматичного відновлення, що забезпечують стабільність функціонування навіть у разі часткових відмов. Блокчейн-технологія розглядається як одна з перспективних платформ для вирішення цих завдань завдяки своїм унікальним характеристикам. Серед них – децентралізований підхід, криптографічний захист, незмінність записів та прозорість даних. Інтеграція блокчейну у системи моніторингу руху дозволяє створювати відмовостійкі архітектури, які можуть функціонувати навіть за умов часткових збоїв у вузлах системи. Також використання механізмів децентралізованого консенсусу та смарт-контрактів сприяє автоматизації процесів і підвищенню загальної ефективності управління транспортними потоками. В статті розроблено архітектуру програмного забезпечення, що інтегрує блокчейн-технологію, децентралізовані механізми консенсусу та смарт-контракти для автоматизації процесів управління та забезпечення адаптивності систем.

Ключові слова: блокчейн, розподілені інформаційні системи, функціональна стійкість, моніторинг транспорту, інформаційна безпека, смарт-контракти.

BANDURKA Olena, ROMANIV Roman, SVYNCHUK Olha
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

ARCHITECTURE OF A DISTRIBUTED FUNCTIONALLY RESILIENT MONITORING SYSTEM FOR VEHICLES BASED ON BLOCKCHAIN TECHNOLOGY

The article is devoted to the study of methods for ensuring the functional resilience of distributed information systems for vehicle movement monitoring using blockchain technology. Given the rapid development of intelligent transportation systems and the growing requirements for their reliability, ensuring the uninterrupted operation of such systems is critically important for the safety and efficiency of road traffic. In particular, the main challenges for such systems remain resilience to hardware and software failures, adaptation to dynamic changes in transportation infrastructure, protection against cyberattacks, and ensuring the integrity and reliability of data.

The aim of the study is to develop an architecture for distributed systems based on blockchain technology, capable of withstanding failures, cyberattacks, and dynamic load changes. The primary focus is placed on the integration of decentralized consensus mechanisms, smart contracts, and automatic recovery algorithms to ensure operational stability even in cases of partial system failures. Blockchain technology is considered one of the most promising platforms for addressing these challenges due to its unique characteristics, including a decentralized approach, cryptographic protection, immutability of records, and data transparency. The integration of blockchain into vehicle monitoring systems enables the creation of fault-tolerant architectures capable of functioning even under conditions of partial node failures. Additionally, the use of decentralized consensus mechanisms and smart contracts facilitates process automation and enhances the overall efficiency of traffic flow management. The article proposes a software architecture that integrates blockchain technology, decentralized consensus mechanisms, and smart contracts to automate management processes and ensure system adaptability.

Keywords: blockchain, distributed information systems, functional stability, transportation monitoring, information security, smart contracts.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному високотехнологічному світі розподілені інформаційні системи моніторингу транспортного руху набувають дедалі більшого значення для ефективного управління транспортною інфраструктурою та забезпечення безпеки дорожнього руху.

Розвиток інтелектуальних транспортних систем (ITS) та впровадження інноваційних технологій суттєво підвищує вимоги до надійності та ефективності систем моніторингу руху транспортних засобів. Функціональна стійкість таких систем стає ключовим фактором, що визначає якість управління транспортними потоками, своєчасність реагування на надзвичайні ситуації та загальну безпеку дорожнього руху.

Блокчейн-технологія, яка зародилася у фінансовій сфері, сьогодні розглядається як потужний інструмент забезпечення функціональної стійкості розподілених інформаційних систем. Її ключові характеристики, а саме децентралізація, криптографічний захист, незмінність та прозорість даних, створюють унікальні можливості для побудови відмовостійких систем моніторингу руху транспортних засобів.

Актуальність дослідження методів забезпечення функціональної стійкості розподілених інформаційних систем зумовлена складністю та критичністю таких систем, які повинні працювати безперебійно та надійно в умовах постійних змін та потенційних загроз.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Застосування блокчейн-технології в контексті забезпечення безпеки даних, пов'язаних з фінансовими транзакціями [1], вже є добре відомим. Тому науковці вже почали вивчати використання цієї технології для автоматизованих транспортних засобів (CAV). Окрім запропонованих застосувань у сферах безпеки водія та користувача, блокчейн-технологія має величезний потенціал для здійснення фінансових транзакцій між користувачами, які керують транспортними засобами, та іншими суб'єктами, що надають послуги користувачеві. Враховуючи велику кількість транспортних платежів, які люди повинні здійснювати щодня, стає зрозуміло, що поширення блокчейн-технології на цю сферу надає користувачам низку нових переваг, які можуть заощадити час, а також забезпечити додаткову доступність таких функцій для користувачів, які не мають доступу до необхідного виду оплати за традиційними методами. Платежі за паркування, страхування, мита та оренда автомобілів — це лише кілька прикладів поширених транзакцій, які можна було б спростити та забезпечити за допомогою блокчейн-технологій, зменшивши час, зусилля та непорозуміння з боку користувача [2].

Оскільки CAV є новою технологією, то вона ще є досить дорогою для середнього користувача. Тому комерційні суб'єкти, ймовірно, будуть серед перших, хто використовуватиме CAV, а ціни знизяться до рівня, доступного для загальних споживачів, набагато пізніше. Зацікавлені сторони, які першими використовують цю технологію, можуть запропонувати такі послуги, як каршеринґ, клієнтам, які хочуть побачити, які галузі приймуть цю технологію першими. У роботі [3] науковці вже провели попереднє застосування блокчейн у системах CAV, звертаючи увагу на вплив на різні сфери та на ті, що можуть бути наступними. У роботі вивчається блокчейн-орієнтована сфера, де технологія використовується для обробки транзакцій між транспортними засобами, що сприяє комунікації через систему. Тому для CAV є великий потенціал у каршерингу, в якому компанії економлять час і гроші, пропонуючи безпілотний транспорт клієнтам.

Оглядаючи попередні застосування блокчейн, як-от його початкове використання в Біткоїн, розширення його на фінансову сферу, пов'язану з транзакціями на основі транспортних засобів, буде відносно простим для застосування. Як додаткова перевага, блокчейн здебільшого відомий завдяки своєму широкому впливу на забезпечення безпеки платежів між підключеними до мережі суб'єктами, і вже має хорошу репутацію серед мільйонів задоволених користувачів. Тому його впровадження може також сприяти прийняттю CAV користувачами, що дозволить подальший розвиток цієї технології та проведення нових досліджень і розробок щодо її майбутніх застосувань.

Міллер в своїх дослідженнях [14] зазначає, що блокчейн-технологія, завдяки своїй здатності дозволяти та керувати транзакціями в безпечному середовищі і фіксувати деталі транзакцій як постійні записи, безпосередньо сприяє можливості використання CAV для здійснення фінансових транзакцій, пов'язаних з перевезеннями. Він також додав, що різні типи транзакцій, такі як заправка або ремонт транспортних засобів, будуть оброблятися по-різному, з різними правилами транзакцій в залежності від конкретного виду послуги, що надається користувачеві.

Досвід забезпечення надійності SCADA-систем у енергетиці [5] демонструє, що інтеграція механізмів виявлення аномалій із децентралізованими архітектурами значно знижує ризики критичних збоїв. Адаптація подібних принципів до транспортного моніторингу дозволяє мінімізувати вплив позаштатних ситуацій на функціонування всієї системи

Питаннями функціональної стійкості в інших сферах займались багато вчених, таких як Машков О.А., Барабаш О.В., Мусієнко А.П., Собчук В.В., Свинчук О.В., Бандурка О.І., та інші. У статті [6] представлено результати дослідження проблем забезпечення функціональної стійкості комплексу бортового обладнання сучасного повітряного судна в умовах дестабілізуючих впливів. Проаналізовано основні види відмов, зокрема загрози інформаційній безпеці комплексу бортового обладнання повітряного судна та можливі наслідки їх впливів на безпеку польоту. Розглянуто основні механізми, що дозволять забезпечити функціональну стійкість комплексу бортового обладнання згідно розробленої стратегії. У статті запропоновано основні шляхи реалізації принципів функціональної стійкості щодо перспективного автоматизованого не обслуговуваного людиною-оператором комплексу бортового обладнання.

Також забезпеченням функціональної стійкості інформаційних систем у критичних галузях, зокрема енергетиці, приділяється значна увага в сучасних дослідженнях. У статті [7] розглянуто проблематику забезпечення надійності та стійкості інформаційних систем електростанцій, які стають дедалі складнішими та масштабнішими через інтеграцію численних взаємопов'язаних компонентів. Авторами запропоновано інноваційну систему моніторингу функціональних параметрів та контролю справного стану модулів інформаційної системи на основі алгоритму самодіагностування тестовим методом. У разі виявлення відмови система автоматично локалізує пошкоджений компонент, перенаправляє його задачі на справні вузли та інформує персонал для ініціювання ремонтних робіт. Це дозволяє мінімізувати простої та підтримувати функціональну стійкість системи навіть в умовах збоїв.

У статті [8] розглядається програмний застосунок для моніторингу параметрів справного стану обчислювальних пристроїв інформаційної системи електростанції на основі алгоритму самодіагностування з блукаючим діагностичним ядром для забезпечення функціональної стійкості. Розроблено алгоритм виявлення відмов в системі на основі дешифрації сукупності результатів тестових перевірок системи. Даний застосунок дозволяє підвищити достовірність діагностування, знизити час діагностування та проводити діагностування із заданою повнотою та глибиною.

У статті [9] описано методологію побудови ефективної системи самодіагностики інформаційних систем на прикладі підприємств металургійної та енергетичної промисловості. Наведено методику організації та здійснення самодіагностики, механізми виявлення, а також ідентифікацію та локалізацію несправних модулів.

У статті [10] розглядається алгоритм перерозподілу навантаження, який спрямований на забезпечення функціональної стійкості розподілених вебзастосунків. Функціональна стійкість є критично важливою для забезпечення надійної роботи та високої доступності вебзастосунків в умовах підвищеного навантаження, технічних несправностей або кібератак. Аналізуються різні методи перерозподілу навантаження, проводиться аналіз існуючого програмного забезпечення, які використовують балансувальник навантаження. Розроблена програмна система, яка забезпечує функціональну стійкість розподілених вебзастосунків на основі нового алгоритму перерозподілу навантаження.

Отже, для всіх складних технічних систем дуже важливо здійснювати неперервний контроль параметрів функціонування та справного стану, оскільки прогнозування дозволяє розв'язувати задачу визначення оптимальних моментів контролю, у проміжках між якими забезпечуватиметься властивість функціональної стійкості системи. За допомогою такого контролю можна забезпечити підвищення продуктивності праці усіх модулів при зменшенні числа зайнятих у виробництві людей та значному зменшенні частки ручної праці.

Дана робота зосереджена на вдосконаленні методів створення надійних розподілених інформаційних систем для управління транспортною інфраструктурою. Такі системи стають критично важливими в умовах прискореного технологічного розвитку, коли зростання складності середовищ вимагає нових підходів до забезпечення стабільності, ефективності та адаптивності. Дослідження інтегрує теоретичні моделі з практичними рішеннями, спрямованими на мінімізацію ризиків збоїв і оптимізацію функціонування систем у реальному часі.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Проблематика забезпечення функціональної стійкості розподілених інформаційних систем є надзвичайно складною та багатогранною. Вона включає в себе низку взаємопов'язаних аспектів: технічні характеристики обладнання, архітектуру системи, алгоритми управління, механізми резервування, протоколи обміну даними, кібербезпеку та адаптивність до різноманітних зовнішніх впливів.

Основними викликами при забезпеченні функціональної стійкості таких систем є:

- необхідність підтримання неперервності роботи в умовах апаратних та програмних збоїв;
- забезпечення цілісності та достовірності даних про рух транспортних засобів;
- швидка адаптація до динамічних змін транспортної інфраструктури;
- стійкість до кібератак та несанкціонованого втручання;

- ефективне масштабування системи при збільшенні навантаження.

Дослідження спрямоване на вирішення актуальних завдань підвищення надійності інформаційної інфраструктури транспортної галузі, забезпечення цілісності та достовірності даних про рух транспортних засобів.

Метою дослідження є розробка архітектури розподілених систем моніторингу руху транспортних засобів на базі блокчейну, здатних протистояти збоям, кібератакам та динамічним змінам навантаження. Робота зосереджена на інтеграції сучасних технологій, таких як децентралізовані мережі та блокчейн, для забезпечення стабільного функціонування систем у умовах динамічних змін і зростаючих вимог до інформаційної безпеки.

Основними завданнями дослідження є:

- вибір оптимальної архітектури, що буде усувати залежність від єдиного центру управління;
- розробка алгоритмів реєстрації транспортних засобів та розподілу завдань із використанням блокчейн-технології;
- створення архітектури розподіленої системи моніторингу транспортних засобів на базі блокчейн-технології.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Централізовану систему багато хто вважає вкрай неефективною та навіть небезпечною, особливо з огляду на постійно змінний характер та широкий масштаб управління даними, потрібний для функціонування CAV (Connected and Autonomous Vehicles) [11]. Швидке отримання даних має вирішальне значення для забезпечення оперативної реакції, а в умовах одного централізованого вузла, який обробляє всі користувацькі дані, це може бути складним завданням. Інша проблема полягає в тому, що зловмисники можуть скористатись єдиною точкою відмови, перевантажуючи центральну систему запитами або маніпулюючи даними користувачів. Це в найгіршому випадку може спричинити серйозні збої у всій мережі CAV [12].

З часом виявлені системні недоліки у повністю централізованих підходах змусили дослідників шукати альтернативні моделі, подібні до тих, що зображені на рисунку 1.

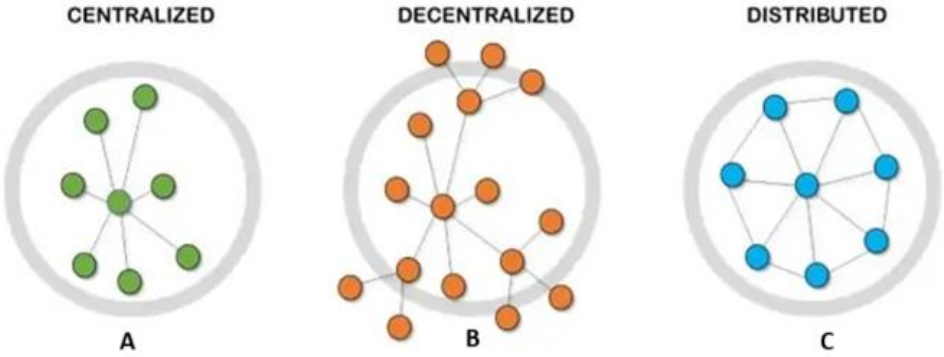

Рис. 1. Візуальне порівняння різних типів систем

Децентралізована архітектура замість одного центрального вузла покладається на складну систему взаємозв'язків між користувачами та іншими сутностями. Серед багатьох можливих рішень найбільш перспективним виявився блокчейн, представлений у 2008 році особою або групою осіб під псевдонімом Сатоші Накамото [13]. Блокчейн може підтримувати роботу масштабних систем, оскільки численні вузли (піри) спільно забезпечують валідацію, ініціацію та завершення транзакцій, працюючи на базі консенсусних протоколів. Завдяки цьому зникає залежність від продуктивності та безпеки єдиного централізованого вузла, а сама технологія блокчейну надає необхідні функції, які були притаманні централізованим системам, але робить це в умовах високої пропускної здатності та масштабованої архітектури рівноправних вузлів.

У гетерогенних додатках та сервісах Інтернету речей (IoT) необхідно приділяти особливу увагу архітектурі моделі довіри з огляду на механізми поширення довіри. Відомо [14,15], що дослідження архітектур довіри можна класифікувати переважно за двома підходами: централізованим та розподіленим. Характеристики кожного підходу мають принципові відмінності (табл. 1).

1. Централізований підхід (рис. 1A):

- централізоване зберігання всієї інформації про менеджерів довіри (TM), агентів довіри (TA), протоколи, алгоритми та математичні моделі обчислення довіри;
- формування централізованої бази даних;
- надання сервісів за запитом;

- повний контроль та управління процесами довіри з єдиного центру.

2. Розподілений підхід (рис. 1С):

- локальне виконання всіх обчислень безпосередньо агентами довіри;
- автономність обчислювальних вузлів;
- відсутність єдиного центру управління;
- висока швидкість локальних обчислень.

Таблиця 1

Порівняльний аналіз характеристик централізованих, децентралізованих та розподілених систем

Властивість/Поведінка	**Централізований підхід**	**Децентралізований підхід**	**Розподілений підхід**
Точки відмови	Одна точка відмови	Скінченна кількість відмов	Нескінченна кількість відмов
Обслуговування	Легке	Помірне	Складне
Стабільність	Дуже нестабільний	Можливе відновлення	Дуже стабільний
Масштабованість/ Максимальна кількість учасників	Низька масштабованість	Низька масштабованість	Нескінченна
Легкість розробки/створення	Менш складний	Помірний	Потрібно більше деталей
Еволюція/Різноманітність	Повільна/маленька	Висока	Висока

Для IoT-додатків використання виключно одного підходу є недостатнім, оскільки обчислення можуть виконуватися як локально, так і віддалено, залежно від доступності ресурсів. Повністю розподілені або повністю централізовані моделі не забезпечують оптимальних результатів. Саме тому для обчислення довіри в умовах складних IoT-сервісів рекомендується застосовувати децентралізовану модель (рис. 1В), яка є оптимальним варіантом архітектури. Основні характеристики децентралізованої моделі:

- гібридний підхід до управління довірою;
- часткова автономія локальних вузлів;
- можливість динамічного перерозподілу обчислювальних навантажень;
- підтримка механізмів консенсусу між вузлами;
- гнучкість архітектури та адаптивність до змінних умов IoT-середовища.

Децентралізована архітектура на основі блокчейну [15, 16] забезпечує не лише захист від кібератак, але й автономність функціонування окремих вузлів системи. Наприклад, у разі виходу з ладу одного з серверів моніторингу, інші вузли продовжують обмін даними через механізми консенсусу, що підтверджує ефективність запропонованого підходу. Таким чином, децентралізована модель довіри забезпечує баланс між централізованим контролем та розподіленою обробкою інформації, що є критичним для ефективного функціонування гетерогенних IoT-систем.

У роботі обрана децентралізована модель архітектури на основі блокчейну, яка поєднує механізми консенсусу (наприклад, Proof-of-Authority) для забезпечення довіри між вузлами системи та смарт-контракти для автоматизації процесів реєстрації транспортних засобів і розподілу завдань.

Для ефективного управління транспортними засобами в інтелектуальних транспортних системах пропонується використовувати технологію блокчейн для децентралізованого верифікування даних про транспортні засоби та розподілу обчислювальних завдань. Нижче наведено ключові функціональні компоненти, що реалізують ці процеси.

Функція реєстрації в ITS (RegisterInIVTP)

Функція RegisterInIVTP(), зображена схемою на рисунку 2, відповідає за реєстрацію транспортного засобу в інтелектуальній транспортній платформі (IVTP). Алгоритм включає отримання ідентифікатора транспортного засобу, його шифрування та додавання відповідного вузла в систему. Повертається зашифрований ідентифікатор для подальшого використання.

ISSN 2219-9365

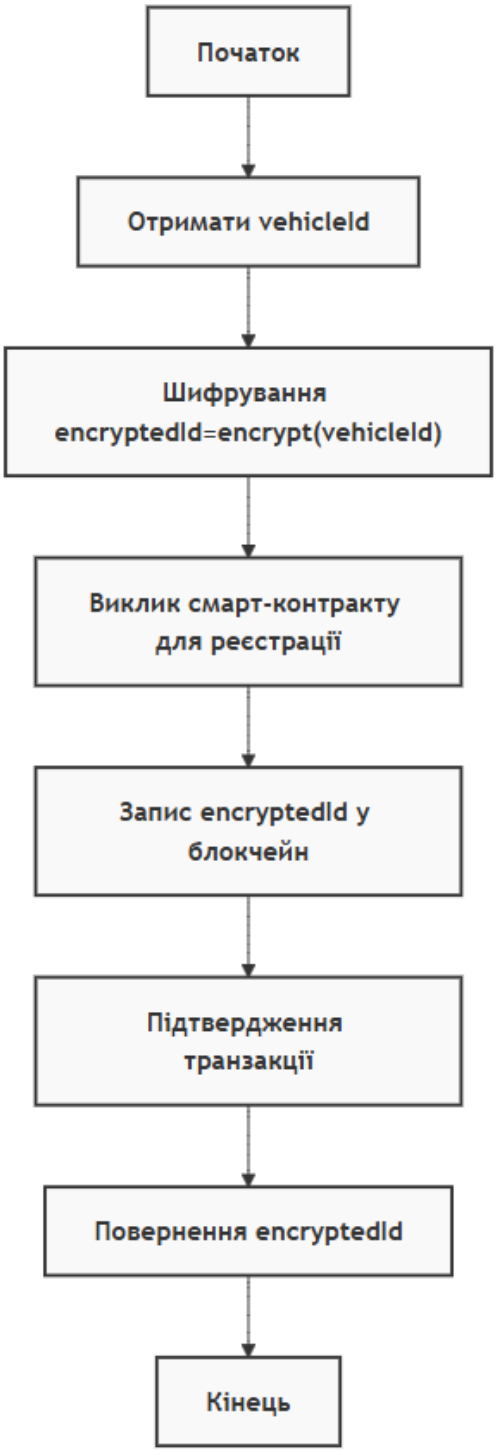

Рис. 2. Послідовність виконання функції RegisterInIVTP()

Ця функція забезпечує цілісність і безпеку процесу реєстрації шляхом шифрування даних транспортного засобу.

Функція реєстрації у блокчейн-системі (RegisterInBFMS)

Функція RegisterInBFMS(), зображена схемою на рис. 3, виконує реєстрацію транспортного засобу у системі управління блокчейном (BFMS). Вона перевіряє відповідність зашифрованого ідентифікатора із записом у базі даних, додає вузол у блокчейн і генерує подію для сигналізації про завершення процесу.

ISSN 2219-9365

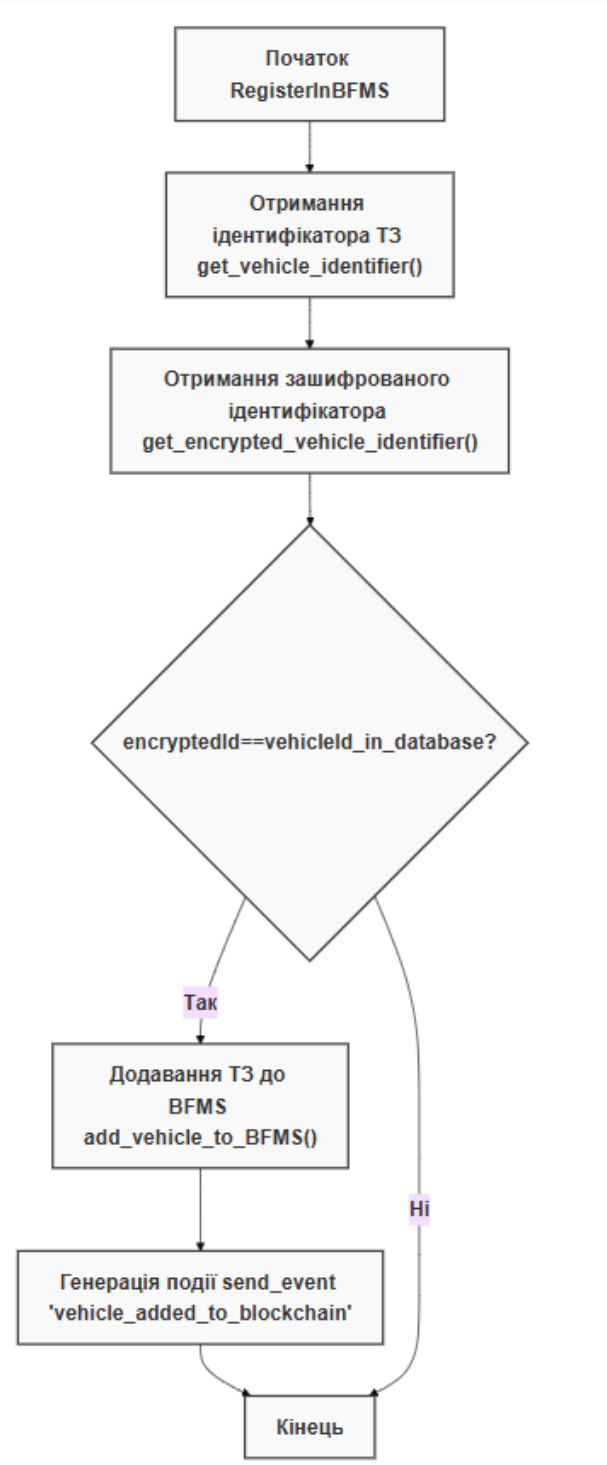

Рис. 3. Послідовність виконання функції RegisterInBFMS()

Цей механізм дозволяє інтегрувати транспортний засіб у блокчейн-систему, забезпечуючи прозорість і відмовостійкість.

Функція розподілу завдань (AssignTask)

Функція AssignTask(), зображена схемою на рисунку 4, реалізує процес розподілу завдань між транспортними засобами, а також перевіряє виконання завдань і здійснює розподіл винагород. Алгоритм включає розподіл задачі, прийняття її одним із вузлів і обробку результатів.

ISSN 2219-9365

Рис. 4. Послідовність виконання функції RegisterInBFMS()

Ця функція демонструє підхід до організації колективної роботи транспортних засобів у розподіленій системі, забезпечуючи ефективний розподіл обчислювальних ресурсів.

Запропонована архітектура системи моніторингу транспортних засобів демонструє комплексний підхід до забезпечення функціональної стійкості розподілених інформаційних систем з використанням блокчейн-технології (рис. 5).

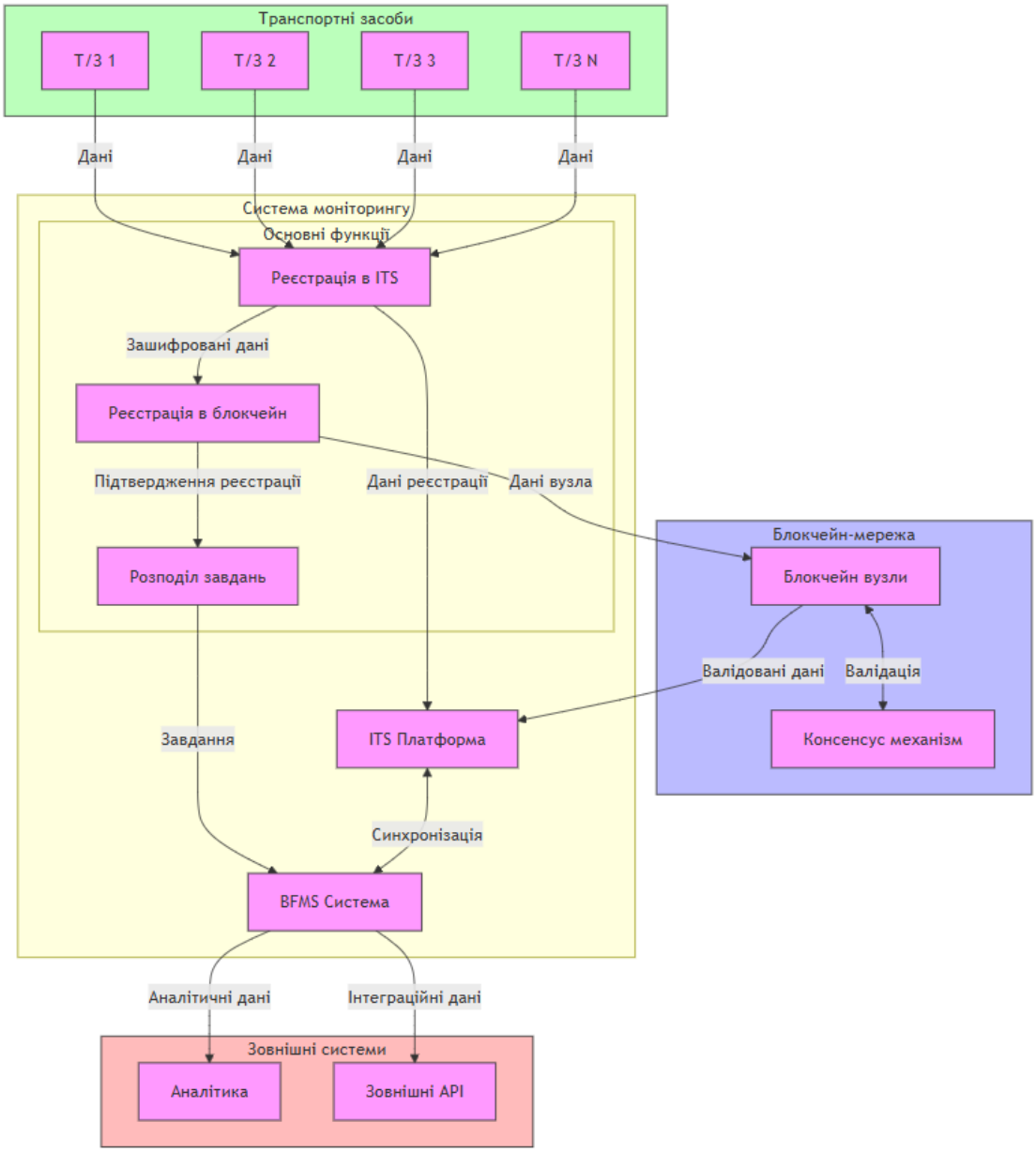

Рис. 5. Архітектура розподіленої системи моніторингу транспортних засобів на базі блокчейн-технології

Архітектура системи представлена у вигляді чотирьох взаємопов'язаних рівнів:

1) рівень транспортних засобів – базовий рівень, де здійснюється збір первинних даних про рух транспорту та їх початкова передача;
2) блокчейн-мережа – забезпечує децентралізовану обробку даних через:
   - розподілену мережу вузлів;
   - механізми консенсусу;
   - криптографічний захист;
   - синхронізацію даних;
3) система моніторингу – центральний рівень управління, що включає:
   - ITS для обробки транспортних даних;
   - BFMS для блокчейн-моніторингу;
   - системи обробки інформаційних потоків;
4) зовнішні системи – верхній рівень для аналітики та інтеграції даних з іншими системами.

Ключові принципи архітектури:

- децентралізація інформаційної інфраструктури;

- забезпечення максимальної відмовостійкості;
- багаторівнева система безпеки;
- прозорість та верифікованість даних;
- динамічне масштабування.

Запропонована архітектура впроваджує інноваційний підхід до створення розподілених систем моніторингу руху транспорту, де ключову роль відіграє блокчейн-технологія. Вона забезпечує стабільну роботу системи навіть за умов збоїв, автоматичне відновлення після критичних подій та ефективний розподіл обчислювальних завдань між учасниками мережі.

Для оцінки функціональної стійкості запропонованої архітектури використано підходи, аналогічні до інструментів аналізу захищеності ICS-CRAT [14]. Вони дозволяють кількісно вимірювати здатність системи протистояти зовнішнім та внутрішнім загрозам, включаючи аналіз часу відновлення після збоїв та ефективність механізмів резервування.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМ

У статті висвітлено сучасні підходи до забезпечення функціональної стійкості розподілених інформаційних систем моніторингу руху транспортних засобів із застосуванням блокчейн-технологій. Проаналізовано ключові виклики, пов'язані з надійністю та безпекою таких систем, та запропоновано децентралізовану архітектуру, здатну протистояти динамічним змінам і зовнішнім загрозам.

Розроблена архітектура інтегрує блокчейн-технологію, децентралізовані механізми консенсусу та смарт-контракти для автоматизації процесів управління та забезпечення адаптивності систем. Це дозволяє забезпечити відмовостійкість, прозорість і масштабованість інформаційної інфраструктури в умовах зростаючих вимог до кібербезпеки. Запропоновані алгоритми резервування, автоматичного відновлення та розподілу завдань у реальному часі забезпечують стабільність функціонування навіть за умов часткових збоїв. Архітектура може бути застосована для вдосконалення інтелектуальних транспортних систем у міських та міжміських інфраструктурах.

Запропоновані підходи можуть бути адаптовані для інших сфер, де потрібна висока функціональна стійкість, зокрема в енергетиці, промисловості та телекомунікаціях. Перспективи подальших досліджень включають розробку гібридних алгоритмів консенсусу, інтеграцію нейромережевих підходів для прогнозування аномалій руху та оптимізації управління транспортними потоками. Це сприятиме створенню безпечних, надійних і ефективних транспортних систем нового покоління.

Література

1. Giannaros A., Karras A., Theodorakopoulos L., Karras C., Kranias P., Schizas N., Kalogeratos G., Tsolis D. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. Journal of Cybersecurity and Privacy. 2023. No. 3(3). Pp. 493–543. https://doi.org/10.3390/jcp3030025

2. Horwitz, L. Data Center-Impact of Driverless Cars Could Broaden with Blockchain. URL: https://www.cisco.com/c/en/us/solutions/data-center/blockchain-driverless-cars.html (дата звернення: 19.01.2025).

3. Saranti P.G., Chondrogianni D., Karatzas S. Autonomous Vehicles and Blockchain technology are shaping the future of Transportation. In the 4th Conference on Sustainable Urban Mobility; Springer: Berlin/Heidelberg, Germany. 2018. Pp. 797–803. https://doi.org/10.1007/978-3-030-02305-8_96

4. Miller D. Blockchain and the Internet of Things in the Industrial Sector. In IT Professional. May/June 2018. Vol. 20, No. 3. Pp. 15–18. https://doi.org/10.1109/MITP.2018.032501742

5. Zhang Y., Wang L., Xiang Y., Ten C.-W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. IEEE Transactions on Smart Grid. July 2015. Vol. 6. No. 4. Pp. 1707–1721. https://doi.org/10.1109/tsg.2015.2396994

6. Калашник Г.А., Калашник-Рибалко М.А. Проблеми забезпечення функціональної стійкості комплексу бортового обладнання сучасного повітряного судна. Наука і техніка Повітряних Сил Збройних Сил України. 2021. № 3 (44). С. 59–65. https://doi.org/10.30748/nitps.2021.44.07.

7. Барабаш О.В., Свинчук О.В., Бандурка О.І. Програмне забезпечення контролю справного стану інформаційних систем в енергетичній галузі для забезпечення функціональної стійкості. Сучасний захист інформації. 2024. № 2 (58). С. 41–49. https://doi.org/10.31673/2409-7292.2024.020005

8. Barabash O., Svynchuk O., Salanda I., Mashkov V., Myroniuk M. Ensuring the functional stability of the information system of the power plant on the basis of monitoring the parameters of the working condition of computer devices. Advanced Information Systems. 2024. Vol. 8, No. 2. P. 107 – 117. https://doi.org/10.20998/2522-9052.2024.2.12

9. Sobchuk V., Barabash O., Musienko A., Svynchuk O. Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. E3S Web of Conferences. 2021. Vol. 250. P. 82–87. https://doi.org/10.1051/e3sconf/202125008002

10. Барабаш О.В., Свинчук О.В., Шуклін Г.В. Алгоритм перерозподілу навантаження для забезпечення функціональної стійкості розподілених вебзастосунків. Зв'язок. 2024. № 5. С. 3–11. https://doi.org/10.31673/2412-9070.2024.050183

11. Baza M., Nabil M., Lasla N., Fidan K., Mahmoud M., Abdallah M. Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles. Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco. 2019. Pp. 1–7. https://doi.org/10.1109/WCNC.2019.8885769.

12. Rowan S., Clear M., Gerla M., Huggard M., Goldrick C.M. Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels. 2017. Pp. 1–10. https://doi.org/10.48550/arXiv.1704.02553

13. Лєнков С.В., Банзак Г.В., Цицарєв В.М., Проценко Я.М. Алгоритм прогнозування для показників надійності і вартості експлуатації об'єктів радіоелектронних засобів озброєння. Системи обробки інформації. 2016. № 9 (146). С. 28–30.
https://books.ndcnangu.co.ua/statti_NDL_2/SOI_2016_9.pdf

14. Haque M.A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019. Pp. 273–281. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00058

15. Nakamoto S. Bitcoin: Peer-to-Peer Electronic Cash System. 2019. Pp. 1–9. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802.

16. Improving Fleet Management with Blockchain Technology. URL: https://www.smartdatacollective.com/improving-fleet-management-with-blockchain-technology/ (дата звернення: 19.01.2025)

References

1. Giannaros A., Karras A., Theodorakopoulos L., Karras C., Kranias P., Schizas N., Kalogeratos G., Tsolis D. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. Journal of Cybersecurity and Privacy. 2023. No. 3(3). Pp. 493–543. https://doi.org/10.3390/jcp3030025

2. Horwitz, L. Data Center-Impact of Driverless Cars Could Broaden with Blockchain. URL: https://www.cisco.com/c/en/us/solutions/data-center/blockchain-driverless-cars.html (дата звернення: 19.01.2025).

3. Saranti P.G., Chondrogianni D., Karatzas S. Autonomous Vehicles and Blockchain technology are shaping the future of Transportation. In the 4th Conference on Sustainable Urban Mobility; Springer: Berlin/Heidelberg, Germany. 2018. Pp. 797–803. https://doi.org/10.1007/978-3-030-02305-8_96

4. Miller D. Blockchain and the Internet of Things in the Industrial Sector. In IT Professional. May/June 2018. Vol. 20, No. 3. Pp. 15–18. https://doi.org/10.1109/MITP.2018.032501742

5. Zhang Y., Wang L., Xiang Y., Ten C.-W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. IEEE Transactions on Smart Grid. July 2015. Vol. 6. No. 4. Pp. 1707–1721. https://doi.org/10.1109/tsg.2015.2396994

6. Kalashnyk H.A., Kalashnyk-Rybalko M.A. Problems of Ensuring Functional Resilience of the Onboard Equipment Complex of a Modern Aircraft. Science and Technology of the Air Force of the Armed Forces of Ukraine. 2021. No. 3 (44). Pp. 59–65. https://doi.org/10.30748/nitps.2021.44.07.

7. Barabash O.V., Svynchuk O.V., Bandurka O.I. Software for Monitoring the Operational Condition of Information Systems in the Energy Sector to Ensure Functional Resilience. Modern Information Protection. 2024. No. 2 (58). Pp. 41–49. https://doi.org/10.31673/2409-7292.2024.020005

8. Barabash O., Svynchuk O., Salanda I., Mashkov V., Myroniuk M. Ensuring the functional stability of the information system of the power plant on the basis of monitoring the parameters of the working condition of computer devices. Advanced Information Systems. 2024. Vol. 8, No. 2. P. 107 – 117. https://doi.org/10.20998/2522-9052.2024.2.12

9. Sobchuk V., Barabash O., Musienko A., Svynchuk O. Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. E3S Web of Conferences. 2021. Vol. 250. P. 82–87. https://doi.org/10.1051/e3sconf/202125008002

10. Barabash O.V., Svynchuk O.V., Shuklin H.V. Load Redistribution Algorithm to Ensure Functional Resilience of Distributed Web Applications. Communications. 2024. No. 5. Pp. 3–11. https://doi.org/10.31673/2412-9070.2024.050183

11. Baza M., Nabil M., Lasla N., Fidan K., Mahmoud M., Abdallah M. Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles. Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco. 2019. Pp. 1–7. https://doi.org/10.1109/WCNC.2019.8885769.

12. Rowan S., Clear M., Gerla M., Huggard M., Goldrick C.M. Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels. 2017. Pp. 1–10. https://doi.org/10.48550/arXiv.1704.02553

13. Lenkov S.V., Banzak H.V., Tsytsaryev V.M., Protsenko Ya.M. Prediction Algorithm for Reliability and Operating Cost Indicators of Radioelectronic Weapon Systems. Information Processing Systems. 2016. No. 9 (146). Pp. 28–30.
https://books.ndcnangu.co.ua/statti_NDL_2/SOI_2016_9.pdf

14. Haque M.A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019. Pp. 273–281. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00058

15. Nakamoto S. Bitcoin: Peer-to-Peer Electronic Cash System. 2019. Pp. 1–9. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802.

16. Improving Fleet Management with Blockchain Technology. URL: https://www.smartdatacollective.com/improving-fleet-management-with-blockchain-technology/ (дата звернення: 19.01.2025)