ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.28.16950

ПЕРСПЕКТИВИ ВІЙСЬКОВОГО ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

Опірський Іван, Василишин Святослав

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання .
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
ORCID ID:0000-0002-8461-8996.

ВАСИЛИШИН Святослав Ігорович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 1995 рік, м. Львів, Львівська область, Україна.
Освіта: Національний університет «Львівська Політехніка».
Посада: асистент кафедри захисту інформації.
Наукові інтереси: засоби захисту інформації в гібридних та кібер війнах, *білий хакінг.*
E-mail: swat2244@gmail.com.
ORCID ID:0000-0003-1944-2979.

Анотація. *Нові передові технології мають, як правило, величезний вплив на те, як бізнес впроваджує інновації для покращення своїх конкурентних переваг. З моменту появи Інтернету технології блокчейну були визнані одними з вибухових інновацій початку XXI століття. Технологія блокчейну даний час використовуються у фінансових додатках (наприклад, для платежів, обміну валюти, грошових переказів і гаманців, торгових фінансів, ринків, мікроугод, інвестиції, брокерства, страхування), а також в нефінансові додатки (наприклад, управління ідентифікацією в електронному вигляді, автентифікація та авторизація, системи зберігання та доставки даних в електронному вигляді, системи сертифікації, смарт-контракти, розробка додатків, електронне голосування на виборах, управління медичними записами пацієнтів, розподіл робочого навантаження для систем зв'язку , комп'ютерні системи, які мають відповідати вимогам законодавства без втручання людини, Інтернету речей і т.д.). І все ж застосування блокчейна найбільш виправдано при вирішенні завдань, пов'язаних в основному із забезпеченням цілісності інформації, що зберігається. Саме тому у цій статті ми розглядаємо перспективи застосування технології блокчейну у військовій справі, аналізуємо її властивості, розглядаємо проблеми та наводимо рішення, які відкриваються з початком використання даної технології. Технологія блокчейну здатна підсилити оборонний сектор держави та впровадити додатковий рівень захисту до вже існуючих.*

Ключові слова: *блокчейн, технології блокчейну, кіберзлочинність, системи захисту, військове застосування.*

Постановка проблеми

Оскільки масштаб і відкритість постійно зростають, Інтернет уже перейшов від Web 1.0 до Web 2.0. Представлений соціальними мережами, Інтернет на основі Web 2.0 також є «інтернетом інформації», який значно підвищує ефективність потоку інформації між компаніями та окремими особами та забезпечує ефективну доставку інформації людям.

Тим не менш, через обмеження операційного механізму Інтернету інформація залишається відтворюваною, її легко підробити та важко відстежити. Лише через централізованих сторонніх посередників ми могли забезпечити відносну надійність даних. Крім того, у міру того, як Інтернет продовжує розширюватися, властиві йому проблеми концентрації вартості, витоку конфіденційності, ненадійності даних і

нерівності розподілу інтересів, здається, стають дедалі помітнішими. Таким чином, очікується, що розподілений, інтелектуальний і персоналізований Web 3.0 лідируватиме в тенденції розвитку Інтернету, порівняння систем можна глянути в таблиці 1.

Технологія Blockchain народжується з реальних потреб, викликаних розвитком Інтернету. Він здатний запропонувати пряму технічну підтримку додатків штучного інтелекту (ШІ), а також децентралізованих мереж із супервузлами, таким чином сприяючи розвитку Інтернету від односторонньої передачі даних до спільного будівництва, а потім інтегрованого зростання за участю кількох сторін [1].

Таблиця 1

Порівняння Web 1.0, 2.0, 3.0

Тип	Web 1.0	Web 2.0	Web 3.0
Передача файлів	Лише читання	Читання та редагування	Читання та редагування та виконання
Тип мереж	Проста мережа	Соціальна мережа	Семантична мережа
Ємність користувачів	Мільйон	Мільярд	Трильйон
Вебсайти	Статичні	Динамічні	Інтелектуальні
Штучний інтелект	Відсутній	Відсутній	Присутній
Вміст	Розроблено експертами	На основі соціальних мереж	Персоналізований інформаційний потік
Пошукові двигуни	Доменні імена	Оптимізовані пошукові системи	побудовані з використанням ШІ
Централізація	Централізований	Централізований	Децентралізований
Мета	Об'єднати інформацію	Об'єднати користувачів	Об'єднати знання

Блокчейн — це свого роду технологія реєстру, керована спільнотою користувачів, яка забезпечує безпеку передачі та доступу за допомогою криптографії, забезпечує послідовне зберігання даних і запобігає будь-яким спробам змінити дані чи здійснити відмову. Типовий блокчейн використовує зв'язану блочну структуру для перевірки та зберігання даних, використовує механізм консенсусу розподіленого вузла для генерації та оновлення даних, використовує смарт-контракти, що складаються з автоматизованих сценаріїв для програмування та обробки даних, і, як зазначено вище, забезпечує безпеку передачі даних і доступу криптографією [2].

Як новий тип обчислювальної парадигми та рішення, що встановлює механізм довіри в неймовірному та конкурентному онлайн-середовищі з низькими витратами, блокчейн зараз змінює сценарії застосування та правила роботи в різних галузях. У цьому сенсі це одна з незамінних технологій для розвитку цифрової економіки та побудови системи довіри. З моменту свого народження в 2008 році технологія була оновлена з Blockchain 1.0 до Blockchain 2.0 і тепер Blockchain 3.0.

Створення Bitcoin знаменує собою початок ери Blockchain 1.0. Біткойн пропонує вирішення проблеми подвійних витрат цифрових валют і представляє справжню цифрову валюту за допомогою розподіленого запису та зберігання на основі блокчейну, що є епохальним. Blockchain 1.0 в основному застосовується в сферах, тісно пов'язаних з цифровою валютою, таких як переказ валюти, обміни та оплата. З Blockchain 1.0 встановлена ланцюгова структура блокових одиниць, яка допомагає забезпечити автентичність інформації, що міститься в реєстрі, шляхом спільного використання реєстру між усіма блоками та перевірки автентичності інформації за допомогою асиметричного алгоритму шифрування та коду з відкритим кодом, таким чином вирішуючи проблему як платіж на основі валюти, так і децентралізований платіж. Загалом, це покоління блокчейнів характеризується технічними особливостями децентралізації, захисту від втручання, колективного обслуговування, відстеження та безпеки [3].

На початковому етапі розробки Blockchain 1.0 враховувалися лише атрибути транзакцій цифрової валюти. Таким чином, Blockchain 1.0 міг підтримувати лише виконання деяких простих наборів інструкцій за багатьох обмежень. Щоб вирішити цю проблему, Blockchain 2.0 з'явився в потрібний момент. Тісно пов'язаний із розвитком контрактних технологій, Blockchain 2.0 найчастіше застосовувався в Ethereum. Потім технології блокчейн почали застосовувати в різних галузях. Ethereum — базова система з відкритим вихідним кодом на основі блокчейну, здатна працювати з усіма блокчейнами та контрактами та підтримувати швидкий розвиток різноманітних блокчейн-додатків. Зокрема, смарт-контракти є однією з найбільш відмінних рис Ethereum [4]. Розумні контракти, як фундаментальна технологія програмованої валюти та програмованих фінансів, можуть зберігати та передавати цінності дуже ефективним способом. Блокчейн створює надійне середовище для виконання смарт-контрактів; і, в свою чергу, смарт-контракти підтримують розширення додатків блокчейну. Глибоке застосування Blockchain 2.0 вивело технологію далеко за межі сфери валют із програмованими характеристиками. Наразі розробка Blockchain 2.0 все ще знаходиться на ранній стадії, і масштабне застосування ще не реалізовано. Blockchain 3.0 запровадить еру комплексного застосування технології блокчейн, у якій технологія блокчейну еволюціонуватиме від «децентралізованої програми (DApp)» до «децентралізованої автономної корпорації (DAC)», потім «децентралізованої автономної організації (DAO)» і, нарешті, «Децентралізоване автономне суспільство (DAS)». На даний момент операційна система блокчейн EOS є типовим інфраструктурним проектом, що розробляється. У майбутньому Blockchain 3.0 буде широко впроваджуватися в таких галузях, як охорона

здоров'я, Інтернет речей (IoT), економіка спільного використання тощо. Здатний розпізнавати право власності, вимірювати та зберігати дані в Інтернеті, Blockchain 3.0 зробить відстежуваність активів, керованість і зчитування вздовж блокчейну реальністю та, зрештою, відкриває «програмоване суспільство» для всіх [5].

В умовах інформаційної асиметрії блокчейн економить зусилля щодо представлення взаємно гарантованої довіри або перевірених сертифікатів достовірності третьою стороною. Натомість, базуючись на механізмі довіри вузлів, створеному алгоритмами шифрування, що підтримують великі дані, блокчейн забезпечує інтелектуальну довіру, а також підвищення цінності для всіх сторін. Основні атрибути такі:

- Децентралізований/слабо централізований. Блокчейн — це розподілена структура зберігання даних без централізованих вузлів. Кожен вузол ланцюга зберігає однакову інформацію; а перевірка, облік, зберігання, підтримка та передача всіх даних блокчейна базуються на розподіленій систематичній структурі. Структура використовує суто математичні методи замість центральних установ для встановлення довірчих відносин між розподіленими вузлами, щоб у випадках інформаційної асиметрії могла бути сформована децентралізована та надійна розподілена система. У спеціальних прикладних сценаріях він також може гнучко використовувати слабко централізовані вузли керування [6].
- Захищений від втручання та відстеження. Після надсилання даних вони залишаються постійними та не можуть бути знищені чи змінені. Блокчейн використовує ланцюгову блочну структуру з мітками часу для зберігання даних, додаючи тим самим часовий вимір до даних, отже, надійну перевірку та відстежуваність.
- Прозорий і надійний. Правила роботи технології блокчейн та інформація про дані, що передаються в блокчейнах, є прозорими, і перевірка ідентичності між вузлами не потрібна. Таким чином можна зменшити як ризики шахрайства, так і посередницькі витрати, а також забезпечити довірену передачу даних у недовіреній мережі.
- Підтримується колективно. Блокчейн використовує певний механізм економічного стимулювання, щоб забезпечити участь усіх вузлів у розподіленій системі в процесі перевірки блоків даних (наприклад, у процесі «майнінгу» біткойнів), і покладається на механізм консенсусу для вибору конкретних вузлів для додавання в ланцюжок нових блоків, що надає технології блокчейн властивість самообслуговування і, таким чином, знижує витрати на експлуатацію та обслуговування мережі [7].
- Програмований. Технологія блокчейн може надавати гнучку систему коду сценаріїв, яка підтримує користувачам створювати розширені смарт-контракти, валюти чи інші децентралізовані програми, дає змогу тісно інтегрувати технологію блокчейну з існуючими технологіями, а потім застосовувати її в різних сценаріях. Наприклад, платформа Ethereum надала повні мови сценаріїв для користувачів, щоб створити будь-який смарт-контракт або тип транзакції, який можна точно визначити [8].
- Покращена безпека. Технологія блокчейн використовує асиметричну криптографію для шифрування даних. У той же час він використовує механізми консенсусу, такі як консенсус підтвердження роботи (PoW) для кожного вузла в розподіленій системі, щоб сформувати потужну обчислювальну потужність, щоб протистояти зовнішнім атакам і запобігати фальсифікації та підробці даних. У порівнянні з традиційними методами безпеки, він, природно, може похвалитися вищою безпекою та непорушністю.

Виклад основного матеріалу дослідження

Технологія блокчейн — це комбінація ряду існуючих технологій, включаючи розподілені мережі, криптографічну технологію, доказ роботи (механізм консенсусу), візантійський протокол відмовостійкості (угода, яка гарантує послідовність і активність розподілених систем, навіть якщо є шкідливі вузли), тощо.. [9]. Ці технології пройшли більше десяти років або навіть десятиліть розвитку та еволюції. Крім поєднання існуючих технологій, були інтегровані нові технології та постійно впроваджувались інновації. Основні задіяні технології в основному такі:

- Блок + ланцюг. Це базова структура для запису даних. Блок складається із заголовка блоку та тіла блоку. Тіло блоку відповідає за запис даних за попередній період, головним чином кількість і деталі, дані покладаються на асиметричне шифрування для забезпечення безпеки та автентичності інформації. Заголовок блоку інкапсулює номер поточної версії, адресу попереднього блоку, мітку часу, випадкове число та цільове хеш-значення поточного блоку (за допомогою певного алгоритму хешування довгий фрагмент даних можна відобразити коротшим; і це коротка частина даних, або малі дані, — це хеш-значення великих даних, яке змінюється разом із змінами великих даних), а також кореневе значення дерева Меркле (двійкове хеш-дерево, яке часто використовується для швидкого запиту даних у галузі інформатики). На основі хешу попереднього блоку, записаного в поточному блоці, блоки можуть сформувати незмінний блокчейн [10].
- Зв'язок «точка-точка». Блокчейн використовує однорангову (P2P) мережу для зв'язку, що робить кожного користувача в мережі не лише вузлом, а й сервером. Ресурси та послуги в мережі розкидані по всіх вузлах, а передача інформації та реалізація послуг здійснюються безпосередньо між вузлами без будь-якої участі посередників або втручання сервера.
- Механізм консенсусу. У одноранговій мережі, оскільки кожен вузол має право пакувати дані та генерувати нові блоки, щоб усі вузли погоджувалися щодо щойно згенерованих блоків у ланцюжку блоків і забезпечували узгодженість блоків запису вузлів у всьому мережі блокчейн встановлює механізм консенсусу [11]. У світлі механізму будь-який вузол у мережі може створювати нові блоки лише за умови, що новий блок відповідає попередньо встановленим вимогам механізму консенсусу (Proof of Work [PoW], механізм Proof of Stake (PoS), механізму Delegated Proof of Stake (DPoS), протоколу Raft, а також Byzantine Fault ToleranceAlgorithm (Practical ByzantineFault-

Tolerant, PBFT), тобто для розпізнавання всіма вузлами всієї мережі та додавання до спільного блокчейну з незалежними зберігання [12].

- Розумний контракт. Це набір процедурних правил і логіки, реалізованих за допомогою децентралізованих, надійних і спільних кодів сценаріїв, розгорнутих у блокчейні. Як правило, розумні контракти підписуються відповідними сторонами, а потім додаються до даних блокчейну у вигляді програмних кодів. Потім вони записуються в окремі блоки в блокчейні після передачі мережі P2P і перевірки вузла. Розумні контракти інкапсулюють ряд попередньо визначених станів і правил переходу, сценарії, які можуть ініціювати виконання контракту, і відповідні дії в конкретних сценаріях. Блокчейн може відстежувати стан смарт-контрактів у режимі реального часу, а також активувати та виконувати контракт після перевірки зовнішніх джерел даних і підтвердження виконання певних умов запуску. Розумні контракти можуть забезпечити відстеження, незворотність і безпеку транзакцій за відсутності третіх сторін.

Взаємозв'язок між технологією блокчейн і ШІ, великими даними та іншими передовими технологіями

Розробка та застосування технології блокчейн були б неможливі без підтримки інфраструктури інформаційних технологій нового покоління, таких як ШІ, великі дані, хмарні обчислення та Інтернет речей. У свою чергу, технологія блокчейн також сприяла розвитку цих інформаційних технологій. Очікується, що ШІ та блокчейн доповнюватимуть один одного відповідними перевагами [13].

Зазначимо, що ШІ може допомогти вирішити проблеми, з якими стикається блокчейн, щодо автономності, ефективності, енергоефективності та інтелекту, особливо достовірності даних у додатках ШІ, щоб ШІ міг більше зосередитися на алгоритмах. Крім того, штучний інтелект здатний більш ефективно керувати автономною організацією блокчейну, розширювати та покращувати функції та ефективність смарт-контрактів, а також оптимізувати операції блокчейну для підвищення безпеки, ефективності та енергоефективності.

Блокчейн може забезпечити розподілений штучний інтелект, реалізувати взаємний виклик різноманітних функцій штучного інтелекту, прискорити розробку штучного інтелекту, порушити наразі закритий режим розробки та сприяти обміну даними. Крім того, блокчейн також можна використовувати для моделей даних журналу аудиту, що забезпечує більш надійні прогнози тощо.

Коли кількість вузлів досягає певного масштабу, вартість атаки також буде величезною, що ускладнить реалізацію атаки. У цьому сенсі проблема витоку даних буде вирішена ефективно.

Вартість експлуатації та обслуговування IoT значно зменшується. Завдяки технології блокчейн IoT може передавати дані за принципом «точка-точка» [14].

Пряме з'єднання без використання центральних процесорів. Розподілені обчислення можна використовувати для обробки сотень мільйонів транзакцій. Більше того, обчислювальна потужність, ємність зберігання та пропускна здатність сотень мільйонів неактивного обладнання значно зменшать витрати на обчислення та зберігання.

Перевірка третьою стороною не потрібна. Технологія блокчейн може допомогти вирішити проблеми масштабованості, одноточкового збою, відміток часу, запису, конфіденційності, довіри та надійності абсолютно послідовним чином. У повністю децентралізованій довіреній цифровій інфраструктурі обладнання IoT може працювати незалежно без необхідності отримання будь-якої централізованої авторизації [15].

Безпека IoT гарантована. Блокчейн може записувати всі дії термінальних пристроїв. Оскільки записана інформація ніколи не може бути переписана, безпека даних і конфіденційність користувачів будуть поставлені під ефективний захист.

Послуги хмарних обчислень характеризуються великим масштабом, високою надійністю, низькою вартістю, гнучкістю та доставкою на вимогу. У поєднанні з децентралізацією та захистом даних від блокчейну він має потенціал для сприяння широкому застосуванню технології блокчейну. У майбутньому на основі інфраструктури та послуг (IaaS), платформи як послуги (PaaS) і програмного забезпечення як послуги (SaaS) буде створено блокчейн як послугу (BaaS) для інтеграції технології блокчейну в платформи хмарних обчислень. і створити ринок хмарних послуг BaaS, таким чином забезпечуючи стабільні та надійні платформи хмарних обчислень для децентралізованих програм [16].

Перспективи військового застосування технології блокчейн

Командно-інформаційна система є важливим методом і обладнанням для реалізації точного й автоматичного командування на полі бою під час війни в реальному часі та допомагає штабам усіх рівнів здійснювати науково ефективне управління підлеглими підрозділами та озброєнням у звичайний час. Будучи органічною системою «людина-машина», в якій командири є ядром, а комп'ютери та використовують комп'ютери та інше інформаційно-технологічне обладнання як передумову та матеріальну гарантію, система органічно поєднує різні методи командування та управління та командирів, щоб забезпечити високу - рівень автоматизації збору, передачі, обробки та використання інформації військового управління. Таким чином, забезпечується цілісність даних, доступність і безпека командної інформаційної системи, а в основному гарантується підвищення боєздатності та успіх у захопленні ініціативи у війні [17].

Інформаційна система Блокчейн + Командування. По-перше, командна інформаційна система має централізовані мережі та бази даних. Будучи важливою ціллю у воєнний і навіть мирний час, він вразливий перед ворогами чи хакерами. Вони можуть використовувати різні інформаційні засоби для проведення мережевих і електричних атак, спричиняючи паралізацію всієї інформаційної системи, або для викрадення та фальсифікації ідентифікаційної інформації, підробки важливих даних. Тому учасники бойових дій стикаються з великими ризиками щодо

достовірності даних і навіть можуть приймати помилкові рішення зі шкідливими даними. По-друге, коли командири покладаються на командну інформаційну систему для прийняття рішень, існуватиме ризик віддавати неправильні команди чи фальшиві накази, спричинені підробкою даних ворогом. Технічний принцип: інформаційну систему команд, засновану на технології блокчейн, можна розділити на рівень даних, мережевий рівень, рівень консенсусу, рівень стимулювання, рівень контракту та рівень додатків. Серед них рівень даних гарантує надійність даних або розвідувальних даних, надійність і безпеку військової інформаційної системи; мережевий рівень гарантує самоорганізацію та децентралізацію функцій військових інформаційних систем; консенсусний рівень інкапсулює різні типи консенсусних алгоритмів для досягнення автономного та надійного прийняття рішень; рівень заохочення використовує програмований механізм заохочення, щоб уникнути всіх видів неправильної поведінки та досягти стимулів позитивної поведінки; договірний рівень допомагає автоматизувати та інтелектуальні військові інформаційні системи, зменшуючи невизначеність, різноманітність і складність, яку люди та інші фактори привносять у бойове командування та військове управління [18].

Рішення: використовуючи переваги децентралізованих і розподілених функцій, механізму консенсусу, автономних характеристик і кредитного механізму алгоритму асиметричного шифрування технології блокчейн, ми можемо створити автоматичну та безпечну систему командування та контролю. Поєднавши його зі штучним інтелектом і військовим Інтернетом речей у майбутньому, ми можемо спочатку змінити бойовий контроль на тактичному рівні з централізованого режиму на децентралізований. Також можна досягти достовірного бойового командування, що означає, що команди, віддані командирами на всіх рівнях, можуть бути повністю записані, а переписані дані є доказами та простежуються. Лише коли ворог або хакери модифікують більше 51% інформації вузла одночасно (атака 51%), дані командної інформаційної системи можуть бути змінені. Завдяки даним часових рядів, спільному обслуговуванню та програмованим і надійним функціям технології блокчейн можна реалізувати динамічний і постійний запис у мережах або базах даних, а також можна ефективно запобігти неправдивій інформації та злому. Таким чином, ми можемо відстежувати в режимі реального часу, чи була підроблена база даних, чи відстежувалась військова система, і виключити ризик атак противника, притаманний командним інформаційним системам. Типовий випадок: DARPA намагається розробити безпечну та надійну інформаційну платформу на основі технології блокчейн. Це буде безпечна система інформаційного обслуговування, здатна ефективно захищати конфіденційні дані та запобігати злому [19].

Блокчейн + операції кластера БПЛА. Кластерні системи БПЛА мають п'ять типових характеристик, а саме децентралізацію, автономне управління, відновлення кластера, посилення функцій і відсутність втрат. Однак поточні БПЛА в кластерах не мають загального сприйняття зовнішнього середовища, а також бракує ефективного обміну інформацією та координації дій між окремими БПЛА та формуваннями БПЛА.

Рішення: використовуючи механізм консенсусу технології блокчейн, ми можемо перетворити особисту довіру й інституційну довіру до машинної. На майбутньому полі бою система управління та управління кластеру БПЛА обмінюватиметься даними бойових команд у децентралізованій манері та таким чином уніфікує операції. Здатність підтримувати боєздатність за будь-яких втрат має велике значення для реалізації нового командно-управлінського режиму «людина-машина/машина-машина», який відповідає безпілотним операціям. Перше стосується безпеки. Завдяки функціям «шифрування та дешифрування відкритих і закритих ключів» і «цифрового підпису» технології блокчейн кожен БПЛА в кластері може служити вузлом мережі. Усі вузли спільно використовують і ведуть ту саму ноду, забезпечують автентичність даних зв'язку та перевіряють ідентичність учасників кластера. Другий передбачає розподілене прийняття рішень. Розподілені алгоритми прийняття рішень є ключем до ефективної роботи кластерних систем БПЛА, а механізм консенсусу гарантує, що всі вузли в розподіленій системі узгоджують мету прийняття рішень. У реальному бою кожна сутність у кластері повинна узгодити оперативні завдання та цілі, такі як групування та форматування, планування шляху та уникнення бар'єрів. Третє – для контролю формування. Технологія сайдчейн блокчейну дозволяє ієрархічно з'єднувати декілька блокчейнів один з одним. З одного боку, БПЛА в різних ланцюгах можуть діяти відповідно до попередньо встановленого протоколу в ланцюжку, де вони розташовані; з іншого боку, міжланцюгова співпраця полегшує перемикання між різноманітними кластерними утвореннями. У процесі скоординованого пошуку, розвідки та атаки кластер БПЛА може змінювати стрій, щоб захистити себе та знищити ворога [20].

Четвертий – про децентралізовані автономні кластери. У майбутньому кожна сутність у кластери БПЛА розглядатиметься як автономний агент із функцією сприйняття, міркування та прийняття рішень. Ці агенти формуватимуть різні децентралізовані автономні кластери за допомогою смарт-контрактів для автономного виконання оптимальних рішень.

Автономне управління БПЛА в режимі «рою»

У сучасних системах боротьби з терористами безпілотники активно розгортаються в польових операціях для спостереження, розвідки та цілеспрямованих атак. Також безпілотники можуть відігравати важливу роль під час рятувальних операцій у зонах, що постраждали від катастроф і природних катаклізмів. Наприклад, дрони доставляють аптечки першої допомоги постраждалим до того, як бригада медиків прибуде на місце.

Система безпілотника включає в себе вбудовані датчики, GPS, стабілізатори та камери високої чіткості для збору та розповсюдження даних для представлення детальної обізнаності про ситуацію на наземному диспетчері. Контролер може наказувати дронам змінювати їх поведінку або фізичне положення. У

відповідь він коригує, збирає та пересилає оновлені дані, щоб представити ситуацію диспетчеру. Для порівняння, автономні безпілотники можуть відстежувати свою швидкість, рух і ресурси для незалежного реконфігурації та перенастроювання для досягнення своєї мети. На продуктивність безпілотників впливає наявність супротивників. Наприклад, перешкоди комунікації супротивників між безпілотником і контролером можуть призвести до провалу місії безпілотника. Змагальні вузли у багатьох випадках вставляють регулятори у вбудоване програмне забезпечення дронів, щоб зламати систему.

Рій складається з кількох автономних дронів, які працюють разом для досягнення мети. Кожен дрон у групі може злітати, приземлятися та зависати. Дрони організовані в шари, які називаються кластерами, і один із дронів обирається лідером рою для зв’язку з наземним диспетчером. Кожен дрон може спілкуватися з лідером зграї та дронами того самого кластера, щоб обмінюватися інформацією. Зв'язок між дронами допомагає безпілотникам коригувати свою поведінку у відповідь на дані в реальному часі. Однак рій вразливий до військових атак, оскільки вороги можуть перехопити зв’язок між дронами, щоб порушити дані. Керування роями за допомогою блокчейну може допомогти зареєструвати кожен безпілотник на платформі блокчейн. Транзакції з цифровим підписом, походження даних і механізм консенсусу можуть допомогти негайно ідентифікувати та звести нанівець дані, які були пошкоджені між дронами. Блокчейн-рішення на основі смарт-контрактів із контролем доступу гарантують, що лише зареєстровані вузли можуть отримати доступ до ноди для участі в ройових операціях [21].

В оборонному секторі рій може ідентифікувати потенційні цілі, середовище та небезпеки на основі даних у реальному часі. Кожен дрон зграї однаково бере участь у розпізнаванні ситуації чи цілі.

Технологію блокчейн можна використовувати для досягнення прозорого та високонадійного глобального прийняття рішень роєм, яке можна перевірити. Наприклад, безпечне голосування за допомогою блокчейну може допомогти зграї дронів прийняти глобальне рішення. У системах військового захисту зграї можна використовувати для (а) виявлення ворогів, (б) ідентифікації моделей пересування, (в) розпізнавання поранених солдатів на полі бою, (г) визначення перешкод і (д) каталогізації жертв у надзвичайних ситуаціях.

На рис. 1 представлена методологія з використанням блокчейну для виявлення зловмисників на полі бою. Камера дрона лідера зграї знімає відео для розпізнавання об’єктів на полі бою. У відповідь лідер створює дві адреси (розумні контракти) на блокчейні, щоб запросити членів рою дізнатися їхню думку. У відповідь кожен зареєстрований дрон запускає свій алгоритм розпізнавання об’єктів і оцінює результат. Він розраховує ймовірність того, що об’єкт є зловмисником, і записує результат у блокчейн. Розумний контракт, що зберігається в блокчейні, автентифікує та перевіряє походження даних. Нарешті, смарт-контракт об’єднує думки всіх безпілотників, щоб опублікувати кінцевий результат. Катастрофи та стихійні лиха, такі як землетруси, можуть пошкодити мережеву інфраструктуру, що призводить до обмеження зв’язку між рятувальними командами.

Відповідно, це впливає на роботу рятувальної групи. Типові системи забезпечують безперервний зв’язок рятувальних команд, таких як пожежні бригади, військові, поліція, медичний персонал і організації соціального забезпечення, щоб обмінюватися даними. Безінфраструктурні спеціальні мережеві технології використовуються для з’єднання рятувальних команд у постраждалих від стихійних лих районах. Захищений і контрольований рій можна використовувати для дистанційного моніторингу рятувальних операцій у певній місцевості. Ройові послуги можуть включати спостереження, зондування та логістику для постраждалих районів. Рій може складатися з різнорідних дронів, якими володіють і керують різні партнери [22].

Процес реєстрації для схеми рою за допомогою блокчейну реєструє кожного власника та дрона в мережі блокчейн. Користувач може відстежувати деталі роя, такі як тип послуги, вартість і репутація в ланцюгу, щоб найняти його (через відстеження незмінних записів). На наступному етапі користувач вносить криптовалюту в гаманець смарт-контрактів, щоб використовувати сервіси роя. Сертифікат угоди про рівень обслуговування (SLA) має цифровий підпис і зберігається на сервері IPFS. Хеші сертифіката реєструються в блокчейні. Рій надає обрані послуги користувачам протягом певного періоду. Усі транзакції та дані з цифровим підписом незмінно записуються в книгу блокчейну для цілей аудиту. Після надання послуги смарт-контракт перераховує суму на гаманець власника для здійснення платежу (підлягає перевірці). Таким чином, технологію блокчейн можна використовувати для створення надійної системи серед ненадійних користувачів.

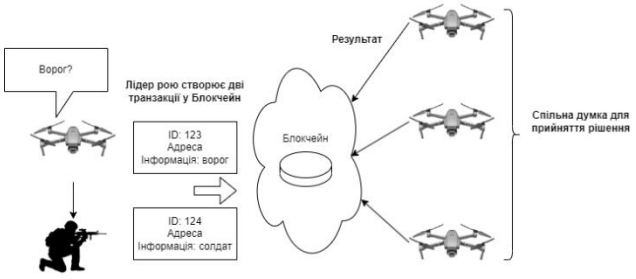

Рис. 1 Методологія з використанням блокчейну для виявлення зловмисників на полі бою

Військове управління

Традиційна структура військового управління — це система «командування та контролю» зверху вниз, яка породжує такі проблеми, як роздуті інституції, високі витрати на управління, нечітке визначення відповідальності, неефективне управління, надмірне управління, погана передача інформації та концентрація влади на верхнього рівня, тоді як нижні рівні мають дуже обмежену автономію і, отже, обмежений інноваційний потенціал.

Блокчейн + управління зброєю. Сучасна війна вимагає кращої чутливості та спритності бойових систем, але інститути, що мають ієрархічну структуру працює неефективно. Необхідно записати велику кі-

лькість даних, таких як проектні плани, результати випробувань і стан бойової техніки протягом усього життєвого циклу зброї, починаючи з проекту, демонстрації, розробки, виробництва та надання послуг до виходу на пенсію. Інформацію легко втратити або підробити в процесі.

Рішення: на основі технології блокчейн ми можемо побудувати систему управління зброєю та обладнанням протягом життєвого циклу, якою спільно керують і взаємно контролюють розробники, виробники та користувачі. За допомогою системи ми можемо відстежувати та керувати параметрами конструкції обладнання, даними випробувань, станом бойової техніки та записами про технічне обслуговування. Жодним вмістом не можна маніпулювати чи видаляти, що покращує інформаційну безпеку, зручність і надійність. Усі дії управління покладатимуться на розумні контракти для відкритих і прозорих рішень, зменшення ієрархії управління, формування плоского режиму управління та, нарешті, підвищення ефективності. У той же час можна простежити походження кожного компонента озброєння та обладнання, що допомагає вирішувати суперечки щодо контрактів на закупівлю та створює повну непорушну систему моніторингу, управління та контролю, таким чином покращуючи безпеку управління, зручність та довіру.

Блокчейн + управління конфіденційними даними. Використовуючи динамічну функцію технології блокчейн, ми можемо забезпечити вирішення проблеми «важко підтримувати докази» в управлінні конфіденційними даними у військовій інспекції та нагляді, людських ресурсах, медицині та охороні здоров'я. «Правдивий запис» усієї інформації можна реалізувати за допомогою «свідка всієї мережі», що дозволяє уникнути підробок документів, втрат файлів і фальсифікації інформації [23].

Військова логістика. Важко вирішити проблеми, пов'язані з мережею, зберіганням даних, обслуговуванням системи, відстежуваністю та контролем якості під час пакування, завантаження та розвантаження, транспортування та розбирання у військовій логістиці.

Рішення: використовуючи технологію блокчейн, ми можемо створити окремий, безпечний, спільний і постійний запис, який можна перевірити, відстежувати та перевіряти транзакції різних ланцюгів постачання та між усіма операційними партнерами, а також здійснювати ефективне управління життєвим циклом ланцюга поставок оборонного призначення та системи закупівлі та логістика. Впровадивши технологію блокчейн у військову логістичну мережу, ми можемо побудувати децентралізовану автономну мережу персоналу та матеріалів у логістичних системах. Дані, пов'язані з виробництвом, закупівлею, транспортуванням і розподілом матеріалів у системах, можуть зберігатися в різних блоках в уніфікований спосіб, що може значно підвищити безпеку військової логістичної інформації та дозволити військовому матеріально-технічному обладнанню та енергії відповідати вимогам. різних служб і відділів, тому завжди в найкращому стані.

Сучасна військова логістика передбачає розумне складування, пакування, транспортування та розподіл. Різні процеси утворюють невеликий військовий IoT на основі динамічної автономної мережі людей і об'єктів. Використовуючи вузли, ми можемо спілкуватися безпосередньо або через ретранслятори, щоб керувати важливими даними у військовому логістичному ланцюгу, такими як потреби користувачів, товари, що зберігаються, завантаження, транспортування, розподіл і транзит. Технічне обслуговування блокчейну контролюватиметься всіма вузлами по всій мережі, а незаконна робота деяких окремих вузлів буде відхилятися та протистояти більшості вузлів. Таким чином підвищиться безпека та зручність транзакцій, а також скоротиться час, який витрачається на інтелектуальну військову логістику [24]. Він також може допомогти вирішити проблеми, пов'язані з мережею, зв'язком, зберіганням даних і обслуговуванням системи під час пакування, завантаження, розвантаження, транспортування та розбирання у військовій логістиці, таким чином забезпечуючи впорядковану та ефективну роботу системи. Це вважається найбільш перспективним військовим застосуванням блокчейна. Типовий випадок: у квітні 2016 року Міністерство оборони США та його союзники по НАТО почали звертати увагу на потенційне застосування технології блокчейн в обороні, включаючи автоматичне виконання смарт-контрактів, безпечне зберігання конфіденційних файлів і зменшення помилок і перерв. під час виконання оборонного контракту. Крім того, технологію блокчейн також можна застосувати для реагування на надзвичайні ситуації, коли трапляються катастрофи, і підвищити прозорість закупівель сировини в ланцюжку поставок і транспортування барж у процесі логістики. У червні 2017 року ВМС США скористалися технологією блокчейн для підвищення безпеки систем адитивного виробництва. Вони записували весь процес проектування компонентів, виготовлення прототипу, тестування, виробництва та остаточної обробки, щоб користувачі могли переглядати будь-які конкретні дані та повідомляти про пошкодження компонентів або в кінці їх життєвого циклу.

Військова безпека

Квантовий блокчейн. Необхідно забезпечити безпеку передачі даних на полі бою, вирішити проблеми перехоплення, дешифрування та розвідки сигналів. Рішення: використовуючи квантовий розподіл ключів як заміну оригінальної структури закритого ключа та використовуючи функції квантової криптографії блокчейн-мережі для захисту від підслуховування та перехоплення, ми можемо значно підвищити захисну здатність мережі блокчейн і справляти руйнівний вплив на проблему перехоплення, дешифрування та виявлення сигналу.

Блокчейн + еластична комунікація. Має бути забезпечена безпека передачі даних на полі бою. Рішення: ґрунтуючись на розподілених характеристиках технології блокчейн, можна побудувати систему зв'язку із широким охопленням, стійку до аварій та високий рівень безпеки, щоб досягти безпечного та стійкого зв'язку в складному середовищі на полі бою. Типовий випадок: у травні 2017 року компанія Tech-

nology and Manufacturing Company зі штату Індіана, фінансована DARPA, використала технологію блокчейн для розробки «недоступної платформи обміну повідомленнями та торгівлі» для військових. Ця платформа розділяє створення та передачу інформації, щоб гарантувати, що надіслані та отримані дані неможливо зламати, і забезпечити безпечний зв'язок між штабом і наземними силами, а також між Міністерством оборони та офіційними особами розвідки. У липні 2019 року в рамках стратегії цифрової модернізації Міністерства оборони DARPA почало використовувати технологію блокчейн для створення ефективнішої, потужнішої та безпечнішої комунікаційної платформи, щоб сприяти безпечній передачі інформації для будь-яких командних, контрольних і комунікаційних систем, що дозволяють персонал для відстеження транзакцій через канал розподіленої книги та гарантування безпеки зв'язку між штабом і сухопутними військами, а також між офіційними особами Міністерства оборони та розвідки в майбутньому.

Висновки. Певною мірою блокчейн — це новий тип інформаційної технології, яка жертвує простором для зберігання, швидкістю доступу та загальною ефективністю заради безпеки та довіри даних. Це в основному підходить для сценаріїв військового застосування з низькою частотою використання, високими вимогами до безпеки, низькою своєчасністю та невеликим обсягом даних.

По-перше, висока надмірність і величезне споживання енергії ускладнюють виконання вимог щодо легкої ваги та розширення. Кожен вузол блокчейну повинен синхронізувати всі дані будуть зберігатися в реальному часі в кожному блоці. Зі збільшенням кількості даних і додаванням нових вузлів система ставатиме більш зайвою, що потребуватиме більше ресурсів зберігання. Це вимагає від бойових одиниць або платформних терміналів великої ємності для зберігання, обчислення та зв'язку, що суперечить тенденції полегшення та мініатюризації обладнання. Зі збільшенням кількості вузлів обчислювальна потужність, пропускна здатність та енергія, споживана кожним вузлом під час синхронізації даних, також збільшаться. З більшою кількістю вузлів вимога до ємності для зберігання наступних нових вузлів буде вищою; складність доступу збільшиться; збільшиться час, необхідний для синхронізації; і ефективність роботи в цілому буде знижуватися, що все перешкоджатиме широкомасштабному розширенню бойової системи за потребою.

По-друге, складним механізмом синхронізації даних важко задовольнити вимоги до високочастотної швидкої реакції. Кожна зміна даних у блокчейні вимагає від усіх вузлів системи синхронного оновлення даних книги, що займає багато часу.

Якщо операція виконується надто часто протягом короткого проміжку часу, буде використано багато смуги пропускання, отже, потенційне перевантаження мережі. Сучасна війна вступила в епоху «другого вбивства», особливо на тактичному рівні та рівні платформи. Це означає, що оновлення ситуаційної інформації зростає швидше, а бойові підрозділи та платформи надсилають програми інформаційної допомоги з більшою частотою. Технології блокчейн важко відповідати цим вимогам у режимі реального часу.

По-третє, механізм консенсусу та алгоритм шифрування все ще мають ризики безпеки. Безпека механізму консенсусу технології блокчейн залежить від криптографічного алгоритму. Криптографічний алгоритм не є абсолютно безпечним, і все ще існує ризик його злому. Наприклад, криптографічний алгоритм на основі еліптичної кривої широко використовується в блокчейні. Хоча за допомогою класичних комп'ютерів зламати дуже важко, для квантових комп'ютерів це завдання досить легко. В даний час світові держави активізують зусилля для досягнення прориву в технології квантових обчислень. Після розробки надійного та практичного квантового комп'ютера більшість сучасних технологій блокчейну втратять гарантії безпеки.

По-четверте, малий масштаб військового блокчейна знижує безпеку системи. З точки зору принципу технології блокчейн, якщо зловмисники не змінять більше ніж 51% вузлів одночасно, вони не зможуть підробити дані, що містяться в блокчейні. Отже, чим більше вузлів, тим важче зловмиснику змінити дані. Для блокчейнів, які використовуються у військовій сфері, кількість вузлів зазвичай набагато менша, ніж кількість вузлів, які містяться в цивільних системах на основі Інтернету. Під час війни, перед обличчям широкомасштабних мережевих атак, запущених противником з величезною обчислювальною потужністю, все ще можливо модифікувати більше половини вузлів і підробити дані.

По-п'яте, використання військових вузлів блокчейну створює проблеми в механізмі стимулювання. Оскільки мережа блокчейнів є децентралізованою розподіленою системою, у процесі взаємодії неминучі ігрові відносини, що включають як конкуренцію, так і співпрацю між вузлами. Розробка механізму консенсусу, сумісного з військовими стимулами, стала ключовим питанням для будь-якого військового блокчейна, перш ніж він стане практичним.

Зрештою, лише добре розроблений механізм консенсусу може дозволити вузлам у децентралізованій системі одночасно виконувати перевірку даних і затримку, збільшуючи вартість здійснення неналежної поведінки в системі та, таким чином, перешкоджаючи атакам і загрозам безпеці.

ЛІТЕРАТУРА

[1] R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: a survey, some research issues and challenges, IEEE Commun. Surv. Tutorials, 21 (2019), pp. 1508– 1532. http://doi.org/10.1109/COMST.2019.2894727.

[2] T. Ma, H. Wang, L. Zhang, Y. Tian, N. Al-Nabhan, Graph classification based on structural features of significant nodes and spatial convolutional neural networks, Neurocomputing, 423 (2021), pp. 639–650. https: //doi.org/10.1016/j.neucom.2020.10.060.

[3] Y. Tian, B. Song, M. Murad, N. Al-Nabhan, Trustworthy collaborative trajectory scheme for continuous LBS, Int. J. Sens. Networks, 38 (2022), pp. 58–69. http://doi.org/10.1504/IJSNET.2022.120275.

[4] L. Fu, Z. Li, Q. Ye, H. Yin, Q. Liu, X. Chen, et al., Learning robust discriminant subspace based on joint

L2,p- and L2,s-norm distance metrics, IEEE Trans. Neural Networks Learn. Syst., 33 (2022), pp. 130–144. https: //doi.org/10.1109/TNNLS.2020.3027588.

[5] Q. Ye, P. Huang, Z. Zhang, Y. Zheng, L. Fu, W. Yang, Multiview learning with robust doublesided twin SVM, IEEE Trans. Cybern., 2021 (2021). https://doi. org/10.1109/TCYB.2021.3088519.

[6] Q. Ye, Z. Li, L. Fu, Z. Zhang, W. Yang, G. Yang, Nonpeaked discriminant analysis for data representation, IEEE Trans. Neural Networks Learn. Syst., 30 (2019), 3818–3832. https:// doi .org/ 10.1109 / TNNLS.2019.294-4869.

[7] Z. Tong, F. Ye, M. Yan, H. Liu, S. Basodi, A survey on algorithms for intelligent computing and smart city applications, Big Data Mining Anal., 4 (2021), pp. 155–172. https://doi.org/10.26599/BDMA.2020.9020029.

[8] J. H. Anajemba, T. Yue, C. Iwendi, M. Alenezi, M. Mittal, Optimal cooperative offloading scheme for energy efficient multi-access edge computation, IEEE Access, 8 (2020), 53931–53941. https://doi.org/10.1109 /ACCESS.2020.2980196.

[9] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: a distributed and trusted authentication system, IEEE Trans. Ind. Inf., 16 (2020), 1972–1983. https://doi.org/10.1109/TII.2019.2938001.

[10] P. Zhang, C. Tian, T. Shang, L. Liu, L. Li, W. Wang, et al., Dynamic access control technology based on zero-trust light verification network model, in 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), (2021), pp. 712–715. https://doi.org/10.1109/CISC-E52179. 2021.9445896.

[11] A. Wylde, Zero trust: Never trust, always verify, in 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), (2021), pp. 1–4. https: // doi.org / 10.1109 / Cyber SA52016.2021. 9478244.

[12] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, et al., A security awareness and protection system for 5G smart healthcare based on zero-trust architecture, IEEE Int. Things J., 8 (2021), 10248–10263. https://doi.org/ 10.1109/JIOT.2020.3041042.

[13] D. Li, X. Gao, A blockchain based terminal security of IoT, in ICBDS 2019, CCIS 1210, (2019), pp. 445–454. https://doi.org/10.1007/978-981-15-7530-3_34.

[14] J. Zhang, Z. Wang, L. Shang, D. Lu, J. Ma, BTNC: A blockchain based trusted network connection protocol in IoT, J. Parallel Distrib. Comput., 143 (2020), pp. 1–16. https://doi.org/10.1016/j.jpdc.2020.04.004.

[15] S. Mehraj, M. T. Banday, Establishing a zero trust strategy in cloud computing environment, in 2020 International Conference on Computer Communication and Informatics (ICCCI), (2020), pp. 1–6. https:/ /doi.org/ 10.1109/ICCCI48352.2020.9104214.

[16] C. Saran, Cliff, Jericho Forum presents strategy for secure access for businesses, Comput. Wkly., 3 (2004), 16. 4216 Mathematical Biosciences and Engineering Volume 19, Issue 4, pp. 4196–4216.

[17] B. Gates, Enabling secure anywhere access in a connected world, 2007. Available from: https://www. metamuse.net/2007/02/bill-gates-enabling-secure-anywhere.html.

[18] A-Gentle-Introduction-To-Bitcoin-WEB.pdf. Режим доступу: https://bravenewcoin.com/ assets / Reference - Papers/ A-Gentle-Introduction / A-Gentle-Introduction-To-BitcoinWEB.pdf.

[19] Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2015). On the malleability of bitcoin transactions. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (Eds.), Financial cryptography and data security (Vol. 8976, pp. 1-18). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007 /978-3-662-48051-9_1.

[20] Antonopoulos, A. (2015). Mastering bitcoin. Retrieved November 15, 2017. Режим доступу: http:// chimera.labs.oreilly.com / books / 1234000001802 / ch07. html.

[21] Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies (pp. 375–392). IEEE. https:// doi.org/ 10.1109 /SP.2017.29.

[22] Araoz, M. (2016, July 29). The hitchhiker's guide to smart contracts in Ethereum. Режим доступу: https://blog.zeppelin.solutions/the-hitchhikers-guide-to- smartcontracts-in-ethereum-848f08001f05.

[23] Asia, O. (2018, January 29). Tracing back stolen cryptocurrency (XEM) from Japan's Coincheck. Режим доступу: https://www.forbes.com/sites/outofasia/ 20-18/01/29/tracing-back-stolen-cryptocurrency-xem-from japans-coincheck.

[24] Ateniese, G., Faonio, A., Magri, B., & de Medeiros, B. (2014). Certified bitcoins. In I. Boureanu, P. Owesarski, & S. Vaudenay (Eds.), Applied cryptography and network security (Vol. 8479, pp. 80-96). Cham: Springer International Publishing. https://doi.org/ 10.1007/978- 3-319-07536-5_6.

УДК 654.071

Opirskyy I., Vasylyshyn S. Perspectives of military application of blockchain technology.

Abstract. *New cutting-edge technologies tend to have a huge impact on how businesses innovate to improve their competitive advantage. Since the advent of the Internet, blockchain technology has been recognized as one of the explosive innovations of the early 21st century. Blockchain technology is currently used in financial applications (e.g. payments, currency exchange, money transfers and wallets, trade finance, markets, microdeals, investments, brokerage, insurance) as well as non-financial applications (e.g. electronic identity management, authentication and authorization, electronic data storage and delivery systems, certification systems, smart contracts, application development, electronic voting in elections, patient medical record management, workload distribution for communication systems, computer systems that must comply requirements of legislation without human intervention, the Internet of Things, etc.). And yet, the use of blockchain is most justified when solving tasks mainly related to ensuring the integrity of stored information. That is why, in this article, we consider the prospects for the application of blockchain technology in military affairs, analyze its properties, consider the problems and provide solutions*

that open up with the beginning of the use of this technology. Blockchain technology is able to strengthen the defense sector of the state and introduce an additional level of protection to the already existing ones.
Key words: *blockchain, blockchain technology, cybercrime, defense systems, military application*

Опірський Іван Романович, доктор технічних наук, професор кафедри захисту інформації Національного університету «Львівська політехніка».
Opirskyi Ivan, Doctor of Technical Sciences, Professor of the Information Protection Department of the Lviv Polytechnic National University.

Василишин Святослав Ігорович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Svyatoslav Vasylyshyn, graduate student of the Information Protection Department of the Lviv Polytechnic National University.

Отримано *16 червня 2022 року,* затверджено редколегією *14 листопада 2022 року*