

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:

В.о. завідувача кафедри
кібербезпеки та захисту інформації

_____ Іван ПАРХОМЕНКО

« _____ » червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань _____ 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність _____ 125 Кібербезпека
(код і назва спеціальності)
освітній ступень _____ бакалавр
освітня програма _____ Кібербезпека
(назва освітньо-професійної програми)
на тему: _____ Програмні засоби токенизації активів на основі блокчейн технології

Виконавець: студент IV курсу, групи КБ-42

_____ Кирило ГІМОН _____
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	Підпис
Керівник	Іван ПАРХОМЕНКО	

Нормоконтроль	Лариса МИРУТЕНКО	
---------------	------------------	--

**Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО:

В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

спеціальності	125 Кібербезпека
освітньої програми	(код і назва спеціальності) Кібербезпека
Студента	(назва освітньо-професійної програми)
Тема кваліфікаційної роботи	КБ-42 (група) Гімона Кирила Миколайовича (прізвище ім'я по батькові)
	Програмні засоби токенизації активів на основі блокчейн технології

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Мова програмування Python, хеш-функції для функціонування блокчейну
SHA-256, засоби реалізації та функціонування застосунку

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Принцип роботи блокчейн технології, явище токенизація активів, види токенів,
механізм перетворення фінансових активів на токени, наслідки токенизації акцій,
програмна реалізація

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Застосунок для перетворення фінансових активів на токени на основі блокчейн технології

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 25 жовтня 2022 року

Завдання видав	_____	Іван ПАРХОМЕНКО
	(підпис)	(ім'я, прізвище)
Завдання прийняв до виконання	_____	Кирило ГІМОН
	(підпис)	(ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 04.11.2022	виконано
2	Аналіз літератури	23.01.2023 – 24.02.2023	виконано
3	Аналіз принципів роботи блокчейн технології	27.02.2023 – 10.03.2023	виконано
4	Дослідження механізму створення токенів	13.03.2023 – 02.04.2023	виконано
5	Дослідження типів фінансових активів	03.04.2023 – 09.04.2023	виконано
6	Дослідження сфер використання технології блокчейн	10.04.2023 – 16.04.2023	виконано
7	Опис розроблюваного застосунку	17.04.2023 – 23.04.2023	виконано
8	Дослідження хеш-функції застосунку та розгляд методів реалізації	24.04.2023 – 07.05.2023	виконано
9	Реалізація застосунку для токенизації активів	08.05.2023 – 28.05.2023	виконано
10	Оформлення пояснювальної записки та підготовка до захисту	29.05.2023 – 12.06.2023	виконано

Завдання видав	_____	Іван ПАРХОМЕНКО
	(підпис)	(ім'я, прізвище)
Завдання прийняв до виконання	_____	Кирило ГІМОН
	(підпис)	(ім'я, прізвище)

Термін подання дипломної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел. Основний текст займає 55 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки, список джерел та 2 додатки. У пояснювальній записці дипломної роботи міститься 11 рисунків та 24 літературних джерела.

Метою роботи є створення програмного засобу для токенизації активів на основі технології блокчейн.

Об'єктом дослідження є створення токену на базі технології блокчейн.

Предметом дослідження є набір механізмів, що реалізують процес шифрування та створення токену.

Методи дослідження:

- аналіз відкритих джерел;
- дослідження механізму токенизації активів;
- порівняння методів програмної реалізації блокчейн.

Практичною цінністю є розроблений програмний засіб та результати досліджень, що демонструють необхідність створення такого роду токенів.

Ключові слова: блокчейн, криптовалюта, актив, шифрування, акції, токенизація, хеш-функція.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	6
ВСТУП	7
РОЗДІЛ 1 ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА ЇЇ ОСОБЛИВОСТІ	9
1.1 Основні терміни та принципи роботи блокчейну	9
1.2 Історія технології блокчейн	12
1.3 Сфери використання технології блокчейн	18
1.4 Переваги і недоліки технології блокчейн	21
Висновки до розділу 1	24
РОЗДІЛ 2 ПРОЦЕС ТОКЕНІЗАЦІЇ ФІНАНСОВИХ АКТИВІВ	26
2.1 Типи токенів	26
2.2 Явище токенізації активів	29
2.3 Процес перетворення акцій на токен	31
2.4 Можливі наслідки глобального запуску токенізованих активів	33
Висновки до розділу 2	43
РОЗДІЛ 3 ПРОГРАМНИЙ ЗАСІБ ДЛЯ ТОКЕНІЗАЦІЇ АКТИВІВ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН	44
3.1 Вибір програмних засобів для реалізації блокчейн для токенізації активів	44
3.2 Алгоритм та функції програмного засобу токенізації активів	46
3.3 Результат роботи програмного засобу	49
Висновок до розділу 3	50
ВИСНОВКИ	51
СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ	53
ДОДАТОК А	56
ДОДАТОК Б	58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

BTC	–	Bitcoin
ITO	–	Initial Coin Offering
NIST	–	National Institute of Standards and Technology
PoS	–	Proof of Stake
PoW	–	Proof of Work
CRM	–	Customer Relationship Management
BAT	–	Basic Attention Token

ВСТУП

В сучасному світі стрімко відбувається перехід від інформатизації основних сфер людської діяльності до їх цифровізації.

У випадку коли інформатизація означає модернізацію майже будь-яких видів людської діяльності з використанням інформаційно-комунікаційних технологій, то цифровізація має на увазі перетворення зрозумілих більшості видів і форм діяльності до нових, що базуються на цифрових моделях та технологіях.

Підтримання та змінення цифрового оточення вимагає дослідження і покращення як вже існуючих умов для виникнення перспективних цифрових платформ і технологій, так і створення умов для виникнення нових платформ і технологій.

Основними наскрізними цифровими технологіями є:

- промисловий інтернет;
- нейротехнології і штучний інтелект;
- blockchain;
- нові виробничі технології;
- компоненти робототехніки та сенсорика;
- технології віртуальної і доповненої реальностей;
- технології бездротового зв'язку.

В роботі проводяться дослідження щодо використання технології блокчейн (ланцюжків блоків / blockchain) для токенизації фінансових активів і перспективні напрямки її використання в сфері інвестування та фінансів.

Метою є дослідження можливості перетворення акцій і цінних паперів на токени за допомогою технології блокчейн.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Аналіз основних напрямків розвитку та застосування технологій блокчейн в освіті.

2. Аналіз методів забезпечення конфіденційності та цілісності даних в розподіленому реєстрі на основі блокчейн.

3. Аналіз алгоритмів хешування технології блокчейн.

4. Дослідження засобів і механізмів забезпечення конфіденційності даних в децентралізованому реєстрі.

5. Моделювання процесів токенизації активів на основі технології блокчейн.

Об'єктом досліджень є процес токенизації на базі технології блокчейн.

Предметом дослідження є механізми та засоби реалізації токенизації.

Методи дослідження:

- аналіз відкритих джерел;
- порівняння методів програмної реалізації блокчейн.

Практична значимість проведеного дослідження полягає в тому, що положення і висновки, викладені в роботі, можуть бути використані чисельними компаніями та різними сферами бізнесу для залучення інвестицій та спрощення ведення торгівлі акціями.

РОЗДІЛ 1

ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА ЇЇ ОСОБЛИВОСТІ

1.1 Основні терміни та принципи роботи блокчейну

«Блокчейн (Blockchain) - це вічний цифровий розподілений журнал економічних транзакцій, який може бути запрограмований для запису не тільки фінансових операцій, але і практично всього, що має цінність», - Дон і Алекс Тапскотт, «Революція блокчейна». Блокчейн - це система, що складається з послідовних блоків, розподілених між учасниками через пірінгові мережі. Ця система функціонує самостійно, без централізованого управління, і створює базу даних. Блокчейн може бути використаний як зручний інструмент для реєстрації подій і операцій з даними, керування ідентифікацією та перевірки походження [1].

У кожного блоку є своя унікальна тимчасова позначка, відома як хеш-сума, і блоки формуються в послідовні ланцюги. Якщо спробувати змінити порядок блоків, система виявить невідповідність структури та хеш-сум. Кожен блок також містить свій власний хеш-код, який обчислюється на основі хеш-коду попереднього блоку, утворюючи ланцюжок залежностей між блоками. Схематично це можна представити як на Рисунку 1.1.

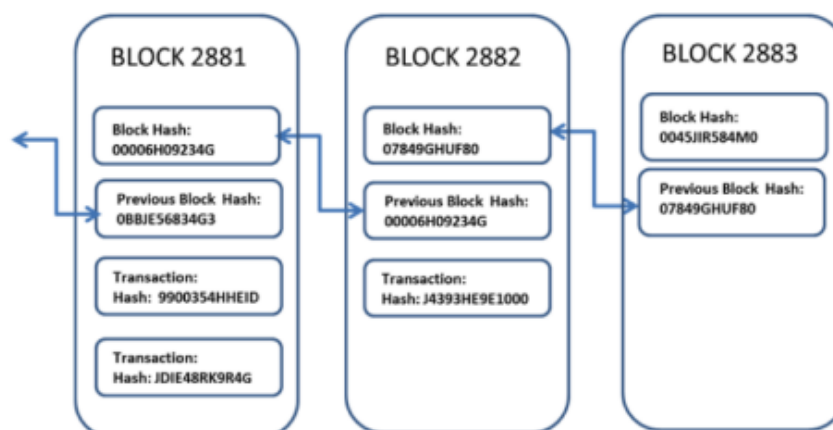


Рисунок 1.1 – Типова структура блокчейн

У блокчейні використовуються два методи захисту від змін тимчасової позначки і правильної хеш-суми: Proof of Work (PoW, доказ роботи) і Proof of Stake (PoS, доказ володіння). Просто кажучи, в механізмі PoW вузли мережі перевіряють, чи виконав майнер фактичні розрахунки. Цей процес включає спробу знайти хеш заголовка блоку, який відповідає встановленому рівню складності. У випадку підходу Proof of Stake, вузли також здійснюють пошук хеш-суми, але складність розподіляється пропорційно до балансу вузла. Іншими словами, складність обчислення залежить від кількості токенів, які знаходяться на рахунку користувача.

Ці два методи забезпечують безпеку блокчейн мережі, роблячи зміну попередньої транзакції вкрай складною, оскільки вона потребує значного обчислювального потужності або значної кількості токенів. Це забезпечує надійність та недоступність для зловмисників змінювати дані, що зберігаються в блокчейні [2].

Узагальнюючи всі факти, можна зробити висновок, що блокчейн є надійною та децентралізованою технологією. Усі учасники мережі блокчейн рівні між собою, і відсутній централізований сервер або процесорний центр. Ключовим елементом цієї технології є формування та закриття блоків. Кожен блок містить певний ключ, і блок не може бути закритий, доки цей ключ не буде розшифрований.

Процес розшифрування ключа в блокчейні відбувається за допомогою майнінгу. Майнери використовують відеокарти та процесори для виконання обчислювальних операцій, метою яких є пошук криптографічного підпису у вигляді хешу для блоку. Коли такий підпис знаходиться, блок закривається, а майнер отримує винагороду у вигляді криптовалюти. Безпеку та функціонування блокчейну забезпечують майнери та інші учасники, відомі як ноди або вузли. Повні ноди включають майнерів та звичайних користувачів, які мають повну версію блокчейну на своєму комп'ютері або пристрої. Чим більше активних повних нод в мережі блокчейн, тим швидше обробляється інформація про транзакції.

Підводячи проміжні підсумки, нижче надані ключові особливості Blockchain:

1. Децентралізація – кожен учасник – це і є сервер, який підтримує роботу всього блокчейна;

2. Прозорість – хоча дані про транзакції неможливо замінити, вся інформація про них зберігається у відкритому доступі;
3. Теоретична необмеженість – теоретично блокчейн можна доповнювати записами до нескінченності. Тому його часто порівнюють з суперкомп'ютером;
4. Надійність – для запису нових даних необхідний консенсус вузлів блокчейна. Це дозволяє фільтрувати операції і записувати тільки легітимні транзакції, тому здійснити підміну хеша неможливо.

Базовим принципом технології блокчейн є застосування криптографії, яка забезпечує конфіденційність та автентичність інформації. Простими словами, процес хешування полягає у перетворенні будь-якої інформації на фіксовану довжину коду за допомогою певного алгоритму хешування. Для безперервної роботи блокчейну важливо постійно оновлювати його, додавати нові записи про транзакції до мережі. Цей процес є найбільш вразливим до атак. Проте завдяки ієрархії в блокчейні, всі записи гарантовано захищені від несанкціонованої зміни [3].

Використання хеш-функцій забезпечує незмінність ланцюжка транзакцій в блокчейні. Кожен новий блок посилається на хеш попереднього блоку, і завдяки цьому створюється єдина цифрова підписка всього блокчейна. Криптографічні хеш-функції є спеціальним типом хеш-функцій, які мають специфічні властивості, необхідні для криптографії. Кожна криптовалюта використовує свій власний алгоритм шифрування, хоча кількість алгоритмів обмежена, і деякі криптовалюти можуть використовувати однакові алгоритми хешування даних.

Алгоритм шифрування або хешування в криптовалютах є набором спеціальних криптографічних механізмів та правил, які забезпечують шифрування цифрової валюти. Існує кілька десятків алгоритмів криптовалюти, але лише кілька з них є популярними та широко використовуваними. Найчастіше використовуються наступні: SHA-256, EtHash, Scrypt, X11, CryptoNight, X13.

Bitcoin і деякі інші криптовалюти використовують алгоритм SHA-256. Хеш-функції з сімейства SHA-2 побудовані на основі структури Меркле-Дамгарда.

Після доповнення оригінальний текст розбивається на блоки, і кожен блок поділяється на 16 слів. Алгоритм пропускає кожен блок повідомлення через цикл з 64

ітераціями. На кожній ітерації два слова перетворюються, при цьому функція перетворення використовує інші слова. Результати обробки кожного блоку сумуються, і ця сума стає значенням хеш-функції. Оскільки ініціалізація внутрішнього стану залежить від результату обробки попереднього блоку, неможливо обробляти блоки паралельно [4]. Графічне представлення однієї ітерації обробки блоку даних продемонстровано на Рисунку 1.2.

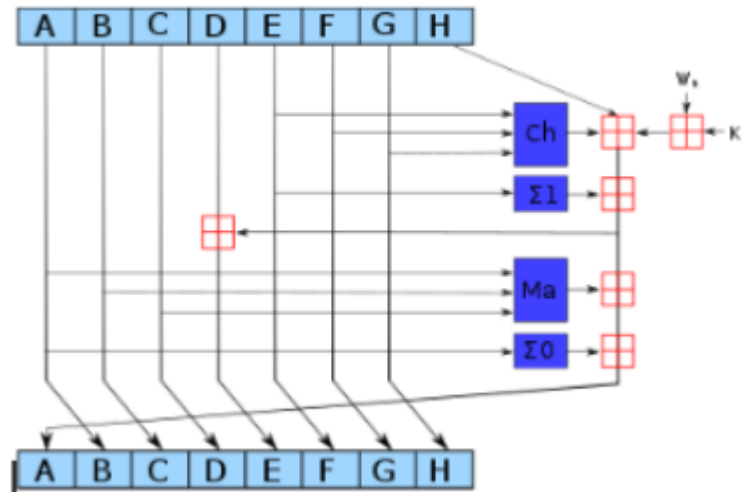


Рисунок 1.2 – Ітерація обробка блоку даних в SHA-256

Хешрейт для криптовалют, працюючих на основі SHA-256, вимірюються в Gigahash на секунду (GH/s).

1.2 Історія технології блокчейн

У кінці минулого століття одним з головних викликів була безпечна збереження і передача інтелектуальної власності. Існуючі методи захисту даних, такі як централізовані бази даних, не були надійними, і інформація могла бути піддана пошкодженню або викраденню зловмисниками. Це спонукало до розробки нових технологій для безпечного зберігання та обміну даними [5].

Багато з технологій, що лежать в основі блокчейн, були розроблені задовго до появи біткоіна. Одним з таких прикладів є дерево Меркла, назване на честь вченого Ральфа Меркла, експерта з комп'ютерної техніки. Вже у 1979 році в своїй докторській

дисертації він описав підхід до розподілу відкритих ключів та цифрових підписів, відомий як "tree authentication". Пізніше він отримав патент на цю ідею як метод надання цифрових підписів. Дерево Меркла надає структуру даних для перевірки цілісності набору даних.

Ральф Меркл не був єдиним, хто вніс свій внесок у створення основи для технології блокчейн. Криптограф Девід Чаум в своїй дисертації "Комп'ютерні системи, створені, обслуговувані та довірені взаємно підозрілими групами", написаній в 1982 році, описав дизайн розподіленої комп'ютерної системи, яка була створена і підтримувалася групою користувачів. У цій системі сховища кожна транзакція була підписана, записана та передана кожним вузлом. У статті також був представлений конкретний код для реалізації такого протоколу. Крім того, Чауму також приписують винахід цифрової готівки, і в 1989 році він заснував корпорацію DigiCash.

У 1991 році два американських дослідники, Скотт Сторнетт і Стюарт Габер, опублікували працю з назвою "Як поставити штамп часу на цифровий документ", в якій вони описали технологію, що запобігала підробленню часу створення та модифікації електронного документа. Їхнім завданням було забезпечити повну конфіденційність документа без необхідності використання служби позначок часу. Для досягнення цього вони використали концепцію криптографічно захищеного ланцюга блоків для зберігання документів. У 1992 році Стюарт Хабер, Скотт Сторнетт і Дейв Байер оновили дизайн, включивши дерева Меркла, що дозволяло кільком сертифікатам документів перебувати в одному блоку. Пізніше в 1996 році була опублікована робота Андерсона, а в 1997 році – Дойла [6].

Протягом 1995-2005 років було проведено багато досліджень, які внесли вагомий внесок у розвиток технології блокчейн. Наприклад, у цей період з'явилася мережа P2P (peer-to-peer), концепція якої стала популярною завдяки проекту Napster, який був активний у 1999 році. Цей сервіс допоміг оживити інтерес до мереж P2P та дозволив побудувати розподілену систему, яка використовувала обчислювальну потужність та ємність зберігання тисяч комп'ютерів.

Також у цей період була введена концепція доказу роботи (proof-of-work, PoW)

для перевірки обчислювальних зусиль та запобігання кібератакам. Одним з ранніх прикладів PoW був алгоритм Hashcash, який був представлений Адамом Беком у 1997 році з метою боротьби зі спамом електронною поштою. У 1998 році комп'ютерний вчений Нік Сабо працював над концепцією "бітового золота", децентралізованої цифрової валюти.

У 2000 році Стефан Конст опублікував свою теорію криптографічно захищених ланцюжків та ідеї щодо їх реалізації. В цьому ж році Хал Фінні впровадив PoW багаторазового використання, яке відіграло важливу роль у механізмі видобутку біткоїнів [7].

У 2008 році компанія Nakamoto, якій приписується винахід біткоїна, опублікувала дослідження під назвою "Біткоїн: електронна готівкова система на основі однорангових даних". Автором цього дослідження є Сатоші Накамото, якого вважають псевдонімом, що може належати окремій особі або групі людей, які представили цю технологію. Згідно з цим дослідженням, блокчейн-інфраструктура забезпечує безпечні однорангові транзакції без необхідності в довірених третіх сторонах, таких як банки або уряди. Накамото значно вдосконалив дизайн, використавши метод, схожий на Hashcash, для визначення часових міток блоків, без потреби попереднього підпису блоків визначеною довіреною стороною, а також вводячи параметр складності, що стабілізує швидкість додавання блоків до ланцюжка. Фактично, він описав електронну монету як "ланцюжок цифрових підписів", де кожен власник передає монету наступному власнику.

У 2009 році Накамото реалізував перший блокчейн як публічну книгу для біткоїн-транзакцій з такими подіями:

- 3 січня 2009 року Накамото створив перший блок біткоїнів, що підтвердив концепцію блокчейну. Цей блок, відомий як блок Genesis або блок 0, містив 50 біткоїнів.
- 8 січня 2009 року Накамото випустив Bitcoin v0.1 на платформі SourceForge як програмне забезпечення з відкритим вихідним кодом. На сьогоднішній день Bitcoin доступний на GitHub.
- 12 січня 2009 року сталася перша транзакція з біткоїнами, коли Накамото

надіслав 10 біткоїнів Халу Фінні в блоці 170.

- 12 жовтня 2009 року був створений канал #bitcoin-dev в Internet Relay Chat (IRC) для розробників біткоїнів.
- 31 жовтня 2009 року була створена перша біржа біткоїнів - Bitcoin Market, яка дозволила обмінювати паперові гроші на біткоїн.
- 22 листопада 2009 року Накамото запустив форум Bitcointalk для обміну новинами та інформацією, пов'язаною з біткоїнами.

Накамото встановив обмеження в 21 мільйон біткоїнів у системі, з яких наразі видобуто понад 18 мільйонів. За поточними темпами майнінгу, досягнення цього ліміту в очікується близько 2140 року. Вартість біткоїна продовжує зростати, незважаючи на постійні коливання ціни. Наприклад, у жовтні 2009 року біткоїн коштував менше 1 цента, а сьогодні кожен біткоїн оцінюється понад 35 000 доларів США [8].

Окрім цього, 22 травня 2010 року біткоїн увійшов в історію, коли Ласло Ханьєц заплатив 10 000 біткоїнів за дві піци Papa John's. Тоді вартість піци оцінювалась приблизно в 25 доларів США, що на сьогоднішній день відповідало близько 350 мільйонам доларів.

В недалекому минулому, програміст по імені Джед Маккалеб запустив Mt. Gox - біржу біткоїнів в Токіо. Назва Mt. Gox складалась зі скорочення "Magic: The Gathering Online eXchange", що походило від назви популярної карткової гри. На своєму піку Mt. Gox обробляла понад 70% усіх транзакцій з біткоїнами. Проте, в серпні 2010 року хакер скористався помилкою в коді блокчейну і створив понад 184 мільярди біткоїнів у блоці 74 638, що серйозно підірвало довіру до біткоїна. Накамото випустив нову версію біткоїн-програми, але до кінця року він повністю зник з публічної сфери біткоїна.

Незважаючи на зникнення Накамото, шлях біткоїна продовжував рухатися стабільними темпами. До кінця січня 2011 року було видобуто четверту частину з ліміту в 21 мільйон біткоїнів. На початку лютого 2011 року вартість біткоїна становила приблизно один долар США. Незабаром після цього Джед Маккалеб продав Mt. Gox Марку Карпелесу. Після цього біткоїн швидко досяг паритету з євро

та британським фунтом стерлінгів. Також у тому ж році WikiLeaks розпочав приймати пожертвування в біткоїнах. Проте Mt. Gox було скомпрометовано, біткоїни було вкрадено, що спричинило штучне зниження вартості та призупинення торгівлі. В жовтні 2011 року був випущений Litecoin, одна з перших альтернативних криптовалют, який виник на основі біткоїна.

Кульмінацією року 2012 було утвердження криптовалюти. Вартість біткоїна коливалась близько 5 доларів протягом більшої частини року, з численними коливаннями вгору і вниз. На початку року Міхай Аліса і Віталік Бутерін запустили журнал Bitcoin Magazine та випустили перший випуск у травні. Також було створено Bitcoin Foundation з метою популяризації біткоїнів та поліпшення сприйняття їх громадськістю.

У тому ж році, в рамках початкового фінансування, компанія Coinbase збрала понад 600 000 доларів США, що дозволило їй стати однією з провідних бірж біткоїнів. Також у цей період Кріс Ларсен і Джед Маккалеб заснували компанію OpenCoin, що призвело до розробки протоколу транзакцій Ripple для проведення валютних операцій та платежів у реальному часі. Ripple став мережею обміну валют і грошових переказів на основі публічної книги.

У 2013 році біткоїн продовжував зміцнювати свою позицію і рости. У лютому Coinbase оголосила, що продає біткоїни на суму понад 1 мільйон доларів за місяць за ціною понад 22 долари за один біткоїн. До кінця березня загальна вартість всіх наявних 11 мільйонів біткоїнів перевищила 1 мільярд доларів. Також у жовтні того ж року було запущено перший біткоїн-банкомат у Ванкувері, Британська Колумбія.

В кінці 2013 року Таїланд і Китай ввели заборону на використання криптовалюти. Федеральний суд США арештував кошти Mt. Gox, що знаходилися в США, а Федеральне бюро розслідувань (ФБР) закрило Silk Road і конфіскувало 26 000 біткоїнів.

Рік 2014 став поворотним для технології блокчейн, оскільки фінансові установи та інші галузі почали визнавати його потенціал і досліджувати, зсуваючи акцент з цифрової валюти на розвиток блокчейн-технологій. Відбулось народження "Блокчейн 2.0", що охоплює застосування блокчейн-технологій поза межами криптовалюти.

У 2015 році було створено Ethereum Foundation, яка відкрила шлях до застосування технології блокчейн не лише у криптовалюті. Однією з ключових особливостей Ethereum стали "розумні контракти" (Smart Contracts) - це невеликі програми, які зберігаються в блокчейні і виконуються при виконанні певних умов. Вони використовуються для укладання угод без посередництва та пропонують децентралізовану мережу з рівними правами для учасників. Основними умовами для "розумних контрактів" є розподілена база даних, сторони договору, що підтверджують свою участь електронним підписом, предмет угоди та умови, які забезпечують коректне виконання всіх частин договору програмною реалізацією.

У 2016 році стали свідками важливих подій. Біржа NASDAQ розпочала випробування технології блокчейну, а Linux Foundation запустила проект Hyperledger. Дев'ять провідних інвестиційних банків утворили консорціум R3 з метою дослідження переваг блокчейну. Протягом півроку, консорціум розширився до понад 40 фінансових установ.

В 2016 році сталося значне подією в світі Ethereum. Використання помилки в коді децентралізованої автономної організації Ethereum призвело до хардфорку мережі Ethereum. Також біржу біткоїнів Bitfinex було зламано, і було вкрадено приблизно 120 000 біткоїнів, що на той час мали вартість близько 66 мільйонів доларів.

2017 рік був також насиченим подіями. Японія офіційно визнала біткоїн легальною валютою. Семь європейських банків створили консорціум Digital Trade Chain з метою розробки платформи торговельного фінансування на основі блокчейну. Компанія Block.one представила операційну систему блокчейн EOS для підтримки комерційних децентралізованих додатків. Близько 15% світових банків використовували блокчейн-технологію у різних сферах своєї діяльності.

У 2018 році Південна Корея заборонила анонімну торгівлю криптовалютою, але вклала мільйони в ініціативи з використання блокчейну. Європейська комісія створила Обсерваторію та Форум Blockchain. Baidu представила свою власну платформу блокчейн як сервіс.

У 2019 році Walmart запустив систему ланцюга поставок на основі платформи Hyperledger. Amazon оголосив про загальну доступність свого сервісу Amazon

Managed Blockchain на AWS. Кількість транзакцій в мережі Ethereum перевищила 1 мільйон на день. Дослідження та розробки в галузі блокчейну зайняли центральне місце, і багато організацій використовували технологію блокчейн та децентралізовані додатки для різних сфер застосування.

У 2020 році Ethereum впровадив Beacon Chain у підготовці до Ethereum 2.0. Стабільні криптовалюти (Stablecoins) зазнали значного зростання популярності, оскільки вони пропонували більшу стабільність у порівнянні з традиційними криптовалютами. Виникає все більший інтерес до поєднання блокчейну з штучним інтелектом для оптимізації бізнес-процесів.

Протягом останніх років спостерігається зростаючий інтерес до використання блокчейну в інших сферах, крім криптовалют. Ця тенденція буде продовжуватися і в 2022 році, оскільки уряди та підприємства прагнуть використовувати блокчейн для розв'язання різноманітних випадків застосування. Це включає голосування, управління нерухомістю, відстеження фізичних активів, захист інтелектуальних прав, інтернет речей та вирішення проблем розповсюдження вакцин.

1.3 Сфери використання технології блокчейн

На сьогоднішній день технологію блокчейн складно переоцінити, тому вона набула велику кількість сфер використання, і чисельні експерименти з впровадження даної технології в нові сфери. Розглянемо деякі з них.

1) **Криптовалюта.** В наш час найбільш розповсюдженим способом використання технології блокчейну стало функціонування криптовалют. Вважається, що блокчейн є ключовим компонентом: він надає можливість користувачам запускати програмне забезпечення, що відстежує дотримання пов'язаних із цими валютами правил, роблячі деякі частини даних цінними завдяки дефіциту [9].

2) **Фінансові послуги.** У зв'язку з тим, що блокчейн зараз може керувати обігом цифрових грошей, великі компанії виявляють інтерес до розширення застосування цієї технології на інші фінансові послуги. Віриться, що блокчейн може

вирішити ефективність проблем в різних аспектах фінансової системи, таких як міжбанківські транзакції, кліринг і розрахунки, що зазвичай потребували втручання великих і непрозорих фінансових установ.

Ідея полягає в тому, що ці установи можуть скоротити витрати, забезпечити виконання регулятивних вимог і загалом оновити застарілі технології за допомогою блокчейну, що дозволить їм працювати більш ефективно.

3) **Бізнес-менеджмент.** Один з найбільш обговорюваних варіантів використання блокчейн-технології полягає в управлінні ланцюгами постачання для бізнесу. Світова торгівля - це велика індустрія з оборотом у трильйони доларів, в якій товари та послуги щодня переміщуються до різних куточків світу. Безліч учасників ланцюгів постачання займаються перевезенням товарів з одного місця в інше, і кожен з них використовує різні системи для затвердження та обробки транзакцій. Технологія блокчейну допомогла б знизити бар'єри, які виникають через розбіжності у цих системах, економлячи витрати і усуваючи потенційні точки відмов на цьому шляху [10].

4) **Ведення обліку.** У сучасний час, для ведення інформаційних записів в різних галузях, таких як охорона здоров'я, нерухомість або голосування, часто використовують централізовані центри оброблення даних. Проте це призводить до додаткових витрат і ризиків для відповідних суб'єктів. Ця централізована модель виявляє інформацію до різних порушень безпеки, а доступ до неї може бути складним і дорогим. Багато галузей потребують більш ефективної та безпечної системи обліку даних для виконання складних транзакцій та реєстрації. Тут технологія блокчейну входить в гру. Вона пропонує рішення для цих довготривалих проблем шляхом свого механізму реєстрації та комплексного обліку даних. Блокчейн також надає більшу контрольованість особистих даних людей, що дозволяє їм краще контролювати свою інформацію.

5) **Логістика.** Блокчейн може бути використаний як електронна накладна, що дозволяє відстежувати повний маршрут доставки товару від постачальника до покупця. Це рішення може замінити традиційну систему керування накладними (CRM), забезпечуючи переваги перед нею. Традиційна система CRM може бути

вразливою до злому, змін або видалення даних, тоді як після розміщення в інформації у відкритому блокчейні вона залишається незмінною і недоступною для видалення.

Один з прикладів організації, що використовує блокчейн як електронну накладну, є транспортна компанія Alibaba, пов'язана з відомою китайською платформою електронної торгівлі AliExpress. Завдяки цьому рішення, Alibaba, його співробітники та підрядники можуть відстежувати потоки транспортних продуктів та їх кількість в режимі реального часу, не маючи можливості внесення змін до записів. Бренди одягу також використовують принцип блокчейну, щоб контролювати весь процес доставки товару.

Це використання блокчейну дозволяє забезпечити прозорість, недоступність до змін та впевненість в доставці товару для різних учасників ланцюга постачання.

б) Боротьба з підробками. Технологія блокчейн може бути надзвичайно ефективною для виявлення контрафактної продукції. Особливо виробники предметів розкоші, такі як модельєри, стикаються з проблемою підробки своїх товарів. Використання блокчейну для аутентифікації продукту допомагає захистити як бренд, так і споживача. Це рішення було використано компаніями LVMH (французький концерн Louis Vuitton), Microsoft та Consensus при створенні платформи Auroga, яка допомагає індустрії розкоші в моніторингу та відстеженні товарів.

LVMH використовує блокчейн майже в 60 своїх брендах і планує розширити його функціональність, включаючи захист інтелектуальної власності та запобігання рекламному шахрайству. Багато інших розкішних брендів прийняли їхній приклад, надаючи своїм продуктам докази автентичності, що дозволяє швидко їх ідентифікувати. Це сприяє просуванню та перевірці етичного виробництва, а також підтверджує його стійкість. Блокчейн-аутентифікація також застосовується в індустрії дорогоцінного каміння. Наприклад, платформа Tracr, спеціально призначена для діамантової промисловості, використовує блокчейн для визначення автентичності природних діамантів, присвоюючи їм унікальні номери.

Зареєстрований діамант з таким цифровим номером можна ідентифікувати, перевіривши його походження та пов'язані з ним транзакції [11].

1.4 Переваги і недоліки технології блокчейн

Серед переваг використання технології блокчейн у рамках багатьох галузей використання можемо визначити:

1) Розподіл

Так, використання технології блокчейн дозволяє створити розподілену мережу вузлів (нод), де дані блокчейна зберігаються на тисячах пристроїв. Ця розподіленість забезпечує високу стійкість системи до технічних збоїв та шкідливих атак. Кожен вузол мережі має свою копію бази даних, яка автоматично оновлюється згідно з правилами протоколу блокчейна. Це означає, що навіть якщо одна нода відключиться або постає проблема на її сервері, інші ноди продовжують функціонувати і забезпечувати безпеку мережі. Така розподіленість робить систему блокчейн стійкою до відмов та атак. У порівнянні зі звичайними базами даних, які використовують лише обмежену кількість серверів, технологія блокчейн має перевагу в плані безпеки. Оскільки дані розподілені на багатьох пристроях, неможливо легко зруйнувати або зламати всю систему шляхом нападу на один сервер або декілька серверів. Це підвищує стійкість блокчейна до шкідливих дій і збоїв, що забезпечує надійність та безпеку збережених даних.

2) Стабільність

Одна з ключових особливостей технології блокчейн полягає в надійності і незмінності зареєстрованих даних. Підтверджені блоки в ланцюжку блоків (блокчейні) є практично нескасовуваними і надійно захищеними від видалення або змін. Ця характеристика блокчейну робить його ідеальним для зберігання фінансових звітів та інших важливих даних, які потребують надійного аудиту. Кожна зміна або транзакція, яка вноситься в блокчейн, фіксується, хешується та прив'язується до попередніх блоків, створюючи надійний і невід'ємний слід.

Це дозволяє компаніям ефективно запобігати шахрайству з боку своїх співробітників. Блокчейн може бути використаний для створення системи фінансової відкритості, де кожна фінансова транзакція фіксується і доступна для перегляду всім зацікавленим сторонам. Це робить небажану діяльність чи підозрілі операції легше виявити і припинити [12].

3) Система, що не вимагає довіри

Технологія блокчейн дійсно може елімінувати потребу в посередниках та третіх особах в платіжних системах. У традиційних системах платежів, таких як банки, емітенти карток чи платіжні провайдери, присутній централізований посередник, який виконує функцію перевірки та підтвердження транзакцій. Це може вимагати довіри до цих посередників і залежності від них.

У блокчейн-мережі, зокрема в публічних блокчейнах, транзакції перевіряються і підтверджуються розподіленою мережею нод, які займаються майнінгом або валідацією. Це означає, що використання блокчейну дозволяє здійснювати безпосередні транзакції між учасниками мережі без посередництва централізованої організації. Кожна транзакція підтверджується розподіленою мережею, і коли вона включається до блоку і стає невід'ємною частиною блокчейну, вона стає практично нескасовуваною.

Це дозволяє знизити ризик, пов'язаний з довірою до окремої організації, оскільки перевірка транзакцій здійснюється розподіленою мережею незалежних вузлів. Крім того, виключення посередників і третіх осіб зменшує загальні витрати та комісії за транзакції, оскільки відпадає необхідність у платі за їх послуги [13].

Таким чином, блокчейн-технологія дозволяє створити систему "не вимагає довіри", де транзакції перевіряються розподіленою мережею нод, а не однією централізованою організацією, що сприяє безпеці, ефективності та зниженню витрат.

Нажаль, як і будь-яка технологія сьогодення блокчейн маю і кілька недоліків, серед яких можна навести:

1) Атака 51%

Алгоритм консенсусу Proof of Work, що використовується в блокчейні Біткоїна, успішно забезпечував його захист протягом багатьох років. Хоча існують різні типи атак на блокчейн, найбільш обговорюваний серед них є "Атака 51%". Ця атака стає можливою, коли атакуючій стороні вдається контролювати понад 50% загальної потужності хешування, що дає змогу виключати або змінювати порядок транзакцій [14].

Хоча теоретично можлива успішна атака 51% на блокчейн Біткоїна, на практиці такого прецеденту не було. З розвитком мережі зростає її загальна безпека, тому малоймовірно, що майнери зроблять великі витрати та зусилля, щоб атакувати Біткоїн. Для майнерів вигідніше продовжувати чесну торгівлю, замість ризикувати довіру до системи. Успішна атака 51% може змінити лише недавні транзакції і тимчасово, оскільки криптографічні докази забезпечують зв'язок між блоками. Зміна старих блоків вимагатиме величезних обчислювальних ресурсів.

2) Зміни даних

Блокчейн також має свої обмеження, а одним з них є складність зміни даних після їх додавання. Хоча стійкість і незмінність є перевагою блокчейну, це може бути недоліком у певних ситуаціях. Зміна даних або коду в блокчейні зазвичай вимагає значних зусиль і, найчастіше, призводить до хардфорку - створення нового ланцюга блоків і припинення роботи з попереднім.

3) Приватні ключі

Блокчейн використовує асиметричну криптографію з публічним ключем, щоб надати користувачам контроль над їхньою криптовалютою (або будь-якими іншими даними в блокчейні). Кожна адреса в блокчейні має свій відповідний приватний ключ. Користувачі можуть вільно розповсюджувати свою адресу, але вони повинні зберігати приватний ключ у таємниці. Цей приватний ключ дозволяє користувачам отримувати доступ до своїх коштів і виступати в ролі свого власного банку. Втрата приватного ключа означає безповоротну втрату доступу до коштів.

4) Неефективність

Блокчейни, зокрема ті, що використовують алгоритм Proof of Work, демонструють низьку ефективність. Для успішного майнінгу необхідно мати високу конкурентоспроможність, оскільки значна кількість майнерів працюють безуспішно. Майнери постійно збільшують обчислювальну потужність, щоб збільшити свої шанси на знаходження валідного хешу блоку. З кожним роком витрати на майнінг Біткоїна зростають, і тепер цей процес вимагає більше енергії, ніж використовують цілі країни, такі як Данія, Ірландія та Нігерія [15].

5) Зберігання

З ростом часу розмір блокчейн-реєстрів може значно збільшуватися. На сьогоднішній день блокчейн Біткоїна вимагає приблизно 200 ГБ дискового простору. Зростання розміру блокчейна випереджає зростання потужності жорстких дисків, що може створювати ризик втрати вузлів мережі, коли реєстр стає занадто великим для завантаження та зберігання користувачами.

Навіть з усіма своїми недоліками, блокчейн продовжує розвиватися і пропонує унікальні переваги. Впровадження блокчейну в широкому масштабі ще далеко, але багато галузей вже досліджують його переваги та недоліки. Ймовірно, у найближчі роки компанії та уряди будуть експериментувати з новими способами використання блокчейну та намагатимуться отримати з нього вигоду [16; 17].

Висновки до розділу 1

У ході аналізу технології блокчейн було виявлено її основні принципи та поняття, історія розвитку, а також різні види блокчейн, такі як публічний, приватний та гібридний. Було встановлено, що блокчейн є інноваційним інструментом, здатним змінити спосіб взаємодії та обміну даними між учасниками ринку.

Переваги технології блокчейн включають високий рівень децентралізації, надійність та прозорість, а також можливість створення розумних контрактів. Однак,

в ході аналізу були виявлені деякі обмеження, включаючи масштабованість, проблеми конфіденційності даних та високі енергетичні витрати при використанні деяких консенсусних алгоритмів.

Технологія блокчейн має широкий потенціал для застосування у різних секторах економіки, включаючи фінансові послуги, логістику, охорону здоров'я та державне управління. Її використання може призвести до покращення ефективності процесів, зниження витрат та покращення безпеки даних.

Таким чином, аналіз технології блокчейн підтвердив її значний потенціал та важливість для сучасної економіки. Однак, перед впровадженням блокчейн рішень необхідно враховувати обмеження та розробляти відповідні стратегії для їх подолання. Подальші дослідження та розробки в галузі блокчейн технології можуть сприяти розширенню її застосування та вирішенню існуючих проблем, відкриваючи нові можливості для інновацій та розвитку економіки.

РОЗДІЛ 2

ПРОЦЕС ТОКЕНІЗАЦІЇ ФІНАНСОВИХ АКТИВІВ

2.1 Типи токенів

Токен — слово, яке перекладається з англійської як "купон" чи "жетон". Що ж таке токен у сучасному світі криптовалют? Токен є своєрідним знаком, за допомогою якого можна отримати певні послуги. Він має значення лише в контексті конкретної компанії, від якої ви його придбали. Ви платите цій компанії за доступ до її внутрішніх послуг. Токен виступає символом цифрового активу, який ви, як інвестор, придбуваєте від емітента токена, тобто від компанії, що його випускає.

До основних функцій токенів можна віднести наступне:

- Токен зберігається в гаманці криптовалюти.
- Токен може бути переданий іншим користувачам. Керування токенами здійснюється за допомогою смарт-контрактів, що дозволяють передавати активи іншим особам.
- Токен може бути випущений будь-ким, при заданих параметрах, таких як назва, символ, вартість і загальна кількість випущених монет.
- Власники токенів можуть отримати послуги за них, а також мати право голосу та активно брати участь у подальшому розвитку компанії.
- Токен може використовуватися як засіб платежу між учасниками конкретної системи.
- Токен є цифровим активом. Наприклад, якщо ви придбали токен, ви отримуєте право володіти цифровим продуктом компанії.
- Токен може використовуватися як одиниця виміру. Він дозволяє враховувати кількість APS-викликів та завантажень на торренті, наприклад.
- Токен може використовуватися як винагорода за різні дії, такі як використання платформи, участь у програмах.

З появою різноманітних стартапів, пов'язаних з блокчейном та проведенням початкових монетних пропозицій (ICO), токени почали еволюціонувати та набувати

своїх власних характеристик. Залежно від мети, застосування, правового статусу, технічного рівня та основної цінності, їх можна розділити на кілька категорій. Деякі категорії tokenів ще не мають чіткого регулювання, тоді як інші, навпаки, підпадають під суворі обмеження регуляторів. Зокрема, токени можуть бути класифіковані як Utility-токени, Security-токени або платіжні токени, також відомі як криптовалюти. Розглянемо кожен з цих категорій окремо [18].

Utility-токени — найпоширеніший тип tokenів. Такі токени використовуються лише в межах конкретного блокчейн-проекту. Утилітарні токени надають різні переваги для інвесторів. Зазвичай, через ці токени люди можуть скористатися товарами або послугами, які компанія планує запуснути у рамках свого проекту. Ці монети також можуть передбачати знижки та привілеї доступу до певних послуг. Однак, купуючи корисні утилітарні токени, інвестор не отримує права власності над активами компанії, такими як акції, майно чи продукція.

Зазвичай компанія випускає обмежену кількість "корисних" tokenів, щоб збільшити їх популярність, в результаті чого курс зростає. На сьогоднішній день фінансові регулятори ще не регулюють утилітарні токени, оскільки вони не мають інвестиційного характеру. Тому багато блокчейн-стартапів позначають свої токени як утилітарні, щоб уникнути проблем з законодавством.

Один з прикладів "внутрішнього" токена - Basic Attention Token (BAT) від браузера Brave. У екосистемі Brave, токен BAT використовується різними сторонами, включаючи глядачів, рекламодавців та авторів контенту. Глядачі отримують токени BAT за перегляд реклами в браузері, а творці контенту отримують винагороду за якісний контент. Іншим прикладом утилітарних tokenів є монети проектів Sia, Storj та Filecoin, які надають власникам можливість використовувати децентралізоване хмарне сховище. Власники tokenів можуть також використовувати їх зі знижкою та навіть виступати в ролі вузла, що надає свої ресурси.

Security-токени схожі на цінні папери на фондовому ринку. Власник tokenів має право на акції компанії, отримує частку її прибутку та дивіденди. Інвестори мають можливість активно брати участь у прийнятті рішень щодо розвитку проекту

і голосувати. Усі ці права зафіксовані в smart-контракті, а інформація про інвесторів та діяльність компанії зберігається на блокчейні. Security-токени регулюються регуляторами, такими як SEC (Комісія з цінних паперів та бірж США) та FINMA (Швейцарський орган нагляду за фінансовими ринками). Ці органи контролюють відповідність обігу Security-токенів законодавству країн, оскільки їх офіційно реєструють. Security-токени є реальними фінансовими інвестиціями і пов'язані зі звичайними цінними паперами. Компанії, що випускають Security-токени, мають додаткові зобов'язання виконувати законодавство про цінні папери та забезпечувати звітність. У порівнянні з Utility-токенами, Security-токени надають інвесторам певні гарантії щодо компенсації у разі невдачі проекту. Акредитовані інвестори можуть придбати Security-токени після запуску проекту, але є певні ризики, оскільки інвестиції не безпосередньо відбуваються в монети, а очікується отримання прибутку у майбутньому. Деякі приклади Security-токенів включають DigixDAO, Siafund і Taas [19].

Криптовалюти, як платіжні токени, мають різноманітні функції і можуть використовуватись як винагорода для майнерів, платіжний засіб або інструмент інвестування. Вони не мають підтримки жодними активами. До криптовалют, таких як Bitcoin, Ethereum, Monero, Litecoin, Dogecoin та інші, відносяться платіжні токени.

Токени можна класифікувати на взаємозамінні і взаємонезамінні. Взаємозамінний токен можна обміняти на подібні монети, наприклад, однакові токени ERC-20. Взаємонезамінний токен є унікальним і не може бути замінений на інший, оскільки має свою унікальну історію і дані, що визначають його цінність. Взаємонезамінні токени можуть мати використання у колекціонуванні або як ігрові предмети, де їх історія і властивості надають їм унікальну цінність. У разі біткоїна його взаємозамінність деякими вважається за обмежену, оскільки кожна монета має свою унікальну історію транзакцій, що може впливати на її цінність та прийняття.

Токен можна розглядати як базову одиницю обліку або вартості, яку емітує зацікавлена сторона в межах певного блокчейну. Фізично токени існують у вигляді запису в розподіленому реєстрі блокчейну. Найпоширеніший тип токенів - це криптовалюти. Однак з технічної точки зору, віднесення криптовалют до токенів є

питанням, що має свої протиріччя. Серед відомих токенів, які не є криптовалютами, можна згадати EOS (токен проекту Block.One) та RNTB (токен проекту Bitrent).

Токени, які не є криптовалютами, зазвичай поділяються на такі категорії:

1. Equity tokens - використовуються для токенизації компаній і надають власникам права, подібні до прав власників акцій у статутному капіталі юридичної особи.

2. Utility tokens - представляють певну цінність в межах бізнес-моделі онлайн-платформи, що випустила токен. Наприклад, такі токени можуть бути еквівалентом певного обсягу хмарного сховища або обмінюватися на послуги, які надає платформа.

3. Asset-backed tokens (токени активів) - представляють оцифровані та збережені в блокчейні реальні товари або послуги, які надають юридичні права на ці товари або послуги. Наприклад, це можуть бути токени, що відображають площу нерухомості, твори мистецтва або певні юридичні послуги.

2.2 Явище токенизації активів

Токенизація - це процес перетворення прав на активи у цифровий токен на блокчейні. Це означає, що інформація про актив прив'язується до блокчейну, в рамках якого випускаються токени. Блокчейн Ethereum є найбільш поширеним для випуску токенів, пов'язаних з активами, з ряду причин.

Завдяки наданню кожній одиниці активу свого унікального ідентифікатора, ми можемо зафіксувати дані про цю одиницю в постійному реєстрі, що захищений від змін, і відстежувати подальший рух активу. Можна сказати, що токенизація активів поєднує цифровий і реальний світи, забезпечуючи максимальний рівень безпеки і захисту інформації.

Чому потрібно токенизувати "реальні" активи? В економічному світі існує безліч активів, таких як цінні папери, нерухомість, золото, нафта, предмети мистецтва та інші. Багато з цих активів вимагають значних зусиль і витрат для фізичної передачі, або вони не можуть бути розподілені на частки.

Тому сьогодні стартапи та фінансові компанії по всьому світу змагаються у

розробці системи, яка стала б наступним етапом еволюції обміну активами - системи та стандартів токенизації активів. Чому ж комусь може знадобитись оцифрований актив (токен), і як саме це може працювати? Для пояснення цього розглянемо приклад.

Представте собі, що Галя володіє золотом або антикварними предметами мистецтва загальною вартістю 300 млн грн і бажає їх продати. Фізична передача таких активів покупцям вимагає значних зусиль, оскільки потрібно забезпечити безпеку та ретельну перевірку, щоб уникнути підробок або підміну активів під час перевезення до покупців.

У той же час Іванко бажає інвестувати декілька сотень тисяч гривень у золото або антикварні предмети мистецтва, але не має бажання займатися організацією фізичного отримання цих активів. Крім того, він не хоче володіти цілим злитком золота або предметом мистецтва. Ідеальним варіантом для нього є володіння невеликою часткою золота та різними частками різних предметів мистецтва, щоб диверсифікувати свої інвестиції.

Галі не варто витрачати час на пошук покупця для такої незначної частки активів, яку бажає Іванко. Вона просто потребує зручний спосіб розподілити свої цінності на менші частки та продавати їх безлічі людей. З іншого боку, Іванко бажає мати можливість безперешкодно продавати свої часткові власності іншим потенційним покупцям.

Можливість, яка задовольняє бажання всіх сторін у даній ситуації, полягає у токенизації часток товару Галі. Кожен токен представлятиме певну частку товару або активу, що значно спростить процес набуття та передачі власності на різні види активів.

Використання технологій блокчейн для токенизації активів може суттєво знизити можливість використання неправдивої інформації, скоротити витрати на торгівлю та спростити систему торгівлі. Токенизація значною мірою звільнить ринок від бюрократичних процедур, зайвих комісійних витрат, системи перешкод та обмежень.

Основною метою токенизації є забезпечення безпеки, простоти передачі і

швидкості активів. Незважаючи на це, ідеальної системи ще не існує, і деякі аспекти можуть вимагати компромісів. В майбутньому є багато можливостей для вдосконалення технології.

Для фіксації права власності в ситуаціях, де це потрібно за законом, команда Bitrent розробила протокол Proof of Ownership. Його головною метою є забезпечення можливості реєстрації права власності на нерухоме майно безпосередньо в державному реєстрі прав. Цей протокол дозволяє здійснювати електронну реєстрацію або працювати на основі блокчейну, передаючи дані зі смарт контрактів.

2.3 Процесс перетворення акцій на токен

Акції представляють собою цінні папери, які надають власникам право на отримання прибутку від компанії у формі дивідендів. У випадку, коли компанія зазнає збитків, вона може утримувати виплату дивідендів до повного погашення збитків. Крім того, у разі ліквідації бізнесу акціонер може претендувати на частку в залишковій вартості або майні компанії.

Простими словами, акції представляють собою долю в бізнесі. Власник акцій може отримувати частку прибутку, а також, якщо має достатню кількість акцій, брати участь в управлінні компанією.

Для компаній акції є засобом залучення додаткових інвестицій, а для акціонерів вони представляють активи, що можуть приносити не лише дивіденди, але й потенційний прибуток від успішної торгівлі. Торгівля акціями відбувається на глобальних фондових біржах, а також на спеціалізованих ринках, наприклад, NASDAQ.

Один з недоліків фондових ринків полягає у тому, що торгівля відбувається пакетами акцій, відомими як лоти, та лише за певним графіком роботи біржі. Якщо трейдер не встигає закрити свою позицію та бажає перенести її на наступний день, йому доведеться сплатити комісію, відому як овернайт.

Токени, навпаки, не мають цих обмежень. Токенізація фінансових активів, таких як акції, розглядається як сектор з великим потенціалом зростання. Це стимулюється популярністю токенів, випущених через нерегульовані початкові

пропозиції монет (ICO), а також зростанням інтересу до "пропозицій токенів цінних паперів" (STO), які дотримуються традиційних регулятивних вимог. STO є наступниками ICO та є способом залучення капіталу шляхом випуску токенів, які представляють цінні папери на розподіленій технології реєстру (DLT). Тип токенів визначається учасниками ринку самостійно, і відповідність чинному законодавству випуску буде залежати від конкретних обставин кожного випадку. STO є структурованими пропозиціями цінних паперів, що включають випуск токенів на основі DLT та відповідають регуляторним вимогам.

Правила, що стосуються пропозиції токенів інвесторам та управління токенами протягом усього їхнього життєвого циклу, представлені у цифровому форматі на блокчейні, наприклад, за допомогою програмованого захисту прав власності та торгових обмежень (так звані "програмовані цінні папери"). Цифрова трансформація фінансових ринків та використання автоматизації для емісії та торгівлі фінансовими інструментами не є новим явищем. Цінні папери протягом тривалого часу існували в електронному форматі, відомому як "дематеріалізована" форма. Токенізовані цінні папери можна розглядати як форму дематеріалізованих цінних паперів, що застосовують криптографію і випускаються та реєструються в децентралізованих реєстрах замість електронних записів у традиційних реєстрах цінних паперів та центральних депозитаріях. Децентралізація токенізованих цінних паперів разом з автоматизованою можливістю укладення угод та проведення розрахунків без посередників може стати потужним рушієм у сфері токенізації. Токенізовані цінні папери усувають необхідність посередників або довірених осіб при розподілі дивідендів або голосуванні, надаючи інвесторам повний контроль над їхнім капіталом [20].

2.4 Можливі наслідки глобального запуску токенизованих активів

Поширення токенизації активів на фінансових ринках може мати важливі наслідки, які стосуються ліквідності та можуть вплинути на торгівлю, ціноутворення, кліринг та розрахунки з цінних паперів, а також на грошово-кредитну політику. При оцінці можливих наслідків цього явища, важливо розрізнити два види токенизації:

1. Токенизація цінних паперів, які можуть існувати як токени як всередині, так і поза блокчейн мережею. Це означає, що цінні папери можуть бути представлені у вигляді токенів, але їх торгівля та розрахунки можуть здійснюватися як внутрішньо блокчейн, так і на традиційних фінансових ринках.

2. Випуск цінних паперів у токенизованій формі безпосередньо всередині блокчейну. Це означає, що цінні папери випускаються та торгуються виключно на блокчейні, без залучення традиційних фінансових ринків.

DLT (розподілені реєстри) надає можливість здійснювати операції з цінними паперами в режимі, де довіра розподіляється між вузлами, які беруть участь у блокчейн-мережі. Це означає, що для врегулювання відносин між сторонами транзакції не потрібна участь центрального інституту або посередника. Замість цього, інвестори можуть виступати як брокери-дилери для своїх власних операцій, а самі транзакції підтверджуються учасниками децентралізованої мережі згідно з встановленою комісією.

Маркет-мейкери забезпечують інвесторам можливість отримати двосторонні котирування при купівлі або продажу цінних паперів. Роль маркет-мейкерів особливо важлива на ринках з обмеженою кількістю інвесторів, де необхідна ліквідність. Особливо це актуально в періоди ринкового стресу, коли маркет-мейкери готові взяти на себе ризик і прийняти заявку на торгівлю незалежно від балансу між попитом і пропозицією. Теоретично, на децентралізованому ринку цінних паперів пошук покупців і продавців відбувається автоматично, без необхідності посередництва. При токенизації цінних паперів підвищення ефективності може бути пов'язане з усуненням посередника, такого як брокер (або

інші посередники, наприклад депозитарій або кліринговий центр), що сприяє дезінтермедіації.

На практиці, оператори систем з токенизацією активів надають послуги маркет-мейкера навіть на блокчейн-ринках. Це свідчить про те, що технологія розподіленого реєстру не обов'язково виключає посередництво брокера, а скоріше свідчить про те, що токенизація на базі DLT-мережі може мати обмежену ліквідність або що оператор торговельної платформи має економічні стимули зберегти модель брокера в токенизованому середовищі. Деякі учасники ринку цінних паперів вважають, що брокери залишаються корисними для виконання великих замовлень навіть у децентралізованих середовищах. Це підкреслює важливість вирішення питання про бажаність децентралізації та наявності належних стимулів для створення повністю децентралізованого ринку токенів. Зараз більшість торгівлі токенами відбувається на централізованих крипто-торговельних платформах, оскільки відмова від традиційної моделі маркет-мейкера може вплинути на нормальне функціонування деяких ринків та перерозподіл ризиків між ними. Наявність маркет-мейкерів може впливати на стійкість ринків, оскільки вони зазвичай беруть активи до себе на баланс та виступають як "амортизатори" волатильності, що може виникати через стадну поведінку інвесторів. Однак, навіть при наявності посередника не завжди можна гарантувати його участь, і існує можливість того, що маркет-мейкери можуть не працювати на ринках під час стресових ситуацій.

У випадку токенизованих активів, відсутність посередника, який бере на баланс токени та забезпечує ліквідність в періоди падіння ринків, може негативно впливати на ліквідність ринку. Цей ефект особливо помітний для "рідних" токенів, які випущені і торгуються виключно в блокчейні, і може бути менш помітним для токенизованих активів, що співіснують з традиційним ринком. Тому питання щодо необхідності повного відмови від посередництва в торгівлі токенизованими активами залишається предметом обговорення.

Розвиток токенизації активів також може вплинути на операції репо, що стосуються фінансування позицій, а також на операції з кредитування цінними

паперами, які використовуються в торговельних стратегіях. Перехід цих видів діяльності до блокчейну потенційно може призвести до швидшого та ефективнішого кредитування цінними паперами, оскільки процес стає менш складним, а забезпечення може бути використано негайно. Це означає, що ринок репо може стати майже миттєвим. Крім того, ринок може скористатися зростанням ліквідності, оскільки забезпечення може бути ефективніше перерозподілено між різними рахунками, які беруть участь в одній блокчейн мережі. Коли активи та операції з ними здійснюються в розподіленому реєстрі, мережа має інформацію про розташування активів в кожний момент часу, і забезпечення може вільно переміщатися між рахунками в системі. Однак, недоліком цього підходу є відсутність можливості нетінгу, і кожна угода, ймовірно, повинна бути повністю фінансово підтримана і розрахована. Це може призвести до більшого обсягу забезпечення, яке потрібно перемістити, замість традиційного нетто.

У випадку поширення токенизації, кількість та різноманітність активів, які можуть бути торговані на публічних ринках та отримувати ліквідність, можуть значно збільшитися. Це особливо важливо враховувати, оскільки теоретично будь-який актив може бути токенизований. Постачальники розподіленого реєстру (DLT) вже пропонують можливість використання їх інфраструктури ринку та протоколів для реалізації різних типів матеріальних та нематеріальних активів під власним брендом.

Збільшення ліквідності, спричинене токенизацією, має свої переваги, але також потребує відповідної глибини ринку.

Токенизація активів може мати як позитивний, так і негативний вплив на ліквідність. З одного боку, токенизація може забезпечити достатню ліквідність для неліквідних активів, таких як цінні папери МСП або приватні фонди. Вона також може покращити ліквідність активів з обмеженою торговельною активністю, наприклад, некотируємих цінних паперів, участі в капіталі приватних компаній та невеликих облігаційних емісій. Деякі учасники ринку навіть сподіваються, що токенизація може розблокувати значні суми коштів, які зараз заморожені у неліквідних активах, що приведе до збільшення обсягів торгівлі. Вторинна торгівля

такими активами є важливою для забезпечення ліквідності, встановлення цін та залучення капіталу.

Однак, слід відзначити, що для досягнення цих переваг необхідний високий попит на регулярну торгівлю, щоб ринки токенизованих активів мали достатню глибину. Це вимагає масштабного переходу до токенизованої форми ринку, який має значний вплив на економіку. Крім того, це передбачає наявність блокчейн-платформ та децентралізованих мереж з великою кількістю активних вузлів. Готовність ринку є ключовим чинником для успішної роботи будь-якої токенизованої екосистеми, що може вимагати зміни мислення учасників ринку, які можуть схильні бути неохочими до участі в блокчейн-системах.

Більш важливою є підвищена ефективність на ринках, де існують складні процеси, багато рівнів посередництва, повільна швидкість та високі витрати, або на ринках з низьким рівнем довіри. Такі ринки могли більш легко використовувати токенизацію активів на велику шкалу, зокрема для приватних розміщень цінних паперів, некотируємих на біржі, невеликих емісій облігацій або фондів прямих інвестицій/венчурного капіталу. З іншого боку, публічні фондові ринки у розвинених країнах вже виграють завдяки високоавтоматизованим та ефективним процесам, тому потенціал для подальшого підвищення ефективності за допомогою використання DLT є обмеженим. Важливо відзначити, що такі ринки вже мають високий рівень довіри серед їх учасників. Таким чином, потенційний приріст ефективності, який можна отримати через перехід до токенизованої форми ринку, може бути обмеженим.

Щодо ліквідності, вона може бути розподілена між внутрішніми (блокчейн) та зовнішніми (традиційними) ринками для одного й того ж активу.

Токенизація частини акцій, які продовжують торгуватися поза блокчейном, може призвести до перенесення ліквідності з традиційних ринків на блокчейн, що в свою чергу може призвести до зменшення ліквідності на ринках поза мережею. Проте цей сценарій не є ризиком, якщо цінні папери та активи взагалі випущені безпосередньо в блокчейн і не мають фізичного активу в реальному світі. Однак, паралельна торгівля токенизованими активами в мережі блокчейн та на традиційних

ринках може призвести до подвоєння ринків для одного й того ж активу, що негативно впливає на ліквідність та створює потенційний ризик арбітражу. Зростання використання токенизованих активів та їх торгівля в мережі блокчейн можуть позбавити традиційний ринок ліквідності з негативними наслідками для учасників ринку та порушенням безперебійності роботи ринків. Рівень взаємодії та сумісності між внутрішніми (блокчейн) та зовнішніми (традиційними) ринками токенизованих активів може визначити масштаб впливу на ліквідність. Потенційне подвоєння ліквідності між внутрішніми та зовнішніми ринками для токенизованих активів залежатиме від рівня взаємозв'язку традиційних ринків та децентралізованих токенів на блокчейні. Ризики арбітражу виникають природним чином тільки на ринках в межах мережі блокчейн, оскільки несумісність між різними мережами DLT та біржами породжує такий ризик арбітражу.

На деяких традиційних фінансових ринках, центральні розрахункові інститути виконують роль центральних контрагентів (ЦК), що забезпечують зведення угоди та розрахунок навіть у випадку дефолту однієї зі сторін, що зменшує ризик контрагента. Клірингові центри підтверджують дані угоди та використовують центральні депозитарії цінних паперів (ЦД) для реєстрації транзакцій. Кастодіани (клієнтські депозитарії), які зберігають активи інвестора, співпрацюють з ЦД, щоб забезпечити безпечний обмін активів та грошей між сторонами операції та здійснити розрахунки. Однак, неефективність у післяторгових процесах виникає через обов'язок кожної сторони угоди вести свої власні записи про транзакції, що призводить до потреби узгодження даних між сторонами та витрат на перевірку відповідності даних кожної сторони з даними контрагента на кожному етапі виконання угоди.

Застосування технології блокчейн у пост-трейдингу дозволяє створити єдиний, незмінний реєстр інформації про транзакції, який оновлюється на кожному етапі процесу і є доступним для всіх сторін угоди. Використання систем, що підтримують розподілену книгу реєстрації та застосовують розумні контракти для клірингу та розрахунків з токенизованими активами, дозволяє перевіряти наявність активів, підтверджувати відповідність угод і реєструвати транзакції миттєво і

автоматично. Розподілений реєстр може виступати як децентралізований реєстр даних про транзакції і як контрагент для всіх сторін, що беруть участь у операціях. Використання блокчейн також може покращити ефективність процесу розрахунків шляхом скорочення часу розрахунків майже до реального часу ($T + 0$), порівняно зі звичайними періодами розрахунків $T + 3$ або $T + 2$. Використання розподіленої книги реєстрації даних може також знизити витрати на бек-офіс та мінімізувати розбіжності в даних між сторонами, що полегшує швидку звірку даних угоди. Технологія блокчейн дозволяє зменшити кількість посередників та оптимізує процес оплати та передачі цінних паперів кінцевим власникам. У разі токенизації активів може статися заміна центральних депозитаріїв розподіленим реєстром як децентралізованою альтернативою. Також, клірингові центри можуть бути зменшені за рахунок використання блокчейн як центрального контрагента для розрахунків. Угоди можуть бути ефективно розраховані за допомогою перевірки транзакцій самими учасниками мережі. Скорочений час розрахунків може підвищити захист інвесторів шляхом зменшення ризику контрагента. Крім того, інвестори зможуть звільнити капітал, який раніше був затриманий у формі забезпечення для централізованого клірингу. Потенційне знищення таких вимог до забезпечення може призвести до зменшення навантаження на активи і покращити ліквідність фінансового ринку. Збільшення ліквідності також досягається шляхом прискорення розрахунків та зменшення затримок при зміні власності активів.

Оцінку технічної реалізованості, операційної економії та ефективності витрат, пов'язаних з дезінтермедіацією в пост-трейдингу, ще потрібно провести на практиці, через реальні застосування цієї технології. Існують деякі перешкоди, які можуть обмежувати повну реалізацію потенційної економічної ефективності клірингу та розрахунків на основі розподіленої книги реєстрації даних (DLT). Наприклад, не всі етапи угоди можуть повністю використовувати DLT, що може потребувати участі бек-офісу для перевірки клірингу та розрахунків, як раніше. Якщо інші аспекти діяльності, які впливають на позиції з цінних паперів, оплату або постачання цінних паперів, такі як кредитування цінними паперами або похідні інструменти, не використовують ту саму технологію, ефективність у сфері пост-трейдингу не

досягне 100%.

У деяких традиційних фінансових ринках центральні розрахункові інститути виконують роль центральних контрагентів (ЦК) для обох сторін угоди, що забезпечує метчинг угоди та її розрахунок, навіть у випадку дефолту однієї зі сторін, що зменшує ризик контрагента. Клірингові центри підтверджують дані угоди та використовують центральні депозитарії цінних паперів (ЦД) для зберігання записів транзакцій. Кастодіани (клієнтські депозитарії), які володіють активами інвестора, співпрацюють з ЦД, щоб забезпечити безпечне постачання/отримання активів та коштів для кожної сторони угоди і розрахувати угоди. Однак, неефективність у пост-торгових процесах виникає з обов'язку кожної сторони угоди вести свої власні записи про транзакції і необхідності звірки даних кожної сторони з даними контрагента на кожному етапі виконання угоди.

Експерименти з перевіркою концепції та можливостей використання DLT в розрахунках показали змішані результати, коли йшлося про ефективність. Наприклад, спільний блокчейн-проект Бундесбанку/Deutsche Borse для розрахунків за цінними паперами виявився придатним для масового використання, але не перевершив існуючі системи клірингу та розрахунків щодо продуктивності. У деяких випадках розрахунок займав більше часу і супроводжувався значними обчислювальними витратами. Це свідчить про необхідність подолати перешкоди на шляху розвитку технології, щоб досягти стадії, коли вона зможе забезпечити вищу продуктивність, ніж традиційні системи, що використовуються в даний час.

У децентралізованому, токенизованому світі існує потреба в центральному адміністраторі, що підкреслює актуальність інституту кастоді.

Для цілей обговорення припустимо, що в нинішньому регуляторному середовищі блокчейн все ще потребує наявності довіреної третьої сторони. Незважаючи на потенційну можливість дезінтермедіації на різних рівнях, успішна токенизація активів вимагає наявності надійного і довіреного центрального інституту, який гарантуватиме зв'язок між токенами та реальними активами, а також їх збереження. Ця роль часто виконується зберігачами (кастодіанами), які діють як довірена сторона і забезпечують зв'язок між блокчейн-мережею та зовнішнім світом.

Вони перевіряють характеристики та належність активу, який планується токенизувати, щоб гарантувати правильність інформації про актив перед його розміщенням у блокчейні. Кастодіани також відповідають за цифрове представлення активів в реєстрі, щоб уникнути дублювання токенів на різних платформах. Роль кастодіанів не обмежується просто підключенням до блокчейн-мережі та забезпеченням зв'язку зовнішнього світу. Вони також мають захищати сам актив і забезпечувати його належне зберігання, аналогічно до традиційного зберігання активів.

У системі з токенами можуть бути розглянуті ліквідовані клірингові центри та центральні депозитарії, а кастодіани відіграють ключову роль у структурі ринку, діючи як централізований довірений інститут, що забезпечує безперешкодне з'єднання платформи на блокчейн з зовнішнім світом. Однак ролі та обов'язки кастодіанів можуть бути переглянуті, включаючи відповідальність за забезпечення токенів реальними активами, а також захист цих активів. Наприклад, недобросовісний кастодіан може продати реальні активи, які використовуються в якості бази для токенів, без їх належного забезпечення або використати їх як заставу в інших угодах, отримуючи таким чином неправомірну вигоду. Ефективне регулювання та нагляд за кастодіанами, пов'язаними з блокчейном, допоможуть захистити інвесторів від таких ризиків. Крім того, центральний інститут може відігравати роль у забезпеченні перенесення реальних активів у блокчейн та перевірці точності інформації про активи, що підлягають токенизації.

Проте, все ще невизначено, які зміни ролей учасників ринку після торгівлі призведуть до суттєвої перерозподілу доходів. Можливо, ролі та відповідні доходи будуть передані іншим учасникам процесу. Розвиток на ринку значною мірою залежатиме від учасників, які будуть готові взяти на себе нові функції.

Крім того, варто зауважити, що наведені вище розгляди не стосуються токенизованих активів, що безпосередньо випущені в блокчейні, де право власності пов'язане зі володінням відповідним закритим ключем (наприклад, активи на пред'явника, як от облігації). У таких випадках кастодіани можуть зберігати приватні ключі учасників та забезпечувати відповідність між ключами та зберіганими на

відповідних адресах активами.

Для забезпечення майже миттєвого розрахунку цінних паперів і гарантування постачання проти платежу (DvP) необхідно, щоб цінні папери і кошти змінювали власників одночасно. Використання токенизованої форми грошей в блокчейні дозволяє зробити обмін швидким і без посередників. Оскільки токенизовані цінні папери вже присутні в блокчейні, наявність токенизованої форми грошей дозволяє забезпечити визначеність щодо постачання цінних паперів і здійснювати розрахунки майже в реальному часі.

У випадку відсутності токенів валют, які підтримуються центральними банками, для розрахунків на розподіленому реєстрі використовуються стейблкоїни (стабільні монети), які забезпечують грошову складову операцій. Такі стейблкоїни також використовуються на платформах для грошових розрахунків, особливо в контексті обслуговування цінних паперів і корпоративних дій протягом усього життєвого циклу цінних паперів, наприклад, при виплатах дивідендів.

У зв'язку з цим, виникає питання про те, яку роль у токенизованих ринках відіграють центральні банки і як вони сприятимуть (якщо сприятимуть) токенизації грошей центрального банку. Іншою альтернативою можуть стати стабільні монети або цифрові валюти центрального банку, якщо вони стануть доступними. Наприклад, проект Ubin у Сінгапурі використовує токенизовану валюту для DvP розрахунків з цінних паперів. Група банків, підтримуваних Грошово-кредитним управлінням Сінгапуру (MAS), створила прототип платіжної системи на базі розподіленого реєстру, де користувачі можуть обмінювати валюту на блокчейні, використовуючи токенизовану форму долара SGD.

Приватні банківські консорціуми також розглядають альтернативні рішення для спрощення розрахунків угод, створюючи дозволені мережі з власною монетою для розрахунків "комунальних послуг". Наприклад, проект розрахункової системи, під керівництвом UBS, в якому беруть участь 14 банків, працює над створенням монети для розрахунків (USC).

Токенизація активів може сприяти покращенню ліквідності та торговельності цих активів, завдяки підвищенню ефективності. Вона може знизити бар'єри для

інвестицій, надаючи інвесторам можливість отримати доступ до активів, які раніше були неліквідними, недоступними або обкладеними спорами. Це може спростити процес залучення капіталу до "розумних" стартапів та малого та середнього бізнесу, шляхом випуску боргових зобов'язань та акціонерного капіталу в приватних компаніях, де відсутня торговельна інфраструктура.

Однак, як і в усіх випадках застосування розподіленого реєстру та блокчейну, токенизація активів потребує чіткої бізнес-обґрунтованості. Використання розподіленого реєстру на фінансових ринках повинно бути обґрунтоване ефективністю та зниженням витрат, підвищенням безпеки, стійкості та довіри, спрощенням процесів та можливістю знищення посередників, або таке використання може обумовлюватись відсутністю наявної торговельної інфраструктури для даного активу.

Таким чином, токенизація активів може мати більший вплив на ринках, де є явні переваги в ефективності витрат, швидкості процесів та зменшенні складності та посередництва, або на ринках з дефіцитом довіри. Тому широке впровадження токенизації активів великого масштабу більш ймовірно на ринках з обмеженою ліквідністю та кількома рівнями посередництва, таких як приватне розміщення незареєстрованих цінних паперів або участь у приватних компаніях з обмеженою відповідальністю, а також при маломасштабному випуску облігацій або токенизації фондів прямих та інвестицій.

Впровадження токенизації публічних акцій у розвинених країнах може призвести до підвищення ефективності, але це вимагатиме уважної оцінки витрат і переваг. Розглядаючи розвинені ринки, які вже мають високий рівень довіри та функціонують на швидких, безпечних та ефективних процесах, можна очікувати лише невелике підвищення ефективності при переході до токенизації. Технічна складність, яка виникла на торгових майданчиках, може полегшити або навіть прискорити процес впровадження токенизації.

Проте слід зазначити, що деякі потенційні переваги токенизації активів можуть бути реалізовані лише при належному масштабуванні блокчейн-мережі. Масштабування є ключовим для повної реалізації переваг, таких як підвищення

ліквідності. Це означає, що в поточному стані справ токенизація активів, мабуть, буде доповненням, а не заміною існуючих традиційних ринків, принаймні на першому етапі її розвитку.

Висновки до розділу 2

У ході дослідження явища перетворення фінансових активів на токени було виявлено, що цей підхід є інноваційною технологією, яка може призвести до істотних змін у фінансовій індустрії. Токенизація дозволяє перетворити традиційні активи, такі як акції та облігації, в цифрові токени на блокчейн платформі.

Переваги токенизації фінансових активів включають збільшення ліквідності, підвищення доступності широкого кола інвесторів, зниження витрат і підвищення прозорості. Токени забезпечують частку в активі і можуть бути легко переданими та проданими, що відкриває нові можливості для інвестицій та управління активами.

Однак у процесі дослідження було виявлено кілька викликів та обмежень, з якими стикаються при реалізації токенизації фінансових активів. Ці проблеми включають правові та регуляторні аспекти, захист даних та конфіденційність, а також необхідність забезпечення надійності та безпеки блокчейн платформ.

В цілому, токенизація фінансових активів є перспективною галуззю, яка може призвести до істотних змін у фінансовій індустрії. Однак перед широким застосуванням цього підходу необхідно враховувати обмеження та розробляти відповідні стратегії для їх подолання. Подальші дослідження та практичні розробки мають бути спрямовані на вдосконалення технології токенизації фінансових активів та створення правових та регуляторних рамок, що сприяють її успішній реалізації.

РОЗДІЛ 3

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ТОКЕНІЗАЦІЇ АКТИВІВ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

3.1 Вибір програмних засобів для реалізації блокчейн для токенізації активів

У просторі блокчейн зустрічається багато людей і підприємств, які бажають реалізувати нові ідеї. Вибір мови програмування для розробки є важливим етапом у пошуку найкращого способу створення цифрових токенів.

Ось кілька найпопулярніших мов програмування, які використовуються для розробки блокчейн:

- C++ є потужною мовою програмування і була використана для побудови Bitcoin. Вона є об'єктно-орієнтованою, що дозволяє зручно зв'язувати дані і робить її відмінною для створення блокчейнів. C++ допомагає розробникам ефективно керувати ресурсами, контролювати пам'ять і швидко обробляти взаємодії, що є важливими для розробки з'єднань між користувачами та майнерами, перевірки транзакцій і побудови блоків.
- Python був створений з метою простоти і легкості використання, і став однією з найпопулярніших мов програмування у світі. Простота Python дозволяє розробникам швидко створювати та тестувати нові ідеї, а відкритий вихідний код надає доступ до безлічі інструментів, які допомагають вирішувати проблеми під час розробки.
- Solidity був створений для написання розумних контрактів на платформі Ethereum. Він дозволяє розробникам писати високорівневий, орієнтований на контракти код, який потім може бути перекладений і використаний на мовах нижчого рівня. Solidity спрямований на полегшення використання та технологій, що лежать в основі блокчейн. Незважаючи на те, що він є новим, він набуває популярності серед розробників.

- Java є дуже популярною мовою програмування у спільноті блокчейн, завдяки своєму об'єктно-орієнтованому підходу, який також використовується в C++. Її головна перевага для розробників блокчейн - мобільність. Завдяки віртуальній машині Java, Java не обмежується архітектурою пристрою і володіє здатністю одночасно обробляти велику кількість користувачів в мережі блокчейн.
- Інша мова, яка зростає в популярності у просторі блокчейн, - це Go. Вона була розроблена в Google у 2007 році і використовується для створення децентралізованих систем. Go відома своєю простотою використання і масштабованістю, що допомагає вирішувати проблеми завдяки своїй простоті.

3.2 Алгоритм та функції програмного засобу токенизації активів

Перед початком створення блокчейн необхідно виконати відповідні налаштування середовища та додаткового програмного забезпечення. Насамперед, встановлюємо Python 3.11.

Розглянемо детальніше програмний код та його реалізацію. Відповідно до опису блокчейн і кожному блоці повинні зберігатися такі дані: відправник, отримувач, кількість переданих токенів, хеш блоку, хеш попереднього блоку, перевірка роботи.

Імпортуємо необхідні для подальшої роботи бібліотеки Python (Рис. 3.1) .

```
from hashlib import sha256
import json
from time import time
```

Рисунок 3.1 - Імпортовані бібліотеки Python

Створюємо блок-генезис за допомогою функції `__init__()`, яка вказана на Рисунок 3.2.

```
def __init__(self, timestamp=None, data=None):
    self.timestamp = timestamp or time()
    self.data = [] if data is None else data
    self.prevHash = None
    self.nonce = 0
    self.hash = self.getHash()
```

Рисунок 3.2 - Функція створення блоку-генезису

В методі `getHash()` все починається з пуского хеша, який ми формуємо спираючись на дані, що зберігається в самому блоці. В ці дані входить наступне: хеш попереднього блоку, відмітка часу, дані, що зберігаються в блоці. Все це преобразується в послідовність байтів за допомогою метода `.encode('utf-8')`, як показано на Рисунок 3.3.

```
class Block:

    def __init__(self, timestamp=None, data=None):
        self.timestamp = timestamp or time()
        self.data = [] if data is None else data
        self.prevHash = None
        self.nonce = 0
        self.hash = self.getHash()

    def getHash(self):

        hash = sha256()
        hash.update(str(self.prevHash).encode('utf-8'))
        hash.update(str(self.timestamp).encode('utf-8'))
        hash.update(str(self.data).encode('utf-8'))
        hash.update(str(self.nonce).encode('utf-8'))
        return hash.hexdigest()
```

Рисунок 3.3 - Хешування блоку

Наступним кроком створюємо окремий клас `Blockchain`. Для того щоб

створити первинний блок, ми просто викликаємо Block з поточною позначкою часу (рис. - 3.4), для одержання якої використовуємо time().

Перетворення числа в рядок виконується в Python за допомогою функції str(). Метод для отримання найсвіжшого блоку використовує функція len() для виясненн довжини блоків.

```
class Blockchain:

    def __init__(self):
        self.chain = [Block(str(int(time())))]
        self.difficulty = 1
        self.blockTime = 30000

    def getLastBlock(self):
        return self.chain[len(self.chain) - 1]
```

Рисунок 3.4 - Отримання поточної позначки часу

Реалізуємо функцію запису наступного блоку (рис. 3.5). Щоб додати блок в блокчейн, ми просто викликаємо метод addBlock(), де використовується метод append().

```
def addBlock(self, block):
    block.prevHash = self.getLastBlock().hash
    block.hash = block.getHash()
    block.mine(self.difficulty)
    self.chain.append(block)
```

Рисунок 3.5 - Функція запису наступного блоку ланцюга

Перевірка цілісності блоків ланцюга виконує наступна функція (рис. 3.6). У головному тілі циклу викликається хеш попереднього файлу і порівнюється з хешем наступного блоку.

```

def isValid(self):
    for i in range(1, len(self.chain)):
        currentBlock = self.chain[i]
        prevBlock = self.chain[i - 1]

        if (currentBlock.hash != currentBlock.getHash() or prevBlock.hash != currentBlock.prevHash):
            return False

    return True

```

Рисунок 3.6 - Перевірка цілісності ланцюга

Обов'язково треба реалізувати алгоритм доказу виконання роботи (рис. 3.7) ми можемо, почавши з додавання до класу Block методу mine() та властивості nonce.

```

def mine(self, difficulty):
    while self.hash[:difficulty] != '0' * difficulty:
        self.nonce += 1
        self.hash = self.getHash()

```

Рисунок 3.7 - Доказ роботи блокчейну

3.3 Результат роботи програмного засобу

Для зручності тестування написаного коду створюємо окремий файл (рис. 3.8), куди викликаємо класи з попереднього файлу та необхідні бібліотеки. До змінної Chain викликається клас Blockchain. Далі вводимо дані для двох блоків.

```

from block import Block
from block import Blockchain
from time import time

Chain = Blockchain()

Chain.addBlock(Block(str(int(time()))), ({"from": "John", "to": "Bob", "amount": 100}))
Chain.addBlock(Block(str(int(time()))), ({"from": "Bob", "to": "Garold", "amount": 10}))

print(Chain)

```

Рисунок 3.8 - Програма запуску блокчейн

Результат роботи всього коду наведених на рисунку 3.9.

```
[
  {
    "data": [],
    "timestamp": "1686704489",
    "nonce": 0,
    "hash": "d21a5bb04848111b68628af23bb542032de1a6a9eb7eeae3a6321fb1d6383700",
    "prevHash": null
  },
  {
    "data": {
      "from": "John",
      "to": "Bob",
      "amount": 100
    },
    "timestamp": "1686705648",
    "nonce": 9,
    "hash": "003ad07db30d5a78a1eb0238177ca24b82a1aff1ba0b000f041b7b1212a0bf3f",
    "prevHash": "9ce245f157a5819090ab69ea33eb60506b293c07d4475518722ac39ede173e9f"
  },
  {
    "data": {
      "from": "Bob",
      "to": "Garold",
      "amount": 10
    },
    "timestamp": "1686705648",
    "nonce": 148,
    "hash": "00bbbc74f07ee04540afc24c43e3e99f427088754dbe02b5b8289492a3db7f51",
    "prevHash": "003ad07db30d5a78a1eb0238177ca24b82a1aff1ba0b000f041b7b1212a0bf3f"
  }
]
```

Рисунок 3.9 - Результат виконання коду

Висновок до розділу 3

В даному розділі ми розглянули базову реалізацію та принципи роботи блокчейн на практиці. Python було обрано як мову програмування.

Розглянуто основні функції для створення блокчейн реєстру:

- функція створення нового блоку,
- функція створення хеша,
- функція перевірки цілісності блоків.

Представлено програмний код на мові програмування Python, який реалізує наведені функції.

ВИСНОВКИ

На сьогоднішній день технології швидко розвиваються, а обсяг отримуваної, передаваної та збереженої інформації постійно зростає. У зв'язку з цим стає важливою технологія "Big Data", що дозволяє працювати з великими обсягами даних, а також набуває популярності нова технологія - блокчейн. За існуючою категоризацією можна виділити три умовні області застосування блокчейн-технології: блокчейн 1.0 - це валюта; блокчейн 2.0 - це контракти; блокчейн 3.0 - додатки, що виходять за межі фінансових транзакцій та ринків. Блокчейн в токенизації активів відноситься до останньої категорії.

Основною метою даної дипломної роботи було дослідження можливостей токенизації акцій та інших цінних паперів з використанням технології блокчейн, а також розробка програмних засобів та рекомендація щодо подальшого розвитку даної сфери.

Було виявлено, що токенизація активів має потенціал революціонізувати фінансову сферу, забезпечуючи більшу ліквідність, доступність та безпеку. Дана ідея визначена мною як необхідна через ситуацію в Україні на даний момент. Після закінчення цих жахливих подій потрібні будуть значні фінансові вливання в економіку та інфраструктуру країни. Не дивлячись на те, що велика кількість країн виказала бажання допомагати з відбудовуванням. Все ще залишається питання з стабілізацією економіки, а саме бізнесу.

Перетворення акцій і інших цінних паперів у токени призведе до такої самої популярності інвестування в бізнес як і в криптовалюту. Даний механізм значно спростить входження на ринок, прибере посередників, виключить фінансові махінації та буде залучати інвесторів можливістю заробити.

У результаті дослідження були запропоновані програмні засоби для токенизації активів на основі технології блокчейн. Ці засоби включають алгоритми та протоколи, які забезпечують безпечну емісію, обіг та обмін токенів на блокчейні. Були розглянуті питання щодо вибору платформи блокчейн, розробки смарт-

контрактів та інтеграції з системами фінансового обліку..

Варто зауважити, що досі існує необхідність правового регулювання як даної сфери, так і обігу криптовалют загалом. Враховуючи потенціал токенизації, необхідно створити сприятливі умови для розвитку цього напрямку, забезпечивши якість та безпеку фінансових операцій.

У цілому, кваліфікаційна робота відкриває широкі перспективи для подальшого дослідження та розвитку програмних засобів токенизації активів. Впровадження таких засобів може позитивно вплинути на фінансову сферу, забезпечуючи більшу ефективність, прозорість та доступність для учасників ринку.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Nakamoto S. A. Peer-to-Peer Electronic Cash System. Bitcoin [Electronic resource]. – Access: <https://bitcoin.org/bitcoin.pdf>
2. Nathaniel Popper Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money [Electronic resource]. – Access: <https://www.goodreads.com/book/show/23546676-digital-gold>
3. Michael Casey, Paul Vigna The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order [Electronic resource]. – Access: <https://www.goodreads.com/book/show/22174460-the-age-of-cryptocurrency>
4. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 2016 [Electronic resource]. – Access: <https://www.tandfonline.com/doi/abs/10.1080/10686967.2018.1404373>
5. Усенко А. Перспективи blockchain для бізнесу та української економіки. [Електронний ресурс]. – Режим доступу: <https://news.finance.ua/ua/news/-/427333/andrij-usenko-perspektyvy-blockchain-dlya-biznesu-i-ukrayinskoyi-ekonomiky>
6. Peters G.W. & Panayi E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Banking Beyond Banks and Money [Electronic resource]. – Access: <https://arxiv.org/pdf/1511.05740.pdf>
7. Що таке блокчейн (blockchain)? [Електронний ресурс]: BTC-UP. – Режим доступу: <https://btc-up.com/shho-take-blokchejn-blockchain/>
8. The World Bank Group [Electronic resource]: The World Bank. – Access: <https://www.worldbank.org/>
9. Blockchain Technology Defined [Electronic resource]: Built In National. – Access: <https://builtin.com/blockchain>
10. How secure is blockchain really? [Electronic resource]: Mike Orcutt archive page MIT Technology Review BLOCKCHAIN. – Access: <https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain->

really/ 62

11. Blockchain [Electronic resource]: Enigma. Paradox. Opportunity. – Access: <https://www2.deloitte.com/content/dam/Deloitte/xs/Documents/technology/Blockchain.pdf>

12. Біловус Л.І. Управління та організація діяльності інформаційних установ [Електронний ресурс]: Навчальний посібник. – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/9171/1/feu_kdidu_sdid_dotudiu_NP.pdf

13. A timeline and history of blockchain technology [Electronic resource]: Tech Accelerator. – Access: <https://www.techtarget.com/whatis/feature/A-timeline-andhistory-of-blockchain-technology>

14. Пояснення дерев та корінь Меркла [Електронний ресурс]. Binance Academy. – Режим доступу: <https://academy.binance.com/uk/articles/merkle-trees-andmerkle-roots-explained>

15. Alan T. Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski On the Origins and Variations of Blockchain Technologies [Electronic resource]: Cyber Defense Lab.University of Maryland, Baltimore County (UMBC). – Access: <https://arxiv.org/ftp/arxiv/papers/1810/1810.06130.pdf>

16. Девід Чаум - David Chaum [Електронний ресурс]. Енциклопедія – Режим доступу: https://wikiukuk.top/wiki/David_Chaum#Vault_systems

17. History of Blockchain [Electronic resource]. – Access: <https://www.javatpoint.com/history-of-blockchain>

18. Stuart Haber , W. Scott Stornetta How to Time-stamp a Digital Document (1991) [Electronic resource]: Journal of Cryptology. – Access: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.8740>

19. Dave Bayer , W. Scott Stornetta , Stuart Haber Improving the Efficiency and Reliability of Digital Time-Stamping (1993) [Electronic resource]: Sequences II: Methods in Communication, Security and Computer Science. – Access: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.71.4891> 63

20. Back, Adam. Hashcash - A Denial of Service Counter-Measure. [Electronic

- resource]. – Access:
<https://web.archive.org/web/20181123130639/http://www.hashcash.org/hashcash.pdf>
21. History of blockchain [Electronic resource]. – Access:
<https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchainarticles/what-is-blockchain/history>
22. Hal Finney Reusable Proofs of Work [Electronic resource]. – Access:
<https://nakamotoinstitute.org/finney/rpow/index.html>
23. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. [Electronic resource]. – Access:
<https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrencytechnologies>
24. bitcoin mining [Electronic resource]. WhatIs.com – Access:
<https://www.techtarget.com/whatis/definition/Bitcoin-mining>
25. БІТКОЇН (BITCOIN, BTC) [Електронний ресурс]. – Режим доступу: <https://mind.ua/tags/473-bitkojn-bitcoin-btc>

ДОДАТОК А

```
from hashlib import sha256
import json
from time import time

class Block:

    def __init__(self, timestamp=None, data=None):
        self.timestamp = timestamp or time()
        self.data = [] if data is None else data
        self.prevHash = None
        self.nonce = 0
        self.hash = self.getHash()

    def getHash(self):

        hash = sha256()
        hash.update(str(self.prevHash).encode('utf-8'))
        hash.update(str(self.timestamp).encode('utf-8'))
        hash.update(str(self.data).encode('utf-8'))
        hash.update(str(self.nonce).encode('utf-8'))
        return hash.hexdigest()

    def mine(self, difficulty):
        while self.hash[:difficulty] != '0' * difficulty:
            self.nonce += 1
            self.hash = self.getHash()

class Blockchain:

    def __init__(self):
        self.chain = [Block(str(int(time())))]
        self.difficulty = 1
        self.blockTime = 30000
```

```
def getLastBlock(self):
    return self.chain[len(self.chain) - 1]

def addBlock(self, block):
    block.prevHash = self.getLastBlock().hash
    block.hash = block.getHash()
    block.mine(self.difficulty)
    self.chain.append(block)

    self.difficulty += (-1, 1)[int(time()) - int(self.getLastBlock().timestamp) <
self.blockTime]

def isValid(self):
    for i in range(1, len(self.chain)):
        currentBlock = self.chain[i]
        prevBlock = self.chain[i - 1]

        if (currentBlock.hash != currentBlock.getHash() or prevBlock.hash !=
currentBlock.prevHash):
            return False

    return True

def __repr__(self):
    return json.dumps([{'data': item.data, 'timestamp': item.timestamp, 'nonce':
item.nonce, 'hash': item.hash, 'prevHash': item.prevHash} for item in
self.chain], indent=4)
```

ДОДАТОК Б

```
from block import Block
from block import Blockchain
from time import time

Chain = Blockchain()

Chain.addBlock(Block(str(int(time()))), ({"from": "John", "to": "Bob", "amount":
    100})))
Chain.addBlock(Block(str(int(time()))), ({"from": "Bob", "to": "Garold", "amount":
    10})))

print(Chain)
```