

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра «Інформаційна безпека та наноелектроніка»
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему Дослідження стану законодавства та міжнародного досвіду
в регулюванні використання технології блокчейн
(назва теми)

Виконав: студент II курсу, групи
БКз-813м

Спеціальності 125 Кібербезпека та захист
інформації
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних
Систем

ЖОРНЯК А.М.
(ПРИЗВИЩЕ та ініціали)

Керівник НЕЛАСА Г.В.
(ПРИЗВИЩЕ та ініціали)

Рецензент САМОЙЛИК С.С.
(ПРИЗВИЩЕ та ініціали)

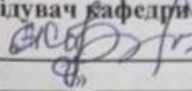
Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Інформаційної безпеки та електронних комунікацій
Кафедра Інформаційна безпека та наноелектроніка
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри

 Андрій КОРОТУН
« 8 » 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЖОРНЯКА Андрія Миколайовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження стану законодавства та міжнародного досвіду в регулюванні використання технології блокчейн. Research the state of legislation and international experience in regulating the application of blockchain technology.

керівник проєкту (роботи) к.т.н. доцент, НЕЛАСА Ганна Вікторівна
(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «05» грудня 2024 року № 507

2. Строк подання студентом проєкту (роботи) 20.12.2024

3. Вихідні дані до проєкту (роботи) теоретичні засади технології блокчейн, законодавство країн світу в цій сфері

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Технологія блокчейн: основні поняття та принципи; Теоретичні засади формування правового регулювання технології блокчейн; Організаційно-правове регулювання технології блокчейн, міжнародний досвід

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (підготовлена в Microsoft PowerPoint)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконав завдання
1-3	НЕЛАСА Г. В., доцент кафедри ІБтаН	04.09.2024	20.12.2024
Нормоконтроль	КОРОЛЬКОВ Р.Ю., доцент кафедри ІБтаН		

7. Дата видачі завдання «04» вересня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження	04.09.24 – 21.09.24	Виконано
2.	Дослідження виникнення та розвитку технології блокчейн, основних принципів функціонування, архітектури та механізмів роботи блокчейн-систем та шляхів удосконалення блокчейн технології з використанням різних протоколів консенсусу	22.09.24 – 07.10.24	Виконано
3.	Аналіз існуючих типів блокчейн-систем, сфер застосування технології блокчейн	08.10.24 – 20.10.24	Виконано
4.	Огляд державних політик країн щодо правового регулювання технології блокчейн	21.10.24 – 17.11.24	Виконано
5.	Розробка рекомендацій щодо модернізації законодавства в галузі регулювання технології блокчейн	18.11.24 – 25.11.24	Виконано
6.	Виконання пояснювальної записки	26.11.24 – 03.12.24	Виконано
7.	Оформлення матеріалів магістерської роботи	03.12.24 – 20.12.24	Виконано

Студент


(підпис)

Андрій ЖОРНЯК
(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)


(підпис)

Ганна НЕЛАСА
(Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 75 с., 36 джерел.

ЗАКОНОДАВСТВО, КІБЕРБЕЗПЕКА, РЕГУЛЮВАННЯ, РОЗПОДІЛЕНИЙ РЕЄСТР, СМАРТ-КОНТРАКТ, ТЕХНОЛОГІЯ БЛОКЧЕЙН

Об'єкт дослідження - процес законодавчого регулювання технології блокчейн.

Предмет дослідження - законодавство країн, що регулює впровадження та застосування технології блокчейн.

Мета роботи - проаналізувати та оцінити сучасний стан законодавчого (правового) регулювання технології блокчейн у різних країнах. Визначити ключові виклики, що виникають у сфері законодавчого регулювання технології блокчейн. Запропонувати рекомендації щодо вдосконалення законодавства в галузі регулювання технології блокчейн.

Методи дослідження - діалектичний (визначені правові явища з визначеного питання у контексті їх розвитку і взаємозв'язку); формально-юридичний (проаналізовано норми чинного законодавства); порівняльно-правовий (використано для порівняння процесу законодавчого регулювання технології блокчейн в різних країнах); системний (окреслено основні рекомендації щодо вдосконалення законодавства в галузі регулювання технології блокчейн); аналітичний (визначено сутність, структуру, стан і проблем політик різних країн щодо вдосконалення законодавчого регулювання технології блокчейн); узагальнення (досліджено кращий досвід зарубіжних країн стосовно політик різних країн з визначеного); праксеологічний (розкрито значення проведеного дослідження для практичного удосконалення законодавчого забезпечення технології блокчейн щодо регулювання технології блокчейн).

1. ABSTRACT

Explanatory note to the master's thesis: 75 p., 36 sources.

LEGISLATION, CYBERSECURITY, REGULATION, DISTRIBUTED LIST,
SMART CONTRACT, BLOCKCHAIN - TECHNOLOGY

The object of the study is the process of legislative regulation of blockchain technology.

The subject of the study is the legislation of countries regulating the implementation and application of blockchain technology.

The purpose of the work is to analyze and assess the current state of legislative (legal) regulation of blockchain technology in different countries. To identify key challenges those arise in the field of legislative regulation of blockchain technology. To propose recommendations for improving legislation in the field of regulation of blockchain technology.

Research methods - dialectical (legal phenomena on a specific issue are identified in the context of their development and interconnection); formal-logical (the essence and features of state policies on the legislative regulation of blockchain technology are analyzed); formal-legal (the norms of current legislation are analyzed); comparative-legal (used to compare the process of legislative regulation of blockchain technology in different countries); systemic (the main recommendations for improving legislation in the field of blockchain technology regulation are outlined); analytical (the essence, structure, state and problems of policies of different countries on improving legislative regulation of blockchain technology are identified); deduction (the current state of legislative regulation of blockchain technology in different countries is summarized and conclusions are formed); generalization (the best experience of foreign countries is studied regarding the policies of different countries on the identified); praxeological (the significance of the research for practical improvement of legislative support for blockchain technology on the regulation of blockchain technology is revealed).

ЗМІСТ

Вступ	7
1 Технологія блокчейн: основні поняття та принципи	10
1.1 Виникнення та розвиток технології блокчейн	10
1.1.1 Класифікація блокчейн-систем	10
1.1.2 Основні принципи функціонування блокчейн-систем	19
1.1.3 Архітектура та механізми роботи блокчейн-систем	28
1.2 Шляхи узагальнення і удосконалення блокчейн технології з використанням різних протоколів консенсусу.	31
2 Теоретичні засади формування правового регулювання технології блокчейн	39
2.1 Типи блокчейн-систем	39
2.1.1 Сфери застосування технології блокчейн	39
2.1.2 Сучасні виклики щодо правового регулювання технології блокчейн	48
2.2 Законодавче (правове) регулювання технології блокчейн як об'єкт наукових досліджень	53
3 Організаційно-правове регулювання технології блокчейн. Міжнародний досвід	55
3.1 Державні політики країн щодо правового регулювання технології блокчейн	55
3.2 Рекомендації щодо модернізації законодавства в галузі регулювання технології блокчейн	67
Висновки	69
Перелік джерел посилання	71

ВСТУП

Переважні траєкторії в еволюції сучасних інформаційних технологій кібербезпеки включають: швидкий розвиток розподіленої обробки інформації, як це проявляється в сучасних інформаційно-телекомунікаційних системах; поява нових парадигм поряд з їх практичним застосуванням; використання фундаментальних принципів побудови інформаційно-комунікаційних систем загального призначення в області автоматизованих систем управління критичною інфраструктурою; і перехід від звичайної інформації та системи зв'язку до кіберпростору, тим самим переходячи від безпосередньо керованого інформаційно-комунікаційного середовища до децентралізованих систем управління, здатних наділити певні сегменти кіберпростору «інтелектуальним» атрибутом.

Інформаційна система (кіберпростір), в межах якої з'являються сигнали, що сприяють управлінню процесами, що беруть участь у підтримці певного стану системи, повинна мати здатність до децентралізації та поширюватися через різні функції та ресурси. Структури даних та процеси, що використовуються в кіберпросторі, повинні дотримуватися фундаментальних принципів, що регулюють роботу інформаційної системи; отже, тенденція до децентралізації управління інформаційно-комунікаційними послугами спричинила появу технології блокчейн.

Технологія блокчейн є одним з найбільш перспективних досягнень сучасної епохи, що має значний потенціал для якісної трансформації та вдосконалення в різних секторах функціонування суспільства. Ця технологічна база (блокчейн) базується на принципі створення децентралізованих, надійних та безпечних систем обліку та обміну інформацією. Технологія блокчейн служить основою для розподілених децентралізованих механізмів захищеної обробки інформації, які призначені для вирішення широкого спектру практичних застосувань - від децентралізованого випуску та обігу електронної валюти (криптовалюти) до

процесів аутентифікації, електронного нотаріального посвідчення, децентралізованого підписання контрактів та адміністрування систем електронного голосування. Впровадження технології блокчейн готове внести суттєві зміни в організаційних рамках в різних галузях, включаючи, але не обмежуючись, державне управління, судову систему, фінансовий сектор, логістику, охорону здоров'я, виборчі системи тощо. [1].

Щоб ефективно використовувати технологію блокчейн, необхідно вирішувати різноманітні теоретичні та практичні проблеми, включаючи:

- розробка та вдосконалення протоколів координації в розподілених системах; дослідження моделей даних в архітектурах блокчейну (звичайною моделлю для технології блокчейн є модель збереження даних максимальної надмірності, де повна копія бази даних підтримується на кожному вузлі в мережі;
- альтернативним підходом є модель мінімальної резервування, що характеризується розподілом сегментів бази даних по всіх вузлах блокчейна, що вимагає колективної участі всіх вузлів для реконструкції цілої бази даних);
- нагальним питанням є формулювання механізму реплікації таких розподілених баз даних, що враховує різний ступінь надмірності збереження даних;
- адаптація існуючих криптографічних фреймворків в рамках блокчейну, наприклад, заміна дерев Merkle, впровадження групових цифрових підписів та заміна обчислювально інтенсивної задачі пошуку прототипів хеш-функції іншими складними математичними проблемами;
- оцінка стійкості хеш-функцій проти інверсії з урахуванням особливостей їх застосування в блокчейні, що відрізняється від традиційного аналізу стійкості до зіткнень та інверсії (пошук прототипів) хеш-функцій; оцінка та розробка криптографічних вразливостей в блокчейні;

- створення криптографічних протоколів, заснованих на технології блокчейн, таких як протоколи підтвердження нульових знань, методи анонімізації та перевірка інтелектуальної власності, серед інших;
- обчислення параметрів, що стосуються практичних блокчейн-систем (таких як оцінка надійності існуючих блокчейнів та тривалості буферів транзакцій, які очікують включення в блокчейн тощо).

Разом із численними перевагами впровадження блокчейн-технології постають значні правові труднощі, пов'язані з її нормативно-правовим регулюванням. Ці питання мають суттєвий вплив як на національні правові системи, так і на міжнародні відносини, зважаючи на глобальний характер функціонування блокчейну. Налагодження ефективного нормативного регулювання технології блокчейн є надзвичайно важливим для забезпечення суспільного добробуту, підтримання соціальної стабільності та безпеки, збереження економічної цілісності, протидії кіберзлочинності, а також для гарантування прав і законних інтересів користувачів.

На міжнародному рівні поки що не розроблено уніфікованих норм і загальновизнаних стандартів, які б регулювали впровадження та широкомасштабне застосування технології блокчейн. Органи державної влади різних країн досі не прийшли до єдиного системного підходу щодо використання цієї технології, акцентуючи увагу на потребі запровадження ефективного моніторингу та державного регулювання. Зокрема, підкреслюється важливість обережного підходу до потенційних ризиків, що можуть виникнути в процесі її використання.

У межах цієї дипломної роботи здійснюється аналіз сучасного стану та ідентифікація основних викликів, пов'язаних із нормативно-правовим регулюванням технології блокчейн. Досліджується міжнародний досвід у цій сфері з метою визначення ключових аспектів правового регулювання як на глобальному, так і на національному рівнях. Крім того, розглядаються перспективи впровадження цієї технології та надаються рекомендації щодо удосконалення законодавчої бази у сфері її регулювання.

1 ТЕХНОЛОГІЯ БЛОКЧЕЙН: ОСНОВНІ ПОНЯТТЯ ТА ПРИНЦИПИ

1.1 Виникнення та розвиток технології блокчейн

1.1.1 Класифікація блокчейн-систем

Блокчейн є передовою технологією, яка забезпечує зберігання та передачу цифрових даних і володіє значним потенціалом для впливу на різні аспекти суспільного життя. Термін «блокчейн» походить від англійських слів "block" (блок) та "chain" (ланцюг) і позначає базу даних, яка функціонує завдяки численним взаємопов'язаним комп'ютерам у мережі, розташованим по всьому світу [2]. У цій системі дані організовані у вигляді ланцюга блоків, причому кожен новий блок містить зашифровані відомості про попередній, формуючи незмінний зв'язок між елементами ланцюга [3].

Криптокультура сформувалася як результат побічного ефекту іншого інноваційного відкриття. У своїй першій і єдиній праці «Bitcoin: A Peer-to-Peer Electronic Cash System», опублікованій наприкінці 2008 року, анонімний винахідник Сатоші Накамото зазначив, що розробив «електронну однорангову систему грошового обігу» [3]. Зокрема, він наголосив на здатності цієї системи запобігати атакам подвійного витрачання коштів, які були поширені в інших онлайн-фінансових системах. Це був перший випадок успішного створення повністю децентралізованої мережі без необхідності використання сервера або централізованого управління [3].

Раніше інші дослідники також намагалися розробити подібні системи. Однією з перших реалізацій цифрових грошей стала ініціатива, спрямована на підвищення безпеки автозаправних станцій у Нідерландах. Розробники запропонували відмовитися від використання готівкових коштів, замінивши їх спеціальними пластиковими картками. Такий підхід дозволив усунути потребу в зберіганні значних сум готівки, що сприяло підвищенню безпеки. Цей приклад, разом з іншими подібними проектами, став основою для виникнення сучасних цифрових валют [4].

Приблизно в той самий період американський криптограф Девід Чаум досліджував іншу концепцію електронних грошей — токени, які дозволяли здійснювати безпечні та конфіденційні платежі. Вчений створив технологію «сліпого» цифрового підпису, яка гарантувала цілісність і конфіденційність даних, якими обмінювалися сторони. Цей підпис забезпечував автентифікацію інформації та можливість її модифікації без можливості відстеження. Через декілька років Чаум заснував компанію DigiCash, яка мала на меті впровадження цієї технології. Попри те, що компанія збанкрутувала у 1998 році, її напрацювання, зокрема математичні формули, концепції та криптографічні протоколи, мали значний вплив на розвиток сучасних цифрових валют [5].

У 1990-х роках багато стартапів прагнули розвинути та вдосконалити концепцію, запропоновану DigiCash. Серед найуспішніших варто виокремити PayPal, яка зробила революцію у сфері онлайн-платежів. Її рішення дозволило користувачам швидко та безпечно переказувати кошти через Інтернет. Значний поштовх до розвитку PayPal отримала завдяки партнерству з платформою eBay, що відкрило доступ до великої аудиторії користувачів і забезпечило стрімке зростання компанії [6]. Нині PayPal залишається одним із найвідоміших і найпотужніших сервісів онлайн-платежів. Іншим визначним прикладом став проєкт e-gold, який пропонував кредитування для приватних осіб під заставу золота та інших дорогоцінних металів, продовжуючи вдосконалення фінансових технологій цифрової епохи.

У 1998 році винахідник Вей Дай представив свою розробку — «анонімну, децентралізовану систему електронних грошей» під назвою B-Money [5]. У своїй концепції він описав два різних протоколи, один з яких передбачав використання синхронного каналу зв'язку. Хоча B-Money значно відрізнялася від Bitcoin і не отримала подальшого розвитку, ця система стала важливою спробою створення анонімної, приватної та безпечної електронної платформи. Особливістю B-Money було використання «цифрових псевдонімів» для передачі валюти через децентралізовану мережу. Система також передбачала можливість автономного виконання контрактів без участі третьої сторони. Незважаючи на публікацію

детального дослідження, ідея Вей Дая не змогла привернути достатньої уваги для реалізації. Проте вплив його роботи на розвиток сучасних криптовалют є безсумнівним. У своєму дослідженні «Bitcoin: A Peer-to-Peer Electronic Cash System» [3] Сатоші Накамото посилався на окремі аспекти В-Money, підтверджуючи значущість ідей Вей Дая для еволюції криптовалютних систем..

Система електронних грошей Bit Gold була створена приблизно в той самий час, що й В-Money [5]. Її автором став Нік Сабо, який розробив концепцію на основі власного алгоритму доведення виконання роботи (Proof-of-Work). Цей алгоритм частково нагадував процес майнінгу біткоїнів, а загальний механізм функціонування мав схожість із принципами сучасного блокчейну. Однією з найінноваційніших особливостей Bit Gold стало усунення централізованого управління. Система була спрямована на ліквідацію залежності від централізованих механізмів розподілу та контролю. Метою Сабо було створення цифрового аналога золота, що працював би без посередників. Попри те, що Bit Gold, як і В-Money, не отримав практичної реалізації, цей проєкт став джерелом ідей і натхнення для багатьох цифрових валют, які з'явилися на ринку через кілька десятиліть [5].

Розроблена в середині 1990-х років, Hashcash була однією з перших успішних цифрових валют, що передували Bitcoin. Її створення мало на меті вирішення кількох завдань, зокрема зменшення поштового спаму та запобігання DDoS-атакам [4]. Hashcash відкрила нові можливості, більшість з яких отримали своє практичне застосування лише через два десятиліття. Як і сучасні криптовалюти, Hashcash застосовувала алгоритм Proof-of-Work для створення та розповсюдження нових монет. Проте вже в 1997 році, зі зростанням вимог до обчислювальних ресурсів, система почала втрачати ефективність і, зрештою, припинила своє існування. Багато з принципів, закладених у Hashcash, були адаптовані в системі Bitcoin [7].

Для створення цифрової валюти необхідна платіжна мережа, яка включає рахунки, баланси та транзакції. Однією з основних проблем, яку повинна вирішити кожна платіжна онлайн-система, є уникнення подвійних витрат, коли

одна й та ж сума витрачається більше ніж один раз. У централізованих системах це контролюється центральним сервером, який фіксує баланс, але в децентралізованій мережі такого серверу немає. Тому для забезпечення правильності транзакцій кожен учасник мережі повинен мати доступ до всього списку транзакцій і мати можливість перевірити кожен з них, щоб запобігти різного роду атакам. Якщо вузли мережі не зможуть дійти згоди хоча б щодо одного балансу, система зруйнується — для її коректної роботи необхідний повний консенсус [3]. У централізованих системах у разі конфліктів або суперечок рішення ухвалює уповноважений центральний орган [8].

Вперше концепція, яка лежить в основі технології блокчейн, була представлена у 1991 році науковцями Стюартом Хабером і В. Скоттом Сторнеттом. Їхня мета полягала у забезпеченні захисту цифрових документів від підробки шляхом застосування криптографічних методів [9]. У своїй науковій праці вони описали методологію, яка дозволяла відстежувати час створення та внесення змін до електронних документів. Використання традиційної клієнт-серверної архітектури для вирішення цієї задачі мало численні недоліки. Серед основних проблем були: можливість перехоплення даних у мережі, недостатній рівень захисту серверів, низька швидкість обробки інформації, а також потреба у великих обсягах пам'яті для зберігання даних. [7]. Науковці запропонували вдосконалити систему шляхом впровадження криптографічно захищених хеш-функцій. Замість передачі всього документа на сервер, надсилали лише його хеш-значення, що дозволило суттєво зменшити обсяг пам'яті, необхідної для зберігання, та збільшити пропускну здатність системи. Крім того, було впроваджено цифровий підпис для підвищення рівня безпеки.

Щоб запобігти можливості видачі сервером некоректних часових міток, запропонували використовувати централізований сервер, який генерував би часові мітки таким чином, щоб максимально ускладнити створення недостовірних даних. Також розглядалась ідея розподілення процесу перевірки достовірності між іншими учасниками системи, що підвищувало її надійність. [8]. Метод із залученням сервера передбачав наступний алгоритм дій: у відповідь на запит

користувача сервер надсилав сертифікат, який містив хеш, ідентифікаційний номер (ID) клієнта, часову мітку, порядковий номер, а також з'єднувальну інформацію (ЗІ). ЗІ включала часову мітку, хеш, ID і хеш ЗІ попереднього сертифіката. Під час обробки нового запиту сервер надсилав клієнту ID наступного запиту, створюючи тим самим зв'язок між попереднім і наступним клієнтами [8]. Для перевірки достовірності достатньо було слідувати побудованій ієрархії та перевіряти відповідність інформації. Виявлення невідповідностей сигналізувало про фальсифікацію даних сервером. Єдиний спосіб обійти систему полягав у створенні "фейкового" ланцюга такої довжини, щоб під час перевірки вдавалося оминати справжню частину ланцюга [10]. У якості остаточного рішення було запропоновано розподілити процес підтвердження серед інших користувачів. Для цього передбачалося використання захищеної схеми, яка дозволяє кожному користувачу підписувати повідомлення. У системі також передбачався псевдорандомний генератор, доступний усім учасникам. Коли клієнт бажав поставити часову мітку на документ, він застосовував хеш документа як основу для роботи генератора. Робота генератора призводить до створення кортежу, що містить ідентифікатори інших учасників мережі. Клієнт надсилає кожному з учасників кортежу повідомлення, яке включає хеш документа та його власний ідентифікатор. У відповідь кожен із зазначених учасників додає до повідомлення свою часову мітку та повертає результат клієнту. Таким чином, у клієнта формується набір часових міток, створених іншими учасниками мережі. Відсутність сервера в мережі забезпечує суттєві переваги, такі як скорочення часу відповіді та усунення потреби клієнтів зберігати значні обсяги сертифікатів із з'єднувальною інформацією [11]. Завдяки цій концепції, Стюарт Хабер та В. Скотт Сторнетт у своїй роботі запропонували рішення та ідеї, які стали основою сучасних блокчейн-систем [2]. З метою покращення системи, у 1992 році вони інтегрували дерева Меркла, що дозволило об'єднувати кілька документів у один блок. Однак, попри свою інноваційність, ця технологія не отримала широкого впровадження [2].

Технологія блокчейн була вперше представлена у 2008 році як частина концепції системи Bitcoin [3]. Розробник, відомий під псевдонімом Сатоші Накамото, запропонував ідею децентралізованої системи електронних платежів, яку назвав Bitcoin (BTC) [3]. 12 січня 2009 року відбулася перша транзакція з використанням біткойна: її одержувачем став Хел Фінні, який отримав 10 BTC від самого Сатоші Накамото [5]. Згодом блокчейн, завдяки своїм перевагам, таким як децентралізація, безпека та прозорість, знайшов застосування в багатьох сферах. Поява Bitcoin у 2009 році започаткувала нову еру цифрових валют. Ключовими особливостями Bitcoin стали його децентралізована природа та використання блокчейн-технології. Сатоші Накамото прагнув створити систему цифрових грошей, яка працювала б без участі центрального органу, використовуючи однорангову мережу для обміну даними. Це нововведення стало основою для народження криптовалют [5]. Ще у 2004 році науковець Хел Фінні розробив систему RPoW (Reusable Proof Of Work), яка розглядається як один із перших прототипів криптовалют [12].

У 2013 році програміст Віталік Бутерін ініціював розробку платформи розподілених обчислень, заснованої на блокчейні, під назвою Ethereum. У 2015 році ця платформа була офіційно представлена світу. Головною інновацією Ethereum стали «розумні контракти» (Smart Contracts) — невеликі програми, які зберігаються у блокчейні та автоматично виконуються при досягненні заданих умов. Ці скрипти, що компілюються в байт-код, дозволяють виконувати домовленості без участі посередників [2].

У 2019 році, з активним розвитком DeFi (децентралізованих фінансових сервісів і інструментів, що працюють на блокчейні), блокчейн почав серйозно конкурувати з традиційними фінансовими системами [13]. Блокчейн функціонує як прозора система, де кожен учасник має доступ до інформації про будь-який блок. Для забезпечення роботи системи та гарантування незмінності блоків транзакцій застосовуються криптографічні алгоритми. Однією з ключових технік є хешування — процес, який перетворює дані довільної довжини на стрічку фіксованої довжини. Ця техніка забезпечує відсутність колізій, тобто виключає

можливість отримання однакового хешу з різних вхідних даних. Хеші також використовуються для зв'язування блоків у ланцюжок. Уся інформація в блоці хешується з метою створення вказівника за допомогою бінарного дерева хешів, відомого як дерево Меркла. Це означає, що будь-яка зміна даних у блоці викликає зміну його хешу, а також впливає на всю структуру ланцюжка [2].

У технології блокчейн активно використовуються цифрові підписи, що базуються на принципах криптографії з відкритим ключем [11]. Відкритий ключ, який доступний усім, застосовується для перевірки електронного підпису, тоді як закритий ключ, який використовується для створення підпису, зберігається в таємниці. Важливо, що відкритий ключ можна обчислити на основі закритого, але зворотний процес є технічно неможливим. Процес транзакції відбувається наступним чином: ініціатор підписує дані своїм закритим ключем, а саме повідомлення шифрує за допомогою публічного ключа одержувача. Одержувач, маючи власний закритий ключ, розшифровує отримані дані. Таким чином, лише власник приватного ключа, на якого адресована транзакція, здатний прочитати повідомлення. Цифровий підпис виконує функцію підтвердження, що саме цей користувач є ініціатором транзакції. Для перевірки авторства достатньо мати доступ до повідомлення, підпису та відкритого ключа підписанта [11]. Завдяки своїм численним перевагам, технологія блокчейн знаходить широке застосування в різноманітних галузях суспільного життя, надаючи нові можливості для вирішення складних задач.

Системи, створені на основі технології блокчейн, мають ряд переваг у порівнянні з традиційними рішеннями:

- відсутність централізованого серверу забезпечує децентралізовану структуру, що позбавляє систему єдиної точки контролю;
- завдяки збереженню копії реєстру транзакцій кожним учасником мережі знижується ризик централізованих атак, забезпечується рівномірний розподіл даних та підвищується стійкість системи до витоку інформації;
- висока швидкість проведення транзакцій досягається завдяки виключенню посередників із процесу обміну;

- використання автоматизованих процесів і смарт-контрактів дозволяє оптимізувати бізнес-процеси, знижуючи витрати та підвищуючи ефективність;
- прозорість і можливість перевірки транзакцій забезпечуються тим, що всі операції доступні для перегляду учасниками мережі, що особливо важливо для фінансових систем, де довіра до процесів є ключовим фактором [11].

Відкрита структура блокчейну сприяє зменшенню випадків шахрайства та підвищенню рівня відповідальності учасників. Однією з ключових характеристик технології є неможливість змінити чи видалити транзакції після їх додавання до реєстру [14]. Це гарантує високий рівень достовірності та точності даних, оскільки кожен запис залишається незмінним і завжди доступним для перевірки. Завдяки незмінності інформації зростає довіра до системи, що дозволяє створювати надійні архіви [14]. Виключення посередників із процесу транзакцій дозволяє суттєво знизити витрати на їх проведення, що робить блокчейн привабливим рішенням для бізнесу та споживачів. Забезпечення безпеки та достовірності транзакцій здійснюється за допомогою криптографічних методів і децентралізованих алгоритмів консенсусу, що відкриває нові перспективи для глобальної співпраці та торгівлі. Ці характеристики демонструють потенціал блокчейну, сприяючи створенню більш ефективних, захищених та прозорих систем [15].

Існує три основних типи платформ на базі технології блокчейн:

- публічні платформи;
- приватні платформи;
- гібридні (консорціумні) платформи.

Публічні платформи не обмежують доступ і дозволяють будь-якому користувачу приєднуватися до системи, переглядати інформацію в блоках, а також брати участь у створенні і верифікації нових блоків. Користувачі залишаються анонімними, оскільки система не вимагає ідентифікації [2].

Перевагами публічних платформ є:

- високий рівень довіри;
- надійний захист системи;
- прозорість процесів.

До недоліків можна віднести:

- низьку швидкість обробки та підтвердження транзакцій;
- значне споживання енергії.

Приватні (корпоративні) платформи, на відміну від публічних, зазвичай використовуються в межах однієї організації. Власник такої платформи контролює безпеку, доступ користувачів і доступ до мережі [2]. Такі системи схожі на публічні, але значно менші за масштабом і, попри використання технології блокчейн, не є децентралізованими, оскільки вони підпорядковуються контролю власника. Ідентифікація користувачів приватних платформ зазвичай не є проблемою, оскільки анонімність не є необхідною [2].

Перевагами приватних платформ є:

- швидка обробка транзакцій;
- можливість власника мережі гнучко налаштовувати кількість вузлів.

До недоліків приватних систем можна віднести:

- відсутність анонімності користувачів;
- низький рівень захисту;
- можливість доступу до системи через її власника, що надає контроль над усією мережею. Приватні (корпоративні) системи знаходять застосування в таких сферах, як організація голосувань, цифрова ідентифікація, аудит та інші.

Гібридні платформи поєднують характеристики як публічних, так і приватних систем. Їх основні особливості полягають у можливості здійснювати контроль кількома організаціями одночасно, обмеженому доступі до інформації в блоках для певних користувачів, а також можливості власника вибирати, яку інформацію зробити доступною для всіх, а яку залишити конфіденційною [2]. Залежно від конкретної платформи, гібридні системи можуть поєднувати переваги та недоліки публічних і приватних платформ. Вони широко використовуються в банківському секторі та державних органах [12]. Отже, вибір

типу платформи для конкретного застосування залежить від специфічних вимог та потреб користувача.

1.1.2 Основні принципи функціонування блокчейн-систем

Блокчейн-системи функціонують як децентралізовані структури, де всі учасники повинні взаємодіяти згідно з певними правилами, що утворюють консенсус. Консенсус в цих системах є набором алгоритмів і правил, які забезпечують досягнення погоджених рішень серед усіх учасників мережі. Він служить основою для забезпечення надійності всієї системи [5].

Важливо зазначити, що блокчейн є системою, яка дозволяє децентралізовано обробляти, зберігати, додавати і змінювати інформацію. При цьому рішення щодо обробки даних приймається більшістю учасників системи на основі спеціальних правил [5]. Блокчейн є системою, в якій обробка інформації визначається за результатами «голосування» учасників у рамках протоколу консенсусу. Всі зміни в такій системі відбуваються в певні моменти часу, що відповідають «транзакціям», які є мінімальними змінами стану системи. Транзакції об'єднуються в блоки, а блоки формують послідовний ланцюг, відомий як блокчейн. Кожен блок у ланцюзі містить посилання на попередній, і перший блок, який не має попереднього посилання, називається генезис-блоком. Цей блок зазвичай вбудований безпосередньо в протокол [5]. Нове додавання блоків до системи здійснюється згідно з певними правилами, що визначаються протоколом консенсусу. Однією з ключових функцій цих правил є забезпечення захисту від атак злоумисників та досягнення консенсусу в ситуаціях, коли з'являються різні варіанти ланцюга блоків.

У контексті блокчейну консенсусом називають процес, що поєднує елементи голосування та узгодження. Його основна мета — забезпечити досягнення єдиного розуміння серед усіх учасників стосовно інформації, яка

зберігається в блокчейні [13]. Протоколи консенсусу виконують кілька важливих функцій:

- забезпечують правильне виконання процесів обробки інформації в блокчейні;
- усувають можливість суперечливих рішень при продовженні ланцюга блоків (наприклад, у випадку розгалуження ланцюга);
- гарантують достовірність учасників мережі.

Протокол консенсусу включає такі компоненти:

- правила формування наступного блоку;
- механізми вирішення конфліктів, що можуть виникнути як через помилки, так і через порушення правил з боку нечесних учасників;
- методи заохочення учасників мережі до підтримки роботи блокчейну та виконання протоколу.

Протокол узгодження представляє собою інтерактивний алгоритм, в якому бере участь більше ніж один учасник, і результатом цього процесу є обчислення спільного значення для всіх учасників. Проблеми, пов'язані з розробкою таких протоколів для розподілених мереж, виникли ще до появи концепції «блокчейн» і були відомі як проблема «візантійських генералів». Це означало необхідність створення інтерактивного алгоритму, який повинен завершуватися за обмежену кількість кроків, навіть якщо кількість «нечесних» учасників перевищує кількість чесних [2]. Враховуючи такі умови, використання традиційних протоколів стає складним. Більшість з них була розроблена для розподілених баз даних у мережах з відомою архітектурою, без врахування асинхронності та непередбачуваності сучасних глобальних інформаційно-телекомунікаційних систем [10]. Тому при створенні нових асинхронних протоколів узгодження необхідно враховувати фактор, що неможливо точно передбачити кількість активних вузлів у мережі на даний момент. Це вимагає випадкового вибору учасників протоколу та створення механізму забезпечення цілісності всіх попередніх транзакцій, який отримав назву «цифрове пломбування». Окрім цього, важливою є розробка системи заохочення участі у протоколі для забезпечення його ефективності [13]. Таким чином, основні

принципи побудови протоколу узгодження в блокчейні включають: синхронізацію за допомогою ланцюга блоків транзакцій; реалізацію «цифрового пломбування» через цифрові підписи та ідентифікатори; встановлення загальних правил для генерації наступного блоку в ланцюзі; створення значної обчислювальної складності для генерування наступного блоку транзакцій; заохочення учасників до активної участі в процесі генерації блоку; та можливість перевірки правильності створення блоку будь-яким учасником мережі [10]. Існує багато різних алгоритмів консенсусу, що дозволяють забезпечити різний рівень безпеки та швидкості обробки транзакцій. Серед найпоширеніших можна виділити: Proof of Work (PoW), Proof of Stake (PoS) і Delegated Proof of Stake (DPoS) [11].

Алгоритм PoW є одним із перших і найбільш розповсюджених. Його головна ідея полягає в використанні складної обчислювальної задачі, яка слугує основою для змагання за право створити наступний блок. Визначальним фактором для перемоги є швидкість розв'язування цієї задачі. Для того, щоб учасники мали рівні шанси та система працювала стабільно, задача не повинна мати швидкого способу розв'язання (алгоритму з поліноміальною складністю) [15]. Тому зазвичай вибирають задачу, для якої є тільки метод прямого перебору. Одним з таких протоколів є повільний, але надійний Proof-of-Work: кожен вузол мережі, створюючи новий блок, підбирає число nonce, яке є одним з параметрів блоку. Блок вважається дійсним, якщо виконано валідність всіх транзакцій, що він підтверджує, і хеш цього блоку має таке значення, що відповідне йому десяткове число менше за заздалегідь задане цільове значення (target) [16]. Таким чином, Proof-of-Work (PoW) є алгоритмом захисту розподілених систем від зловживань (таких як DDoS-атаки, спам тощо), і складається з трьох основних принципів:

- потрібність виконання складного завдання з повільним процесом виконання;
- можливість швидкої і простої перевірки результату;

- неможливість заздалегідь визначити, який учасник створить наступний блок, при цьому ймовірність цього пропорційна його обчислювальним ресурсам (зокрема – частці його обчислювальних потужностей або хешрейту).

Концепція Proof-of-Work вперше була запропонована в 1993 році дослідниками Синтією Дворко та Моною Наор у роботі «Pricing via processing or combatting junk mail, advances in cryptology» [2]. Хоча термін ще не був використаний у статті, автори описали ідею: «Щоб отримати доступ до спільного ресурсу, користувач повинен виконати обчислення деякої функції: складної, але здійсненної; це дозволяє захистити ресурс від зловживань» [2].

У 1997 році Адам Бек реалізував проект Hashcash, що мав на меті боротьбу зі спамом. Для виконання цієї задачі потрібно було провести 252 обчислення хешу. Якщо відправлення кількох звичайних листів не створювало труднощів, то постійне виконання обчислень робило спам дуже витратним. При цьому перевірка правильності виконаних обчислень була дуже швидкою: для цього потрібно було лише одне обчислення з заданим аргументом [11].

У 1999 році Маркус Якобссон і Арі Джуелс описали механізм Proof-of-Work у статті «Proofs of Work and bread pudding protocols». У мережі Bitcoin алгоритм PoW використовується як метод досягнення консенсусу [11]. Сатоши Накамото адаптував концепцію проекту Hashcash, додавши до нього механізм зміни складності, який дозволяє варіювати цільове значення або кількість нулів у хеш-значенні. Алгоритм Proof-of-Work (PoW) гарантує, що вузол, який додає новий блок до блокчейну, дійсно виконав необхідні обчислення [16]. Процес включає пошук хешу заголовка блоку, який відповідає поточному рівню складності. Кожному вузлу, який прагне сформувати блок, потрібно вирішити хеш-задачу, підбираючи значення nonce (один з параметрів блоку), щоб хеш всього блоку (включаючи список транзакцій, хеш попереднього блоку та значення nonce) відповідало заданому критерію (наприклад, початковим нулям у хеш-результаті) [17]. Оскільки хеш-функція є криптографічною, єдиним способом розв'язати цю задачу є перебір значень nonce, поки результат не потрапить у визначену область.

Вузли в системі постійно конкурують, обчислюючи значення *nonce* у своїх блоках, щоб отримати винагороду. Система є децентралізованою, тому вибір формувача блоку не залежить від одного центра. Основними характеристиками механізму Proof-of-Work є значні обчислювальні витрати, швидка перевірка результатів та параметризована вартість обчислень. З часом складність розрахунків коригується таким чином, щоб новий блок формувався кожні 10 хвилин в середньому [2]. Нагорода за обчислення блоку змінюється залежно від виконаних обчислень. Процес вирішення хеш-задачі є ймовірнісним, оскільки передбачити, який *nonce* призведе до успіху, неможливо. Тому існує невелика ймовірність, що новий блок буде знайдено навіть через кілька секунд, але також можливо, що це займе значно більше часу, наприклад, годину. Для конкретного вузла середній час знаходження блоку, що становить 10 хвилин, залежить від частки гешпотужності, яку він контролює [16]. Навіть якщо вузол обчислює мільярди хешів для формування блоку, значення *nonce*, знайдене методом перебору та підстановки в хеш-функцію, буде внесене до нового блоку. Це дає можливість іншим вузлам легко перевіряти вміст блоку, хешуючи всі його частини і перевіряючи, що отримане значення відповідає заданим критеріям. Така можливість важлива для запобігання централізації, оскільки система не потребує централізованого контролю за виконанням майнерами своїх завдань. Кожен вузол може самостійно перевірити, що знайдений блок відповідає вимогам Proof-of-Work, що гарантує, що майнер дійсно витратив значні обчислювальні ресурси для його формування. Однак протокол PoW має свої недоліки, серед яких високі витрати та необхідність у спеціалізованому, дорогому обладнанні для виконання складних обчислень [11]. Ця діяльність має сенс лише в разі об'єднання ресурсів в пули або з'єднання обладнання. Генерація нових блоків потребує значних енергетичних витрат і постійного обчислення. Розрахунки, які проводяться системою, не мають іншого застосування, окрім як для забезпечення стабільності мережі, і не можуть бути використані в інших сферах [2]. Атака більшості або атака на 51% полягає в тому, що один або кілька учасників мережі захоплюють контроль над більшістю обчислювальних потужностей, що дозволяє їм

маніпулювати системою. Хоча теоретично можна спробувати здійснити таку атаку з меншою кількістю потужностей, шанс на успіх буде значно нижчим. В умовах «атаки 51%» процес створення нових блоків стає монополізованим, що дає таким учасникам винагороду і перешкоджає іншим ефективно брати участь у процесі [11]. У формуванні блоку беруть участь всі вузли мережі. Користувачі змагаються за право додати новий блок, використовуючи список останніх транзакцій. Кожен має доступ до цього списку і вирішує задачу перевірки, що всі транзакції є валідними. Алгоритм вимагає значних обчислювальних ресурсів для досягнення результату [2]

У процесі роботи кожен учасник створює хеш-значення, що генерується на основі оброблених даних через хеш-функцію. Якщо хоча б одна транзакція є підробленою, результат хешування змінюється. Алгоритм обчислення хеш-значень ускладнений введенням обмеження на значення хешу (встановлюється певне цільове значення, яке не повинно бути перевищене). Для цього до даних додається додаткове число – *nonce* (зазвичай випадково згенероване), що змінює результат хешування [17]. Щоб ускладнити обчислення, необхідно зменшити значення *target*, що змусить учасників системи перевіряти більше значень *nonce*. Коли один з учасників знаходить хеш, який відповідає умовам, він повідомляє іншим вузлам, які перевіряють правильність обчислення. Основні переваги цього алгоритму – надійність і простота, однак серед недоліків можна виділити значні енергетичні витрати та низьку швидкість обробки транзакцій, що призвело до розробки нових консенсусних протоколів, заснованих на інших принципах [2].

Механізм консенсусу Proof-of-Stake (PoS) передбачає, що права на створення нових блоків у блокчейні розподіляються пропорційно до внеску користувача в систему. Іншими словами, чим більша частка криптовалюти належить учаснику мережі, тим вищі його шанси на генерування наступного блоку. Такий підхід робить атаку на систему менш привабливою з економічної точки зору, оскільки для успішного проведення атаки необхідні значні фінансові ресурси. На відміну від традиційного алгоритму Proof-of-Work (PoW), де безпека мережі забезпечується за рахунок обчислювальної потужності, в PoS ставка

робиться на економічні інтереси учасників. Таким чином, PoS перетворює процес валідації блоків на своєрідну лотерею, де шанси на виграш залежать від розміру ставки. Цей механізм не лише підвищує енергоефективність блокчейну, але й сприяє децентралізації мережі.

Однією з ключових переваг алгоритму Proof-of-Stake є його енергоефективність та висока швидкість обробки транзакцій. На відміну від моделей, що базуються на вирішенні складних математичних задач, PoS пропонує учасникам мережі інший підхід: замість конкуренції за обчислювальні ресурси, вони роблять "ставки" у вигляді своїх криптовалют. Чим більший внесок, тим вищі шанси бути обраним для валідації блоків. Такий механізм створює сильний економічний стимул для учасників підтримувати стабільність мережі, оскільки будь-які спроби маніпуляції можуть призвести до значних фінансових втрат. [18]. Незважаючи на значну перевагу в швидкості обробки транзакцій порівняно з традиційними системами, заснованими на алгоритмі Proof-of-Work, Proof-of-Stake також має свої особливості. Зокрема, для участі в процесі валідації блоків необхідні власні токени мережі. Крім того, існує ризик поступової концентрації валідаторських потужностей в руках невеликої групи користувачів з найбільшими ставками, що може потенційно підірвати децентралізований характер блокчейну. Однак, теоретично, кожен учасник мережі, який володіє достатньою кількістю токенів, має можливість стати валідатором [19]. На відміну від енергомісткого PoW, алгоритм PoS пропонує більш екологічне та масштабоване рішення. Замість використання потужних комп'ютерів для вирішення складних математичних задач, PoS базується на економічних стимулах. Це дозволяє значно знизити енергоспоживання та збільшити швидкість обробки транзакцій. Крім того, механізми консенсусу PoS, такі як DPoS, дозволяють делегувати права на валідацію блоків обраним представникам спільноти, що підвищує ефективність та спрощує управління мережею [18]. Кожен власник токенів має право голосу, хоча й не отримує за це безпосередньої винагороди. Голоси власників більших кількостей монет мають більшу вагу при формуванні списку валідаторів. Крім того, спільнота має можливість впливати на розвиток мережі шляхом голосування

за зміну параметрів. Валідатори в таких системах несуть значно більшу відповідальність, оскільки вони повинні відкрито заявити про свою участь і забезпечити безперебійну роботу мережі. Вибір валідаторів відбувається на основі голосування усіх учасників, де вага голосу кожного визначається його внеском у мережу. [18]. Для забезпечення коректності роботи системи DPoS передбачено, що більшість голосів має належати добросовісним учасникам. Такий механізм гарантує надійність мережі при відносно невеликих енерговитратах. Однак, існує ризик централізації, оскільки великі гравці можуть отримати значний вплив на процес прийняття рішень. Суть DPoS полягає в тому, що власники токенів делегують свої права на валідацію блоків обраним представникам – "свідкам". Вибір "свідків" відбувається шляхом голосування, де вага голосу кожного учасника пропорційна його внеску. Такий підхід дозволяє підвищити швидкість обробки транзакцій та масштабованість мережі. Варто зазначити, що DPoS є лише одним з багатьох алгоритмів консенсусу, і вибір оптимального рішення залежить від конкретних потреб кожної системи. Постійні дослідження в цій галузі спрямовані на створення більш ефективних та безпечних механізмів консенсусу. [2].

На відміну від традиційних централізованих баз даних, блокчейн є розподіленою системою, яка не залежить від єдиного центру управління [17]. Інформація в блокчейні зберігається в блоках, які з'єднані між собою за допомогою криптографічних хеш-функцій. Це робить блокчейн надзвичайно стійким до зломів та маніпуляцій. Кожен блок містить інформацію про попередній блок, що створює незмінний ланцюжок записів. Для того, щоб змінити дані в блокчейні, необхідно зламати криптографічні алгоритми та перерахувати велику кількість блоків, що є практично неможливим. [11].

Існуючі системи електронних платежів зазвичай використовують централізованих посередників, таких як банки, для підтвердження транзакцій. Це призводить до збільшення вартості платежів, особливо дрібних, та вимагає від користувачів надавати значну кількість персональних даних. Блокчейн пропонує альтернативне рішення. Завдяки децентралізованій структурі та використанню

криптографії, він дозволяє здійснювати прямі платежі між користувачами без посередників, знижуючи витрати та підвищуючи безпеку. Крім того, блокчейн робить транзакції незворотними, що захищає продавців від шахрайства [15].

Система працює на принципі цифрового підпису, де кожна транзакція пов'язана з попередньою. Учасники мережі створюють ланцюжок транзакцій, підписуючи хеш попередньої та додаючи свій публічний ключ. Такий підхід забезпечує незмінність інформації та доказовість володіння. Кожен може перевірити достовірність будь-якої транзакції, прослідкувавши її історію в ланцюжку. Це дозволяє уникнути подвійних витрат, коли одна і та ж сума коштів намагається бути витрачена двічі. На відміну від централізованих систем, де порядок транзакцій визначає третя сторона, в цій системі учасники самостійно досягають консенсусу щодо послідовності транзакцій. [14]. Щоб гарантувати, що транзакція є першою та унікальною, система використовує механізм міток часу. Суть полягає в тому, що кожен блок даних отримує унікальний цифровий відбиток (хеш), який містить інформацію про попередній блок. Цей ланцюжок хешів створює незмінний запис про всі транзакції, що робить практично неможливим підробити або змінити будь-яку з них. Таким чином, система забезпечує доказовість того, що транзакція відбулася саме в той момент часу, який зазначений в мітці часу [16].

Традиційні методи підтвердження даних часто вимагають довіри до централізованих серверів. Для уникнення цього, в системі використовується механізм "доказу роботи". Цей механізм забезпечує високий рівень безпеки, оскільки для підробки даних потрібно виконати велику кількість обчислень. Кожен новий блок в ланцюжку підтверджує правильність всіх попередніх, створюючи таким чином незмінний запис про всі транзакції [16].

1.1.3 Архітектура та механізми роботи блокчейн-систем

Механізм "доказу роботи" дозволяє мережі досягти згоди щодо послідовності транзакцій. Суть полягає в тому, що учасники мережі змагаються за право додавати нові блоки до ланцюжка, виконуючи складні обчислення. Той, хто першим знайде правильне рішення, отримує винагороду і право записати новий блок. Такий підхід забезпечує, що найдовший ланцюжок блоків відображає думку більшості учасників мережі. Для того, щоб змінити минулі записи, зломисник повинен перерахувати велику кількість блоків, що є практично неможливим завданням. Складність обчислень автоматично регулюється для підтримки стабільної швидкості створення нових блоків [11].

На відміну від централізованих систем, де довіра до даних базується на авторитеті центрального органу, ця система використовує децентралізований механізм консенсусу. Кожен вузол в мережі має рівні права і бере участь у підтвердженні транзакцій. Це робить систему більш безпечною і стійкою до збоїв. Якщо виникає розбіжність між різними версіями ланцюжка, мережа швидко об'єднується навколо найдовшого і найбезпечнішого ланцюжка [2]. Мережа спроможна обробляти нові транзакції навіть за умови, коли інформація про них не доходить до кожного вузла. Достатньо, щоб про транзакцію дізналася достатня кількість учасників мережі, і вона буде включена до блоку. Крім того, мережа має механізми самовідновлення. Якщо якийсь вузол пропустить блок, він може відновити пропущену інформацію, запитавши її у інших учасників [2].

Для ефективного використання дискового простору система застосовує спеціальну структуру даних, відому як дерево Меркла. Ця структура дозволяє зберігати великі обсяги даних у компактному вигляді. Коли транзакції стають "архівними", їх деталі можуть бути видалені, оскільки для перевірки їхньої автентичності достатньо зберігати лише корінь дерева Меркла. Це дозволяє зменшити розмір блоків і, відповідно, зменшити вимоги до дискового простору. [8].

Для того, щоб переконатися в достовірності транзакції, не обов'язково запускати повний вузол. Достатньо зберігати основну інформацію про блоки і при необхідності запитувати деталі про конкретну транзакцію. Таким чином, будь-хто може легко перевірити, чи була транзакція підтверджена мережею. Цей метод забезпечує високий рівень безпеки, оскільки для підробки транзакції зломисник повинен контролювати більшу частину обчислювальної потужності мережі [10]. Хоча кожен вузол може перевіряти транзакції самостійно, існує ризик, що зломисник спробує обдурити мережу, створивши альтернативний ланцюжок блоків. Для протидії таким атакам, мережа використовує механізм оповіщення. Якщо вузол виявляє підозрілий блок, він попереджає інших учасників, які можуть провести більш детальну перевірку. Це дозволяє виявити і відкинути некоректні блоки, забезпечуючи безпеку мережі [8].

Для зручності користувачів система дозволяє об'єднувати та розділяти кошти в межах однієї транзакції. Це нагадує роботу з готівкою, коли можна використовувати кілька купюр для оплати однієї покупки і отримати решту. Такий підхід робить систему більш гнучкою та ефективною. Крім того, мережа спроможна обробляти складні транзакції, де одна операція залежить від результатів кількох попередніх [11].

Класична фінансова модель будується на принципі строгого контролю доступу до інформації. Тобто, ознайомитися з фінансовими даними можуть лише безпосередні учасники операцій та уповноважені посередники. Це забезпечує високий рівень конфіденційності [10]. У децентралізованих системах всі транзакції є публічними, проте ідентичність учасників може залишатися прихованою. Завдяки використанню криптографічних ключів, інформація про транзакції містить лише суму та адресата, без прив'язки до конкретних осіб. Для посилення конфіденційності, користувачі можуть генерувати нові ключі для кожної операції, ускладнюючи відстеження руху коштів [11]. Незважаючи на прагнення до анонімності, повністю приховати всі зв'язки між транзакціями в публічних блокчейнах неможливо. Наприклад, якщо кілька різних транзакцій надходять на один і той же гаманець, це може вказувати на те, що всі вони

належать одному власнику. Тому існує ризик, що розкриття інформації про одного з таких гаманців може призвести до розкриття всіх пов'язаних з ним транзакцій [8].

Якщо шкідливий учасник спробує створити альтернативну історію транзакцій, йому доведеться обчислити більше доказів роботи, ніж всі чесні учасники мережі разом узяті. Однак, навіть якщо йому вдасться створити довший ланцюжок, інші вузли не приймуть його як дійсний, оскільки він порушує правила консенсусу. Таким чином, зловмисник не зможе змінити вже підтверджені транзакції [8]

Блокчейн-системи побудовані на принципі децентралізації та перевірки транзакцій за допомогою математичних алгоритмів. Замість того, щоб покладатися на довіру до централізованих установ, вони використовують цифрові підписи для підтвердження права власності на активи. Це робить систему більш безпечною та прозорою [2]. Система має простий, але ефективний механізм роботи. Всі вузли працюють незалежно один від одного, обмінюючись інформацією лише за необхідності. Це дозволяє кожному вузлу приєднуватися до мережі або покидати її в будь-який момент, не впливаючи на загальну роботу системи. Гнучкість системи забезпечується механізмом підтвердження нових блоків, який дозволяє вузлам, що пропустили частину транзакцій, швидко синхронізуватися з основним ланцюгом [11].

Основою блокчейну є мережа взаємопов'язаних програмних модулів, які автоматизують процеси запису, зчитування та зберігання даних у розподіленій базі. Ці модулі, зазвичай написані на спеціальних мовах програмування, забезпечують цілісність та безпеку інформації [9]. Блокчейн розподіляє дані по великій кількості пристроїв, створюючи безліч однакових копій. Це гарантує, що інформація буде збережена навіть у разі виходу з ладу окремих вузлів. Процес додавання нових записів (транзакцій) передбачає складні обчислення, в яких кожен учасник мережі пропонує свою версію нового блоку. Для підтвердження блоку використовується спеціальний алгоритм, що вимагає значних обчислювальних ресурсів [21]. Щоб додати новий блок до блокчейну, учасники

мережі виконують складні математичні обчислення. Мета цих обчислень – знайти число, яке при обробці за допомогою криптографічної функції дасть результат, менший за задане значення. Цей процес називається майнінгом. Після того як блок буде доданий до ланцюжка, він ще кілька разів перевіряється іншими учасниками мережі, щоб забезпечити його достовірність [3].

Всі операції в блокчейні є відкритими для загального доступу. Будь-хто може переглянути повну історію транзакцій, скориставшись спеціальними інструментами та сервісами. Кожен учасник мережі зберігає власну копію блокчейну, що гарантує доступність даних і запобігає їх втраті [2].

1.2 Шляхи узагальнення і удосконалення блокчейн технології з використанням різних протоколів консенсусу, сфери застосування технології блокчейн

Сучасні криптовалюти пропонують новий підхід до здійснення платежів, який не залежить від централізованих установ. Транзакції в таких системах записуються в загальнодоступний, але незмінний журнал, який створюється спільною роботою всіх учасників мережі. Цей журнал захищений від фальсифікацій завдяки використанню складних математичних алгоритмів [15]. Початковий протокол блокчейну, розроблений Сатоші Накамото, сьогодні сприймається як історичний етап. Сучасні блокчейни активно досліджують альтернативні алгоритми консенсусу, які дозволяють значно підвищити швидкість обробки транзакцій [2]. Перший блокчейн стикається з вибором між безпекою та швидкістю. Збільшення розміру блоків або скорочення часу на їх створення може призвести до зниження стійкості мережі до атак та збільшення ймовірності виникнення розбіжностей між різними копіями блокчейну. Тому розробники блокчейну постійно шукають способи оптимізації цих параметрів, зберігаючи при цьому високий рівень безпеки [6]. Будь-які зміни в базових

параметрах протоколу, таких як розмір блоку або частота його генерації, можуть суттєво вплинути на безпеку мережі. Зокрема, збільшення цих параметрів може створити умови для того, щоб зломисники, які мають доступ до більшої обчислювальної потужності, отримали перевагу над чесними учасниками мережі [2]. Швидке поширення нових блоків у мережі може створити умови для успішних атак навіть при відносно невеликій частці обчислювальних ресурсів, контрольованих зломисником. Це пов'язано з тим, що зломисник може скористатися затримкою в поширенні інформації про нові блоки та провести атаку подвійної витрати. Таким чином, збільшення швидкості транзакцій може призвести до зниження безпеки мережі [16]. Кожен блок у блокчейні містить криптографічний відбиток попереднього блоку. Це створює незмінний ланцюжок даних, де зміна інформації в одному блоці автоматично призводить до зміни всіх наступних блоків. Така структура робить блокчейн надзвичайно стійким до підробок та маніпуляцій [11].

Технологія блокчейн дозволяє створювати незмінні, прозорі та безпечні записи різноманітної інформації, від фінансових транзакцій до результатів голосування. Завдяки своїй децентралізованій структурі, блокчейн може бути використаний для створення надійних систем голосування, які унеможливають фальсифікації та забезпечують точність підрахунку голосів. [11].

На відміну від централізованих банківських систем, які зберігають дані про фінансові операції на своїх серверах, технологія блокчейн використовує децентралізований підхід. Інформація про транзакції в блокчейні записується в спеціальні блоки, які об'єднані в ланцюжок. Це забезпечує вищу ступінь безпеки та прозорості [20]. Завдяки блокчейну, клієнти банків отримують можливість миттєво відстежувати свої платежі в режимі реального часу. Ця технологія також спрощує та прискорює міжбанківські перекази, знижуючи витрати та ризики, пов'язані з традиційними методами. На відміну від тривалих процесів на фінансових ринках, блокчейн пропонує швидкі та безпечні розрахунки [1]. Впровадження технології блокчейн дозволяє значно прискорити обробку фінансових операцій, мінімізуючи проміжки часу між транзакціями [22].

Технологія блокчейн, що лежить в основі криптовалют, пропонує новий підхід до здійснення міжнародних платежів, оминаючи традиційні фінансові бар'єри. Завдяки децентралізованій структурі, блокчейн забезпечує безпечне та прозоре зберігання інформації, що робить його ідеальним інструментом для захисту медичних даних та реєстрації прав власності, особливо в регіонах з обмеженим доступом до централізованих систем. [23].

Самовиконуючий код, вбудований безпосередньо в блокчейн, відомий як смарт-контракт, автоматизує виконання угод за певних умов. Це забезпечує високий рівень довіри та прозорості у проведенні транзакцій [11].

Завдяки автоматизації процесів верифікації за допомогою блокчейну, значно зменшується ймовірність людської помилки, що підвищує точність даних. Відсутність необхідності в посередниках знижує витрати на обробку транзакцій [2]. Технологія блокчейн забезпечує високу точність та безпеку транзакцій завдяки розподіленій мережі, де кожна операція підтверджується тисячами пристроїв. Це усуває потребу в централізованому контролі та знижує ризик помилок. Блокчейн дозволяє скоротити витрати на обробку платежів, оскільки не вимагає участі третіх сторін. Швидкість проведення транзакцій, особливо важлива для міжнародних операцій, також є значною перевагою блокчейну [11]. Замість того, щоб зберігатися на одному централізованому сервері, дані в блокчейні розподіляються по тисячах комп'ютерів по всьому світу. Кожна зміна в блокчейні автоматично відображається на всіх пристроях мережі, що робить систему надзвичайно стійкою до зломів та маніпуляцій. Така децентралізація гарантує, що інформація є достовірною та не може бути легко підроблена [2]. Хоча кожна транзакція в блокчейні є публічною та доступною для перегляду, особисті дані користувачів, як правило, залишаються прихованими. Ідентифікація учасників мережі відбувається за допомогою унікальних адрес, які не пов'язані з реальними іменами. Після того, як транзакція підтверджена мережею, її неможливо змінити або видалити [11].

Кожна підтверджена транзакція стає невід'ємною частиною ланцюжка блоків, де кожен блок пов'язаний з попереднім за допомогою унікального

цифрового відбитка. Це робить систему надзвичайно стійкою до змін, оскільки будь-яка спроба змінити одну транзакцію призведе до порушення цілісності всього ланцюжка. Крім того, відкритий код блокчейну дозволяє незалежним експертам перевіряти систему на наявність уразливостей [11]. Деякі блокчейни можуть функціонувати як закриті системи, обмежуючи доступ до інформації лише авторизованими учасниками. Враховуючи потенціал блокчейну забезпечити прозорість і незмінність даних, у майбутньому може з'явитися вимога для публічних компаній використовувати цю технологію для ведення фінансової звітності, що унеможливить маніпуляції з фінансовими показниками [1].

Технологія блокчейн, незважаючи на свої переваги, має і певні недоліки. Серед них можна виділити високий поріг входу для розуміння та застосування, значні енергетичні витрати, особливо для систем, що використовують доказ роботи. Крім того, втрата криптографічних ключів може призвести до безповоротної втрати доступу до активів, а відсутність чіткої регуляції створює певні ризики для користувачів [2]. Продуктивність блокчейн-мереж варіюється: деякі обробляють транзакції повільно, інші швидше, але всі мають обмеження за обсягом даних в одному блоці. Хоча блокчейн забезпечує високий рівень конфіденційності, це ж створює сприятливе середовище для незаконної діяльності. Державна політика щодо криптовалют залишається нестабільною, викликаючи тривогу в криптоспільноті, оскільки деякі юрисдикції вводять обмеження на певні види цифрових активів, не зачіпаючи при цьому базову технологію блокчейн [20].

Технологія блокчейн потребує значних ресурсів для зберігання великих обсягів інформації. Зі зростанням кількості блокчейн-мереж, вимоги до обчислювальних потужностей та сховищ даних будуть лише збільшуватися. Хоча блокчейн наразі найчастіше використовується для управління криптовалютами, його потенціал значно ширший і охоплює різноманітні галузі [24]. Технологія блокчейн активно впроваджується в різноманітні сфери, від державного управління до комерційних проектів. Її популярність зумовлена високою безпекою та децентралізованим характером, що мінімізує ризики втрати даних.

Спочатку блокчейн знайшов застосування в сфері цифрових валют, проте його потенціал значно ширший [5].

Нестабільність традиційних фінансових систем спонукала людей шукати більш надійні способи збереження своїх активів. З'явилася потреба в децентралізованих фінансових інструментах, які не залежали б від центральних банків. Криптовалюти, як новий клас активів, задовольнили цей попит, запропонувавши інноваційну модель зберігання вартості. Криптовалюти пропонують низку переваг порівняно з традиційними банківськими системами. Серед них: цілодобовий доступ до коштів, фіксовані комісії за перекази незалежно від відстані, швидке проведення транзакцій та можливість користування послугами з будь-якого пристрою з доступом до інтернету. Крім того, криптовалюти забезпечують високий рівень анонімності та стійкість до цензури [20]. Традиційні фінансові системи, такі як банки, піддаються різним ризикам, включаючи банкрутство та знецінення валют. Криптовалюти, хоча й більш волатильні, пропонують альтернативу. Для тих, хто шукає більшої стабільності, були створені стейблкоїни – криптовалюти, прив'язані до вартості фіатних валют або товарів. З іншого боку, фінансові інститути можуть підвищити ефективність своїх операцій за рахунок інтеграції технології блокчейн [1].

Сфера охорони здоров'я все активніше впроваджує технологію блокчейн для зберігання медичних даних пацієнтів. Завдяки криптографії з використанням публічних та приватних ключів, доступ до цієї інформації можуть отримати лише уповноважені особи. Це дозволяє забезпечити високий рівень конфіденційності та безпеки персональних даних [11]. Хоча блокчейн не є універсальним рішенням для зберігання всіх медичних даних, він ідеально підходить для тих, які потребують високого рівня безпеки та прозорості. Завдяки блокчейну пацієнти можуть бути впевнені, що їхні медичні записи є точними, повними та недоступними для несанкціонованого редагування. Лікарі, в свою чергу, отримують надійний інструмент для ведення медичної документації та співпраці з колегами [2]. Завдяки блокчейну, медичні дані пацієнтів отримують надійний захист від несанкціонованого доступу. Це значно знижує ризики шахрайства та

шантажу, оскільки зловмисникам буде вкрай складно змінити або підробити інформацію, зашифровану в блокчейні. Багато медичних установ вже успішно впроваджують такі системи [15].

Технологія блокчейн також може ефективно використовуватися для створення незаперечного доказу володіння майном, що забезпечує надійну фіксацію прав власності [25]. Безпека даних, особливо при використанні блокчейну, є пріоритетом. Ця технологія забезпечує незмінність записів, що унеможливорює підробку або втрату інформації про право власності. Це означає, що довести свої права на майно буде значно простіше і швидше [25]. Навіть у разі виходу з ладу окремих елементів системи, загальна працездатність мережі та цілісність даних залишаться недоторканими [11]. Головна відмінність розумних контрактів полягає в їхній самодостатності. Вони автоматично виконують умови угоди без потреби в посередниках, що суттєво спрощує процедури та знижує витрати [25].

Блокчейн забезпечує високий рівень безпеки для споживачів, дозволяючи відстежувати шлях продукту та виявляти потенційні загрози для здоров'я. У разі виявлення неякісних товарів, всі учасники ланцюга поставок будуть негайно проінформовані [2].

Проблема чесних та прозорих виборів є актуальною вже століттями. Маніпуляції з результатами голосування підривають довіру до демократичних інститутів. Впровадження технології блокчейн у виборчий процес може радикально змінити ситуацію, забезпечивши повну прозорість підрахунку голосів та унеможлививши будь-які спроби фальсифікацій [25].

Можливості застосування блокчейну в державному секторі надзвичайно широкі: від забезпечення прозорості виборів до оптимізації процесів в охороні здоров'я та освіти [23].

Блокчейн має широкий спектр застосування, включаючи охорону здоров'я та критичну інфраструктуру. Наприклад, він може використовуватися для відстеження поширення інфекційних хвороб та забезпечення безпеки енергетичних систем [26]. Проект "Енергетичний Інтернет" демонструє потенціал

блокчейну у створенні децентралізованого та прозорого енергетичного ринку. Завдяки цій технології, кожен споживач може самостійно керувати своїм споживанням електроенергії, а виробники можуть ефективніше керувати своїми ресурсами. Це відкриває нові можливості для розвитку відновлюваних джерел енергії та підвищення енергоефективності. [11].

Японський уряд інвестує в розробку інноваційної платформи для торгівлі відновлюваною енергією, яка працюватиме за принципами вільного ринку. Ця платформа дозволить споживачам купувати електроенергію за динамічними цінами, що формуються залежно від попиту та витрат на доставку, сприяючи таким чином розвитку "зеленої" енергетики.

Малакка готується стати першим у світі блокчейн-містом, де туристи зможуть насолодитися комфортом сучасних технологій та екзотичної природи. Це буде не просто курорт, а справжнє місто майбутнього, де всі фінансові операції будуть здійснюватися за допомогою криптовалюти, забезпечуючи прозорість та безпеку [11].

Блокчейн стає ключовим елементом цифрової трансформації Європи. 22 країни ЄС вже інвестували понад 350 мільйонів євро в проекти, спрямовані на впровадження блокчейн-технологій у державні послуги. Це свідчить про визнання блокчейну як надійного інструменту для захисту персональних даних та підвищення якості життя громадян [11].

Естонія продемонструвала, як блокчейн може перетворити державні послуги. Завдяки цій технології, естонці отримали зручний доступ до своїх медичних даних, а також інших важливих документів через онлайн-платформу. Це зробило Естонію одним з лідерів у сфері цифрової трансформації [11].

Блокчейн відкриває нові можливості для оптимізації державних послуг. Грузія та Швеція довели ефективність блокчейну для реєстрації нерухомості, а Мальта – для зберігання освітніх документів. Завдяки цій технології, громадяни отримують надійний захист своїх даних та зручний доступ до потрібної інформації.

Україна демонструє світові лідерство у використанні блокчейну для модернізації державних послуг. Платформа "Дія" та партнерство з компанією BitFury сприяють створенню безпечної та прозорої системи реєстрації, що відповідає найвищим світовим стандартам [11].

Блокчейн перетворюється на фундамент для побудови сучасних державних систем. Його здатність забезпечувати високий рівень безпеки та доступності робить цю технологію незамінною для захисту критично важливих даних. Все більше країн розуміють стратегічну важливість блокчейну та активно впроваджують його у свої системи.

Проблема масштабування блокчейну залишається однією з найактуальніших у цій галузі. Існуючі рішення мають свої обмеження і не можуть забезпечити повну ефективність мережі. Для досягнення оптимальних результатів необхідно вирішити такі завдання, як збільшення пропускну здатності, забезпечення безпеки та зменшення часу підтвердження транзакцій. Пошук компромісів між цими вимогами є ключовим для подальшого розвитку технології блокчейн [11]. Незважаючи на те, що лінійний порядок блоків може здаватися другорядним для простих транзакцій, він відіграє критичну роль у функціонуванні смарт-контрактів. Саме лінійний порядок гарантує коректність виконання умов контрактів, особливо в процесі голосування. Зміна цього порядку може призвести до непередбачуваних результатів та порушення логіки роботи мережі. Рівень формалізації оцінок безпеки різних типів атак на блокчейн відрізняється. Для деяких атак, таких як подвійна витрата, вдалося отримати точні кількісні оцінки ймовірності успіху. Однак, для інших атак, особливо пов'язаних з часовими параметрами, оцінки носять більш загальний характер і базуються на спрощених припущеннях про безперервність часу [15]. Створення надійного лінійного порядку блоків є складним інженерним завданням, що вимагає врахування широкого спектру можливих атак.

2 ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Типи блокчейн-систем

2.1.1 Сфери застосування технології блокчейн

Завдяки своїй універсальності, блокчейн знаходить застосування в різних сферах від економіки до права. В залежності від функціональності та складності, технологію блокчейн можна класифікувати на три основні типи [11].

Проста модель: Блокчейн 1.0 запропонував спрощену модель децентралізованих цифрових валют.

Розширені можливості: Блокчейн 2.0 додав нові функціональні можливості, такі як смарт-контракти, що ускладнили архітектуру систем.

Комплексні рішення: Блокчейн 3.0 прагне створювати комплексні рішення для різних галузей, що вимагає ще більшої складності та масштабованості.

Блокчейн – це незмінна, розподілена база даних, що складається з ланцюжка взаємопов'язаних блоків. Кожен новий блок, доданий учасниками мережі, містить інформацію про нові транзакції та посилання на попередній блок, створюючи тим самим хронологічний ланцюжок. [3]. Кожен вузол в мережі Bitcoin є одночасно клієнтом і сервером, зберігаючи повну копію блокчейну та беручи участь у валідації нових транзакцій. [27]. Bitcoin використовує блокчейн як фундаментальну технологію для створення довірчого середовища, де кожна транзакція реєструється та верифікується всіма учасниками мережі. [11]. Револьюційна концепція блокчейну полягає в створенні довірчого середовища для проведення транзакцій без необхідності залучення посередників. Замість того, щоб покладатися на довіру до окремих учасників, система використовує розподілену базу даних, що підтримується всіма учасниками мережі. Блокчейн вирізняється тим, що він пропонує механізм проведення транзакцій, який не вимагає довіри до окремих сторін. Замість централізованого контролю, безпека забезпечується за рахунок розподіленої бази даних, що дублюється на багатьох

комп'ютерах. [16]. Блокчейн пропонує новий підхід до проведення транзакцій, який дозволяє усунути потребу в централізованих посередниках. Завдяки розподіленій структурі, блокчейн забезпечує автономність і безпеку кожної транзакції. Блокчейн революціонізує спосіб проведення транзакцій, надаючи можливість взаємодіяти безпосередньо між собою, без втручання третіх сторін. Ця технологія створює справді глобальну мережу, де кожен учасник має рівні права. [20]. Технологія блокчейн не обмежується лише криптовалютами. Її можна використовувати для обміну будь-якими видами активів, від фінансових інструментів до нематеріальних цінностей, забезпечуючи при цьому високий рівень безпеки та прозорості. [12]. Блокчейн пропонує масштабовану та децентралізовану платформу для управління різноманітними активами. Ця технологія дозволяє створити глобальну систему обліку, яка не залежить від централізованих органів і доступна всім учасникам мережі. Блокчейн – це інструмент для створення глобального, децентралізованого реєстру, який може використовуватися для обліку та управління будь-якими активами. Ця технологія дозволяє усунути посередників і забезпечити прозорість всіх операцій. [11].

Технологія блокчейн вже закріпилася як «валюта інтернету», виступаючи глобальною цифровою платіжною платформою, яка може еволюціонувати у повноцінний «інтернет грошей», аналогічно тому, як «інтернет речей» об'єднує різноманітні пристрої [28]. Найочевиднішою та найпершою сферою використання блокчейна стали фінансові операції. Впровадження альтернативних систем грошових розрахунків обґрунтоване навіть з погляду економічної доцільності: вони дозволяють значно зменшити витрати на комісії за платежі, зокрема при використанні кредитних карток у міжнародних транзакціях. Окрім цього, блокчейн забезпечує миттєве надходження коштів, позбавляючи користувачів необхідності чекати кілька днів для завершення переказу. [1]. Використання біткойна та інших криптовалют здатне кардинально змінити наше розуміння грошей, торгівлі та комерції [11]. Біткойн — це не просто вдосконалена альтернатива платіжній системі VISA; він відкриває можливості, які раніше навіть не розглядалися, адже валюта та платежі — лише одна з багатьох сфер його

застосування [5]. Ключова перевага грошових операцій на базі блокчейна полягає в тому, що вони дозволяють проводити будь-які угоди в інтернеті без участі посередників. Завдяки альткойнам можна здійснювати перекази коштів і вести комерційну діяльність децентралізовано, розподілено і на глобальному рівні [6]. Таким чином, криптовалюта має потенціал стати відкритою програмованою платформою для децентралізованого обміну будь-якими ресурсами, виходячи за межі валюти та платежів. У цьому контексті Блокчейн 1.0, який спершу використовувався для грошових операцій і платежів, уже трансформується у Блокчейн 2.0, що дозволяє більш повно розкрити функціональні можливості біткойна як програмованих грошей [11].

Блокчейн 2.0 являє собою наступний ключовий етап у розвитку блокчейн-технологій, який все ще перебуває в активній стадії становлення і постійного вдосконалення. Ця галузь включає безліч різноманітних категорій, описів і концепцій, які продовжують формуватися. На сьогоднішні стандартні визначення та класифікації знаходяться в процесі розробки. У рамках поняття Блокчейн 2.0 можна зустріти такі терміни, як Біткойн 2.0, протоколи Біткойн 2.0, смарт-контракти, смарт-активи, децентралізовані додатки (DApps), децентралізовані автономні організації (DAO) та децентралізовані автономні корпорації. Якщо первісна версія блокчейна, відома як Блокчейн 1.0, зосереджувалася на децентралізації фінансових операцій, то основне призначення Блокчейн 2.0 полягає у створенні децентралізованих ринків і розширенні можливостей використання технології в значно ширшій перспективі. [11]. Блокчейн 2.0 забезпечує можливість передавати через розподілений реєстр не тільки валюту, а й інші типи активів, починаючи від їх створення і до моменту передачі або розподілу. Його можна уявити як аналог стеку інтернет-протоколів. Протоколи Блокчейн 2.0 або інтегруються з розподіленим реєстром біткойна, або формують власні розподілені журнали, при цьому залишаючись у межах тієї ж децентралізованої моделі технічної архітектури криптовалют, що включає три рівні: блокчейн, протокол і валюту. Однак важливо враховувати, що ці «нові базові рівні інтернету» наразі знаходяться у стадії активного розвитку, тому будь-

які метафоричні визначення можуть швидко втратити свою актуальність. [29]. Концепція базується на використанні функціональності децентралізованого реєстру транзакцій для реєстрації, підтвердження та передачі різноманітних типів контрактів і форм власності. Серед категорій і прикладів активів та угод, які можуть бути передані через блокчейн, є фінансові операції, угоди з цінними паперами, частками в компаніях, краудфандингові інструменти, боргові зобов'язання, пайові інвестиційні фонди, ануїтети, пенсійні активи, а також похідні фінансові інструменти, такі як ф'ючерси, опціони чи свопи [1]. Крім того, до розподіленого реєстру можна інтегрувати офіційні документи, наприклад, свідоцтва на право власності на нерухомість або земельні ділянки, реєстраційні документи для транспортних засобів, бізнес-ліцензії, свідоцтва про шлюб або смерть. Також технологія блокчейна дозволяє підтверджувати цифрові ідентифікаційні дані, включно з водійськими посвідченнями, паспортами та іншими посвідченнями особи. [11]. Зберігання приватних документів, таких як боргові зобов'язання, кредитні угоди, контракти, парі, підписи, заповіти та довіреності, може здійснюватися за допомогою блокчейна. За допомогою цієї технології можна також виконувати засвідчення страхових полісів, документів про право власності та здійснювати нотаріальне посвідчення. Ключі до фізичних об'єктів можуть бути закодовані в децентралізованому реєстрі у вигляді цифрових активів, які забезпечують контрольований доступ до будинків, номерів у готелях, орендованих автомобілів або транспортних засобів для спільного користування. Крім того, нематеріальні активи, як-от патенти, торгові марки, авторські права, бронювання чи доменні імена, також можуть бути захищені та передані через розподілений реєстр [25]. Наприклад, для захисту інновації, замість стандартної реєстрації патенту або торгової марки, її можна закодувати в блокчейні із зазначенням точної дати й часу. Це дозволить підтвердити існування винаходу на конкретний момент часу [25]. Смарт-контракти можна розглядати як автономні децентралізовані програми, які працюють під псевдонімами завдяки використанню блокчейн-технології. У цьому контексті розподілений реєстр може стати одним із потенційних шляхів до розвитку штучного інтелекту, оскільки

платформи для смарт-контрактів розробляються з урахуванням потреб у підвищенні рівня автоматизації, автономності та складності. У процесі поширення децентралізованих програм, організацій, корпорацій і суспільств можуть виникати нові форми складної та непередбачуваної поведінки, які нагадують дії штучного інтелекту [11]. Один із шляхів розвитку полягає у впровадженні в блокчейн існуючих систем, заснованих на заздалегідь визначених правилах, які безпосередньо не пов'язані зі штучним інтелектом або блокчейном. Це сприятиме підвищенню автоматизації та ефективності таких операцій. До прикладів таких систем належать моделі поведінкової симуляції, а також платформи з відкритим вихідним кодом, які надають можливість створювати агентів для моніторингу ситуацій і виконання дій від імені користувачів [12]. Технологія блокчейн здатна вплинути не тільки на фінансові ринки, платіжні системи, економіку та різноманітні фінансові послуги, але й на інші галузі та майже всі аспекти людської діяльності [1]. Вона представляє собою принципово нову концепцію, яка дає змогу організовувати процеси з меншою витратою зусиль, підвищуючи їх ефективність і масштаби до рівнів, недосяжних для інших існуючих підходів. Децентралізована модель функціонування може досягти своєї максимальної ефективності лише за умов існування гнучкої глобальної мережі, здатної здійснювати транзакції без участі посередників [3]. Проте особливість блокчейна полягає не лише в його децентралізованій природі. Його ключова перевага – це універсальність і глобальний масштаб, які раніше здавалися недосяжними. Блокчейн може бути використаний для автоматизованого управління та розподілу різноманітних ресурсів, зокрема матеріальних активів і людських ресурсів [20].

Технологія блокчейн сприяє спрощенню координації різних форм взаємодії між людьми, забезпечує ефективну організацію спільної діяльності та може стати основою для нового етапу взаємодії людини з машинами [5]. Існує припущення, що всі сфери людської активності можуть бути певною мірою оптимізовані за допомогою блокчейна або адаптовані з використанням його принципів. Організаційна модель, заснована на блокчейн-технології, демонструє вищу ефективність з точки зору функціональності, практичності та масштабності.

Блокчейн, завдяки вимозі досягнення консенсусу, створює умови для більшої свободи, рівноправності та залученості, у порівнянні з традиційними системами [11]. Ця технологія виступає як універсальне рішення, що забезпечує значні переваги як у кількісному, так і в якісному аспектах.

Блокчейн-технологія має потенціал для розкриття творчих і винахідницьких здібностей кожного, хто опанує її основи, такі як криптографія з використанням відкритих і закритих ключів, піринговий обмін файлами, розподілені обчислення, мережеві структури, псевдонімність, журнал блокчейн-записів, криптовалюти та їхні протоколи. Ці складові ставлять під сумнів традиційні підвалини сучасного суспільства, включаючи готівкові гроші, економічні системи, довірчі відносини, механізми ціноутворення та роботу бірж [1]. Оволодіння цими новими концепціями дозволяє не тільки розробляти інноваційні рішення на основі блокчейна, а й застосовувати їх у зовсім інших контекстах. Завдяки своїй гнучкості та адаптивності блокчейн-технологія може глибоко вплинути на розвиток суспільства, адже люди будуть освоювати її концепції та переносити їх у найрізноманітніші сфери діяльності [6].

Блокчейн-технологія дозволяє зрозуміти, що все, що оточує нас і що ми сприймаємо, кожна система в нашому житті є певною формою розподілу ресурсів. Її дискретна структура, що дає змогу відслідковувати транзакції через єдиний реєстр записів, надає набагато більше інформації, ніж ті облікові та ресурсні системи, які використовуються сьогодні [7]. Використання блокчейна для моніторингу ресурсів дозволяє автоматично, без затримок, оцінювати наслідки будь-яких транзакцій з участю всіх залучених сторін і проводити їх аналіз на глобальному рівні [11]. Це можна уникнути, якщо система цінностей суспільства не дозволяє відкрито відстежувати активність користувачів. Морально-етичні аспекти такого контролю є важливою темою для подальших соціологічних та наукових досліджень.

Блокчейн може значно спростити автоматизацію обчислень, створюючи універсальну модель координації, яка здатна підтримувати величезну кількість транзакцій [22]. Ця система, яка має глобальний масштаб, що раніше був уявний,

відкриває нові можливості для обробки даних. Використання великих даних дозволяє здійснювати передбачувальне моделювання численних процесів, які відбуваються у реальному світі, а блокчейн-технологія здатна посилити можливості для реалізації прогнозів. Комбінація блокчейна та великих даних дозволяє не тільки покращити реактивність, а й перевести процеси в режим прогнозування, що відкриває великі перспективи для автоматизації різноманітних завдань на основі смарт-контрактів та економічних механізмів [11]. Передбачувальний аналіз великих даних добре доповнюється автоматизацією виконання смарт-контрактів [12]. Блокчейн-технологія може також слугувати вбудованою платіжною системою та механізмом адміністрування дискретних даних, забезпечуючи функціональність через смарт-контракти, децентралізовані додатки, автономні організації та корпорації. Автоматизація виконання широкого спектра завдань дозволить знизити навантаження на операторів, передавши їх функції на універсальну, децентралізовану та глобально розподілену обчислювальну систему. Дискретизація, моніторинг і управління завданнями в усіх сферах діяльності за допомогою блокчейн-технології відкриють набагато більше можливостей, ніж ті, що надають сьгоднішні технології великих даних [11].

Головним аргументом на підтримку технологій Блокчейн 1.0 і 2.0 є їхня економічна вигідність і зменшення витрат завдяки використанню децентралізованих мережевих структур, що не потребують довіри до єдиного органу, який здійснює транзакції [1]. Окрім цього, існують й інші суттєві переваги, зокрема свобода та розширення прав і можливостей для учасників. Децентралізовані моделі можуть сприяти розвитку економічних відносин без жорсткого контролю в країнах, де рух капіталу регулюється обмеженнями [20]. Важливим аспектом є псевдонімні транзакції, які не підлягають контролю та регулюванню з боку державних органів [14]. Це має особливе значення для країн, що розвиваються, де контроль над капіталом, обмеження в економічній політиці та інші фактори ускладнюють ведення бізнесу, включаючи створення нових

підприємств. В умовах державного контролю та недовіри до фіатних грошей спостерігається зростання інтересу до криптовалют [20].

Свобода, яку надають технології Блокчейн 3.0, дає змогу реалізовувати рішення, не пов'язані безпосередньо з фінансовими операціями чи ринковими транзакціями. Глобальна децентралізована природа цієї технології відкриває можливості для обходу обмежень, накладених географічними юрисдикціями [29]. Існує переконання, що блокчейн може забезпечити об'єктивне вирішення питань, пов'язаних зі свободою, юрисдикцією, цензурою та регулюванням, в способи, які можуть бути недоступні для державних і міжнародних організацій, що займаються захистом прав людини [25]. Деякі операції, незалежно від того, як їх класифікують державні закони, є глобальними, транснаціональними транзакціями. Тому їхнє управління, координація та моніторинг можуть бути набагато ефективнішими на організаційних рівнях, таких як Всесвітня торгова організація. Таким чином, йдеться про усунення обмежень, накладених державними юрисдикціями на транснаціональні організації та перенесення їх діяльності в глобальний простір [20]. По-перше, для транснаціональних організацій необхідна відповідна транснаціональна структура управління. Блокчейн-технологія дозволяє створити таку структуру, що є ефективною завдяки забезпеченню масштабованості, доступності та прозорості. Управління за допомогою блокчейна є більш адекватним для транснаціональних організацій порівняно з традиційним державним управлінням. По-друге, блокчейн не лише робить управління ефективнішим, а й забезпечує неупереджене транснаціональне управління. Децентралізована модель, заснована на хмарних технологіях, може забезпечити більшу рівність, свободу та справедливість для організацій та їхніх учасників. Розподілений реєстр транзакцій гарантує неможливість фальсифікації записів, прозорість і доступність [25]. Кожна людина в будь-якій точці світу може переглядати і перевіряти операції, що здійснюються транснаціональними організаціями. Отже, блокчейн функціонує як глобальна система стримувань і противаг, сприяючи довірі серед усіх учасників. Це ключовий інфраструктурний елемент, який дозволяє створювати глобальні організації та механізми

координації, відкриваючи шлях до швидкого прогресу [11]. Технологія блокчейн вирішує проблему адміністрування транснаціональних громадських організацій, пропонуючи при цьому ефективні рішення. Завдяки демократичному, розподіленому характеру та участі багатьох сторін механізми блокчейна можуть забезпечити найефективніше та справедливе управління транснаціональними громадськими організаціями [20].

Ще однією значущою сферою застосування технології Блокчейн 3.0 є так зване блокчейн-урядування, що передбачає використання цієї технології для більш ефективного, економічного і персоналізованого надання послуг, які традиційно забезпечуються державними органами [23]. Блокчейн створює нові можливості для розробки альтернативних моделей управління та надання державних послуг. Блокчейн-урядування засноване на використанні технологій для збереження загальнодоступних записів у розподіленому реєстрі, який є універсальним, постійним, узгодженим, безперервно працюючим, повноцінним і доступним для громадського контролю архівом [23]. Технологія блокчейн може стати основою для управління інформацією в реальному часі та виступати сховищем всіх документів і історичних даних, що використовуватимуться в майбутньому, перетворюючись на універсальну систему зберігання записів [20]. Хоча не всі запропоновані моделі і державні послуги потребують блокчейн для своєї реалізації, їх впровадження за допомогою цієї технології може забезпечити додаткові переваги, зокрема підвищення рівня довіри та можливість зберігання відкритих записів. Результатом створення блокчейн-урядування стане перехід від жорсткої єдиної моделі до більш гнучкої, яка зможе адаптуватися до індивідуальних потреб громадян, що може сприяти розвитку більш демократичного суспільства [22]. Це можливо реалізувати через використання смарт-контрактів на базі блокчейна та децентралізованих автономних корпорацій, що дозволяє уникнути участі чиновників і виключити людський фактор із процесу [23]. Технології блокчейн і децентралізовані моделі ставлять під сумнів ефективність традиційних управлінських структур. Блокчейн-урядування використовує переваги інформаційних технологій цієї технології, що дозволяє

створити нову, максимально ефективну систему для організації, адміністрування, координації та запису всіх дій, здійснюваних людьми, будь то корпораціями, урядами чи окремими особами. Застосування блокчейн-технології порушує питання про підвищення ефективності державних функцій, а також про права, які повинні бути забезпечені державою [23].

2.1.2 Сучасні виклики щодо правового регулювання технології блокчейн

Технологія блокчейн і спроби її впровадження знаходяться на стадії початкового розвитку і стикаються з рядом обмежень. Серед них можна відзначити технічні характеристики базових технологій, питання безпеки, соціальне прийняття та необхідність державного регулювання [20]. Попри це, блокчейн має великий потенціал і перспективи для трансформації різних секторів. Він виступає потужним інструментом для надійного зберігання ідентифікаційних даних фізичних і юридичних осіб, ведення реєстрів, реєстрації фінансових операцій, виконання юридичних дій та інших застосувань [1]. Проте є низка технічних складнощів, що виникають через особливості моделі блокчейна. Для вирішення цих проблем науковцями пропонуються різні рішення, і процес реалізації супроводжується активними обговореннями та новими ідеями. Одним із запропонованих варіантів є використання розподіленого журналу записів з найрозвиненішою інфраструктурою в якості універсального стандарту. Водночас інші спеціалісти займаються розробкою нових блокчейн-систем або криптехнології, застосовуючи альтернативні підходи [23].

Одним із важливих завдань для технології блокчейн є подолання існуючого обмеження щодо кількості транзакцій, які можуть оброблятися за секунду. Інші важливі проблеми включають безпечне збільшення обсягу блоку в розподіленому журналі записів, захист від «атаки 51%», а також внесення змін до коду, які можуть порушити зворотну сумісність [16]. Системи, побудовані на основі

блокчейн-технології, повинні враховувати ризики, пов'язані з «атакою 51%», яка може статися, якщо зловмисник отримає контроль над понад 51% обчислювальних потужностей [16]. Це дає можливість для подвійної витрати, де зловмисник може змусити користувача повторно здійснити транзакцію через маніпуляції з кодом. Ще однією загрозою є можливість зламу еліптичної криптографії, яка використовується в блокчейн-системах [14]. Для усунення цієї вразливості розробники працюють над оновленнями. Крім того, блокчейн-системи вимагають значної кількості електричної енергії для забезпечення їхньої стабільної роботи, що спричиняє значні енергетичні витрати. Однак така енергетична витрата є частиною механізму децентралізованої довіри: користувачі змагаються між собою, виконуючи роботу для підтримки безпеки системи. Окремою технічною проблемою є швидке збільшення кількості розподілених журналів записів [17]. Зростаюча кількість нових систем, що базуються на технології блокчейн, призводить до того, що в деяких випадках стає легше здійснити «атаку 51%». Іншою значною проблемою є ситуація, коли блокчейн розщеплюється (наприклад, через адміністративні причини або під час оновлення мережі), що призводить до утворення двох несумісних ланцюжків. В такому випадку, об'єднання цих ланцюжків або здійснення транзакцій між ними виявляється складним процесом. Крім того, важливим технічним викликом є необхідність створення повної екосистеми рішень, які підтримують усі етапи ланцюга створення цінності [16]. Для розподіленого журналу записів, наприклад, необхідно забезпечити наявність безпечного децентралізованого сховища, системи повідомлень, транспортної інфраструктури, протоколів взаємодії, просторів імен, управлінських сервісів для адрес, інструментів для мережевого адміністрування та архівування. Деякі дослідники вважають, що найбільш перспективним є розвиток блокчейн-технології як моделі хмарних обчислень, де вже на початкових етапах будуть визначені та впроваджені стандартні інфраструктурні компоненти, такі як хмарні сервери та транспортні системи. Це дозволить сконцентруватися на високорівневих послугах додавання цінності, замість того, щоб витрачати зусилля на розбудову базової інфраструктури [20].

Для економічного розвитку блокчейн-технології це є критично важливим через складність процесів шифрування та гарантування конфіденційності в умовах децентралізованих мереж. Наразі активно розробляються оптимальні підходи до забезпечення мережевої безпеки, криптографії та математичних основ для блокчейн-стартапів. Важливо, щоб ці вимоги не були надмірно високими, і щоб існувала надійна інфраструктура, в якій ці функції були б автоматично доступні [14]. Це, у свою чергу, сприятиме швидшому впровадженню блокчейн-технологій, дозволяючи організаціям не турбуватися про сумісність електронних гарантів, таких як підтримка мультипідпису або будь-яких інших стандартів безпеки, що можуть бути визначені на той час [16].

На сьогодні технологія блокчейн та її потенціал знаходяться на початковій стадії досліджень. Існує ряд нормативних питань, які потребують вирішення перед тим, як ця технологія стане широко впровадженою та застосовуваною [20]. Законодавча база для регулювання технології блокчейн повинна включати положення щодо визначення відповідальності та умов застосування правових норм у різних юрисдикціях, оскільки розподілені реєстри не мають фіксованого місця розташування і централізованого управління [22]. Ці питання становлять серйозну проблему для правового регулювання блокчейн-технології, оскільки вона діє в глобальному масштабі та не підпорядковується конкретним територіальним межах. Рішення щодо юрисдикції та правових норм потребують міжнародної співпраці та укладання угод, оскільки вплив блокчейна може зачіпати різні сфери діяльності на територіях різних країн. Тому для розв'язання цих проблем необхідно спільно працювати над створенням міжнародних правових стандартів [1].

Поки що блокчейн не має повної юридичної сили і не може бути використаний як самостійний доказ у судових справах. Це пов'язано з відсутністю чітких правил та стандартів, які б регулювали використання цієї технології. Потенціал блокчейну як інструменту для забезпечення безпеки та прозорості транзакцій обмежений відсутністю відповідної правової бази. Доки не будуть

ухвалені необхідні закони та нормативи, блокчейн не може бути повноцінно використаний у багатьох сферах. [25].

Незмінність даних в блокчейні створює правову невизначеність, оскільки суперечить існуючим нормам, які передбачають можливість зміни або видалення інформації. Це ускладнює використання блокчейну в сферах, де важливий захист персональних даних. Правовий статус блокчейну як незмінного реєстру є спірним питанням, оскільки він може суперечити іншим важливим правам, таким як право на забуття. Ця правова невизначеність гальмує розвиток технології блокчейн. [30]. Концепція блокчейну, як незмінного сховища даних, суперечить європейському принципу права на забуття. Це означає, що інформація, раз записана в блокчейн, фактично стає недоступною для видалення, навіть якщо це стосується персональних даних громадян. Неможливість видалити дані з блокчейну створює розбіжності з європейським законодавством, яке гарантує кожному громадянину право на контроль над своїми персональними даними, включаючи право на їх видалення.

Компромісним рішенням може стати введення механізму, який дозволить обмежити доступ до персональних даних в блокчейні, не порушуючи при цьому принцип незмінності записів. Замість фізичного видалення інформації з блокчейну можна запропонувати механізм, який забезпечить логічне видалення, тобто обмеження доступу до цих даних для всіх користувачів мережі. [25]. Одним із можливих шляхів узгодження незмінної природи блокчейну з правом на забуття є впровадження автоматичних механізмів шифрування даних за умови, визначеними користувачем. Це дозволить приховати інформацію від сторонніх осіб без її фізичного видалення з системи. Для забезпечення конфіденційності даних в блокчейні можна застосувати смарт-контракти, які автоматично обмежать доступ до певних записів за запитом користувача. Це дозволить зберегти цілісність блокчейну, водночас гарантуючи право індивіда на приватність.

Розробка міжнародних стандартів та уніфікація підходів до визнання юридичної сили документів, що зберігаються в блокчейні, є важливим завданням для забезпечення глобальної довіри до цієї технології. Для створення ефективної

правової бази для блокчейну необхідна тісна співпраця між різними країнами та міжнародними організаціями. [23]. Документи, що зберігаються в блокчейні, повинні мати таку ж юридичну силу, як і традиційні паперові документи, підписані власноруч. Це означає, що вони повинні бути визнані як достовірне підтвердження прав та фактів. Для того, щоб блокчейн міг замінити традиційні реєстри та бази даних, необхідно забезпечити рівнозначність юридичної сили документів, що зберігаються в цих системах. Незважаючи на те, що технологія блокчейн забезпечує високий рівень захисту даних, відсутність чітких правових норм, що регулюють використання інформації, зафіксованої в блокчейні, стримує її широке застосування в юридичній сфері. Недостатня розробленість правового поля для технології блокчейн перешкоджає повноцінному використанню потенціалу цієї технології для підтвердження прав та фактів. [23].

Для того, щоб фінансові інструменти, що існують виключно в цифровому вигляді та засновані на технології блокчейн, могли вільно обертатися на ринку, необхідно отримати визнання їхньої юридичної сили з боку регуляторних органів. Використання блокчейну для емісії та обігу фінансових інструментів вимагає створення чіткого правового поля, яке б забезпечувало захист прав інвесторів та стабільність фінансового ринку. [22].

Широке розповсюдження цифрових активів, створених на базі блокчейну, відкриває нові можливості для фінансового сектору, але водночас створює ряд викликів для регуляторів та центральних банків. Застосування блокчейну у сфері фінансів, зокрема для створення нових видів грошей, може мати далекосяжні наслідки для макроекономічної стабільності та монетарної політики [22]. Для забезпечення стабільної та безпечної роботи ринку цифрових валют необхідне розроблення чіткого правового механізму, який би визначав їхній статус, права та обов'язки учасників цього ринку. Держава повинна відігравати активну роль у формуванні правового поля для цифрових валют, забезпечуючи їхню інтеграцію в існуючу фінансову систему та захищаючи інтереси громадян [30].

Смарт-контракти, як цифрові угоди, що виконуються автоматично, створюють нові виклики для традиційного правового регулювання. Особливо

гостро стоїть питання визначення місця укладення та виконання таких контрактів, а також відповідальності за їхні недоліки. Створення ефективної системи правового регулювання смарт-контрактів вимагає комплексного підходу, який враховує як технічні особливості цієї технології, так і традиційні правові принципи.

Застосування технології блокчейн для створення єдиного цифрового профілю кожного пристрою Інтернету речей відкриває нові можливості для безпечної взаємодії між пристроями. Однак, для реалізації такого підходу необхідна чітка правова основа, яка визнає блокчейн як надійний інструмент для ведення обліку та зберігання даних. Створення глобальної системи ідентифікації пристроїв Інтернету речей на основі технології блокчейн вимагає узгодження зусиль на міжнародному рівні та розробки спільних стандартів та правил.

Складна взаємодія між фізичним світом, представленим пристроями Інтернету речей, та цифровим світом, де функціонують смарт-контракти на основі блокчейну, вимагає розробки нових правових інструментів та механізмів. Питання правового регулювання смарт-контрактів, що лежать в основі функціонування Інтернету речей, є надзвичайно актуальними, оскільки вони стосуються як визначення місця укладення та виконання таких контрактів, так і відповідальності за їхні наслідки.

2.2 Законодавче (правове) регулювання технології блокчейн як об'єкт наукових досліджень

Швидкий розвиток технології блокчейн та її інтеграція в глобальний економічний простір виявили гостру потребу в міжнародному співробітництві для створення єдиних правил гри. Відсутність чітких правових норм створює перешкоди для розвитку цього перспективного напрямку та породжує нові ризики, пов'язані з кібербезпекою та відмиванням коштів. Для мінімізації цих

ризиків необхідне впровадження ефективних механізмів регулювання, які б, з одного боку, стимулювали інновації, а з іншого – забезпечували захист інтересів суспільства. [1]. Для успішного впровадження технології блокчейн державам необхідно розробити чіткі правові рамки, що визначають статус криптовалют та інших цифрових активів, а також правила їх обігу. При цьому важливо забезпечити сумісність нового законодавства з існуючими нормативними актами у сфері фінансів та податків. Глобальний характер технології блокчейн вимагає розробки міжнародних правових норм, які б забезпечили стабільність та безпеку цього ринку. [23].

Тема застосування блокчейну стала об'єктом пильної уваги науковців по всьому світу, включаючи українських дослідників, які внесли значний вклад у розвиток цієї галузі. Роботи вітчизняних та зарубіжних вчених є цінним джерелом інформації для розуміння потенціалу та особливостей технології блокчейн, а саме: С. Накамото, М. Свон та ін. Дослідники приділяли значну увагу можливостям застосування блокчейну для покращення взаємодії з громадськістю. Цей напрямок досліджували Р. Радейко, І. Клименко, Г. Лозова, Л. Акімова та ін. Науковці активно вивчають можливості застосування блокчейну для оптимізації логістичних процесів, цех досліджували А. Харченко, М. Мокляк, Е. Хаустової, а маркетингу – Р. Бек, М. Россі, Л. Северейнс, Дж. Татчер та ін. Питання правового регулювання електронних грошей та криптовалют детально аналізуються у численних наукових працях, а саме: М. Березіна, А. Беліч, А. Дьяков, Б. Івасіна, Д. Кочергін, Л. Красавіна, С. Криворучко, Ю. Крупнов, С. Міщенко, А. Мороз, І. Пенькова, М. Савлук, І. Трубін, В. Усоткін, М. Шаренко та ін. Питання правового статусу та застосування блокчейну в різних галузях економіки детально аналізуються у наукових працях А. Гурова, М. Кірпачова, Р. Ботвінов, О. Кравченко, Н. Небаба, О. Шаповал та ін. Незважаючи на значний інтерес до технології блокчейн, систематичні дослідження щодо її інституціоналізації та правового регулювання на міжнародному рівні залишаються недостатніми.

3 ОРГАНІЗАЦІЙНО-ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН. МІЖНАРОДНИЙ ДОСВІД

3.1 Державна політика країн щодо правового регулювання технології блокчейн

Світова спільнота ще не виробила єдиного підходу до регулювання технології блокчейн, що призводить до різноманітності національних законодавств у цій сфері. Незважаючи на потенціал блокчейну, його впровадження на міжнародному рівні відбувається поступово, що пов'язано з необхідністю вирішення низки правових та технічних питань.

Україна. Наряду із іншими країнами, впровадження технології блокчейн в Україні також знаходиться на початковому рівні [24]. Важливим кроком спрямованим на регулювання правовідносин, що виникають у зв'язку з застосуванням технології блокчейн, стала розробка проекту Закону України «Про віртуальні активи» [31]. Цей Закон має регулювати правові відносини, що виникають у зв'язку із обігом віртуальних активів в Україні, визначає права та обов'язки учасників ринку віртуальних активів, а також засади державної політики у цій галузі. Після набуття чинності Закону України «Про віртуальні активи» [31] зарубіжні та українські криптовалютні біржі матимуть можливість працювати на території України на законних засадах. Українські банки матимуть право відкривати рахунки для криптокомпаній. Інвестиції в віртуальні активи матимуть охоронятися законом, українська влада має гарантувати судовий захист прав на віртуальні активи [3]. Президент України висловив ініціативу класифікувати послуги віртуальних активів як фінансові послуги. З цими кроками застосування технології блокчейн в Україні має стати повністю легалізованими [26].

Метою інтеграції цифрового економічного простору з Європейським Союзом є розширення міждержавного партнерства України з блокчейн-мережами інших країн, сприяючи зміцненню співпраці та обміну досвідом у галузі

цифрових технологій [25]. Україна стала третьою країною (після Норвегії і Ліхтенштейну) поза межами ЄС, яка наголосила про намір приєднатися до Європейського блокчейн-партнерства. Ця ініціатива була запропонована 27 державами-членами з метою надання транскордонних державних послуг [29]. Міністерство цифрової трансформації України оголосило про свій намір розширити міжнародне партнерство з блокчейн-мережами інших країн і приєднатися до Європейської інфраструктури блокчейн-сервісів. Також відзначено зацікавленість уряду України у запуску пілотних проектів щодо використання транскордонних державних послуг на основі технології блокчейн. Ці кроки спрямовані на сприяння впровадженню технологій блокчейн в урядову діяльність держави.

Крім того, уряд України має намір розміщення широкого спектру електронних державних даних на блокчейн-платформі, чим відзначає зростаючу тенденцію серед урядів країн, які використовують цю технологію для підвищення ефективності та прозорості. Захищена державна система, заснована на технології блокчейн, може забезпечити захист інформації і суттєво вплинути на суспільні та економічні процеси у всьому світі, задовольняючи потребу у прозорості та обліковості [32]. Ця ініціатива може стати початком створення зовсім нової, інноваційної екосистеми для державних проектів у сферах ведення державних реєстрів, наданні державних послуг, соціального забезпечення, охорони здоров'я, енергетики та кібербезпеки [25]. Наступним кроком для України є намір отримати повноправне членство в Європейському блокчейн-партнерстві та для надання громадянам України транскордонних державних послуг. Ці послуги мають включати в себе перевірку документів про освіту та дипломів, особистих документів, а також реєстрацію внутрішньо переміщених осіб та підтримку біженців в Європі [24].

Сполучені Штати Америки (США). У Сполучених Штатах Америки існують загальні законодавчі норми, які стосуються використання технології блокчейн і застосовуються в штатах Нью-Йорк та Вайомінг [28]. Проте в багатьох інших штатах США відбувається процес оновлення або розробки нових законів

щодо грошових переказів, з метою включення в них використання технології блокчейн. Також створюються робочі групи для проведення наукових досліджень і випробувань цієї технології [33]. У 2017 році у штаті Аризона Сполучених Штатів Америки був прийнятий перший закон, спрямований на регулювання та застосування технології блокчейн, який надає можливість створювати юридично важливі угоди за допомогою смарт-контрактів. Зазначені смарт-контракти ґрунтуються на автоматизованому коді, побудованому на встановлених умовах в мережі блокчейн. Законодавство Аризони забезпечує захист прав операторів вузлів, які використовують технологію блокчейн в Арізоні.

У штаті Колорадо також були розроблені норми, спрямовані на регулювання використання криптовалюти. Цей штат прийняв закон, який дозволяє політичним кандидатам приймати криптовалюту як пожертвування для виборчих кампаній, але встановлює індивідуальний ліміт для таких пожертв. Пожертвування з використанням криптовалюти може додати додатковий рівень конфіденційності для донорів, проте розмір пожертвування від анонімних донорів обмежено.

Штат Міннесота може прийняти протилежну позицію щодо приймання пожертвувань в криптовалюті порівняно зі Штатом Колорадо. На розгляд був внесений законопроект, який містить заборону приймати пожертвування в криптовалюті.

Делавер був одним з перших штатів в США, який прийняв правила щодо криптовалют та технології блокчейн. Сенат розглянув законопроект, в якому дозволяється корпораціям використовувати технологію блокчейн для створення та ведення корпоративних записів, включаючи реєстр акцій корпорації. Податкова служба Сполучених Штатів Америки з 2015 року використовує програмне забезпечення, яке дозволяє відстежувати рух криптовалют, визначати її походження та ідентифікувати її власників.

Ініціатива створення законодавчої бази, щодо регулювання криптовалюти, в окремих штатах, поширило тенденцію створення національної законодавчої

структури для впровадження та використання технології блокчейн, на всій території США [34].

Китай. У 2018 році Міністерство промисловості та інформаційних технологій Китаю опублікувало документ під назвою «Біла книга індустрії блокчейну Китаю», який містить вказівки, щодо політики, в галузі впровадження та використання технології блокчейн в Китаї. До цього часу в Китаї не існувало законів або нормативних актів, які регулювали технологію блокчейн.

10 січня 2019 року Адміністрація кіберпростору Китаю прийняла «Адміністративні положення щодо інформаційних послуг блокчейн» (Положення про блокчейн), які набрали чинності з 15 лютого 2019 року. Положення про блокчейн стали першими офіційними правилами, які регулюють галузь застосування технології блокчейн в Китаї. Цей документ застосовується до інформаційних послуг в мережі блокчейн в Китаї, які визначаються як інформаційні послуги, надавані населенню через Інтернет, або за допомогою застосунків що базуються на технології блокчейн. Центральні та місцеві органи Адміністрації кіберпростору Китаю взяли на себе обов'язок нагляду та управління блокчейн-сервісами в Китаї. Додатково, були створені декілька об'єднань, які використовують технологію блокчейн, з метою сприяння дослідженням і розробкам надаючи можливість її впровадження [27].

Положення про впровадження та застосування технології блокчейн встановлюють певні вимоги до постачальників послуг, які використовують технологію блокчейн з метою забезпечення відповідності діючому законодавству та нормативним актам Китаю. Відповідно до цих положень, постачальники послуг, що використовують технологію блокчейн, повинні проводити перевірку ідентичності користувачів шляхом перевірки відповідних кодів організацій, номерів документів особистості та номерів мобільних телефонів, а також зберігати записи про вхід користувачів у систему не менш як протягом шести місяців. Згідно з цими вимогами, якщо постачальник послуг, який використовує технологію блокчейн, планує впровадити нові продукти, додаткові застосунки або

функції, він повинен надавати звітність Адміністрації кіберпростору Китаю і пройти оцінку безпеки.

Положення про впровадження та застосування технології блокчейн накладають відповідальність на постачальників послуг у випадку порушення зазначених вимог [27]. Відповідно до цих положень, китайські органи мають право покарати порушників у відповідності до чинного законодавства Китаю та нормативних актів, включаючи Закон Китаю про кібербезпеку. У разі порушення встановлених норм, порушники можуть бути притягнуті до кримінальної відповідальності. Важливо зауважити, що положення не обов'язково передбачають отримання спеціальних дозволів для надання послуг з використанням технології блокчейн. Такі послуги вважаються технічним бізнесом і, як правило, не вимагають спеціальних ліцензій чи дозволів для їх надання. Оскільки послуги, що використовують технологію блокчейн, надаються через Інтернет або за допомогою додатків, вони також підпадають під загальні закони та правила Китаю, включаючи Адміністративний регламент про інтернет-послуги та Каталог категоризації телекомунікаційного бізнесу. Як результат, послуги, які використовують технологію блокчейн, можуть вимагати отримання відповідних дозволів. Положення також встановлюють вимогу представляти Адміністрації кіберпростору Китаю документи, які стосуються постачальників послуг. Постачальники послуг з використанням технології блокчейн повинні подати звіт в Адміністрацію протягом десяти робочих днів з моменту початку надання таких послуг, а також подавати заяви у випадку змін чи припинення своєї діяльності. Невиконання цієї вимоги може призвести до видання попереджень чи покарання з боку Адміністрації кіберпростору Китаю. Для здійснення обліку поданих заявок, що відповідають Положенням, Адміністрація кіберпростору Китаю, 28 січня 2019 року впровадила систему адміністрування записів інформаційної служби технології блокчейн (<https://bcbeian.ifcert.cn/>). Важливо відзначити, що технологія блокчейн стала невід'ємною частиною національних технологічних стратегій Китаю і була включена до 13-го п'ятирічного плану інформатизації країни, який був опублікований у грудні 2016 року. Технологія блокчейн може надати значні

переваги підприємствам у різних галузях промисловості завдяки її технічним та бізнес-функціям, таким як підвищена прозорість, збільшена безпека, поліпшена відстежуваність, підвищена ефективність та прискорення процесу транзакцій [27]. Великі китайські інтернет-компанії взяли участь у наукових дослідженнях технології блокчейн та впроваджують її застосування в різних галузях, починаючи від фінансів, охорони здоров'я, електронної торгівлі, логістики та навіть судової практики. Зокрема, інтернет-суди в Пекіні та Ханчжоу в Китаї успішно використовують технологію блокчейн для створення платформ для зберігання судових записів і їх безпечної передачі.

Незважаючи на важливість та актуальність Положень про блокчейн, певні аспекти вимагають додаткових пояснень та конкретизації. Наприклад, вказано, що постачальники послуг блокчейн повинні відповідати «технічним умовам», проте відсутнє чітке визначення або стандарт, який конкретизував би критерії відповідності таким «технічним умовам». Крім того, Положення вимагають, щоб постачальники послуг з використанням технології блокчейн дотримувалися національних стандартів для галузі, яка використовує цю технологію, проте наразі такі стандарти ще не розроблені. Тому додаткові роз'яснення та розробка конкретних правил можуть бути необхідними для ефективного впровадження та дотримання Положень про застосування технології блокчейн. Положення про блокчейн, призначено для сприяння розвитку технології блокчейн та регулювання її застосування та спрямовані на зменшення можливих фінансових ризиків. Ці положення несумнівно матимуть істотний вплив на галузь використання технології блокчейн в Китаї. Міжнародні та китайські компанії, які займаються бізнесом у сфері технології блокчейн в Китаї, мають переглянути свої бізнес-моделі та стратегії з метою забезпечення відповідності новим правовим вимогам відповідно до положень про блокчейн [27].

Німеччина. В даний час в Німеччині відсутні спеціальні законодавчі акти чи будь яка нормативна база що регламентують використання технологій блокчейн.

У вересні 2019 року федеральна влада Німеччини розглянула комплексну стратегію розвитку технології блокчейн, яка сприяє розвитку цієї технології та

зменшує ризики, пов'язані з її впровадженням. У документі підкреслюється важливість розробки рішень на основі технології блокчейн як у державному, так і в приватному секторі. Метою уряду є створення правової бази, що забезпечує належну інвестиційну безпеку. Місто Берлін стало центром для стартапів, які працюють з технологією блокчейн.

Існує значний інтерес до впровадження технології блокчейн з боку потенційних учасників і інвесторів із різних галузей, включаючи автомобілебудування, фармацію, енергетику та управління сферою державного сектору. В компаніях, які використовують технологію блокчейн, ця технологія застосовується переважно в таких сферах, як бухгалтерський облік, фінанси, логістика, зберігання інформації, маркетинг, обслуговування клієнтів, дистрибуція, управління проектами, кадровий облік, дослідження та розробка, а також юридичний відділ і управління контрактами.

Уряд Німеччини визнає потенціал технології блокчейн та висловлює готовність використовувати її для «цифрової трансформації». Вони ставлять перед собою завдання використовувати можливості, які надає технологія блокчейн, та мобілізувати її потенціал для цифрової трансформації. За їхньою думкою, молоду та інноваційну спільноту, зацікавлену в впровадженні технології блокчейн в Німеччині, необхідно підтримувати, а Німеччина повинна стати привабливим місцем для розробки блокчейн-додатків та інвестицій в цю технологію. Для досягнення цієї мети уряд заявив, що він буде прагнути до того, щоб застосунки, побудовані на технології блокчейн, відповідали чинному законодавству. Рекомендації уряду спрямовані передусім на потенційних користувачів, які розглядають можливість використання технології блокчейн та мають базові технічні знання. Мета полягає в наданні структурованого та всебічного огляду аспектів, пов'язаних з кібербезпекою.

У березні 2019 року Федеральне відомство з інформаційної безпеки Німеччини оприлюднило рекомендації щодо впровадження та використання технології блокчейн. У цих рекомендаціях Федеральне відомство з інформаційної безпеки Німеччини висловлює свою точку зору щодо різних аспектів

впровадження технології блокчейн, включаючи захист даних, юридичні аспекти та практичні застосування. Також у березні 2019 року федеральний уряд опублікував документ, який стосується ключових аспектів регулювання електронних цінних паперів. Цей документ є першим кроком в рамках стратегії розвитку та впровадження технології блокчейн. Головною метою цих ініціатив є започаткування німецького законодавства для електронних, дематеріалізованих цінних паперів та створення законопроекту, який регулює публічні випуски конкретних криптовалютних tokenів. Правила, які стосуються електронних цінних паперів, повинні бути технологічно нейтральними, тобто дозволяти емітувати електронні цінні папери на основі технології блокчейн. Ці заходи спрямовані на впровадження технології блокчейн у фінансовому секторі Німеччини.

Використання самої технології блокчейн в Німеччині не вимагає отримання дозволу. Однак, в залежності від бізнес-моделі, може знадобитися дозвіл на відповідну діяльність від влади.

Криптовалюта у Німеччині є законною. Її правове регулювання здійснюється в двох сферах: банківському наглядовому праві та законодавстві щодо протидії відмиванню грошей. Федеральне центральне податкове управління Німеччини розглядає віртуальні валюти як приватні гроші для цілей оподаткування. Криптовалюта не вважається іноземною валютою, законним засобом платежу або майном згідно з податковим законодавством Німеччини. Рішення Апеляційного суду Берліна від 25 вересня 2018 року визначило, що біткоїни не є розрахунковими одиницями. Оскільки судових рішень, що стосуються криптовалют, дуже мало, ця постанова розглядається як фундаментальна. У Німеччині відсутні чіткі юридичні положення, що регулюють оподаткування криптовалют. Застосовуються загальні податкові правила. Використання криптовалют як заміни готівки або депозитів для участі в обмінних операціях у межах економічного циклу не потребує дозволу. Постачальник послуг може приймати оплату за свої послуги в криптовалютах, не здійснюючи банківську або фінансову діяльність. Те ж саме стосується і клієнта. Комерційний

обіг з криптовалютами відповідно до вимог Закону про банківську діяльність Німеччини потребує отримання дозволу. Невиконання цієї вимоги є кримінальним злочином. Законодавство, що застосовується до смарт-контрактів, ґрунтується на загальних принципах, оскільки смарт-контракти кодують традиційні контракти. Ризики, пов'язані із смарт-контрактами, передусім впливають із відсутності центрального органу, який міг би вжити заходів стосовно незаконних дій. Крім того, смарт-контракти можуть породжувати юридичні ризики. Смарт-контракти виявляють свою корисність для вирішення завдань у галузях щодо архівування, перевірки, аутентифікації, ліцензування, надання інформації та інших функцій та впроваджуються в структурах підприємств.

Індія. В Індії також не існує спеціальних законів, щодо правового регулювання технології блокчейн та регулюється загальними законами Індії. Криптовалюти засновані на технології блокчейн також не регулюються законодавством Індії, але Резервний банк Індії видав попередження для громадськості щодо потенційних ризиків, пов'язаних з обігом та застосуванням криптовалют. Наразі в країні немає ані конкретного регулювання, ані заборони щодо використання технології блокчейн та криптовалют, але уряд Індії запропонував законопроект, який передбачає заборону всіх криптовалют, за винятком тих, які використовуються в дослідженнях та розробці.

Швейцарія. 18 червня 2021 року Федеральна Рада Швейцарії прийняла Федеральний закон «Про адаптацію федерального законодавства до розвитку технології розподіленого реєстру», який спрямований на адаптацію федерального законодавства до використання технології блокчейн та включає рішення про розробку платформ на основі розподілених реєстрів. Цей крок сприятиме впровадженню інноваційних систем у сфері торгівлі та підвищить рівень правової визначеності. Поправки до Швейцарського кодексу зобов'язань, що дозволяють використовувати блокчейн для фінансових продуктів цього типу, набули чинності 1 лютого 2021 року. На даний момент Швейцарія є однією з перших країн у світі,

яка має чіткі, конкретні та сучасні правила, що регулюють ці інноваційні технології на фінансовому ринку [35].

Однією з ключових ініціатив є авторизація торговельних систем заснованих на технології розподіленого реєстру, яка дозволяє записувати і спільно використовувати дані в мережі., що представляють собою вид інфраструктури фінансового ринку для торгівлі цифровими цінними паперами. Крім того, чітке регулювання криптоактивів у разі банкрутства підвищить юридичну визначеність в питаннях неплатоспроможності. Закон «Про адаптацію федерального законодавства до розвитку технології розподіленого реєстру», включає в себе комплексні зміни в десятих федеральних законах з метою створення сприятливого середовища для розвитку Швейцарії як інноваційного та стійкого центру передового досвіду для компаній, що діють у сфері розподіленого реєстру та використовують технологію блокчейн. Ця законодавча норма спрямована на зміцнення домінуючого становища Швейцарії в Європі, і відкриває шлях до впровадження нових юридичних визначень, які краще відповідають потребам інноваційного криптобізнесу, ніж традиційні. Швейцарія активно просуває ці нововведення, зокрема заохочуючи криптобізнес до розширення своєї діяльності на її території. Регулювання криптовалют в Швейцарії передбачає процедуру реєстрації на криптовалютних біржах та вимагає отримання ліцензії від Управління з нагляду за фінансовими ринками Швейцарії.

У вересні 2020 року швейцарський парламент прийняв Закон про блокчейн, який визначив законність обміну криптовалют і регулювання криптовалютних бірж в швейцарському законодавстві. Швейцарський уряд наголосив на своїй меті щодо створення сприятливого середовища для розвитку цифрових грошей заснованих на технології розподілених реєстрів та виразив намір продовжувати регулювати цю галузь. У 2016 році місто Цуг, яке відоме як світовий центр криптовалют, прийняло біткоїн як засіб оплати муніципальних податків. З цією метою, наприкінці 2020 року Міністерство фінансів Швейцарії розпочало консультації з метою встановлення нових загальних правил для регулювання

криптовалют, що сприятимуть використанню переваг технології блокчейн та сприятимуть інноваціям [35].

Австралія. На сьогодні в Австралії не існує конкретних правил або законів, пов'язаних з технологією блокчейн. Австралія вважається відносно нейтральною та стабільною юрисдикцією для бізнесу, пов'язаного з використанням технології блокчейн. Модель регулювання технології блокчейн в Австралії представляє собою адаптовану структуру ліцензування для постачальників послуг у сфері криптоактивів, яка доповнює існуючі австралійські режими ліцензування фінансових послуг та ринку фінансових продуктів з криптоактивами. Уряд Австралії підтримує стимулювання інновацій у технологічному секторі, і в цьому контексті приділяє значну увагу технології блокчейн через кілька ключових ініціатив у різних галузях, включаючи фінансові послуги, енергетику, видобуток корисних копалин, сільське господарство, продукти харчування і напої, а також громадський сектор [36].

У громадському секторі уряд Австралії розглянув можливість спільного використання технології блокчейн разом з Австралійським податковим управлінням для перевірки історії автомобілів з точки зору дотримання податкового законодавства. Національна схема страхування недієздатності правління також має досвід з використанням технології блокчейн та новою платіжною платформою, з метою створення «розумних грошей», які здатні керувати страховими виплатами, бюджетуванням та довірчим управлінням. Австралійська комісія по цінним паперам та інвестиціям, яка відповідає за регулювання корпоративних, ринкових і фінансових послуг, а також споживчих кредитів в Австралії, підтвердила, що законодавчі та регуляторні вимоги Австралії є технологічно нейтральними і застосовуються незалежно від способу використання технології блокчейн для надання регульованих послуг. Попри внесені законодавчі поправки, спрямовані на регулювання використання криптовалют, вони на сьогодні в основному обмежені транзакційними відносинами, такими як процес випуску та обміну, а також діяльністю, пов'язаною з криптовалютами [36]. У результаті регулювання криптоактивів в Австралії

головний акцент було зроблено на застосуванні встановленої нормативно-правової бази фінансових послуг, яка включає в себе ліцензування фінансових послуг і послуг з споживчих кредитів, обов'язки реєстрації та розкриття інформації, вимоги законодавства щодо захисту прав споживачів, конфіденційність і вимоги щодо протидії відмиванню грошей та фінансуванню тероризму. Постачальники послуг обміну цифровими валютами мають зобов'язання, визначені Законом про запобігання відмиванню грошей та фінансуванню тероризму, і повинні реєструватися у відповідних державних органах. Крім того, Австралійські компанії активно використовують технологію блокчейн для різних цілей, включаючи управління поставок, здійснення міжнародних платежів, торгівлю деривативами, керування активами та обмін цифровими валютами. Застосування технології блокчейн в цих сферах сприяє покращенню ефективності та прозорості операцій, а також допомагає підвищити конкурентоспроможність австралійських компаній на міжнародному ринку. Зокрема, багато проектів в приватному секторі використовують технологію блокчейн для надання послуг споживачам більш ефективним і безпечним способом. [36]. Австралійська фондова біржа працює над інтеграцією технології блокчейн в різні аспекти своєї діяльності, включаючи процеси розрахунків, реєстрації активів та інші послуги. Це свідчить про визнання потенціалу технології блокчейн для оптимізації операцій на фондовому ринку та підвищення ефективності фондових торгів. Додатково, у 2020 році австралійська влада ініціювала запуск Національної Дорожньої Карти Блокчейн, спрямованої на декілька сфер, включаючи регулювання, розвиток навичок, інвестиції, а також міжнародну конкурентоспроможність та співробітництво. Уряд виділив фінансові ресурси для підтримки ряду ініціатив та програм, спрямованих на створення блокчейн-альянсів. Це було здійснено з метою підтримки транскордонних проектів та програм обміну. З метою сприяння інноваціям та співпраці в сфері застосування технології блокчейн, завдяки державним програм, підтримку отримав приватний сектор, підприємці та дослідницькі організації. Крім того,

уряд надав фінансову підтримку для розробки міжнародних стандартів у галузі блокчейну, співпрацюючи з Міжнародною Організацією зі стандартизації [36].

Норвегія. На сьогодні в Норвегії відсутні конкретні закони чи правила, спеціально регулюючі впровадження та використання технології блокчейн. Позиція норвезької влади щодо впровадження технології блокчейн та цифрових активів, залишається не визначеною. Враховуючи це, в Норвегії діють галузеві закони, які можуть бути застосовані до діяльності та послуг, пов'язаних з технологією блокчейн.

Ураховуючи сучасну ситуацію, вважаю, що необхідність адаптації та гнучкості при формуванні правової бази для регулювання технології блокчейн у різних галузях вимагає контекстуальних підходів. Це передбачає здатність враховувати відмінності та застосовувати різні стратегії, щоб досягти оптимального балансу між інноваціями, захистом прав, безпекою та інтересами учасників конкретної сфери використання технології блокчейн.

3.2 Рекомендації щодо модернізації законодавства в галузі регулювання технології блокчейн

Розглядаючи питання необхідності модернізації законодавства в галузі регулювання технології блокчейн, рекомендується враховувати наступні аспекти:

- створити єдино визнані визначення та терміни, такі як «блокчейн», «криптовалюта», «смарт-контракт»;
- інституалізувати процес управління, забезпечивши створення централізованих регулюючих органів наділених відповідними повноваженнями для регулювання галузі застосування технології блокчейн. Забезпечити спеціалізовану експертизу та здатність реагувати на швидкозмінну природу процесів пов'язаних з технологією блокчейн;

- передбачити у законодавстві стандарти кібербезпеки та розробити план заходів для протидії кіберзлочинності з метою захисту користувачів технології блокчейн від кримінальної діяльності;

- розробити систему оподаткування для криптовалют та криптоактивів;

- розвивати міжнародне партнерство та сприяти створенню стандартів регулювання для спільної роботи на міжнародному рівні, створити сприятливі умови, включаючи підтримку стартапів, для розвитку технології блокчейн;

- розробити заходи для захисту прав споживачів, пов'язаних з використанням технології блокчейн;

- розробити механізми регулювання діяльності фінансових установ, які використовують технологію блокчейн для мінімізації ризиків та забезпечення фінансової стабільності;

- залучити галузевих експертів, представників бізнесу та науковців для формування рекомендацій щодо поліпшення законодавства. створити та впровадити механізми для відкритого діалогу між урядовими органами, бізнесом та громадськістю;

- впровадити заходи для постійного оновлення законодавства відповідно до динаміки процесів у галузі технології блокчейн;

- стандартизувати технічні аспекти технології блокчейн для забезпечення сумісності та взаємодії між різними системами;

- розробити та впровадити державні програми, спрямовані на фінансування досліджень у галузі блокчейн та підготовку кваліфікованих кадрів;

- розробити спеціалізоване законодавство для контролю та нагляду в галузі застосування технології блокчейн.

Зазначені рекомендації мають на меті створення прозорого, безпечного та сприятливого законодавчого середовища для розвитку та впровадження технології блокчейн. Врахування цих аспектів сприятиме інноваціям та інтеграції технології блокчейн в різні галузі, створюючи нові можливості для бізнесу та суспільства в цілому, гарантуючи безпеку а також захист інтересів користувачів.

ВИСНОВКИ

У процесі роботи були розглянуті теоретичні відомості про технологію блокчейн. Досліджено історію та передумови її виникнення та ключові події. Проаналізовано типи блокчейн платформ та типи консенсусу. Розглянуто особливості, переваги та недоліки технології, приклади її використання в різних сферах. Розглянуто сфери застосування технології блокчейн для медичної, державної, енергетичної та інших сфер.

Розробка та застосування законодавчої бази для правового регулювання децентралізованих мереж вимагають інноваційних підходів, які повинні бути належним чином обґрунтовані та спрямовані на забезпечення загального добробуту суспільства збереження соціальної стабільності, стійкості та безпеки, цілісності економічних систем, боротьби з кіберзлочинністю, та захисту прав і інтересів користувачів.

Державна політика України в питанні правового регулювання технології блокчейн досить динамічна та знаходиться у стадії розвитку. Саме тому в умовах пошуку оптимальної моделі державної політики України щодо правового регулювання технології блокчейн важливе значення має вивчення досвіду провідних країн світу.

Прагнення держав щодо правового регулювання технології блокчейн базується на раціональному баченні цього питання. Саме тому в різних розвинутих країнах застосовуються достатньо різні підходи, та політичні інструменти щодо законодавчого регулювання технології блокчейн, які передбачають створення нових організаційних форм та закріплення відповідальності за учасниками системи (юридичними та фізичними особами) які несуть відповідальність за свою діяльність в системі блокчейн, відповідно до їх внеску в систему. Методи які застосовують різні країни коливаються від суворого контролю до більш ліберальних регулятивних режимів. Деякі країни вводять повну заборону на використання технології блокчейн. Цей підхід влаштовує

найбільше консервативні уряди, які бояться фінансових ризиків та можливих зловживань. Багато країн вирішили регулювати системи які засновані на технології блокчейн, застосовуючи офіційне ліцензування та оподаткування яке здійснюють спеціалізовані органи створені для нагляду та контролю у цій галузі. Деякі країни заохочують галузеві організації розробляти саморегулювальні стандарти для галузі блокчейн, що зберігає цю сферу діяльності від надмірного державного втручання сприяючи інноваціям, або заохочують дослідження технології блокчейн, аналізуючи дані про її вплив, модернізуючи законодавство на підставі практичного досвіду. Інші, створюють спеціальні фінансові зони, щоб привабити компанії та інвесторів. Підхід кожної країни залежить від її конкретних потреб та пріоритетів.

Розробка та впровадження ефективного законодавчого регулювання технології блокчейн вимагає виважених рішень та участі всіх сторін, включаючи державні органи, представників бізнесу та громадськості, враховуючи прозорість, зрозумілість, а також практичні та етичні аспекти застосування технології блокчейн у різних галузях. Важливим аспектом для вироблення єдиної методології регулювання є ефективна спільна міжнародна співпраця всіх учасників, оскільки децентралізовані системи мають глобальний світовий масштаб та можуть функціонувати поза національними кордонами. Забезпечення такої співпраці сприятиме уніфікації підходів до регулювання технології блокчейн та створенню єдиної методології, яка враховуватиме специфіку цієї технології та забезпечить її сталий розвиток та застосування в глобальному масштабі. Стрімкий розвиток технології блокчейн часто випереджає створення відповідного законодавства, що ускладнює процес правового регулювання технології блокчейн.

Законодавче регулювання відіграє ключову роль у забезпеченні заходів щодо впровадження технології блокчейн, захисті користувачів та забезпеченні більш широких соціально-економічних інтересів, служачи засобом боротьби зі злочинністю, сприяючи фінансовій стабільності, захисту інвесторів та зменшення ризиків, пов'язаних із впровадженням цієї інновації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Даньшина Ю. В., Брітченко І. Г. Переваги, можливості та недоліки технології блокчейн // Фінансово-кредитний механізм активізації інвестиційного процесу: збірник матеріалів III Міжнародної науко-во-практичної конференції (м. Київ, 10 листопада 2017 р.). Київ : КНЕУ, 2017. С. 106–109.
2. Теоретичні засади та застосування блокчейн технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень. А.М. Кудін, Л.В. Ковальчук, Б.А. Коваленко. // Математичне та комп'ютерне моделювання, вип. 19, 2019р, с. 62-68.
3. Nakamoto, Satoshi (31 October 2008). «Bitcoin: A Peer-to-Peer Electronic Cash System» [Електронний ресурс], - Режим доступу: <https://nakamotoinstitute.org/library/bitcoin/> (дата звернення 10.12.24).
4. Graphchain: a blockchain-free scalable decentralised ledger. Xavier Boyen, Christopher Carr, and Thomas Haines. // In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, pages 21–33. ACM, 2018.
5. Bitcoin confirmed transactions per day stats., 2018 [Електронний ресурс], - Режим доступу: <https://www.blockchain.com/charts/n-transactions> (дата звернення 10.12.24).
6. Lyudmila Kovalchuk, Dmytro Kaidalov, Oleksiy Shevtsov, Andrii Nastenکو, Mariia Rodinko, Roman Oliynykov. Analysis of Splitting Attacks on Bitcoin and GHOST Consensus Protocols // Proc. of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Romania, Bucharest, 2017.
7. Serguei Popov. «The Tangle» (2017)., 2017 [Електронний ресурс], - Режим доступу: https://iota.org/IOTA_Whitepaper.pdf (дата звернення 10.12.24).
8. Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenکو, Mariia Rodinko, Oleksiy Shevtsov, and Roman Oliynykov. 2020. Decreasing security threshold against double spend attack in networks with slow synchronization. Computer Communications 154 (2020), 75–81.

9. Yaoqi. Jia. Demystifying hashgraph: Benefits and challenges [Электронный ресурс], - Режим доступа: <https://hackernoon.com/demystifying-hashgraph-benefits-and-challenges-605e5c0cee5> (дата звернення 10.12.24).

10. Matthias Fitzi, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition. Cryptology ePrint Archive, Report 2018/1119, 2018 [Электронный ресурс], - Режим доступа: <https://eprint.iacr.org/2018/1119> (дата звернення 10.12.24).

11. J. Dilley, A. Poelstra, and J. Wilkins. Unfreezable blockchain. bitcoin forum., 2016 [Электронный ресурс], - Режим доступа: <https://bitcointalk.org/index.php?topic=57647.msg686497#msg68649> (дата звернення 10.12.24).

12. Meni Rosenfeld. «Analysis of hashrate-based double-spending». In: arXiv preprint (2014) DOI: <https://arxiv.org/abs/1402.2009> (дата звернення: 10.12.2024).

13. Kyle Butt, Derek Sorensen, Michael Stay. Casanova. In: arXiv preprint (2018) [Электронный ресурс], - Режим доступа: <http://arxiv.org/abs/1812.02232> (дата звернення 10.12.24).

14. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive 2018, 46 (2018), available at [Электронный ресурс], - Режим доступа: <https://eprint.iacr.org/2018/046.pdf> (дата звернення 10.12.24).

15. Aggelos Kiayias, Alexander Russell, Bernardo David and Roman Oliynykov Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol [Электронный ресурс], - Режим доступа: <https://eprint.iacr.org/2016/889.pdf> (дата звернення 12.12.24).

16. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly practical verifiable computation. In: IEEE Symposium on Security and Privacy. pp. 238–252. IEEE Computer Society (2013). doi: 10.1109/SP.2013.47 (дата звернення: 10.12.2024).

17. Hopwood, D., Bowe, S., Hornby, T., Wilcox, N.: Zcash protocol specification: Version 2019.0-beta-37 [overwinter+sapling]. Tech. rep., Zerocoin Electric Coin Company (2019), available at [Електронний ресурс], - Режим доступу: <https://github.com/zcash/zips/blob/master/protocol/protocol.pdf> (дата звернення 12.12.24).

18. Aggelos Kiayias, Alexander Russell, Bernardo David and Roman Oliynykov Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol [Електронний ресурс], - Режим доступу: <https://eprint.iacr.org/2016/889.pdf> (дата звернення 12.12.24).

19. Lorenzo Grassi and Reinhard Lüftenegger and Christian Rechberger and Dragos Rotaru and Markus Schofnegger.: On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy [Електронний ресурс], - Режим доступу <https://eprint.iacr.org/2019/1107.pdf> (дата звернення 12.12.24).

20. Літошенко А. В. Технологія Blockchain: переваги та неочевидні можливості використання у різних галузях» [Електронний ресурс], - Режим доступу: http://www.economy.in.ua/pdf/8_2017/20.pdf (дата звернення 12.12.24).

21. Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Arnab Roy, Christian Rechberger, and Markus Schofnegger. Starkad and Poseidon: New Hash Functions for Zero Knowledge Proof Systems, [Електронний ресурс]: (IACR Cryptology ePrint Archive 2019), - Режим доступу: <https://eprint.iacr.org/2019/458.pdf> (дата звернення: 10.12.2024).

22. Пантелєєва Н. М. Інноваційна технологія блокчейн у системі управління державними фінансами. Науковий вісник Ужгородського університету. Серія «Економіка». 2018. Вип. 1. С. 363–369. DOI: [https://doi.org/10.24144/2409-6857.2018.1\(51\)](https://doi.org/10.24144/2409-6857.2018.1(51)) (дата звернення: 10.12.2024).

23. Бондаренко О. В. Запровадження технології блокчейн у державному секторі [Електронний ресурс]: (Протокол), - Режим доступу: <https://bit.ly/3lFNCET> (дата звернення: 10.12.2024).

24. Чекаловська Г. З., Лось А. А. Сучасні тенденції розвитку blockchain технологій в Україні. Регіональна економіка та управління. 2019. № 4. Ч. 2. С. 153–157.

25. Стефанчук Р. Інформаційні технології та право: quo vadis? Право України. 2018. № 1. С. 30–50. DOI: <https://doi.org/10.33498/louu-2018-01-030> (дата звернення: 10.12.2024).

26 Кравченко О. В., Шаповал О. Б., Небаба Н. О., Ботвінов Р. Г. Блокчейн-технології: стан та перспективи розвитку в Україні. Вісник Хмельницького національного університету. Економічні науки. 2021. № 6. Т. 2. С. 267-272.

27. China has a blockchain ambition – But the reality? Cryptopolitan [Електронний ресурс]: (Hamid J. 2023), - Режим доступу: <https://www.cryptopolitan.com/china-blockchain-ambition-but-the-reality/> (дата звернення: 20.12.2024).

28. H.R. 6154, 2019 [Електронний ресурс]: (Crypto-Currency Act of 2020), - Режим доступу: <https://www.congress.gov/bill/116th-congress/house-bill/6154/text> (дата звернення: 08.05.2024).

29. Cooperation on a European Blockchain Partnership [Електронний ресурс]: (Declaration 2018), - Режим доступу: <https://www.scribd.com/document/398159396/2018DeclarationonEuropeanPartnershiponBlockchainpdf-pdf> (дата звернення: 08.05.2024).

30. Гурова А., Кірпачова М. Правові засади застосування блокчейну в космічній діяльності: особливості регулювання технології на національному, регіональному та міжнародному рівнях. Підприємництво, господарство і право. 2021. № 1. С. 265-275.

31. Закон «Про віртуальні активи» [Електронний ресурс]: (Відомості Верховної Ради України (ВВР), 2074-IX, не набрав чинності, поточна редакція - Прийняття від 17.02.2022), - Режим доступу: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення 10.12.24).

32. Бородіна О.А., Ляшенко В.І. Повоєнне відновлення економіки: світовий досвід та спроба його адаптації для України. Вісник економічної науки України. 2022. 1 (42). С. 121-134.

33. Blockgeeks. What is Blockchain Technology? A Step-by-Step Guide For Beginners [Електронний ресурс]: (October, 2022) - Режим доступу: <https://blockgeeks.com/guides/what-is-blockchain-technology/> (дата звернення: 08.05.2024).

34. Blockchain policy matters: U.S. Congressman Patrick McHenry (R-NC 10), EPISODE 1 [Електронний ресурс]: (BSV Association 2021) - Режим доступу: <https://www.youtube.com/watch?v=aRldRdk50JQ> (дата звернення: 08.05.2024).

35. Innovation Booster – Blockchain Nation Switzerland [Електронний ресурс]: (Blockchain Nation Switzerland) - Режим доступу: <https://www.blockchainnation.ch/en/home> (дата звернення: 08.05.2024).

36. What We Do [Електронний ресурс]: (Blockchain Australia) - Режим доступу: <https://blockchainaustralia.org/> (дата звернення: 08.05.2024).