

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

**СКИРДА АНТОН ВЯЧЕСЛАВОВИЧ**

Допускається до захисту:

Завідувач кафедри інформаційних  
технологій, к.т.н, доцент

\_\_\_\_\_ Т.В.Нескородева

« \_\_\_\_ » \_\_\_\_\_ 2021 року

**АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ  
ТЕХНОЛОГІЙ «БЛОКЧЕЙН» І ЦИФРОВИХ ВАЛЮТ**

Спеціальність 125 Кібербезпека

**Кваліфікаційна (бакалаврська) робота**

Керівник:

Загоруйко Л.В., доцент кафедри  
інформаційних технологій,

к.т.н., доцент

\_\_\_\_\_  
підпис

Оцінка: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

( бали за шкалою ЄКТС / за національною шкалою )

Голова ЕК: \_\_\_\_\_

(підпис)

Вінниця – 2021

## АНОТАЦІЯ

**Скирда В.А. Аналіз сучасних тенденції розвитку технології «блокчейн» та цифрових валют.** Спеціальність 125 Кіберзахист. Донецький національний університет імені Василя Стуса, Вінниця, 2021.

В роботі досліджені теоретичні аспекти технології «блокчейн» та визначені технологічні основи її інноваційності. Проведений аналіз сучасного стану та здійснена оцінка рівня розвитку технології. За результатами аналізу визначені тенденції розвитку технології «блокчейн» та цифрових валют. Розроблено програмну модель «блокчейну».

Ключові слова: блокчейн, розподілений реєстр, криптовалюта, цифрова валюта.

70 с., 4 табл., 11 рис., 1 дод., 83 джерела.

**Skyrda Anton. Analysis of current trends in blockchain technology and digital currencies.** Specialty 125 Cybersecurity. Vasyl' Stus Donetsk National University, Vinnytsia, 2021.

The theoretical aspects of blockchain technology are investigated in the work and the technological bases of its innovation are determined. An analysis of the current state and an assessment of the level of technology development. According to the results of the analysis, trends in the development of blockchain technology and digital currencies have been identified. The blockchain software model has been developed.

Keywords: blockchain, distributed register, cryptocurrency, digital currency.

70 p., 4 tabl., 11 fig., 1 applications, bibliography: 83 items.

## ЗМІСТ

ВСТУП .....	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ТЕХНОЛОГІЇ «БЛОКЧЕЙН» ТА ЦИФРОВИХ ВАЛЮТ НА ЇЇ ОСНОВІ .....	8
1.1 Технологічні основи інноваційності .....	8
1.2 Поняття та сутність технології «блокчейн» .....	11
1.3 Особливості криптографічної хеш-функції в «блокчейні».....	16
1.4 Поняття та сутність цифрових валют .....	18
РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЇ РОЗВИТКУ «БЛОКЧЕЙН» ТА ЦИФРОВИХ ВАЛЮТ .....	24
2.1 Огляд глобального ринку .....	24
2.2 Еволюційний розвиток .....	25
2.3 Галузі використання технології .....	28
2.4 Оцінка рівня розвитку технології .....	37
РОЗДІЛ 3. КОНКУРЕНТНІ ПЕРЕВАГИ, НЕДОЛІКИ ТА ПЕРЕШКОДИ РОЗВИТКУ ТЕХНОЛОГІЙ НА ОСНОВІ «БЛОКЧЕЙН» .....	42
3.1 Переваги та недоліки технології «блокчейн» та криптовалют .....	42
3.2 Огляд потенційних кібератак .....	45
3.3 Конкурентні переваги технології «блокчейн».....	48
3.4 Технологічні перешкоди та обмеження архітектури .....	51
3.5 Суттєві бар'єри впровадження .....	53
3.6 Програмна модель «блокчейну» .....	57
ВИСНОВКИ .....	59
СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ .....	61
ДОДАТОК А .....	70

## ВСТУП

**Актуальність теми дослідження.** Поява в січні 2009 році першої криптовалюти Bitcoin, концепт якої побудований на технології «блокчейн», дала поштовх до стрімкого розвитку як самої технології, так й до появи інших цифрових валют. За прогнозами [1] компанії Bloomberg, світовий ринок продуктів на основі блокчейн-технологій у 2021 році сягне 2,3 млрд. дол. США. За даними звіту [2] аналітичного агентства Markets and Markets очікується, що обсяг глобального ринку блокчейнів зросте з 3,0 млрд. доларів США в 2020 році до 39,7 млрд. доларів США до 2025 року при річному темпі приросту (CAGR) 67,3% протягом 2020–2025 років. В жовтні 2020 року міжнародна консалтингова компанія «PricewaterhouseCoopers» представила аналіз [3], згідно з яким до 2030 року блокчейн-технології забезпечать зростання світової економіки на 1,7 трлн. доларів США.

Лідерами ринку блокчейн-технологій аналітики називають такі гіганти IT-індустрії як: IBM, SAP, Apple, Samsung, Microsoft, Hewlett Packard Enterprise, Amazon Web Services, Alibaba, Oracle, Huawei, Blockstream, Stratis Group Ltd, стартап PayStand, банки Bank of China, Bank of America [4].

В 2016 році у міжнародній організації стандартизації ISO створено технічний комітет 307 – «блокчейн» і технології розподіленого реєстру.

В Україні у 2017 році технологія «блокчейн» була впроваджена для оновленої системи електронних торгів конфіскованим майном CETAM. Державне підприємство «CETAM» вже провело 23 202 аукціона на загальну суму 6 213 016 108 грн. з використанням технології «блокчейн» [5]. Того ж року Кабінет Міністрів України ухвалив здійснення заходів, спрямованих на запровадження використання системи зберігання та захисту даних Blockchain під час проведення електронних земельних торгів та у роботі Державного земельного кадастру [6].

Агенція Dow Jones & Company, фондова біржа Nasdaq, Чикагська біржа опціонів (Cboe) впродовж 2019-2021 років впровадили відповідні індекси на криптовалюти [7].

Для прогнозування цін криптовалют пропонується застосування штучних нейронних мереж [8].

Разом із цим, після того як в 2018 році лопнув спекулятивний «міхур» криптовалют, в експертному середовищі різко посилилася обґрунтована критика надійності цифрових валют та перспектив технології «блокчейн» [9, 10]. Вразливим місцем технології називають можливості квантових комп'ютерів, які можуть подолати криптозахист. В лютому 2021 року з'явилася інформація [11], що IBM практично повністю скоротила свій підрозділ з розробки блокчейн-технологій.

На тлі злетів і падінь цифрових грошей та буму стартапів набагато скромніше виглядають новини про досягнення використання технології «блокчейн» в галузях, де їй з самого початку пророкували блискуче майбутнє: реформування державних органів, протидія ухиленню від сплати податків, оптимізації бізнес-процесів. Розвиток «блокчейн» тут протікає набагато повільніше, ніж в сфері криптовалют, та стикається з численними перешкодами, в тому числі тими, які виходять з самої концепції технології (ще недостатньо зрілої). Амбітний проект переходу «блокчейн» від «криптовалютної» до «генералізованої» технології привів до створення множини її поколінь, причому найчастіше у вигляді незавершених розробок та конкуруючих версій, що створює труднощі та помилки при практичному застосуванні [10].

Суперечливість прогнозів щодо перспектив розвитку та впровадження інноваційної технології «блокчейн», складності правового регулювання криптовалют, вразливість цифрових валют з точки зору інформаційної безпеки, відсутність у відкритому доступі фундаментальних наукових та прикладних праць, які розкривають деталі технології, обґрунтовує необхідність аналізу сучасних тенденцій розвитку технології «блокчейн» і цифрових валют, що й обумовило актуальність дослідження.

**Мета дослідження:** здійснити аналіз сучасних тенденцій розвитку технології «блокчейн» і цифрових валют.

Виходячи з поставленої мети дослідження, необхідно вирішити наступні **завдання:**

- дослідити теоретичні аспекти технології та визначити технологічні основи її інноваційності;
- розкрити поняття та сутність технології «блокчейн» та цифрових валют;
- розглянути особливості криптографічної хеш-функції в «блокчейні»;
- проаналізувати сучасний стан та тенденції розвитку «блокчейн» та цифрових валют;
- оцінити рівень розвитку технології;
- встановити та оцінити із застосуванням сучасних методів аналізу: перспективи, конкурентні переваги (конкурентоспроможність) та перешкоди розвитку технологій на основі «блокчейн»;
- дослідити можливості практичного застосування технології розробкою програмної моделі «блокчейну»;
- розробити програмну модель «блокчейну».

**Об'єкт дослідження:** технологія «блокчейн» та цифрові валюти на її основі.

**Предмет дослідження:** тенденції та перспективи розвитку технології «блокчейн» і цифрових валют, перспективи, конкурентні переваги та перешкоди розвитку.

**Методи дослідження.** Для реалізації визначеної мети та вирішення поставлених завдань використано комплекс взаємодоповнюючих загальнонаукових та спеціальних методів дослідження та аналізу, зокрема:

- історичний та логічний методи;
- методи синтезу та системного аналізу;
- методи спостереження, порівняння, графічні та статистичні методи обробки інформації;

- методологію Harvard Business School (з обґрунтуванням її застосування) для оцінки рівня розвитку технології;
- методику матричного SWOT-аналізу для об'єктивного виявлення переваг та недоліків, можливостей та загроз, конкурентоспроможності технології «блокчейн» та цифрових валют.

***Теоретичне та практичне значення одержаних результатів.***

Теоретичне значення роботи полягає в уточненні понять та сутності технології «блокчейн», цифрової валюти та її різновиду - криптовалюти, виділенні фундаментальної розбіжності між ними. Досліджені та систематизовані: технологічні основи інноваційності «блокчейн», еволюційний розвиток технології, перспективні галузі використання, що можуть бути використані у подальших дослідженнях. Практичне значення результатів роботи полягає у виявленні технологічних перешкод, суттєвих бар'єрів впровадження та конкурентних переваг технології, що матимуть визначальний вплив на тенденції розвитку в найближчій перспективі, а також для урахування при здійсненні заходів правового та законодавчого регулювання в Україні. Розроблену програмну модель можливо використовувати з практичною метою.

***Структура кваліфікаційної (бакалаврської) роботи.*** Кваліфікаційна (бакалаврська) робота складається зі вступу, трьох розділів основної частини, висновків, списку використаних посилань. Загальний обсяг роботи складає 68 аркушів. Робота містить 4 таблиці, 11 рисунків, 1 додаток. Список використаних посилань налічує 82 найменування.

## РОЗДІЛ 1

### ТЕОРЕТИЧНІ АСПЕКТИ ТЕХНОЛОГІЇ «БЛОКЧЕЙН» ТА ЦИФРОВИХ ВАЛЮТ НА ЇЇ ОСНОВІ

#### 1.1. Технологічні основи інноваційності

Технологія «блокчейн» (англ. Blockchain, від block - блок, chain - ланцюг) заснована на використанні розподіленої бази даних (англ. distributed ledger). Розподіленість полягає в тому, що база (англ. ledger - реєстр транзакцій) зберігається у вигляді великої кількості рівноправних копій в учасників (англ. peer) «блокчейн». Немає еталонної копії або центрального сховища (як єдиної точки відмови), а значить, немає необхідності оточувати його файєрволом, захищати від хакерських атак чи інших загроз з використанням вартісних та складних систем. Незважаючи на те, що розподілена база доступна всім учасникам (англ. peer - рівноправний), вона захищена від внесення ними недостовірних даних і ретроспективних змін записаної інформації. Захищеність даних, що зберігаються у відкритій розподіленій системі, є першою важливою перевагою технології «блокчейн».

Розподілена база зберігає інформацію про транзакції, що здійснюються над токенами. Токен (англ. Token - знак, жетон, талон) - цифрове абстрактне подання активів, прав чи зобов'язань, яке є об'єктом кількісного обліку в цій базі даних.

Транзакції є відображенням угод між власниками токенів. Адміністративний центр, який гарантує достовірну реєстрацію угод, в даному випадку не потрібен. Його роль в «блокчейн» виконує консенсус учасників системи. Будь-який учасник може ініціювати реєстрацією транзакції, для цього він повинен направити зміни в базу. Але тільки тоді, коли такі зміни будуть узгоджені системою (досягнутий консенсус), вони будуть передані (синхронізовані) по всім копіям (всім учасникам) [12].

Алгоритм консенсусу визначає правила, за якими автоматично обчислюється та гарантується справжній зміст розподіленої бази даних, що особливо актуально, коли ряд учасників можуть спробувати сфальсифікувати інформацію (класична криптографічна задача «візантійських генералів»). При

цьому на практиці вимагається висока надійність та одночасно висока продуктивність таких алгоритмів.

На даний момент, використовуються два основних алгоритми консенсусу: Proof of Work (PoW, «доказ виконаної роботи») та Proof of Stake (PoS, «доказ володіння») [13, 14]. У першій ситуації гарантом достовірності є виконана обчислювальна робота, яку може перевірити ще раз будь-який інший учасник мережі. У другій - певний грошовий внесок і подальша можливість гаранта взагалі брати участь в процесі. У найбільш популярної на даний момент криптовалюти Bitcoin застосовується алгоритм консенсусу PoW. Щоб імітувати підтвердження алгоритму консенсусу, потрібні значні ресурсні витрати - необхідно компенсувати як криптографічні методи захисту, так і обчислювальні потужності постійно діючої мережі. Втім, навіть цей алгоритм не забезпечує стовідсоткової стійкості до зовнішніх впливів. Однак досвід реального застосування показує, що розроблений в «блокчейні» алгоритм консенсусу, найбільш оптимальне рішення цієї проблеми на даний момент [14].

Таким чином, в технології «блокчейн» відсутність довіри між сторонами угод (і взагалі учасниками), а також авторитетного центру (арбітра, єдиного реєстру) не є проблемою. Реєстрація угод та зберігання інформації про них відбуваються розподілено (англ. peer-to-peer (P2P) – від рівного до рівного), але при цьому абсолютно безпечно. Розподіленість є другою важливою перевагою технології «блокчейн». Слід зауважити, що філософія «блокчейн» полягає в тому, що захищеність інформації забезпечується саме розподіленістю системи (перша перевага обумовлена другою).

Розподіленість «блокчейн» також дозволяє поширити цю технологію на будь-який тип взаємодії учасників, будь то H2H (англ. human-to-human – від людини до людини), H2M (англ. human-to-machine – від людини до машини) або M2M (англ. machine-to-machine – від машини до машини) [9]. Щодо M2M-систем, то згідно із прогнозом GSMA, до 2025 року кількість підключень «розумних пристроїв» досягне майже 25 млрд по всьому світу [15].

Завдяки притаманним їм властивостям, токени можуть виступати цифровою формою подання більшості видів активів та зобов'язань, а «блокчейн» - зручною середою зберігання та реєстрації різних економічних та фінансових даних. На сьогоднішній день основне застосування tokenів - це емісія криптовалют, здійснення платежів за допомогою криптовалют без участі центрального банку та банків взагалі. Тобто криптовалюта виступила інструментом апробації та популяризації «блокчейн» на першому етапі розвитку технології.

На другому етапі свого розвитку «блокчейн» надав можливість альтернативного способу залучення інвестицій (англ. crowdfunding) для нових проектів та стартапів у вигляді ICO (англ. Initial coin offering - первинне розміщення tokenів). В даний час розпочинається третій етап розвитку цієї технології: вишукуються кращі способи широкого застосування tokenів для обліку майнових прав, оподаткування, в тому числі транснаціонального, реалізації права вибору (голосування, експертиза), для продажу, обміну, спільного використання будь-яких активів (в тому числі інтелектуальної власності), тарифікації в системах масового обслуговування та іншого.

Відносини клієнта (власника tokenів) та блокчейн-системи починаються з відкриття клієнтом рахунку (т. зв. «гаманця») в системі, на якому зберігається нуль або більше tokenів. Вся історія переміщення tokenів між «гаманцями» клієнтів (транзакції) зберігаються в базі даних нескінченно (у більшості реалізацій технології «блокчейн»), починаючи з першої миті роботи системи.

Технологія забезпечує майже абсолютну гарантію того, що тільки володілець tokenів може ними суверенно скористатися, а також авторизацію володільця та недоторканність його активів за допомогою стійких криптографічних методів (асиметричне шифрування, дерево Меркле та інші методи). Завдяки цій властивості, система «блокчейн» має можливість одночасного використання як механізм децентралізованої та високонадійної перевірки особистості учасників та надання їм прав (тобто для автентифікації та авторизації).

## 1.2. Поняття та сутність технології «блокчейн»

«Блокчейн» - багатофункціональна і багаторівнева інформаційна технологія, призначена для надійного обліку різноманітних активів. Технологія надійного розподіленого зберігання записів про всі коли-небудь здійснені трансакції. По суті «блокчейн» є ланцюжком блоків даних, обсяг якого постійно зростає в міру додавання нових блоків із записами останніх трансакцій. Це хронологічна база даних, тобто така база даних, у якій час, коли було зроблено запис, нерозривно пов'язаний із самими даними, що робить її незмінною.

Дані представлені послідовністю записів, яку можна доповнювати. Записи разом із допоміжною інформацією зберігаються у блоках, а блоки зберігаються у формі однозв'язного списку. Кожен учасник представлений вузлом (node), який зберігає весь актуальний масив даних і контактує з іншими вузлами. Вузли можуть додавати нові записи в кінець списку, а також повідомляють одна одну про зміни списку.

Базову модель розподілу даних у системі, побудовану на «блокчейні», можна відобразити у формі такої послідовності дій [16]:

1. Нову трансакцію відправляють усім вузлам мережі, яка побудована за принципом пірингової мережі, і потрапляє в пул необроблених даних на цих вузлах;

2. Спеціалізовані машини учасників (в принципі, процес майнінгу може проводитися й на звичайному персональному комп'ютері), тобто майнери (від англ. mining - видобуток), додають у блок трансакції, які розташовані в пулі необроблених даних.

3. Кожен майнер намагається підібрати хеш блока, який задовольняє задані розробниками умови (у блокчейні біткоїна умовою була наявність на початку хеша блока певної кількості нулів), цю операцію називають підтвердженням роботи (proof-of-work, PoW). На даний момент з'явився інший спосіб підтвердження права на здійснення операції зі внесення блока - метод підтвердження частки (proof-of-stake, PoS);

4. Як тільки майнер отримує відповідний хеш блока, блок даних відправляють всім учасникам мережі, а сам майнер отримує винагороду за додавання блока. Не критично, якщо блок отримають не всі вузли, оскільки тільки вузол, який пропустив один із блоків, отримає вже наступного за ним та здійснить запит про недостатню інформацію, щоб заповнити очевидний пропуск.

5. Вузли, які отримали цей блок, проводять перевірку на коректність транзакцій і відсутність так званих подвійних витрат. Якщо блок не проходить перевірку, його відкидають.

6. Якщо досягається згода (висновок алгоритму консенсусу) щодо коректності блока, майнери починають працювати над новим блоком даних, заснованим на хеші тільки що доданого блока [17].

Варто уточнити, що всі транзакції здійснюються з криптографічним підтвердженням. В узагальненому варіанті цей процес представлено на рис. 1.1:

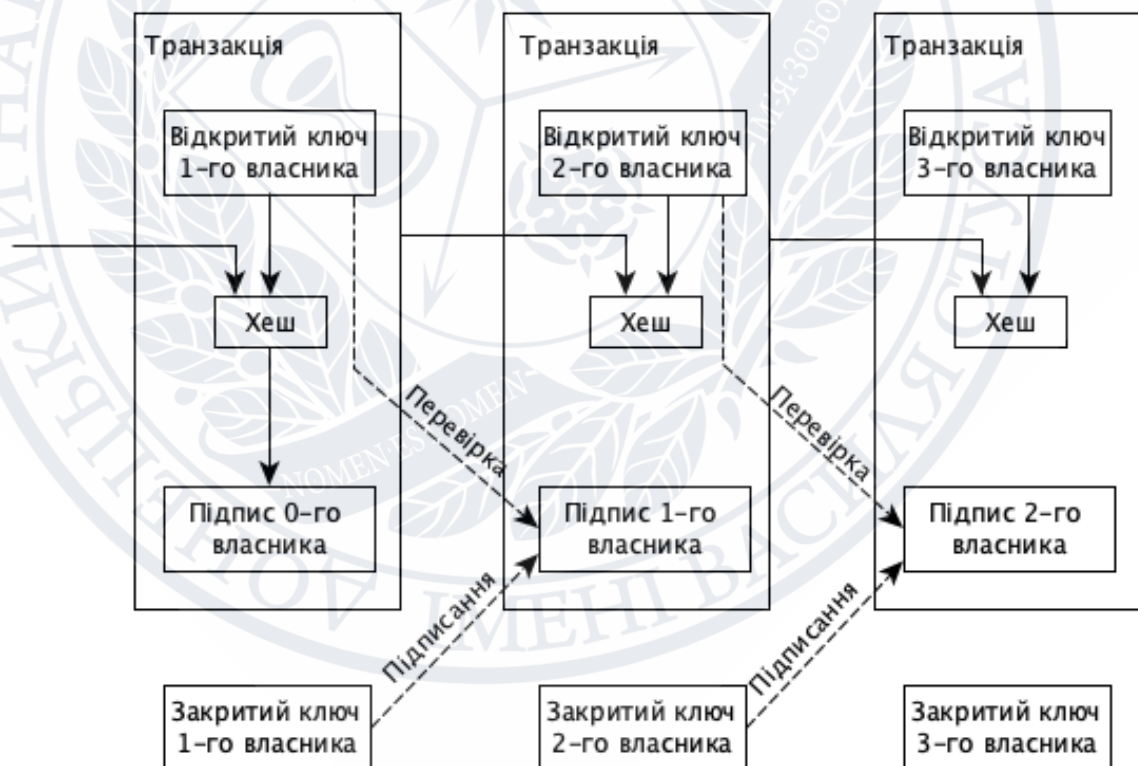


Рисунок 1.1 - Схема здійснення транзакції

[16, 17]

Кожен учасник мережі при реєстрації та встановленні потрібного програмного забезпечення на робочу станцію отримує набір із двох криптографічних ключів: закритого - для шифрування транзакції і відкритого - для верифікації транзакції. Кожен черговий учасник, відправляючи транзакцію наступному, підписує хеш попередньої транзакції і публічний ключ наступного й додає цю інформацію в кінець транзакції (рис. 1.2):

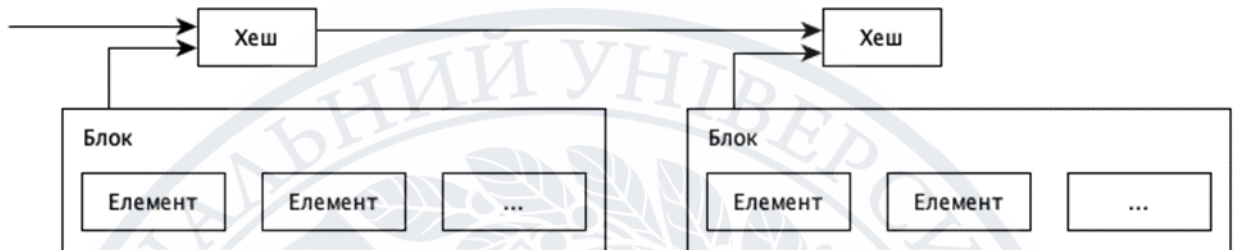


Рисунок 1.2 - Використання хешу попереднього блоку

[17]

Тобто, кожний наступний блок даних заснований на хеші попереднього блока. Таким чином, одержувач може перевірити весь ланцюжок транзакцій, перевібивши всі підписи попередніх учасників транзакцій [17]. У цій схемі хеш виступає масивом даних, який перетворений за допомогою хеш-функції. У результаті перетворення отримується практично унікальний, крім випадків колізій хешування, буквено-числовий рядок, який характеризує початковий елемент, який не може бути зміненим у зворотний бік.

Загальний вигляд блоків, в які майнери додають підтверджені транзакції та правила, за якими такі блоки додаються в ланцюжок блоків розподіленого реєстру, показано на рис. 1.3:

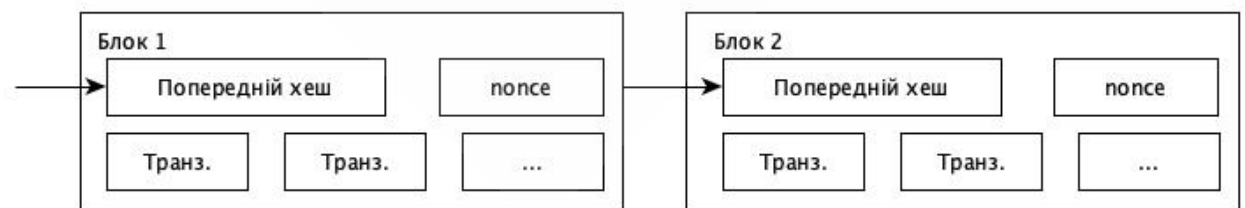


Рисунок 1.3 - Загальний вигляд блоків даних в розподіленому реєстрі

[16, 17]

Якщо один із майнерів намагається додати блок, який не відповідає цьому правилу, такий блок автоматично відхиляється іншими учасниками блокчейн-мережі. Щоб майнер зміг додати недійсний блок, потрібно змінити хеш усіх попередніх блоків, аж до так званого «генезис-блока» - першого блока в системі. Такий блок зазвичай задається розробниками системи. З цього виникає одна з істотних особливостей технології розподіленого реєстру - інформація, яка потрапляє в ланцюжок блоків, не може бути змінена постфактум.

Кожен блок містить велику кількість транзакцій. Буде дуже неефективно зберігати всі дані всередині кожного блоку у вигляді серії. Це зробить пошук будь-якої конкретної операції вкрай громіздким та займе багато часу. Для скорочення часу, необхідного для з'ясування приналежності конкретної транзакції до цього блоку, використовується принцип «дерева Меркла».

Дерево Меркла (або хеш-дерево) - це двійкове дерево, кінцеві вузли якого - це хеші транзакцій, а внутрішні вершини - результати складання значень пов'язаних вершин. Побудова дерева Меркла [18] відбувається наступним чином (рис. 1.4):

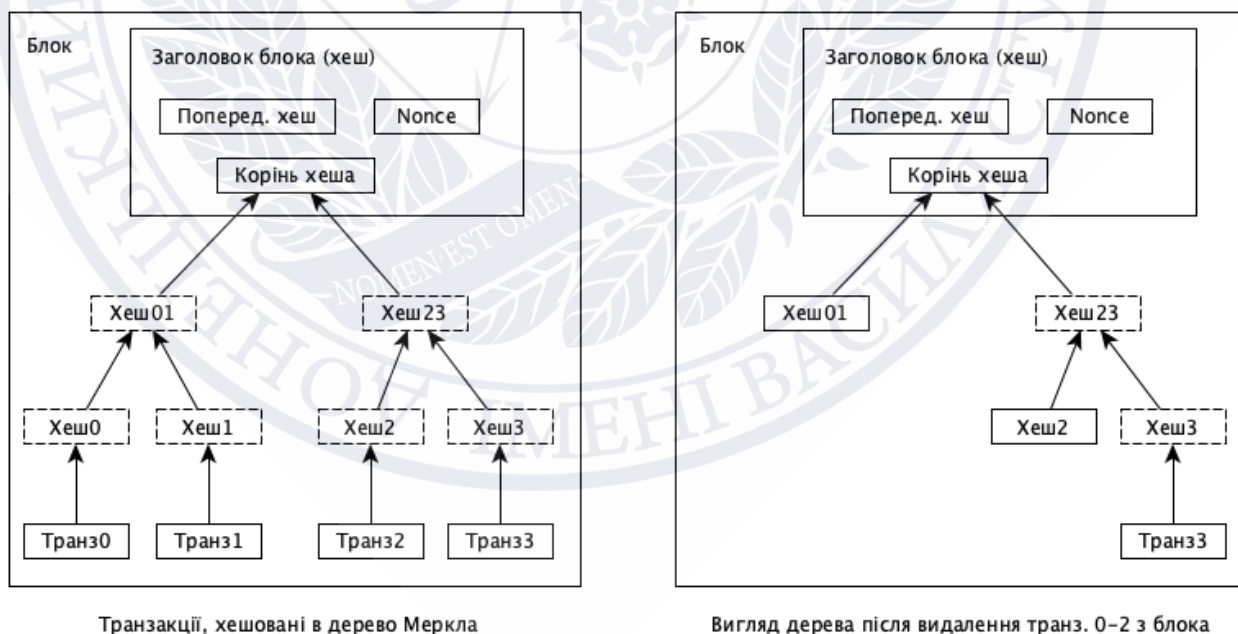


Рисунок 1.4 - Використання принципу «дерево Меркла»

[17, 18]

Обчислюються значення хеш-функції транзакцій, розміщених в блоці: Хеш0 (Транз0), Хеш1 (Транз1), Хеш2 (Транз2), Хеш3 (Транз3).

Обчислюються значення хеш-функції від суми хешів транзакцій:  $\text{Хеш0} + \text{Хеш1} = \text{Хеш01}$ ,  $\text{Хеш2} + \text{Хеш3} = \text{Хеш23}$ . Так як дерево Меркла є бінарним, то число елементів на кожній ітерації має бути парним. Тому якщо блок містить непарну кількість транзакцій, то остання дублюється і складається сама з собою.

Далі знову обчислюються хеш-кодування від суми хешів. Процес повторюється, доки не буде отримано єдиний хеш-корінь дерева Меркле (корінь хеша). Він є криптографічним доказом цілісності блоку (тобто того, що всі транзакції знаходяться в заявленому порядку). Значення кореня фіксується в заголовку блоку.

Щойно остання транзакція буде підтверджена достатньою кількістю блоків, то попередні транзакції можна видалити, оскільки всі транзакції хешуються в дереві Меркла, то щоб не розривати хеш блоку, в блок записується лише корінь дерева, після цього старі блоки можна згуртувати, видаляючи зайві гілки дерева Транз0, Транз1, Транз2 [17].

Використання дерев Меркла в «блокчейн»-системах дозволяє проводити спрощену верифікацію платежів (SPV) [17, 18], рис. 1.5:

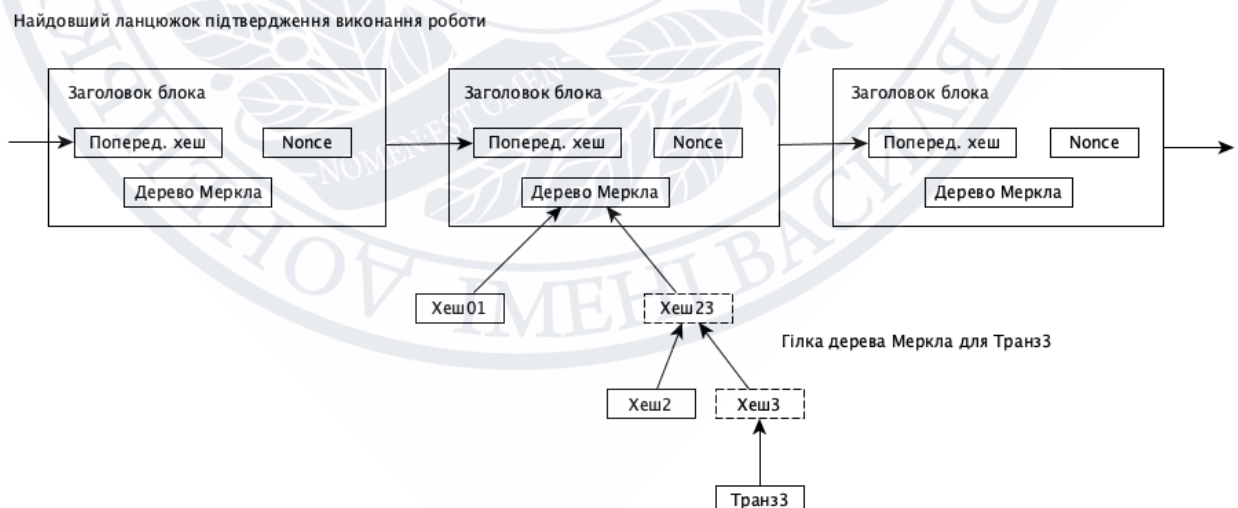


Рисунок 1.5 - Спрощена верифікацію платежів

[17]

Спрощену верифікацію платежів, називають легкими SPV-клієнтами (бо вони зберігають тільки заголовки блоків, а не їх вміст), для перевірки інформації про транзакції не перераховують всі хеші, а запитують доказ Меркла. Він складається з кореня дерева Меркла та гілки, що включає хеші від запитованої транзакції до кореня, оскільки клієнтові не потрібна інформація про інші операції. Склавши запитані хеш та порівнявши їх з коренем, клієнт переконується, що транзакція знаходиться на своєму місці. Такий підхід дозволяє працювати з великими обсягами даних, оскільки значно знижує навантаження на мережу, так як викачуються тільки необхідні хеші. Наприклад, вага блоку з п'ятьма транзакціями максимального розміру становить понад 500 кілобайт. Вага доказу Меркла в цьому ж випадку не перевищить 140 байт [18].

### 1.3. Особливості криптографічної хеш-функції в «блокчейні»

Криптографічна хеш-функція - це спеціальний клас хеш-функцій, який має властивості, необхідні для криптографічного захисту. Існують певні вимоги до властивостей криптографічної хеш-функції, щоб її застосування вважалося безпечним. В загальному випадку, хешування означає введення інформації будь-якої довжини і розміру в заданій стрічці і видачу результату фіксованої довжини заданої алгоритмом функції хешування. В контексті криптовалют, таких як біткоіни, транзакції після хешування на виході виглядають як набір символів заданої алгоритмом довжини.

Розглянемо процес хешування з використанням безпечного алгоритму хешування SHA-256 з сімейства SHA-2 розміром 256 біт, табл. 1.1:

Таблиця 1.1 - Результати хешування алгоритмом SHA-256

Вхідні дані (A)	Хеш (H)
Антон	dd96b10cdfb490fffbcd2bdb6a23c08c1dc3e54f39b3f80cd1436e9b836b87b4
Скирда	5709c73748e232a305f663b6aca567375a08925db260e2ce274b6f16e46834d0
криптографія	e696e7be7a39a4d56a5793f96b694bac4c8e0b6c1e8bc4095a65014f04084a3c

*Складено автором*

З табл. 1.1 видно, що в разі застосування SHA-256, незалежно від об'єму вхідних даних, отримане значення хешу завжди матиме фіксовану 256-бітну довжину. Це вкрай необхідна властивість для опрацювання великої кількості даних та транзакцій, яка дозволяє замість вистежування їх великих об'ємів, відстежувати їх хеш розміром 256 біт.

Існують вимоги до властивостей криптографічних хеш-функцій, для того щоб вони вважалися безпечними [19-22]:

*Властивість 1: детермінування.* Це означає, що незалежно від того, скільки разів ви аналізуєте певний вхід через хеш-функцію, ви завжди отримаєте той самий результат. Це важливо, тому що якщо ви будете отримувати різні хеші кожен раз, буде неможливо відстежувати введення.

*Властивість 2: швидке обчислення.* Хеш-функція повинна бути здатна швидко повертати хеш-вхід. Якщо процес не досить швидкий, система просто не буде ефективна.

*Властивість 3: Складність зворотного обчислення.* Складність зворотного обчислення означає, що з урахуванням  $H(A)$  неможливо визначити  $A$ , де  $A$  – вхідні дані,  $H(A)$  - хеш. При цьому «неможливо» не означає «нездійснено», але використовуючи зворотний алгоритм, не вийде.

*Властивість 4: навіть невеликі зміни вхідних даних змінюють хеш.* Внесення невеликих змін у вихідні дані, повністю змінюють їх хеш-значення (т.зв. «ефект лавини»). Результати перевірки цього ствердження відображені в табл. 1.2:

Таблиця 1.2 - Результати доказу, що зміни вхідних даних змінюють хеш

Вхідні дані (A)	Хеш (H)
Антон	dd96b10cdfb490fffbcd2bdb6a23c08c1dc3e54f39b3f80cd1436e9b836b87b4
антон	8487a6325840958d219d84329624176e86e78b218036e9e5ba36dda4c210cb4c
Скирда	5709c73748e232a305f663b6aca567375a08925db260e2ce274b6f16e46834d0
скирда	c2f6c1b51059d46b9d483cbcc0c471339de646ad4fbb7cf216e3c69ff2509d7a
криптографія	e696e7be7a39a4d56a5793f96b694bac4c8e0b6c1e8bc4095a65014f04084a3c
Криптографія	47ce0efded8266fc8a4f3ed911a626cf53f43284044d2994a1face12a9cb1d02

Складено автором

З табл. 1.2 видно, що навіть зміна регістру першої літери, повністю змінює значення вихідного хеш. Ця властивість хешування впливає на основну якість та перевагу «блокчейну» - його незмінність.

*Властивість 5:* колізійна стійкість. Для двох різних типів вихідних даних  $A$  та  $B$ , можуть бути обчислені відповідні хеш  $H(A)$  та  $H(B)$ , при цьому  $H(A)$  не може дорівнювати  $H(B)$ . Це означає, що в більшості випадків кожен вхід буде мати свій власний унікальний хеш з урахуванням існування т.зв. «парадоксу днів народження» [23].

*Властивість 6:* ступінь складності. Криптографічна хеш-функція повинна витримувати всі відомі типи криптографічних атак. Безпека хеш-функції може забезпечуватися складністю деякої математичної задачі при наявності доказу того, що атаки, спрямовані на порушення вимог до неї, настільки ж складні, наскільки й рішення цього завдання. Більшість існуючих доказово безпечних алгоритмів хешування занадто обчислювально складні для того, щоб широко використовуватися на практиці [22]. У порівнянні зі звичайними хеш-функціями вони досить повільні.

#### **1.4. Поняття та сутність цифрових валют**

*Цифрова валюта* - це електронний аналог звичайної валюти, яка існує у віртуальному форматі, без фізичного еквівалента в реальному світі, але має всі характеристики валюти. Як і класичні гроші, цифрову валюту можна отримувати, переводити або обмінювати на іншу валюту, оплачувати нею товари та послуги. Цифрова валюта не має державних кордонів: гроші з електронного гаманця, що відповідає цій валюті, можуть бути переведені звідкіль завгодно і куди завгодно.

*Криптовалюта* є різновидом цифрової валюти. Це актив, який використовується як засіб обміну і вважається надійним, тому що в його основу покладено криптографію, технологію «блокчейн» і розподілений реєстр. При її створенні використовується особливий криптографічний код-шифр, який

складається з послідовного хешування транзакцій та електронного цифрового підпису [24].

Проте між криптовалютою та цифровою валютою можна виділити фундаментальні розбіжності [21]:

*1. Цифрова валюта централізована.* Платіжна система цифрової валюти передбачає наявність центрального органу, який контролює мережеві транзакції. Цей орган може скасувати або заморозити транзакцію на вимогу, чи в разі підозри шахрайства або незаконної операції. Платіжна система криптовалюти має пірингову архітектуру (P2P), тобто вся система, що забезпечує здійснення транзакцій і збереження інформації про них, заснована на децентралізованій комп'ютерній мережі. Не існує центрального сервера, який вів би облік усіх транзакцій криптовалюти. Вся інформація про транзакції зберігається на тисячах серверів, причому на кожному з них зберігається повна копія реєстру, що включає всі транзакції криптовалюти, здійснені будь-коли і будь-де. Таким чином, безліч комп'ютерів по всьому світу утворюють гігантську автоматичну, працюючу цілодобово електронну платіжну систему. Децентралізація підвищує рівень безпеки криптовалюти, оскільки якщо й можна допустити можливість зловмисного втручання в роботу якогось одного центрального органу управління, то будь-які спроби внесення змін на окремі вузли розподіленої системи просто безглузді: доведеться зламати тисячі комп'ютерів одночасно, а не один центральний сервер. Додавання або видалення транзакцій у розподіленій системі повинні бути прийняті всіма вузлами розподіленої мережі, в іншому випадку вони відкидаються. Таким чином, децентралізація і застосування розподіленого реєстру в обліку криптовалюти є важливим аспектом безпеки самої криптовалюти.

*2. Цифрова валюта не підтримує анонімність.* Для користування цифровою валютою потрібна ідентифікація користувача в платіжній системі та реєстрація певних документів, виданих банками або державними структурами. При цьому встановлюється особа, що здійснює операцію з валютою. Для покупки, продажу, інвестування і будь-яких інших маніпуляцій з криптовалютою ніякої реєстрації

особистості не потрібно, непотрібно також вказувати будь-якого роду особисті дані відправника та отримувача коштів. Для здійснення транзакції необхідно знати тільки публічний ідентифікатор одержувача (номер гаманця для криптовалюти), який може змінюватися для кожної транзакції.

Для запобігання шахрайству при транзакціях використовується електронний цифровий підпис (ЕЦП) власника криптовалюти. Підписуючи передання прав з використанням ЕЦП, власник бере на себе зобов'язання передання. Алгоритми ЕЦП, що застосовуються при переданні криптовалюти, не відрізняються від алгоритмів ЕЦП, застосовуваних у банківській та інших економічних сферах, рис. 1.6:



Рисунок 1.6 - Механізм дії електронного цифрового підпису

Різниця в застосуванні тут полягає в тому, що при перевірці підписаних ЕЦП транзакцій в банківській сфері встановлюється, крім іншого, й особистість власника ЕЦП [26] (за даними, що містяться в сертифікаті). При перевірці ЕЦП транзакцій криптовалюти визначається тільки номер електронного гаманця власника криптовалюти, сам же власник залишається невідомим. З точки зору захисту персональних даних, анонімність також може розглядатися як елемент технології безпеки.

*3. Цифрова валюта непрозора.* Інформація про транзакції цифрової валюти конфіденційна і відповідно недоступна для публічного перегляду. Транзакції криптовалюти навпаки прозорі. Можна побачити список транзакцій будь-якого власника криптовалюти, знаючи його публічний (відкритий) ключ ЕЦП, оскільки всі його дії з криптовалютою фіксуються в «блокчейні». Більш того, для криптовалюти виключено шахрайство, пов'язане з транзакцією неіснуючих активів, оскільки за будь-якої транзакції передаються і відповідно перевіряються платіжною системою криптовалюти всі надходження і витрати з електронного гаманця, з якого здійснюється транзакція. Власник електронного гаманця не може передати з нього суму більшу, ніж він отримав на нього з підтверджених системою транзакцій. Така технологія насамперед є технологією, що забезпечує безпеку використання криптовалюти.

Надійність та безпека функціонування платіжної системи криптовалюти заснована на використанні криптографічних методів. Можливо, завдяки домінуючій ролі криптографії у платіжній системі криптовалюти і з'явився префікс «крипто» в назві цього виду цифрової валюти.

Платіжні системи більшості криптовалют, що використовують технологію «блокчейн» децентралізовані та функціонують на вузлах розподіленої мережі, що підтримують цю систему. За такої архітектури, система для зберігання виконаних транзакцій використовується ланцюжок блоків (блокчейн). Кожен блок такого ланцюжка містить заголовок і обмежений список транзакцій. У заголовку записані параметри, серед яких є хеш-значення попереднього блоку. Сам попередній блок має точно таку ж структуру: заголовок з хеш-значенням

відповідно попереднього блоку і список попередніх транзакцій і т.д. Таким чином, весь ланцюжок блоків зберігає всі транзакції за весь час роботи платіжної системи. Безпеку такого зберігання можна проаналізувати, якщо детальніше розглянути роботу платіжної системи.

Платіжна система криптовалюти на основі технології «блокчейн» працює за сценарієм [21], представленим на рис. 1.7:



Рисунок 1.7 - Сценарій роботи платіжної системи криптовалюти

[27]

Умовний покупець, маючи намір відправити гроші умовному продавцю, передає інформацію про транзакцію у мережу платіжної системи, яка розсилає запис про транзакцію усім вузлам мережі у вигляді «блоку». Кожен вузол мережі об'єднує транзакції, що прийшли за певний період у блок і обчислює хеш-значення всього блоку, яке повинно задовольняти заданому рівню складності. Як тільки хеш-значення із заданим рівнем складності для всього блоку транзакцій буде обчислено, вузол мережі, який виконав це, відправляє тепер уже новий блок транзакцій у розподілену мережу. Вузли (учасники) мережі перевіряють блок і транзакції усередині нього на валідність і приймають цей блок, тільки якщо всі транзакції в ньому коректні та не використовують уже витрачені кошти. Свою згоду з новими даними вузли висловлюють, починаючи роботу над наступним

блоком, використовуючи хеш-значення попереднього блоку. Підтверджена транзакція додається до загального «ланцюга». Умовний продавець отримує гроші.

За такої схеми роботи платіжної системи, щоб ввести зміни в якусь транзакцію в блоці без втрати довіри до нього з боку всієї мережі, потрібно буде забезпечити незмінність хеш-значення всього блоку. А це практично неможливо, так як використовується криптографічно стійка хеш-функція для отримання хеш-значення всього блоку. Щоб платіжна система прийняла блок транзакцій зі зміненим хеш-значенням усього блоку, потрібно буде змінити хеш-значення і в подальшому блоці, в заголовку якого міститься інформація про хеш-значення попереднього блоку і т.д. Таким чином, для того, щоб поміняти інформацію про транзакції в одному з блоків, потрібно буде регенерувати весь ланцюжок блоків. Імовірність реалізації такої процедури незначна і сильно корелює з обчислювальною потужністю мережі біткойн, яка нині перевищує обчислювальні ресурси гіпотетичної мережі з 500 найпотужніших суперкомп'ютерів, наявних у світі [21].

## РОЗДІЛ 2

### АНАЛІЗ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЇ РОЗВИТКУ «БЛОКЧЕЙН» ТА ЦИФРОВИХ ВАЛЮТ

#### 2.1. Огляд глобального ринку

За даними [28] аналітичного агентства International Data Corporation, в 2021 році на технології «блокчейн» витрачено не менше 6,6 млрд доларів, що більше на 50% ніж в минулому році. Така тенденція до високого росту збережеться - за період з 2020 по 2024 середньорічні темпи зростання складуть 48%. Ключовими варіантами використання «блокчейна» в 2021 році залишаються транскордонні платежі та розрахунки, а також рішення, пов'язані з визначенням перевірки походження продукту, його справжності при переміщенні його по ланцюжку формування цінності. Банки забезпечують майже третину всіх витрат на «блокчейн» в 2021 році. На технологічне та дискретне виробництво в сумі доводиться не менше 20% світових інвестицій. Кращі результати зростання показують професійні послуги (CAGR 56,0%), витрати місцевих, центральних органів влади (CAGR 53,0%), охорону здоров'я (CAGR 52,7%), на IT-послуги та бізнес-послуги приходить дві третини загальних витрат.

За оцінками [29] аналітичної компанії Novum Insights, інвестиції в «блокчейн»-індустрію досягли позначки 2,4 млрд. доларів - на 340% вище аналогічного показника за попередній рік, при цьому 25% цих коштів залучено через венчурні фонди, інші 75% - засобом первинного розміщення цифрових монет (ICO).

США в 2021 році залишаються найбільшим ринком: на пов'язані з «блокчейном» рішення витрачено близько 2,6 млрд доларів, Західна Європа (1,6 млрд дол.), Китай (777 млн. дол.), один з кращих середньорічних показників зростання (CAGR 50,0%) в Центральній та Східній Європі [28].

Станом на квітень 2021 року налічується 5058 криптовалют, а їх загальна ринкова капіталізація складає 2 057 395 854 548 доларів США [30, 31].

## 2.2. Еволюційний розвиток

За час свого розвитку, технологія «блокчейн» пройшла декілька етапів [9, 16, 32-34], які характеризуються як перше та друге покоління, в теперішній час третє покоління знаходиться в процесі свого становлення [9, 32, 34], а окремі автори [33, 41] вже виділяють появу четвертого покоління технології.

До першого покоління «блокчейн» (т.зв. Blockchain 1.0) відносять «класичний блокчейн» криптовалюти біткоїн. Він характеризується алгоритмом консенсусу по виконаній роботі (протоколу Proof-of-Work, «доказ виконаної роботи»). Відкритий ключ електронного підпису зберігається в попередньому блоці і захищений хеш-функцією (закритий ключ знаходиться в новому блоці). Ключовою особливістю «блокчейн» першого покоління є виконання транзакції в мережі по протоколу Proof-of-Work. Архітектура першого покоління здатна виконувати лише прості транзакції та характеризується швидко деградуючою продуктивністю.

Другим поколінням «блокчейн» (т.зв. Blockchain 2.0) є «блокчейн» криптовалюти Ethereum. Її розробник, Віталій Бутерін, запропонував ідею смарт-контрактів (англ. smart contract). Смарт-контракти - це додатки у сфері економіки, ринків і фінансів, що працюють з різними видами інструментів: акціями, облігаціями, ф'ючерсами, заставними, правовими титулами, активами і контрактами), та мають алгоритми автоматичної перевірки виконання договірних зобов'язань та логічних умов. Це дозволило застосувати «блокчейн»-системи в нових галузях діяльності аніж криптовалюти та створювати принципово нові прикладні програми. В другому поколінні технології використовується протокол Casper, ключова особливість якого - зміна алгоритму консенсусу: замість протоколу Proof-of-Work (PoW, «доказ виконаної роботи») використовується протокол Proof-of-Stake (PoS, «доказ володіння»). Швидкість транзакцій збільшена до 30 в секунду.

Особливістю «блокчейн»-систем третього покоління (т.зв. Blockchain 3.0), як вважають окремі автори [35], є застосування ациклічного графа замість «блокчейна» або спільно з «блокчейном». У криптосистемах ациклічного графа

транзакції здійснюються миттєво, оскільки їх не треба збирати у блоки. Структура називається DAG (англ. directed acyclic graph, «направлений або орієнтований ациклічний граф») - це структура блоків з топологічним деревом в основі. Блоки можуть підтверджувати не одну, а декілька транзакцій, що допомагає уникнути так званої «подвійної витрати». Ациклічні графи застосовуються, наприклад, в криптосистемі для промислового інтернету IOTA, що займає зараз 16-е місце по ринковій капіталізації (896 млн. доларів). Досягнута швидкість 1000 транзакцій в секунду. У криптосистемах третього покоління застосовується алгоритм консенсусу Delegated Proof-of-Stake (DPoS, «делегований доказ володіння»). За цим алгоритмом блоки, що підтверджують консенсус, визначаються голосуванням з розділенням на дві групи: учасник використовують свої токени для того щоб обрати валідаторів (англ. valid, «дійсний, маючий силу, правомірний»), які за винагороду здійснюють перевірку та додавання блоків транзакцій. Таким чином, учасники мережі, які мають право голосу (або власники цифрових монет), не є при цьому валідаторами транзакцій, до того ж валідатори повинні розкрити свою особистість (перестати бути анонімними учасниками) та надати гарантії безперебійної підтримки роботи вузлів мережі та своєчасної верифікації транзакцій та формування нових блоків. Однією з новацій у складі третього покоління «блокчейн» є використання «шардінгу» (англ. shard, «осколок, шматочок») при створенні розподіленої системи, тобто сегментація розподіленої бази даних на невеликі фрагменти (шматки) [33, 36]. На відміну від класичного зараз способу зберігання на кожному вузлі повної копії бази даних, технологія «шардінгу» пропонує зберігати на окремих нодах тільки фрагмент бази даних. Повна база формується як мозаїка, що складається з усіх фрагментів, що окремо зберігаються. «Шардинг» істотно збільшує продуктивність системи [33].

Широке використання та розвиток технології третього покоління виявив наявність т.зв. «трилемми» «блокчейн» [37]. Ця «трилемма» характеризує внутрішнє обмеження «блокчейн», що не дозволяє йому бути одночасно

продуктивним, розподіленим та залишатися безпечним. Досягнення будь-яких двох цілей суперечить третій.

До четвертого покоління «блокчейн» (т.зв. Blockchain 4.0) відносять платформу Seele, бета-версію 1.0 якої впроваджену в експлуатацію 31.03.2019. Платформа підтримує управління різними сценаріями для бізнесу та інтернету речей. До нових рішень платформи Seele можна віднести наступні [33, 38, 39]:

1. Застосований новий, спеціально розроблений алгоритм NCA (англ. neural consensus algorithm, «алгоритм нейронного консенсусу»), який істотно підвищує безпеку системи. Алгоритм працює за принципом зорового аналізатора людини: спочатку охоплюється уся картина, а потім вона деталізується. Застосування нового протоколу також дозволить на 30-40% прискорити роботу мережі [39].

2. Застосований спеціально розроблений для платформи Seele швидкісний транспортний протокол інтернету QVIC та протокол VHTTP для мережі «передачі цінностей».

3. Платформа містить різні «блокчейн»-системи, які можна спеціалізувати для вирішення різних завдань, у тому числі: контроль виконання фінансових операцій, управління підприємством, зберігання прав власності, авторських прав, прав на мультимедіа-контент, управління бездротовим зв'язком, у тому числі супутниковим. На платформі Seele можливий інформаційний зв'язок між ланцюжками блоків різних «блокчейнів». Заявлена швидкість роботи платформи складає 1 млн транзакцій в секунду.

Стартап MetaHash стверджує [41] про використання Blockchain 4.0, який заснований на протоколі TraceChain, що працює в режимі реального часу, та побудований на автоматичному самонавчальному протоколі маршрутизації сигналів. Заявлено про початкову швидкість в 50 000 транзакцій в секунду, що дорівнює швидкості в платіжних системах Visa та MasterCard.

Проте, на сьогодні попередні випробування проєктів Seele, MetaHash ще не завершені, що ускладнює оцінку декларованих можливостей та ефективності технології «блокчейн» четвертого покоління.

### 2.3. Галузі використання технології

Технологія «блокчейн» стрімко розвивається не тільки в сфері розвитку та обігу криптовалют, але й в інших галузях, які прагнуть скоротити витрати, підвищити ефективність та відмовитися від застарілої інформаційної інфраструктури.

*Міжнародні платежі.* Спрощення платежів є дуже вигідним для банків: у 2019 році транскордонні транзакції принесли 224 мільярди доларів доходів від платежів [42]. Саме технологія «блокчейн» пропонує безпечний та дешевий спосіб надсилання платежів, що скорочує необхідність перевірки від третіх сторін і перевершує час обробки для традиційні банківські перекази. Компанія Blockchain Ripple співпрацює з понад 300 клієнтами, включаючи такі фінансові установи, як Santander та Western Union, з метою підвищення ефективності транскордонних платежів [42]. Продукт xCurrent надає банкам двосторонній протокол зв'язку, що дозволяє обмінюватися повідомленнями та здійснювати розрахунки в режимі реального часу. Компанія R3, забезпечує використання технології «блокчейн» центральним банком Швейцарії для пілотного розрахунку великих операцій між фінансовими установами з використанням цифрових валют [42]. Таким чином, «блокчейн» ідеально підходить для сфери фінансів та, зокрема, для проведення міжнародних платежів. Процес міжнародних переказів, який зазвичай займає велику кількість часу, коштів і сторін-учасниць, завдяки «блокчейну» значно скорочує час транзакцій, витрати, а також заміняє складні інформаційні структури. Так, у вересні 2016 британський банк Barclays і стартап Wave провели першу успішну торгову угоду з використанням «блокчейна» [43]. Більш того, багато представників фінансового сектора об'єднуються в альянси та консорціуми, такі як EEA, R3 і Hyperledger, для розвитку і впровадження «блокчейн»-рішень в своєму секторі [42]. В березні 2020 року банк Credit Suisse почав співпрацювати з стартапом Paxos по використанню технології «блокчейн» для врегулювання торгівлі акціями США. JPMorgan Chase увійшов у «блокчейн»-простір разом з монетою JPM, яку він збирається використовувати для полегшення транзакцій між інституційними рахунки. Інші банки, такі як

Goldman Sachs та Citigroup, також експериментують з «блокчейном»: у лютому 2020 року здійснили обмін акціями в системі, що побудована на «блокчейні» Axoni Axcore [42].

*Мікроплатежі.* Використання «блокчейн» для здійснення мікроплатежів вважається одним із самих перспективних напрямків [29]. Наприклад, до недавнього часу платежі розміром в долі centa були занадто скрутними та не вигідними для користувачів Інтернету. Застосування додатків на основі «блокчейн» робить такі платежі можливими та практичними. Вони дозволяють ефективно монетизувати соціальні мережі, а також зробити їх альтернативним способом плати за невеликі роботи, такі як, заповнення опитувань або позаштатне редагування для різних клієнтів. Аналітики фінансових ринків вважають, що система мікроплатежів дуже прибутковий та перспективний проект у світі бізнесу. Так, фінансова компанія Wedbush Securities прогнозує [42] розмір биткоїн-мікроплатіжного ринку на рівні 925 млрд. доларів до 2025 року.

*Управління ідентифікаційною інформацією.* Сервіси управління ідентифікаційною інформацією дозволяють користувачам переносити персональні дані на «блокчейн», тим самим створюючи цифровий ідентифікатор особистості (digital identity). Таким чином, у користувачів з'являється широкий інструментарій для зберігання такої інформації, як: паспортні дані, свідоцтва про народження та шлюб, водійські права, посвідчення особи, логіни і паролі та інші персональні дані. А за допомогою «блокчейн», користувач може вибирати, якою інформацією ділитися та хто саме може мати до неї доступ. Більш того, пройшовши процес ідентифікації особистості один раз, користувач зможе авторизуватися в мережі та в інших сервісах без повторного введення інформації. У 2017 році консалтинговий гігант Accenture і найбільша ІТ-корпорація Microsoft об'єдналися для розробки і впровадження «блокчейн»-платформи, за допомогою якої більше 1 мільярда людей по всьому світу отримають діючі посвідчення особи [43]. Крім цього, на станом на початок 2021 року вже існує 20 компаній, що надають різні послуги в галузі управління персональною ідентифікаційною інформацією [43, 44].

*Цифрові активи та токенизація.* Цифровим активом вважається будь-який актив, який представлений в цифровому форматі. Такі активи зберігаються на будь-якому носії: від комп'ютера та мобільних пристроїв до медіаплеєра. У свою чергу, токенизація - це процес перекладу прав на актив в токен, цифровий «двійник» якого зберігається в реєстрі «блокчейн». Оскільки токенизація відбувається з використанням технології «блокчейн», то компанії можуть ввести нову систему управління активами, що дозволяє підвищити ліквідність, надати можливість управління активами всім учасникам, застосовувати сценарії колективного використання, ефективно інтегрувати такі компоненти традиційного ринку цінних паперів, як депозитарій, фондову біржу, розрахунковий центр, програмне забезпечення. Так, стартапи Vaultoro, OneGram і Orebits займаються токенизацією фізичного та сертифікатного золота, де користувачі за криптовалюту можуть придбати цифрові активи на даний дорогоцінний метал. Компанія LAToken забезпечує токенизацію цінних паперів та акцій через протокол LAT Protokol, який дозволяє токенизувати права на активи та здійснювати торгівлю ними за криптовалюту. Міжнародна «блокчейн»-платформа Atlant дозволяє токенизувати об'єкти нерухомості з подальшим розміщенням токенів ATL на децентралізованих біржах [43].

*Захист авторського права.* Порухення авторських прав вважається однією з найбільших проблем у таких сферах творчості, як мистецтво, музика, кіноіндустрія та література. Застосування «блокчейн» дозволяє авторам підтверджувати та захищати авторські права, права володіння інтелектуальною власністю. Більш того, технологія дозволяє забезпечити безпечне зберігання та оперативне оновлення інформації про будь-яких об'єктах. Так, компанія Ascribe завдяки застосуванню «блокчейну» допомагає художникам підтверджувати своє авторське право на створені предмети мистецтва за допомогою унікальних ідентифікаторів та цифрових сертифікатів. Також передбачена передача права володіння від художника або автора до покупця або колекціонера. Проект SingularDTV запускає децентралізовану систему поширення цифрового

відеоконтенту на блокчейне Ethereum, який дозволить користувачам розміщувати свої твори, монетизувати та управляти їх розповсюдженням [43].

*Смарт-контракти.* Смарт-контракти (англ. smart contract, «розумний контракт») – це різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання та розірвання яких можливо лише з використанням комп'ютерних програм («блокчейн»- платформ) в рамках мережі Інтернет. Вони дозволяють укласти т.зв. «самовиконувані» контракти на «блокчейні». Такий вид контрактів ідеально підходить для використання в комерційних угодах, оскільки вони гарантують переказ коштів або якихось інших дій, як тільки всі сторони виконають всі зазначені в контракті зобов'язання. Смарт-контракти не потребують участі посередників і виконуються автоматично, що робить їх особливо зручним інструментом для стартапів. Проект JoyToken розробив протокол інфраструктури для ігрової індустрії, де смарт-контракти використовуються для забезпечення безпеки, можливості ведення записів і проведення аудиту. А міжкорпоративна платформа Jincor дозволяє будь-якому бізнесу використовувати смарт-контракти та кріптовалютні платежі без будь-яких спеціальних технічних знань і великих фінансових витрат. Також, згідно з звітом консалтингової компанії Deloitte, страхова галузь активно працює над впровадженням смарт-контрактів, які дозволять знизити витрати, підвищити ефективність і автоматизувати велику частину процесів. Використовуючи «блокчейн» як сховище, представники ринку страхування можуть сформувати єдину і глобальну базу страхових контрактів і заяв. Найбільшу в світі реалізацію смарт-контрактів здобула DAO, розподілена автономна організація для венчурного фінансування, яка була запущена у травні 2016 року [42-46].

*Інтернет речей.* Інтернет речей (англ. Internet of Things, IoT) являє собою клас пристроїв M2M (англ. machine-to-machine, «від машини до машини»), які можуть обмінюватися будь-яким видом даних між собою, тим самим створюючи мережу взаємодії. Використання «блокчейна» може гарантувати збереження та цілісність даних в IoT, а також забезпечувати надійну систему безпеки. Компанія Chronicled в серпні 2017 року запустила «блокчейн»-платформу [43] для

інтернету речей, що дозволяє компаніям та виробникам реєструвати та підтверджувати фізичні предмети в «блокчейн»-мережі. Компанія Filament пропонує [43] ряд власних програмних та апаратних рішень для управління промисловими системами і обладнанням. В основі розробок компанії лежать принципи децентралізації, криптографічного захисту та автономності. Щодо M2M-систем, то згідно із прогнозом GSMA, до 2025 року кількість підключень «розумних пристроїв» досягне майже 25 млрд по всьому світу [15].

*Організація «електронних урядів» та систем голосування.* У світі близько 192 країн намагаються впроваджувати в державні структури «блокчейн»-технологію, серед них Швеція, Грузія, Бразилія і Естонія [44]. Останні кілька років уряд Естонії розробляв платформу для ідентифікації людей, які не є громадянами країни, - e-Residency. Учасники проекту ставали так званими електронними резидентами і отримували можливість верифікувати документи і користуватися послугами електронного банкінгу та іншими сервісами, які доступні естонцям. Тепер розробники e-Residency впроваджують «блокчейн» в інфраструктуру проекту, щоб підвищити його захищеність. Розподілені реєстри здатні перетворити практично кожен аспект урядової діяльності. Наприклад, стати основою для систем голосування. На початку 2018 року американська біржа Nasdaq успішно застосувала систему e-Voting для голосування акціонерів компанії [44]. Вибори з застосуванням «блокчейн»-технологій схожі на кріптовалютну угоду, але з використанням спеціальних «забарвлених» монет, які виборці переводять на рахунок обраного ними кандидата. Для визначення переможця досить перевірити рахунки після закінчення виборів. Так як публічний «блокчейн» прозорий, долю свого голосу може відстежити будь-який користувач. Також системи для електронного голосування дозволяє створювати платформа Exonum [43]. Стартап Voatz, пропонує мобільну платформу голосування, побудовану на «блокчейн» [43]. Дана платформа забезпечує безпечний облік голосів та гарантує справжність результатів. Платформу вже використовують кілька університетів, політичних груп та некомерційних організацій для проведення внутрішніх голосувань. Також платформа Follow My

Vote представляє програмне забезпечення з відкритим вихідним кодом на «блокчейні», яке дозволяє користувачам проводити електронні голосування і брати участь в них. Системи голосування з використанням технології «блокчейн» використовують [43]: датська партія Liberal Alliance для внутрішнього голосування, Лібертаріанська партія США штату Техас для голосування за кандидатів на внутрішньопартійні посади, Республіканська партія США штату Юта в ході голосування за кандидатів на етапі «праймеріз», біржа NASDAQ за підтримки місцевого уряду провела голосування серед власників акцій в Естонії.

*Анонімна передача повідомлень.* Стартапом Obsidian запропоновано [43] використання технології «блокчейн» для безпечного обміну інформацією в чатах, месенджерах та соціальних мережах. На відміну від WhatsApp та iMessage, які використовують кінцеве шифрування, Obsidian застосовує «блокчейн» для забезпечення збереження метаданих користувачів, таких як пошта, номери телефонів або будь-яких інших ідентифікаторів особистості. Замість цього платформа Obsidian використовує випадкові метадані з розподіленого реєстру і, таким чином, гарантує конфіденційність користувачів та їх повідомлень. Схожі за функціоналом послуги пропонують компанія Embedded Downloads (додаток Embedded Messenger) та стартап-додаток Chain-chat Blockchain messenger [43].

*Боротьба з DDoS-атаками.* Згідно щоквартальним звітів Kaspersky Lab, збільшилася тривалість і складність DDoS-атак, за цими даними, у другому кварталі 2017 року зафіксована безпрецедентно найдовша атака, яка тривала 227 годин [43]. Експерти відзначають [36, 46] зростання кількості атак, спрямованих на майданчики, які проводять ICO (англ. initial coin offering, «первинна пропозиція монет, первинне розміщення монет» - форма залучення інвестицій в нові технологічні проекти та стартапи у вигляді емісії та продажу інвесторам нових криптовалют). Блокчейн-стартап Gladius розробив проект по запуску децентралізованої тимчасової мережі, що працює без головного сервера, та яка забезпечує захист від DDoS атак [43]. Gladius дозволяє користувачам монетизувати невикористану пропускну здатність своїх інтернет-мереж,

об'єднуючи їх в децентралізовану CDN (англ. Content Delivery Network, «мережа розповсюдження контенту»). Завдяки високій пропускній здатності та географічному розподілені ця мережева інфраструктура нівелює DDoS-атаки, а користувачі можуть автоматично підключатися та переключатися до різних безпечних пулів захисту.

*Медицина та охорона здоров'я.* В 2018 році дослідницьке агентство Institute for Business Value провело опитування [44] в 16 країнах серед 200 керівників організацій охорони здоров'я. Порядку 72% з них зазначили, що управлінські плани розвитку містять впровадження рішень на базі технології «блокчейн» - до 2020 року, при цьому 16% вже використовують «блокчейн»-рішення в своїй роботі. «Блокчейн» дозволяє виключити випадки підробки медикаментів та оптимізує процеси їх перевезення, оскільки на кожному етапі постачання походження препарату легко перевірити. Розподілені реєстри також формалізують та убезпечать процес обміну медичними записами, допомагають захистити важливу інформацію від хакерів та надати пацієнтам більше контролю над своїми показниками здоров'я. Наприклад, станом на 2020 рік, в Бостоні працюють 26 різних систем управління електронними медичними записами, кожна з яких по-своєму уявляє і передає дані. Важлива інформація (наприклад, відомості про алергічні реакції на препарати у пацієнта) часто «розкидана» між декількома базами і іноді виявляється недоступною в критичні моменти. За словами Джона Халамки (John Halamka) [44], технічного директора Beth Israel Deaconess Medical Center, в рішенні цих проблем допоможе «блокчейн». Тому Халамка спільно з вченими з MIT Media Lab розробили платформу MedRec, засновану на Ethereum. Система використовує смарт-контракти для підкріплення всіх операцій: контракт Patient-Provider Relationship Contract (PPR) укладається між двома вузлами системи, коли один з них керує медичними записами другого (зокрема, коли відбувається зміна списку призначених препаратів для хворого). Контракт Summary Contract (SC) дозволяє пацієнтам переглядати історію медичних записів. В Естонії з 2008 року всі госпіталі та лікарні країни повинні переводити інформацію про здоров'я населення в цифровий формат,

забезпечення безпечного зберігання якого побудовано з використанням «блокчейн». Розподілений реєстр виступає в якості бази даних для медичних записів. Коли в медичну карту пацієнта вносяться зміни, ця подія відразу записується в мережу, разом з інформацією про те, що саме було змінено, видалено, додано. Такий рівень прозорості дозволяє терапевтам, хірургам, фармацевтам і іншим фахівцям отримати актуальну та коректну інформацію про пацієнта, з якої «згідно» співтовариство. Система дає можливість ставити більш точні діагнози з урахуванням повністю задокументованої історії хвороби, направляти дії лікарів в кризових ситуаціях (наприклад, надавати інформацію про алергічні реакції на ліки) і навіть коригувати лікування при хронічних хворобах з плином часу (в залежності від зміни стану пацієнта). Додатково до медичної інформації на «блокчейні» можуть звертатися страхові компанії або відділення поліції, відповідальні за видачу водійських посвідчень. У 2015 році органи управління дорожнім господарством Естонії отримали доступ до 80 тис. медичних карт жителів країни, які прийшли обміняти водійські посвідчення, щоб підтвердити їх стан здоров'я. Компанією Nashed Health розроблено систему перевірки облікових даних, засновану на «блокчейні», для медиків, щоб довести, що вони мають ліцензію на лікарську діяльність у певних областях [42].

За даними [45] міжнародної аналітичної корпорації IDC Health Insights до 2021 року технологія «блокчейн» надійно закріпиться в сфері охорони здоров'я, а використання розподіленого реєстру допоможе:

1. Виключити втрату, фальсифікацію і передачу третім особам медичних документів.
2. Перевіряти та проконтролювати ланцюжки постачання медикаментів від фірми-виробника (або постачальника) до точок збуту.
3. Забезпечити необхідними даними про пацієнта лікарів з будь-якої точки світу. Інформація синхронізується між комп'ютерами, тому в разі потреби та з дозволу пацієнта кожен медик швидко отримає доступ до потрібних аналізів та діагнозів.
4. Автоматизувати робочі процеси медичного закладу будь-якого типу.

5. Прискорено виносити рішення по страхових випадках та іншим спірним ситуаціям за станом організму пацієнта.

*Нотаріальна справа.* Збіг та схожість функцій нотаріусу (збереження, захист, автентифікація даних клієнтів, гарантування достовірності та прозорості укладених угод) та функцій технології «блокчейн» (збереження даних у відкритому реєстрі, їх захист від знищення, крадіжки, спотворення, неправомірної зміни шляхом криптографічного шифрування, підтвердження достовірності угод та гарантії незмінності інформації, забезпечення довіри та прозорості при укладенні договорів), розкривають широкі можливості застосування технології в нотаріальній справі.

Технологія «блокчейн» здатна зменшити об'єми робіт нотаріусів по архівації та тим самим підвищити їх продуктивність. Нотаріуси за допомогою програми для ПК або додатку для смартфона зможуть відкривати клієнтам цілодобовий доступ до всіх даних, а клієнти у свою чергу, при необхідності, зможуть надавати доступ до окремих документів медичним працівникам, адвокатам або членам родини.

Нотаріальна Палата міста Париж у співробітництві з компанією Digitalberry в 2019 році запустила пілотний проект ведення нотаріального реєстру на «блокчейні» [47].

Нотаріальна палата України в рамках реалізації Концепції розвитку нотаріату з 2018 року працює над питанням впровадження Е-нотаріату, зокрема, з використанням технології «блокчейн» [48].

Разом із цим, ряд експертів [48-52] обґрунтовано піддають сумніву доцільність та перспективність застосування технології «блокчейн» у вказаних галузях.

Крім того, ряд авторитетних фінансистів та науковців [9, 10, 53, 54] та навіть офіційні установи [55] попереджають, що незважаючи на існування в світі численних практик використання криптовалют у якості міри вартості, засобу обміну та накопичення, її складна правова природа не дозволяє ототожнити її з будь-яким із суміжних понять (грошові кошти, валюта, валютна цінність,

законний платіжний засіб, електронні гроші, цінні папери, грошовий сурогат тощо), а тому криптовалюти – нічим не забезпечений «фінансовий пухирь».

#### **2.4. Оцінка рівня розвитку технології**

Як показав аналіз [56], на сьогоднішній день всі можливості технології «блокчейн» та індикатори ефективності її застосування вивчені недостатньо, традиційні моделі оцінки не підходять для криптовалют, оскільки останні не є традиційними активами (такими як акції, облігації або нерухомість).

У криптовалют відсутні регулярні грошові потоки, дивідендні виплати або кінцева вартість, яку б можна було розрахувати. Тому застосування визнаної в світі (та фактично єдиної для подібних досліджень) методики [57, 58] на основі 9-рівневої шкали TRL (англ. technology readiness level, «рівень готовності технології») для загальної оцінки «блокчейн» та цифрових валют на її основі, буде неефективним, зайве громіздким та занадто суб'єктивним.

З урахуванням цього, для оцінки рівня розвитку технології обирається методологія [59, 60], запропонована експертами Harvard Business School.

Згідно цієї методології, для будь-якої перспективної фундаментальної інновації пропонується розробити структуру, що деталізує чотири етапи її розвитку.

Така структура складається з двох аспектів (новизна та складність) та чотирьох етапів розвитку: одиничного використання, локалізації, заміщення та трансформації, які утворюють квадранти (рис. 2.1):

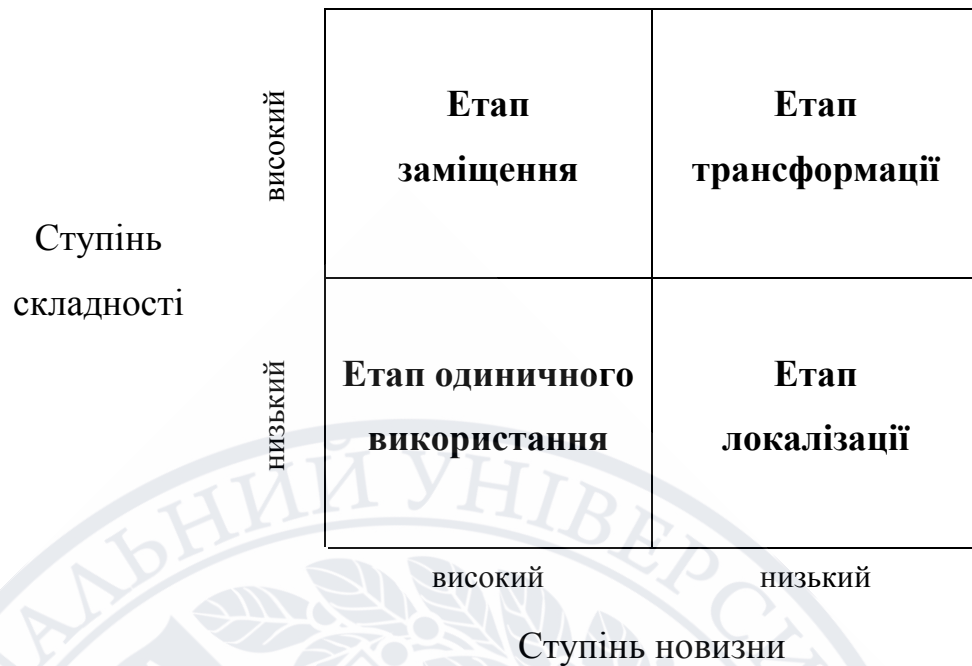


Рисунок 2.1 - Структура оцінки розвитку інноваційної технології

[60]

*Аспект новизни* (в сенсі поняття інноваційність) є ступенем, який визначає, наскільки технологія є новою у світі, тобто чим більш новою вона є, тим більше зусиль буде потрібно для того, щоб споживачі (користувачі, замовники, бізнес) зрозуміли, які проблеми технологія вирішує та які конкурентні переваги надає.

*Аспект складності* -це ступінь складності рівня координації екосистеми технології, тобто кількість та різноманітність сторін (учасників), яким потрібно співпрацювати (або яких потрібно залучити), щоб впроваджена технологія почала приносити користь або прибуток. Наприклад, соціальна мережа з одним користувачем малоприваблива та має сенс тільки тоді, коли до неї приєднуються багато учасників співтовариства, необхідно залучення до такої мережі інших користувачів, збільшення їх кола, щоб соціальна мережа почала приносити користь для всіх її учасників. Те саме можна стверджувати у відношенні до технології «блокчейн»: із збільшенням масштабу та впливу технології, для її впровадження потрібні значні інституціональні зміни (наприклад, правове або законодавче визначення).

*Етап одиничного використання.* Характеризується низькими ступенями новизни та складності. Топологія такої технології, як правило, проста, зрозуміла, дешева. Рішення - вузькоспеціалізовані. Так сервіс електронної пошти, що впроваджувався як більш швидкісна та дешева альтернатива традиційній пошті, телефонному та факсимільному способам спілкування, був одиничним використанням технології ТСП/ІР. Щодо технології «блокчейн», то до категорії одиничного використання можна віднести платіжну систему Bitcoin, оскільки навіть в перші дні свого існування, система надавала негайну вигоду для небагатьох людей, які обрали його для використання у якості альтернативного способу оплати [32].

*Етап локалізації.* Характеризується високим ступенем новизни та низьким ступенем складності. Тобто для розвитку інновації потрібна лише обмежена кількість користувачів, щоб негайно отримати віддачу від технології та прибуток від її впровадження. Такий підхід сприяє легкому впровадженню технології. Якщо конкретний варіант «блокчейну» піде шляхом мережевих технологій, які прийняті в бізнесі, можна очікувати, що інновації в цій галузі будуть побудовані на основі додатків одиничного використання (процес адаптації), направлених на створення локальних приватних мереж, в яких декілька організацій будуть підключені через розподілений реєстр «блокчейну». Більша частина первинних розробок приватних «блокчейнів» проводиться в галузі фінансових послуг або в невеликих мережах. Так, Nasdaq співпрацює з інфраструктурним провайдером технологій «блокчейн» Chain.com, для провадження фінансових транзакцій [42]. Банки Bank of America, JPMorgan, Нью-Йоркська фондова біржа, інвестиційні фонди Fidelity Investments, Standard Chartered тестують технологію «блокчейн» для заміни «паперових» транзакцій, які відпрацьовуються в ручному режимі, в таких сферах, як валютні операції, проведення розрахунків [46]. Банк Канади тестує цифрову валюту CAD-coin для здійснення міжбанківських операцій. В стадії пілотних проєктів знаходиться безліч приватних вузькоспеціалізованих «блокчейнів» для використання в конкретній галузі [42-47].

*Етап заміщення.* Характеризується низькою новизною, оскільки інновація пропонує модернізацію існуючої технології одиничного використання або ґрунтується на базі локалізованих версій, при цьому характеризується високим ступенем складності з причини прагнення до більш широкого та загальнодоступного варіантів використання. Такі інновації спрямовані на те, щоб кардинально замінити способи ведення бізнесу. Вони стикаються з високими перешкодами для впровадження оскільки потребують не тільки більшої координації, адже процеси, які вони сподіваються замінити, можуть бути повномасштабними та глибоко вбудованими в організації та установи [29]. Прикладом такого заміщення є криптовалюти – нові, повністю сформовані валютні системи, які засновані на простій технології оплати біткоїнами.

*Етап трансформації.* Характеризується високими ступенями новизни та складності. Технологія на цьому етапі розвитку спроможна змінити природу економічних, соціальних та політичних систем [61]. Яскравим прикладом технології, яка дійшла до цієї стадії, є Інтернет. На даний момент до цієї категорії можна умовно віднести смарт-контракти (англ. smart contract, «розумний контракт»), різновид технології «блокчейн» другого покоління. Але для практичної реалізації та широкого застосування технології смарт-контрактів необхідно вирішити рід технологічних проблем, пов'язаних з інформаційною безпекою [29].

За результатами проведеного в підрозділах 2.2, 2.3 аналізу можна побудувати структуру розвитку технології «блокчейн» (рис. 2.2):

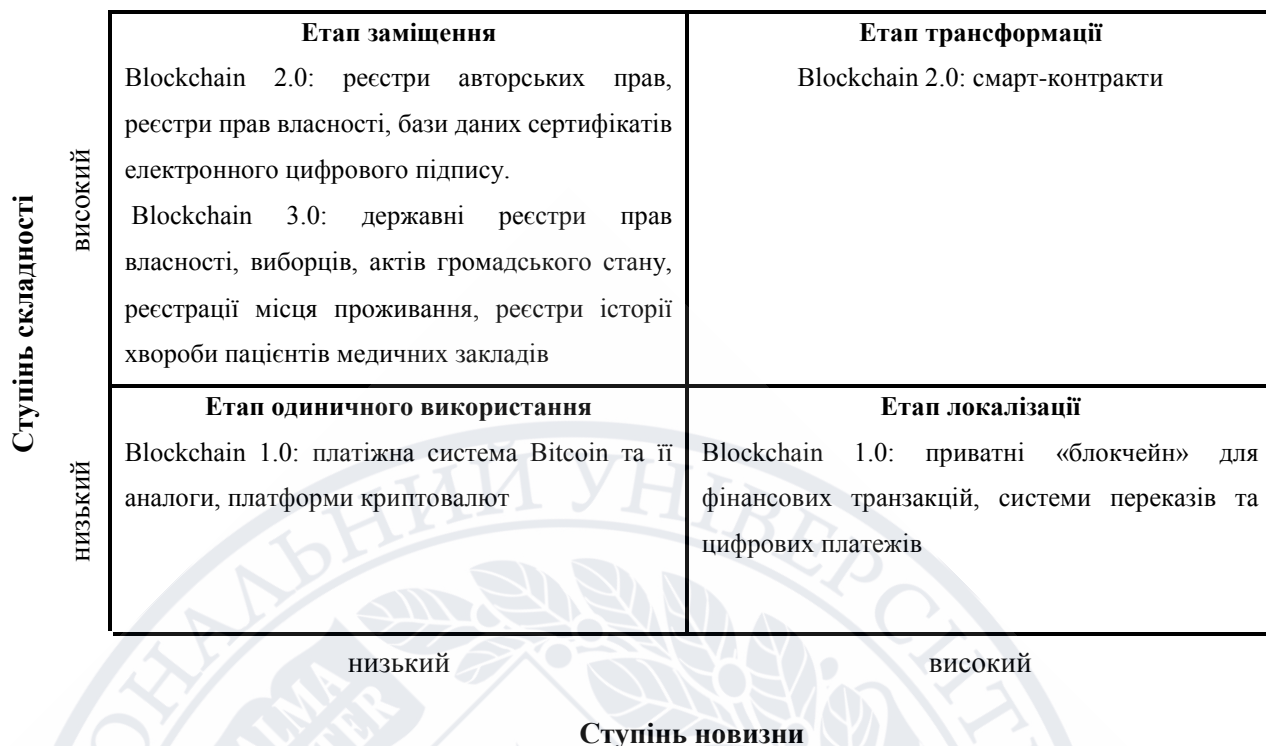


Рисунок 2.2 - Структура оцінки розвитку технології «блокчейн»

*Складено автором*

Побудована структура свідчить, що з оглядом на поширення використання та реальною практикою застосування, технологія «блокчейн» знаходиться на етапі локалізації в своєму розвитку. Отримана оцінка співпадає з висновками альтернативних досліджень [9, 16, 29, 56, 60-62].

### РОЗДІЛ 3

## КОНКУРЕНТНІ ПЕРЕВАГИ, НЕДОЛІКИ ТА ПЕРЕШКОДИ РОЗВИТКУ ТЕХНОЛОГІЙ НА ОСНОВІ «БЛОКЧЕЙН»

### 3.1. Переваги та недоліки технології «блокчейн» та криптовалют

До переваг використання технології «блокчейн» належать [64, 65]:

1. *Децентралізована база даних*: певним чином організована сукупність даних, в якій управління даними в кожному з вузлів бази виконується незалежно, при цьому усі вузли рівноправно важливі та самостійні. Це забезпечує прозорість мережі, універсальність та простоту використання таких баз даних.

2. *Використання смарт-контрактів* (своєрідного комп'ютерного алгоритму, що призначений для перевірки та укладання комерційних угод на базі технології «блокчейн», а тому виступає інструментом підвищення надійності та регуляції комерційних операцій. Оскільки смарт-контракти виключають участь людини це дає можливість провести контракт максимально чесно, відкрито, без помилок ненавмисних чи навмисних, а також значно скорочує кількість посередників при проведенні таких операцій. Також за допомогою смарт-контрактів можна максимально автоматизувати та уніфікувати проведення нескладних угод.

3. *Прозорість та доступність інформації*: максимально високий захист даних у системі «блокчейну» дозволяє створювати великі за обсягами бази даних, якими можуть користуватися декілька різних установ, що дає можливість скоротити витрати на самостійне обслуговування такої бази даних та збільшити її інформаційне наповнення за рахунок інформації інших установ. Загалом, користувачі мають доступ до результатів транзакцій в системі, які записуються у відкритому реєстрі, що підвищує рівень довіри та прозорості роботи.

4. *Високий рівень захисту*: технологія «блокчейн» унеможливорює шахрайські дії, мінімізує кількість помилок системи та гарантує високий рівень безпеки щодо зовнішнього втручання та атак, що є надзвичайно важливим у сучасній ситуації проблемності збереження анонімності інформації. Наприклад, збір та збереження особистих даних клієнтів у системі, побудованій за

допомогою розподіленого реєстру «блокчейн», має набагато вищий ступінь захисту, оскільки інформація не міститься на одному сервері, який можна зламати. Всі операції надійно захищені криптографічними функціями.

5. *Економія на витратах*: спеціалісти вважають, що, скажімо, запровадження «блокчейн» у сфері банківських переказів здатне скоротити витрати до 30%. Загалом за допомогою «блокчейн» фінансові установи зможуть значно скоротити свої комісійні та операційні витрати.

6. *Скорочення тривалості транзакцій*: для прикладу зараз тривалість завершеної операції купівлі-продажу цінних паперів на фондовій біржі становить три дні, оскільки учасників операції багато: продавець, покупець, інвестиційний банк, брокер і у кожного своя система обліку операції, в той час як технологія «блокчейн» здатна скоротити цей часовий діапазон до декількох годин [16]. Отже, технологія «блокчейн» не лише може значно скоротити час проведення транзакцій, але й усунути непотрібних посередників, роблячи проведення операції не лише швидшими, але й значно простішими та дешевшими як для клієнтів, так і для фінансових інституцій.

До недоліків використання технології «блокчейн» можна віднести [64, 65]:

1. *Обмежене масштабування та пропускна здатність*: сучасні технології «блокчейн» важко справляються з великими транзакціями, на рівні окремого банку чи іншої фінансової установи потужності ще достатньо, але якщо взяти міжнародний, транскордонний чи загальнодержавний рівні, то тут виникають проблеми з пропускну здатністю, які поки що невирішені та накладають певні ліміти на обсяги транзакційних операцій.

2. *Висока вартість розробки*: «блокчейн»-технології дуже вартісні та ресурсоємні проекти, тож лише крупні компанії чи консорціуми, які мають значні бюджети на науково-технічні розробки, можуть їх впроваджувати або купувати готові рішення компаній-стартапів.

3. *Висока вартість використання*: попри значні економії на використанні, застосування технологій «блокчейн» має свою високу вартість, оскільки вимагає великої обчислювальної потужності та місця зберігання масиву даних. Саме

тому багато «блокчейн»-проектів попри свою перспективність не реалізуються або термін їх використання дуже короткий.

4. *Невизначеність державного регулювання:* потребує додаткового регулювання багато питань, що стосуються глибокого впровадження «блокчейну» у будь-який сектор і не тільки. Скажімо, технологія «блокчейн» тісно пов'язана з криптовалютами, регулювання та статус яких в Україні абсолютно невизначений та позбавлений законності [55, 68]. Для повномасштабного впровадження «блокчейну» необхідно, щоб державні регулятори підтвердили надійність, стійкість та ефективність останнього та розробили оновлені процедури регулювання.

5. *Відсутність висококваліфікованих спеціалістів:* попит на кваліфікованих спеціалістів у галузі «блокчейн» значно переважає їх пропозицію на ринку. І це не лише ситуація, що склалася в Україні, світові фінансові гіганти також відчують значний брак кваліфікованої робочої сили [11].

До переваг криптовалют відносять наступні [66, 67]:

1. *Негайна доступність активів:* криптовалюта є доступною без будь-якого періоду очікування.

2. *Ліквідність* створюється миттєво за вимогою.

3. *Вивільнення оборотного капіталу:* необхідність для банків тримати резерви зведено до мінімуму і кошти доступні для інших цілей.

4. *Ефективність угоди:* відсутність процесів узгодження.

5. *Анонімність:* на відміну від класичних електронних грошей, операції за якими легко відслідковуються, отримати інформацію про власника криптовалютного гаманця неможливо, оскільки доступний тільки номер і обмежені дані за сумою на рахунку.

6. *Надійність:* неможливо зламати, підробити або здійснити інші подібні маніпуляції.

7. *Обмеженість:* випускається в обмеженому обсязі, що привертає підвищену увагу з боку інвесторів і виключає ризики інфляції через надмірну активність емітента.

8. *Криптовалюта є незалежною грошовою одиницею*: її емісію ніхто не регулює і не контролює рух коштів на рахунку.

9. *Відсутня комісія за здійснення переказу грошових коштів між країнами*.

Недоліки криптовалют [66, 67]:

1. *Складність контролю*: банки та інші органи нагляду не мають можливості контролювати операції по випуску й руху криптовалют.

2. *Ризик заборони*: багато країн вже ввели обмеження щодо її використання, а на порушників може бути накладено штраф.

3. *Відсутня можливість відкликання операції платіжу*.

4. *Волатильність*: криптовалюта залежить від поточного попиту, який, в свою чергу, може змінюватися в результаті змін в законодавстві.

5. *Небезпека втрати*: «ключем» доступу до електронних грошей є спеціальний пароль, при його втраті, активи криптогаманця стають недоступними.

6. *Відсутність гарантій*: криптовалюта нічим не забезпечена, кожен користувач персонально несе відповідальність за свої заощадження; через відсутність регулюючих механізмів немає гарантій збереження електронних криптогаманців.

### **3.2. Огляд потенційних кібератак**

Як й в будь-якій інформаційній технології, в «блокчейні» та криптовалютах на його основі, були виявлені критичні вразливості, через які зловмисниками проведений ряд успішних кібератак [68-70]:

*Атака 51%*. Суть атаки в тому, що зловмисник, контролюючи більше п'ятдесяти відсотків підтверджених ресурсів «блокчейн»-мережі, може запустити свій сфальсифікований ланцюжок блоків, який «обжене» реальний ланцюжок «блокчейна» та в результаті стане основним. При цьому він легко та безперешкодно скасує частину транзакцій, зроблених в відкинутих їм блоках. Наприклад, транзакції про грошові перекази. Таким чином, теоретично можна скасувати транзакцію «заднім числом». По суті майнінг подібний перебору

лотерейних квитків з різною ймовірністю виграшу. Так що для успішної атаки можна мати у володінні навіть менше 51 відсотка потужності або ресурсів мережі. Ймовірність успіху при цьому буде падати, але злочинець може сподіватися, що йому пощастить. На ранніх етапах свого розвитку біткоїни і будь-яка подібна до них валюта вразлива до так званої «Атаки 51%»: поки в розпорядженні атакуючого знаходяться потужності більші, ніж у всій решті мережі, то він зможе не підтверджувати чужі блоки, підтверджуючи тільки свої, а значить отримувати 100% всіх нових монет біткоїна та блокувати за своїм розсудом будь-які транзакції. На даний момент для здійснення такої атаки в мережі Bitcoin потрібна обчислювальна потужність, що у багато разів перевищує потужність всіх суперкомп'ютерів з рейтингу TOP-500 [21].

*Атаки на відмову в обслуговуванні (DoS).* Відправлення великої кількості «сміттєвих» даних на вузол, що обробляє транзакції, може ускладнити його роботу. Bitcoin має вбудований захист від атак типу «відмова в обслуговуванні»: розмір блоку обмежений до 1 МБ, щоб ускладнити забивання пулів пам'яті повних вузлів, а розмір кожного скрипту не перевищує 10 тис. байт. Також обмежено число перевірок підпису, яке може зажадати блок (20 тис.) та кількість підписів (20 ключів максимум). При цьому клієнти біткоїнів блокують всі підозрілі вузли та транзакції. Наприклад, в останній версії 0.7.0 клієнта Bitcoin Satoshi додали функцію для реєстрації нестандартних транзакцій (більше 100 кілобайт). Також при обробці транзакцій клієнт перевіряє, що всі виходи є «невитраченими».

*Злам криптографічних алгоритмів хеш-функцій.* Алгоритми для обчислення хеш-функції стандартів SHA-256 та ECDSA вважаються достатньо стійкими при існуючих обчислювальних потужностях. Однак, поява високопродуктивних квантових комп'ютерів може збільшити ризик злому цих криптографічних функцій. Наприклад, існуюча канадська система D-Wave, що використовує квантову технологію, в 100 мільйонів разів швидше звичайних комп'ютерів [21].

*Атака Сібілли.* Хакер може спробувати наповнити мережу підконтрольними йому вузлами, а інші користувачі зможуть підключитися тільки до блоків, створеним для шахрайства. Наприклад, зловмисник блокує транзакції від інших користувачів, від'єднавши конкретного користувача від загальної мережі. Після цього зловмисник під'єднує цього користувача тільки до блоків, які він створив, в окремій мережі. В результаті цього будуть з'являтися транзакції, які будуть пересилати гроші повторно (так зв. double-spending).

*Уповільнення часу в системі.* Сценарій цієї атаки такий: зловмисники атакують мережу в якій знаходяться користувачі «блокчейн»-продукту, наприклад, біткоїнів, та шляхом створення великого обчислювального навантаження на систему, уповільнюють час всередині мережі, що ускладнює передачу даних, повідомлень між користувачами, оновлення інформації в мережі, формування блоків, ланцюжків та їх фіксацію учасниками транзакцій.

*Уразливість транзакцій.* Незважаючи на те, що транзакції в Bitcoin підписуються, цей підпис охоплює не всю інформацію, яка використовується для отримання хешу транзакції. Фактично, існують можливість змінити параметри транзакції так, що зміниться хеш, але підпис залишиться незмінним. На основі цього може бути організована атака на виведенні коштів. У вихідній транзакції замінюється ідентифікатор, гроші доходять до адресата, але той повідомляє в технічну підтримку сервісу, що вихідна транзакція не дійшла. В результаті, сервіс може зробити повторну відправку коштів. Відомий також ще один різновид цієї атаки, який отримав назву «гнучкість транзакцій». Суть атаки в тому, що зловмисник змінює унікальний ідентифікатор транзакції біткоїна до її підтвердження в мережі Bitcoin.

*Помилки коду.* Помилки програмного коду можуть привести до нестабільності в захисті системи. Наприклад, на кожному вузлі інформація повинна оновлюватися за короткий відрізок часу. Якщо через помилки коду це не відбулося, в ланцюжку не з'явилася потрібна інформація, а неправильні дані почнуть поширюватися по мережі. Все це може стати причиною зупинки роботи мережі на кілька годин.

### 3.3. Конкурентні переваги технології «блокчейн»

Для об'єктивного виявлення конкурентних переваг технології «блокчейн» доцільно застосувати методику матричного SWOT-аналізу [71, 72]. Аббревіатура SWOT походить від начальних букв англійських слів strengths (сильні сторони), weaknesses (слабкі сторони), opportunities (можливості), threats (загрози).

Застосування методу SWOT-аналізу дає можливість встановити лінії зв'язку між сильними та слабкими сторонами, які притаманні об'єкту аналізу, із зовнішніми факторами можливостей та загроз. Таким чином, для визначення конкурентоспроможності технології необхідно поєднати дослідження внутрішніх можливостей об'єкту аналізу (його сильні та слабкі сторони) та зовнішню ситуацію (частково відображену у можливостях і загрозах).

Після складення конкретизованого (методика [72] допускає й узагальнений) переліку слабких та сильних сторін технології (її переваг та недоліків), а також можливостей та загроз, настає етап встановлення зв'язків між ними. Для цього необхідно скласти матрицю SWOT. Матриця SWOT будується в двох векторах: стан зовнішнього середовища (горизонтальна вісь) та стан внутрішнього середовища (вертикальна вісь), кожний вектор розбивається на два рівні: можливості та загрози, сила та слабкість (переваги та недоліки) технології, які притаманні об'єкту аналізу. На перетинах окремих складових груп факторів формуються чотири поля (квадранти), які повинні бути детально описані при заповненні матриці (рис. 3.1):

<b>S</b> trengths (сильні сторони)	<b>W</b> eaknesses (слабкі сторони)
<b>O</b> pportunities (можливості)	<b>T</b> hreats (загрози)

Рисунок 3.1 - Структура матриці SWOT

[71, 72]

З урахуванням того, що «блокчейн» та криптовалюти не синонімічні поняття, проведемо SWOT-аналіз кожної з технологій окремо на основі даних, що отримані та описані в підрозділах 3.1, 3.2 та детально розібрані в альтернативних дослідженнях [67, 68, 73-75].

Результати SWOT-аналізу технології «блокчейн» відображені в табл. 3.1:

Таблиця 3.1 – Результати SWOT-аналізу технології «блокчейн»

<b>S</b> trengths (сильні сторони)	<b>W</b> eaknesses (слабкі сторони)
<ol style="list-style-type: none"> <li>1. Надійне шифрування та захист від несанкціонованого доступу.</li> <li>2. Зниження витрат на зберігання даних.</li> <li>3. Полегшує обмін та поширення інформації.</li> <li>4. Ведення самостійного обліку та формування «потрійного запису».</li> <li>5. Дає можливість зацікавленим особам відстежувати всі проведені транзакції.</li> <li>6. Підтримка смарт- контрактів.</li> </ol>	<ol style="list-style-type: none"> <li>1. Програмне забезпечення слабо поширене на ринку.</li> <li>2. Низька кількість товарів, що продаються та послуг, пов'язаних з технологією.</li> <li>3. Можливість злому (атака 51%).</li> <li>4. Складність інтеграції з сучасними системами</li> </ol>

<b>O</b> pportunities (можливості)	<b>T</b> hreats (загрози)
<ol style="list-style-type: none"> <li>1. Застосування в різних сферах суспільства значно скоротить витрати паперової роботи.</li> <li>2. Використання криптовалют дозволяє уникати санкцій.</li> <li>3. Зниження рівня корупції.</li> <li>4. Зміна банківської сфери та відмова від багатьох банківських послуг, як наслідок, скорочення витрат.</li> <li>5. Можливість запуску нових бізнес-стартапів на новій технології.</li> <li>6. Прискорення та оптимізація бізнес-процесів.</li> </ol>	<ol style="list-style-type: none"> <li>1. Зростання тіньового сектора економіки.</li> <li>2. Використання технології для відмивання грошей та фінансування тероризму.</li> <li>3. Зростання шахрайства.</li> <li>4. У більшості країн відсутня правове та законодавче визначення.</li> <li>5. Явище «хайпу»: виникають завищені очікування від технології, які створюють образ деякої «панацеї». При невиправдані цих очікувань інтерес до технології різко згасне.</li> <li>6. Зникнення деяких професій.</li> </ol>

*Складено автором*

Результати SWOT-аналізу криптовалют відображені в табл. 3.2:

Таблиця 3.2 – Результати SWOT-аналізу криптовалют

<b>S</b> trengths (сильні сторони)	<b>W</b> eaknesses (слабкі сторони)
<ol style="list-style-type: none"> <li>1. Швидкозростаюча популярність.</li> <li>2. Підтримка смарт- контрактів.</li> <li>3. Прозорість транзакцій.</li> <li>4. Відсутність адміністратора, який здійснює емісію монет.</li> <li>5. Відсутність інфляції.</li> <li>6. Висока надійність системи.</li> <li>7. Відсутність оподаткування.</li> <li>8. Вартість транзакцій не залежить від суми переказу.</li> <li>9. Простота здійснення платежів.</li> </ol>	<ol style="list-style-type: none"> <li>1. Волатильність.</li> <li>2. Можливість ухилення від податків, фінансування тероризму та вплив тіньової економіки.</li> <li>3. У разі втрати приватного ключа від електронного гаманця повернути «монети» стає неможливим.</li> <li>4. Кожен «видобутий» блок ускладнює і збільшує вартість видобутку наступного.</li> <li>5. Неврегульований правовий статус.</li> <li>6. «Хайп» навколо криптовалют.</li> <li>7. Шахрайство.</li> <li>8. Величезна кількість різних монет в обігу.</li> </ol>

Opportunities (можливості)	Threats (загрози)
<ol style="list-style-type: none"> <li>1. Відсутність адміністратора значно скорочує витрати, тобто криптовалюта здатна значно змінити банківський сектор.</li> <li>2. Проведення розрахунків з будь-якої точки світу.</li> <li>3. На даний момент тестуються системи, які не вимагають Інтернету.</li> <li>4. Прозорість розрахунків значно спростить аудиторську діяльність.</li> <li>5. Популярні криптовалюти (зокрема Bitcoin) можуть стати універсальною альтернативною валютою</li> </ol>	<ol style="list-style-type: none"> <li>1. «Атака 51%».</li> <li>2. Ознаки фінансової піраміди.</li> <li>3. Можливість різкого знецінення криптовалюти.</li> <li>4. Через залучення до тематики криптовалют широкого кола пересічних громадян, виникає загроза незадоволення їх інтересів, в результаті чого багато хто може відвернутися від цифрових валют.</li> </ol>

*Складено автором*

### **3.4. Технологічні перешкоди та обмеження архітектури**

Експерти [9, 29] відокремлюють ряд суттєвих технологічних недоліків технології «блокчейн» та криптовалют на її основі:

- низька пропускна здатність (мережа Bitcoin в даний час максимізована до 7 транзакцій в секунду, для порівняння, VISA здійснює 2000, а Twitter - 5000 транзакцій в секунду) [75];

- великий час затримки (для забезпечення Bitcoin транзакції «блокчейн» потрібно близько 10 хв., щоб закінчити одну угоду, в той час як завершення угоди в VISA займає кілька секунд) [32];

- розмір і ширина смуги пропускання (в мережі Bitcoin існує обмеження на кількість транзакцій, які можуть бути оброблені, якщо блокчейн повинен контролювати більше угод, розмір і проблеми з пропускною спроможністю повинні бути вирішені) [32];

- проблеми з безпекою (на даний момент головною загрозою для «блокчейну» представляє т.зв. «атака 51%» [69, 70];

- висока енерговитратність майнінгу Bitcoin (до 15 млн. дол. / день), за 2017 року на майнінг біткоїнів було витрачено 32,7 Тв/год., що дорівнює річному споживанню енергії Сербії, Данії або Білорусі, а на майнінг Ефіріума - 11,1 Тв/год., що приблизно дорівнює річним витратам енергії Замбії або Литви, для порівняння, в 2017 році мегаполіс Москва витратила 105 Тв/год. [75].

*Обмеження архітектури «блокчейн» [9].* У структурному відношенні система «блокчейн» - це сама розподілена база плюс алгоритми та комп'ютерна інфраструктура, що реалізують взаємодію з ній. Вся ця система забезпечує збереження в розподіленій базі інформації про транзакціях, упакованої в блоки (англ. block), нероздільно пов'язані між собою в ланцюжки (англ. chain). При цьому кожен блок є архівом для визначеної кількості послідовних транзакцій, а весь ланцюжок блоків відображає історичну послідовність всіх транзакцій. Блоки пов'язані між собою нерозривно завдяки криптографічним алгоритмам. Вставити (або викинути) блок з середини ланцюжка неможливо, така операція буде відкинута системою. Можливо тільки приєднання нових блоків до кінця ланцюжка. Розподіленість системи передбачає, що база даних зберігається у вигляді повних копій на великій кількості комп'ютерів (вузлів - англ. node). Пасивні вузли тільки читають інформацію, а активні мають право (за власною ініціативою або дорученням пасивних вузлів) вставляти нові блоки транзакцій в базу (приєднувати до chain). У перших криптоваютних системах всі вузли зазвичай активні (біткоїни). В окремих архітектурах існують службові вузли, що відповідають за упорядкування транзакцій, маршрутизацію в мережі, балансування навантаженням). Все розмаїття версій «блокчейн» зазвичай поділяють на такі форми (за режимом доступу до інформації): публічні (англ. permissionless), коли будь-який бажаючий може стати вузлом; напівпублічні, коли активні вузли - це коло обраних, пасивні можуть приєднуватися більш-менш вільно; непублічні (англ. permissioned) - доступ всіх учасників адмініструється. Для більш точного уявлення суті «блокчейн» слід виділити його основні архітектури (по режиму зберігання інформації): розподілені, коли реєстр транзакцій зберігається у кожного учасника; децентралізовані, коли реєстр

транзакцій зберігається не у кожного учасника, а на деякій (як правило, невеликій) кількості вузлів; централізовані, коли тільки один вузол (сервер бази даних) використовується для зберігання всього реєстру транзакцій.

Оскільки реєстр транзакцій з моменту створення «блокчейн» був названий «розподіленим», однойменна архітектура розглядається як класична. Публічні системи є розподіленими. Потенціал таких систем для розвитку економічних інститутів найбільш очевидний, але існує ряд серйозних обмежень даної архітектури. Децентралізована архітектура використовується в основі непублічних та напівпублічних систем. В принципі, непублічні, напівпублічні (обмежено децентралізовані та централізовані) архітектури є «квазіблокчейн» (іноді в джерелах згадується як «ексклюзивний блокчейн»). Вони жертвують фундаментальною властивістю - розподіленою структурою, як основою захисту даних, на користь простоти реалізації та високої продуктивності. Криптовалюти в основному ґрунтуються на публічних формах. Попит на непублічні системи пред'являють в даний час реальний та державний сектори економіки [9].

### **3.5. Суттєві бар'єри впровадження**

В ході аналізу правових аспектів законодавчого та державного криптовалютного регулювання та контролю виявлено існування суттєвих бар'єрів впровадження технології «блокчейн» та цифрових валют на її основі:

*Правова та законодавча невизначеність.* Криптофеномен «блокчейна» важко об'єднати одним поняттям, тому що він складений з двох суперечливих галузей: технологічної - «блокчейн»-технології, та фінансової - криптовалюти. Хоча вони нерозривно пов'язані, значення у них дуже різні та ставлення до них теж: на фінансовий подразник - криптовалюту, в урядах спрацьовували заборонні рефлексії; а технологічний феномен - «блокчейн», викликав зацікавленість та бажання впровадження. Більшість урядів одночасно розглядали криптовалюту як потенційну загрозу, та вивчали можливості «блокчейна» для власних політичних потреб. «Блокчейн», в результаті, зійшов з дистанції - застосування йому не знайшлося, законодавчого інтересу в його

регулюванні теж. Саме криптовалюта стала основним предметом розгляду для відповідного законодавчого врегулювання. Серед регуляторів провідних країн світу, зокрема країн Європейського Союзу, немає єдиного підходу до визначення правового статусу криптовалют та регулювання операцій з ними [80]. Більшість з зарубіжних регуляторів [77, 80] та національні регулятори [55]: Національний банк України, Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює регулювання у сфері ринків фінансових послуг, зайняли позицію переконання в тому, що незважаючи на існування в світі численних практик використання криптовалюти у якості міри вартості, засобу обміну та накопичення, її складна правова природа не дозволяє ототожнити її з будь-яким із суміжних понять (грошові кошти, валюта, валютна цінність, законний платіжний засіб, електронні гроші, цінні папери, грошовий сурогат тощо). Така позиція означає що будь-яка законодавча заборона використання та, відповідно, введення юридичної (навіть кримінальної) відповідальності за її порушення, здатні знищити криптовалюту у будь-який час. «Сірий» та «чорний» (нерегульований та нелегальний) ринок при цьому нічого не втратить: наявність законів нічого не змінює для тих, хто цілеспрямовано використовує криптовалюту для їх обходу. Однак тільки при зусиллі держави в вузьких рамках правового регулювання можлива поява «білої криптоекономіки» - сектора економіки, в якому звичайні бізнеси можуть зустрітися з криптовалютою, а технологія «блокчейн» може спробувати конкурувати з традиційною банківською системою в рівних ринкових умовах.

*Цифрові валюти центральних банків.* Державні уряди користуються монополією на створення грошей через центральні банки, та не збираються поступатися цією монополією криптовалютам [78, 79]. При цьому наявність готівкових грошей (а це основа монетарної та валютної політики держав) заважають центральним банкам ввести негативні відсоткові ставки, тому що в такому випадку це викликає виведення збережень з банківської системи. Коли ж всі гроші будуть цифровими, варіанту вивести накопичені грошові активи та уникнути негативних ставок не залишиться. Тому введення центральними

банками національних цифрових валют вже відбувається. Цифрові валюти центральних банків (ЦВЦБ) можуть використовувати ту саму технологію розподіленого реєстру, що й криптовалюти. Але на відміну від криптовалюти, ЦВЦБ - це не нові валюти, а ті самі долари, євро, ієни та юані, що і сьогодні. Але ці валюти будуть повністю цифровими, «паперової» готівки не буде, зміниться формат і платіжні канали. Баланси можна тримати на цифрових гаманцях або в цифрових сховищах без використання традиційних банків. В окремих випадках, технологія «блокчейн» може не використовуватися: реєстр ЦВЦБ може вестися в зашифрованому вигляді самим центральним банком без потреби в банківських рахунках або фондах грошового ринку. В першу чергу, вони залучають своєю зручністю і відсутністю транзакційних комісій кредитних карт. Платежі можна здійснювати за допомогою смартфона або іншого пристрою без необхідності в кредитних картах або дорогих банківські перекази. Здатність ЦВЦБ знищити будь-яку нерегульовану державою криптовалюту чітко видно зі схеми класифікації (таксономії) грошей, що представлена у вигляді так званої «грошової квітки» на рис. 3.2:

## Грошова квітка: таксономія грошей

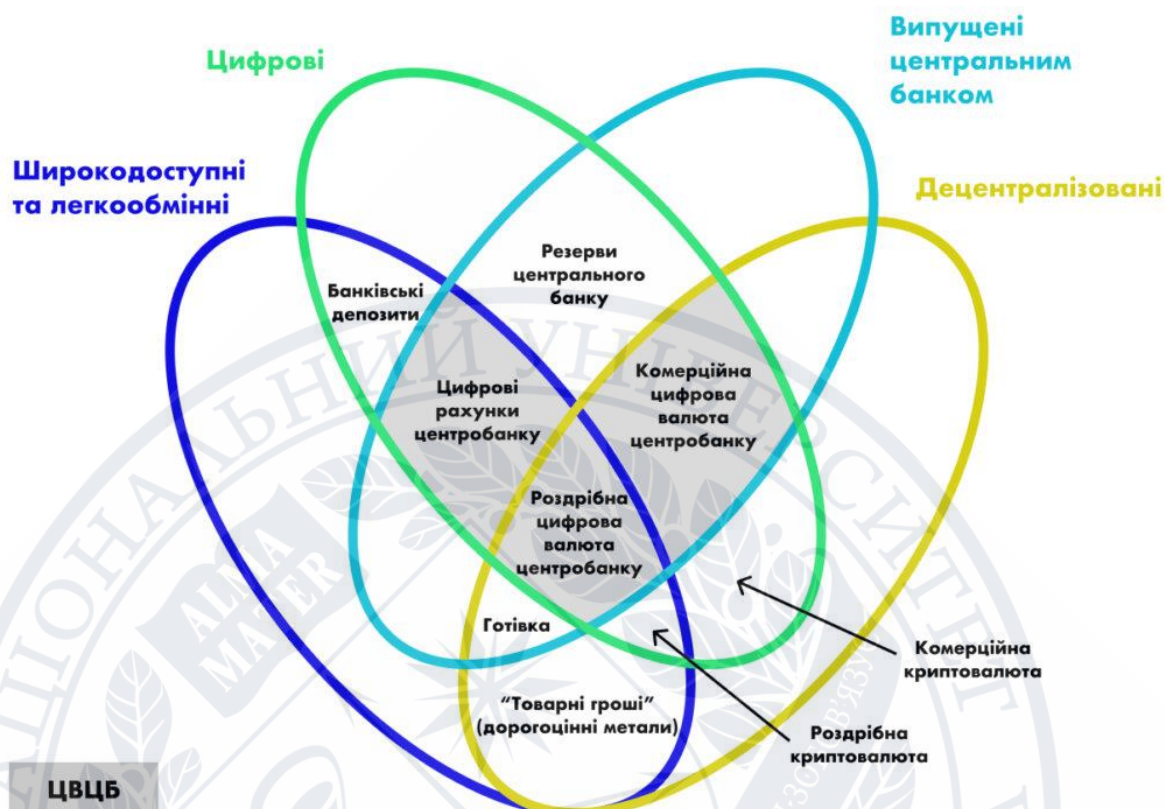


Рисунок 3.2 - Грошова квітка: таксономія грошей

[34, 81, 82]

Впровадження ЦВЦБ може знищити існуючі криптовалюти також з іншої причини: «блокчейн» залежить від критичної інфраструктури, включаючи сервери, телекомунікаційні мережі, банківську систему та електромережу - все це контролюється урядами. В будь-який час уряди можуть створити криптовалютам безліч технологічних перешкод. Реакція на такий варіант розвитку подій вже почалася. Великі банки бояться, що можуть бути повністю виключені з платіжної системи. MasterCard і Visa теж стурбовані, що їх платіжні канали стануть непотрібними. Коли нова технологія цифрових платежів зміцниться, можуть випаруватися трильйони доларів багатства у вигляді ринкової капіталізації приватних банків та фінансових структур JPMorgan, Citi, MasterCard і Visa.

*Проблеми патентування.* Суттєвою перешкодою для розвитку та впровадження технології «блокчейн» може стати проблема патентування рішень, що пропонуються розробниками. У США, які є лідером по розвитку «блокчейн»-технологій, розгорнулася справжня війна за право на використання розробок в цій сфері [29]: заявки на патенти, пов'язані з «блокчейн», подані заявниками - юридичними особами, серед яких виступають великі банки та корпорації, що викликало сильну та неоднозначну реакцію в «блокчейн»-співтоваристві. Якщо патенти будуть видаватися таким заявникам, то виникає ризик, що володільці патентів, отримавши 20-річну монополію на різні аспекти застосування патенту на «блокчейн», отримають можливість стягувати мільйони доларів в якості ліцензійних платежів з користувачів «блокчейн», або навіть забороняти використання технології. Більш того, власник прав може використовувати модель «патентного троллінгу». В 2014 році в США був створений прецедент [29] у вигляді рішення Верховного суду США у справі Alice Corp. проти CLS Bank International, 573 U.S., 134 S. Ct. 2347 (2014), який ухвалив, що більшість або, можливо, всі патенти на програмне забезпечення є абстрактними ідеями, які не мають права на патентний захист. А оскільки «блокчейн» є формою програмного забезпечення, всі заявки на патенти на технології «блокчейн» будуть стикаються з цим прецедентом.

### **3.6. Програмна модель «блокчейну»**

Для дослідження можливостей практичного застосування технології «блокчейн», розроблено програмну модель «блокчейну». Модель створено мовою програмування високого рівня Python версії 3.6. Код програми містить 56 стрічок (додаток А).

За основу взятий код, запропонований Т.Л.Майзенбергом [83]. Вихідний код мав критичні помилки в стрічках 28, 30, 41, 42, 43, 44, які були виправлені в ході роботи.

Код в стрічках 1-17 визначає вид блоку. Кожен блок містить мітку часу та номер. Для перевірки цілісності всього «блокчейну», кожен блок буде мати

ідентифікаційний хеш. На зразок біткоїну, хеш кожного блоку буде криптографічним хешем номера блоку, його тимчасової мітки, даних та хешу попереднього блоку. В якості даних може бути що завгодно (файл, умовні одиниці, кодові слова).

Код в стрічці 14 ініціює процес хешування з використанням криптографічного алгоритму хешування SHA-256 розміром 256 біт.

Після створення структури блоку, необхідно створити ланцюжок таких блоків (тобто «блокчейн»). Для цього необхідно додавати блоки в якусь послідовність. Для цього необхідно створити та додати перший блок (genesis block). Він додається вручну та має особливу логіку, що дозволяє його додати. Код в стрічках 18-23 створює функцію, яка буде повертати genesis block, з номером 0 та довільні дані з довільним значенням хешу «попереднього блоку».

Після створення genesis block, необхідно запустити функцію, яка буде створювати послідовні блоки в ланцюжку. Ця функція буде приймати попередній блок в ланцюзі, як параметр, створювати дані та повертати новий блок з перевіреним хешем. Коли новий блок хешує інформацію з попереднього блоку, надійність всього ланцюгу збільшується з кожним новим блоком. Якщо цього не робити, зловмисникам буде простіше «змінити минуле» і замінити справжній ланцюжок на інший. Хеш ланцюгу блоків виконує роль криптографічного доказу та надає гарантію того, що доданий в «блокчейн» блок не можна буде змінити або зовсім видалити. Означену функцію виконує код в стрічках 24-30.

Код в стрічках 32-56 запускає процес створення та роботи «блокчейн». У випадку створеної моделі, це буде простий Python-список (list). Першим елементом виступить штучно створений перший блок (genesis block). В моделі обмежено число можливих блоків «блокчейна» числовим значенням 30 можливих блоків (код в стрічці 46).

Після запуску програми створюється ланцюг блоків заданої структури та їх хеш-значення.

## ВИСНОВКИ

Поява першої криптовалюти Bitcoin, концепт якої побудований на технології «блокчейн», мала провокаційний характер та дала поштовх до стрімкого розвитку як самої технології, так й до появи інших цифрових валют. Створені на основі «блокчейн» криптовалюти, незважаючи на волатильність, незручність в сфері обміну та ризик для накопичення (в тому числі в зв'язку з нелегалізованим статусом), мають капіталізацію, що дорівнює річним бюджетам окремих країн. Такий стан речей привів до того, що 2018 році лопнув спекулятивний «міхур» криптовалют, а в експертному середовищі різко посилювалася обґрунтована критика надійності цифрових валют та подальших перспектив технології «блокчейн».

За час свого розвитку інновація зазнала переходу від «криптовалютної» до «фундаментальної» стадії у вигляді чотирьох поколінь від т.зв. Blockchain 1.0 до Blockchain 4.0, причому найчастіше у вигляді незавершених розробок та конкуруючих версій. Проведення оцінки рівня розвитку технології за методологією Harvard Business School показало, що технологія «блокчейн» в своєму розвитку знаходиться на етапі локалізації, особливості та характеристики якого наведені в роботі. «Блокчейн» має потенціал для свого розвитку. Отримана оцінка співпадає з висновками альтернативних досліджень.

Проведено дослідження та систематизацію переваг та недоліків, можливостей та загроз технології «блокчейн» та цифрових валют, що дозволило застосувати методику матричного SWOT-аналізу для об'єктивного виявлення конкурентних переваг (конкурентоспроможності) технології «блокчейн». З урахуванням того, що «блокчейн» та криптовалюти не синонімічні поняття, додатково проведено SWOT-аналіз криптовалют. Технологічні недоліки, технічні перешкоди в провадженні, обмеження архітектури, наявність вразливих місць криптозахисту в цілому, та зокрема, вирішуються, та не є перешкодою для подальшого розвитку технології «блокчейн» та цифрових валют.

Натомість в ході аналізу правових аспектів законодавчого та державного криптовалютного регулювання та сфери контролю, виявлено існування трьох суттєвих бар'єрів впровадження технології «блокчейн» та цифрових валют на її основі. По-перше, це правова та законодавча невизначеність. Серед регуляторів провідних країн світу немає єдиного підходу до визначення правового статусу криптовалют та регулювання операцій з ними. Зарубіжні та національні регулятори (зокрема, Національний банк України, Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює регулювання у сфері ринків фінансових послуг) зайняли позицію переконання в тому, що незважаючи на існування в світі численних практик використання криптовалюти у якості міри вартості, засобу обміну та накопичення, її складна правова природа не дозволяє ототожнити її з будь-яким із суміжних понять (грошові кошти, валюта, валютна цінність, законний платіжний засіб, електронні гроші, цінні папери, грошовий сурогат тощо). Така позиція означає, що будь-яка законодавча заборона використання та, відповідно, введення юридичної (навіть кримінальної) відповідальності за її порушення, здатні знищити криптовалюту у будь-який час. По-друге, в роботі обґрунтовано, що введення центральними банками національних цифрових валют здатне знищити будь-яку нерегульовану державою криптовалюту. В третє, суттєвими перешкодами для розвитку та впровадження технології «блокчейн» можуть стати проблеми в сфері патентування рішень, що пропонуються розробниками.

## СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Силантьєв С.О. Фінансові супермаркети на основі блокчейн технологій. *Нові форми грошей та фінансових активів: становлення, перспективи, ризики: Тези І Міжнар. наук.-практ. конф. (Київ, 29 лист. 2017).* Київ, 2018. С. 169–171.
2. Звіт «Ринок блокчейнів за компонентами (платформа та послуги), провайдером (додатки, проміжне програмне забезпечення та інфраструктура), типом (приватний, публічний та гібридний), розміром організації, сферою застосування (BFSI, уряд, IT та телекомунікації) та регіонами - Глобальний прогноз до 2025 року», URL: <https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html> (дата звернення 01.03.2021).
3. Стаття «Блокчейн (мировой рынок)» від 15.03.2021. URL: [https://www.tadviser.ru/index.php/Статья:Блокчейн\\_%28мировой\\_рынок%29](https://www.tadviser.ru/index.php/Статья:Блокчейн_%28мировой_рынок%29) (дата звернення 01.03.2021).
4. del Castillo M. Big Blockchain: The 50 Largest Public Companies Exploring Blockchain. Forbes. URL: <https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/bigblockchain-the-50-largest-public-blockchain> (дата звернення: 06.03.2021).
5. Інформаційне повідомлення на офіційному сайті ДП «СЕТАМ» Міністерства юстиції України: «СЕТАМ продав майна за допомогою Blockchain на 6 млрд грн». URL: [https://setam.gov.ua/article/setam-prodav-mayna-za-dopomogoyu-blockchain-na-6-mlrd-grn?fbclid=IwAR09-QmIK\\_nTjq0oG6Jn7gTsDonRm8PWTgzmR0XRPdcaYyVtFiDzDP3PEko](https://setam.gov.ua/article/setam-prodav-mayna-za-dopomogoyu-blockchain-na-6-mlrd-grn?fbclid=IwAR09-QmIK_nTjq0oG6Jn7gTsDonRm8PWTgzmR0XRPdcaYyVtFiDzDP3PEko) (дата звернення 06.03.2021).
6. Постанова Кабінету Міністрів України від 21.06.2017 № 688 «Деякі питання реалізації пілотного проекту із запровадження електронних земельних торгів і забезпечення зберігання та захисту даних під час їх проведення». *Офіційний вісник України від 29.09.2017.* 2017. № 76. С. 11.
7. Стаття «526% за 10 місяців. Яким був шлях біткоіна до історичного максимуму» від 17.12.2020. URL: <https://www.rbc.ru/crypto/news/5fdb410f9a7947872fc3e79b> (дата звернення 06.03.2021 ).

8. Осипова О.І. Прогнозування ціни на біткоіни за допомогою нейронних мереж. *Нові форми грошей та фінансових активів: становлення, перспективи, ризики*: Тези І Міжнар. наук.-практ. конф. (Київ, 29 лист. 2017). Київ, 2018. С. 150-153.

9. Липницький Д.В. Возможности и вызовы для блокчейн в новой индустриализации. *Економіка промисловості*. 2019. № 1(85). С. 82-100.

10. Стаття «Прошло 10 лет, а никто не придумал, как использовать блокчейн» від 12.01.2018. URL: <https://habr.com/ru/company/raiffeisenbank/blog/346534/> (дата звернення 06.03.2021).

11. Стаття «IBM сократила отдел по работе с блокчейном» від 02.02.2021. URL: <https://habr.com/ru/news/t/540518/> (дата звернення 06.03.2021).

12. Спасітелева С.О., Бурячок В.Л. Перспективи розвитку додатків блокчейн в Україні. *Кібербезпека: освіта, наука, техніка*. 2018. № 1(1). С. 35-48.

13. Гумеров Э.А. Тенденции развития блокчейн систем. *Образовательные ресурсы и технологии*. 2019. № 2 (27). С. 59-63.

14. Стаття «Задача Візантійських генералів» від 17.03.2020. URL: <https://exbase.io/uk/wiki/zadacha-vizantijskikh-generaliv> (дата звернення 08.03.2021).

15. Стаття «Інтернет речей, IoT, M2M. Світовий ринок» від 04.03.2021. URL: [https://www.tadviser.ru/index.php/IoT,\\_M2M,\\_BA](https://www.tadviser.ru/index.php/IoT,_M2M,_BA) (дата звернення 07.03.2021).

16. Слобода Л.Я., Сенькович Ю.А. Розвиток та імплементація технології блокчейн у проведенні розрахунків фінансових установ. *Економіка та управління національним господарством*. 2018 Випуск 2 (130). С. 40-47.

17. Стаття Nakamoto, S.A. (2009). «Peer-to-Peer Electronic Cash System. Bitcoin. Retrieved from» <https://bitcoin.org/bitcoin.pdf>. (дата звернення 07.03.2021).

18. Стаття «Как это работает: Деревья Меркла в биткойн сети» від 10.01.2018. URL: <https://habr.com/ru/company/bitfury/blog/346398/> (дата звернення 07.03.2021).

19. Миронець І.В., Шкребтій А.В. Криптографічні алгоритми та особливості їх використання в блокчейн системах. *Безпека інформації. Ukrainian Scientific Journal of Information Security*. 2019. Том 25, № 2. С.82-87.
20. Якименко І.З., Тимошенко Л.М., Касянчук М.М. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків. *Сучасна спеціальна техніка*. 2018. № 2. С. 63–71.
21. Пашорін В.В. Технології безпеки криптовалют та блокчейн-мережі. *Зовнішня торгівля: економіка, фінанси, право*. 2019. № 3. С.93-101.
22. Касянчук М.М., Карпінський М.П., Казмірчук С.В. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах. *Захист інформації*. 2019. Том 21, №2. С. 65- 73.
23. Козлов М.В. Элементы теории вероятностей в примерах и задачах. М.: Изд-во МГУ, 1990. 344 с.
24. Хватов К.Ю. Ключевая концепция и терминология криптовалют и их сравнение с фидуциарными валютами. *ИТпортал*. 2018. №1 (17).С. 2-11.
25. Хижняк О.С. Використання електронного документообігу і електронного цифрового підпису промисловими підприємствами у збутовій і закупівельній діяльності: переваги і недоліки. *Причорноморські економічні студії*. 2016. Вип.10. С.154-157.
26. Закон України «Про електронні довірчі послуги». *Відомості Верховної Ради*. 2017, № 45, ст.400.
27. Васильев В.И. Принцип работы Blockchain. *Молодой ученый*. 2019. № 21. С. 25-27.
28. Стаття «Рост глобальных расходов на блокчейн в 2021 превысит 50%» від 20.04.2021. URL: [https://ko.com.ua/rost\\_globalnyh\\_rashodov\\_na\\_blokchejn\\_v\\_2021\\_prevysit\\_50\\_137108](https://ko.com.ua/rost_globalnyh_rashodov_na_blokchejn_v_2021_prevysit_50_137108) (дата звернення: 15.03.2021).
29. Цветкова Л.А. Перспективы развития технологии блокчейн: конкурентные преимущества и барьеры. *Экономика науки*. 2017. № 4. С. 275-296.
30. Official cite Investing.com [Electronic resource] URL: <https://ru.investing.com/crypto/currencies> (дата звернення 16.03.2021)

31. Official website CoinMarketCap [Electronic resource] URL: <https://coinmarketcap.com> (дата звернення 15.03.2021)
32. Свон М. Блокчейн: схема новой экономики: [пер. с англ.]. М.: Издательство «Олимп-Бизнес». 2017. 240 с.
33. Гумеров Э.А. Тенденции развития блокчейн систем. *Образовательные ресурсы и технологии*. 2019. № 2 (27). С. 59-63
34. Варнавский А.В. Токен или криптовалюта: технологическое содержание и экономическая сущность. *Финансы: теория и практика*. 2018. №22. С.122-140.
35. Стаття «Блокчейн третьего поколения (blockchain 3.0) и DAG-сети» від 17.02.2021 URL: <https://ecrypto.ru/blokchejn/blokchejn-tretego-pokoleniya-blockchain-3-0-i-dag-seti.html> (дата звернення 17.03.2021)
36. Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Анализ современных тенденций развития технологии «блокчейн» и цифровых валют. *Вопросы кибербезопасности*. 2019. № 5(33). С. 57-62.
37. Ometorowa T. Solving the Blockchain Trilemma: Decentralization, Security & Scalability. Coinbureau. URL: <https://www.coinbureau.com/analysis/solving-blockchaintrilemma> (дата звернення 17.04.2021).
38. Стаття «Трилемма масштабируемости блокчейна» від 03.06.2020. URL: <https://bitnovosti.com/2020/06/03/trilemma-masshtabiruemosti-blokchejna/> (дата звернення 15.04.2021).
39. Стаття «Платформа Seele – главные преимущества системы». 2019. URL: <https://steemit.com/seele/@simbalion/platforma-seele-glavnye-preimushhestva-sistemy> (дата звернення 17.03.2021).
40. Стаття «Продукт криптовалюты Seele» від 15.01.2021. URL: <https://coincryptobase.com/currency/seele/product> (дата звернення 25.04.2021).
41. Козлов С.Д., Слоботчиков О.Н. и др. Цифра и власть: цифровые технологии в государственном управлении: коллективная монография. М.: Институт мировых цивилизаций. 2020. 268 с.

42. Стаття «Banking Is Only The Beginning: 58 Big Industries Blockchain Could Transform» від 03.03.2021. URL: <https://www.cbinsights.com/research/industries-disrupted-blockchain/#healthcare> (дата звернення 25.03.2021).

43. Стаття «Применение блокчейна, или какие варианты использования DLT внедряются уже сегодня» від 08.02.2018. URL: <https://decenter.org/ru/primenenie-blokcheina> (дата звернення 25.03.2021).

44. Стаття «Кроме криптовалют: для чего еще используется блокчейн» від 12.04.2018. URL: <https://habr.com/ru/company/bitfury/blog/353350/> (дата звернення 25.03.2021).

45. Стаття «Обзор 17-ти сфер применения технологии блокчейн» від 23.02.2020. URL: [https://maff.io/sfery\\_primeneniya\\_blockchain/](https://maff.io/sfery_primeneniya_blockchain/) (дата звернення 25.04.2021).

46. Стаття «42 индустрии, меняющиеся под влиянием блокчейна» від 22.07.2019 URL: <https://dx.media/articles/analytics/42-industrii-menyayushchiesya-pod-vliyaniem-blokcheyna/> (дата звернення 25.03.2021).

47. Стаття «Блокчейн и нотариусы: как изменится нотариат в будущем» від 11.07.2020. URL: <https://bitbon.today/ru/staty/blokchejn-i-notariusy-kak-izmenitsya-notariat-v-budushem/> (дата звернення 25.03.2021).

48. Інформаційне повідомлення на офіційному сайті Нотаріальної палати України від 19.9.2018: «НПУ працює над питанням впровадження технології блокчейн в Україні. URL: <https://npu.ua/news/npu-pracyuye-nad-pitannjam-vprovadzhennya-tehnologi%D1%97-blokchejn-v-ukra%D1%97ni/> (дата звернення 25.03.2021).

49. Стаття «Вам не нужен блокчейн: 8 популярных юзкейсов и почему они не работают» від 31.01.2019. URL: <https://habr.com/ru/company/solarsecurity/blog/438028/> (дата звернення 25.03.2021).

50. Стаття «Блокчейн нужен там, где нет доверия» від 25.03.2021. URL: <https://www.vedomosti.ru/opinion/articles/2021/03/25/863032-blokchein-nuzhen> (дата звернення 25.03.2021).

51. Стаття «There's No Good Reason to Trust Blockchain Technology» від 02.06.2019. URL: [https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/?CNDID=56304861&CNDID=56304861&bxid=MzUwMDI5Mjg5MTg5S0&hasha=213c5e146025f758e2247c99ff0ea592&hashb=397e2c97c2888bb47ead2087e1c134fe4d1f2cba&mbid=nl\\_020619\\_daily\\_list3\\_p1&source=DAILY\\_NEWSLETTER&utm\\_brand=wired&utm\\_mailing=WIREDE%20NL%20020619%20\(1\)%20A&utm\\_medium=email&utm\\_source=nl](https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/?CNDID=56304861&CNDID=56304861&bxid=MzUwMDI5Mjg5MTg5S0&hasha=213c5e146025f758e2247c99ff0ea592&hashb=397e2c97c2888bb47ead2087e1c134fe4d1f2cba&mbid=nl_020619_daily_list3_p1&source=DAILY_NEWSLETTER&utm_brand=wired&utm_mailing=WIREDE%20NL%20020619%20(1)%20A&utm_medium=email&utm_source=nl) (дата звернення 26.04.2021).

52. Стаття «Каждый второй CEO мечтает впихнуть блокчейн в свой проект, почему это может стать провальной идеей?» від 03.07.2019. URL: <https://rb.ru/opinion/pochemu-biznesu-ne-nuzhen-blokchejn/> (дата звернення 26.04.2021).

53. Стаття «Биткоин - финансовая пирамида. Как закончится майнинговая лихорадка» від 30.07.2017. URL: <https://www.vedomosti.ru/opinion/columns/2017/07/31/727052-bitcoin-piramida> (дата звернення 25.04.2021).

54. Безверхий К.П., Кувшинова А.М. Криптовалюта: гроші чи мильна бульбашка. *Науково-практичний журнал «Бухгалтерський облік і аудит»*. 2018. С.29-38.

55. Інформаційне повідомлення на офіційному сайті Національного банку України «Спільна заява фінансових регуляторів щодо статусу криптовалют в Україні» від 30.11.2017. URL: <https://bank.gov.ua/ua/news/all/spilna-zayava-finansovih-regulyatoriv-schodo-statusu-kriptovalyut-v-ukrayini> (дата звернення 26.04.2021).

56. Клочкова Е.Н., Овешникова Л.В. Оценка эффективности использования технологий распределенного реестра в условиях цифровой экономики *Статистика и экономика*. 2019. Т. 16. № 2. С. 15-24.

57. Комаров А.В., Петров А.Н., Сартори А.В. Модель комплексной оценки технологической готовности инновационных научно-технологических проектов. *Экономика науки*. 2018, Т. 4, № 1. С. 47-57.

58. Гранич В. Ю., Дутов А. В., Мирошкин В. Л., Сыпало К. И. Об уровнях готовности технологий и применении Калькулятора УГТ для их оценивания. *Экономика науки*. 2020. Т. 6. № 1-2. С. 6-10

59. Баданов А.Ю., Рызванов Р.А. Адаптация лучших мировых практик по оценке уровней готовности технологий, уровней готовности интеграции, системного уровня готовности. *Актуальные проблемы гуманитарных и естественных наук*. 2017. С. 71-82.

60. Marco Iansiti, Karim R. Lakhani. The Truth About Blockchain. *Harvard business review*. 2017. P.118-127.

61. Сухарев О.С. Цифровые технологии: условие технологического замещения. *Эргодизайн*. 2019. № 3. С.115-121.

62. Мазуренко О. К. Технології Blockchain в інформаційному забезпеченні логістичних послуг. *Бізнесінформ*. 2019. № 12 С.255-261.

63. Помазкова Е.Е. Сравнительный анализ блокчейна и альтернативных технологий распределенного реестра. *International Journal of Humanities and Natural Sciences*, 2019. № 4-2. С.127-131.

64. Хмара М.П., Михайлов Р.В. Блокчейн-революція як перехід до промислової революції 4.0. *Проблеми системного підходу в економіці*. 2020. № 6(80). С.139-153.

65. Бондаренко Л.П., Мороз Н.В., Лащик І.І. Функціональні особливості застосування блокчейн технології у фінансовому секторі. *Інвестиції: практика та досвід*. 2019. № 3. С.21-25.

66. Шкляр А.І., Шаповал Ю.І. Традиційний банкінг в умовах нової технологічної революції. *Нові форми грошей та фінансових активів: становлення, перспективи, ризики*: Тези І Міжнар. наук.-практ. конф. (Київ, 29 лист. 2017). Київ, 2018. С. 181–185.

67. Кобрин М.Ю. Криптовалюта и blockchain как основа шестого цикла Николая Кондратьева. *Цикличность в развитии социальных систем разного уровня*: Сб. науч. ст. по материалам XXII регион. науч.-практ. конф. (Барнаул, 17 мая 2018). Барнаул, АлтГУ. 2018. С. 302-315.

68. Устенко С.В., Загоровський І.В. Можливості та перспективи криптовалют та технології blockchain. *Моделювання та інформ. системи в економіці*: Зб. наук. праць. 2019. № 97. С.229-240.

69. Стаття «Что угрожает блокчейн-сетям: рассматриваем атаки и способы защиты» від 15.01.2018. URL: (дата звернення 25.04.2021)

70. Колесников П.И., Бекетнова Ю.М., Крылов Г.О. Технология блокчейн. Анализ атак, стратегия защиты. *LAMBERT Academic Publishing*. 2017. 76 с.

71. Носонова Л.В. Застосування SWOT-аналізу для визначення конкурентоспроможності. *Глобальні та національні проблеми економіки*. 2015. Випуск 4. С.506-512.

72. . Кривда В.І., Кривда О.В., Нараєвський С.В. Можливості удосконалення методики SWOT-аналізу. *Економіко-математичне моделювання соціально-економічних систем*: Зб. наук. праць МННЦ ITiC. 2007. № 12. С. 74-77.

73. Кобрин М.Ю. Влияние blockchain-технологий на экономическую безопасность: преимущества и угрозы. *Наука. Технологии. Инновации*: Мат. Конф. (Новосибирск, 04–08 декабря 2017). 2017. С. 510-513.

74. Якушкин С. А., Осипов И. В. Блокчейн-технология: значение, категории, правовая перспектива. *Бюллетень науки и практики*. 2019. Т. 5. №8. С. 134-139.

75. Синельникова-Мурылева Е.В., Шилов К.Д., Зубарев А.В. Сущность криптовалют: дескриптивный и сравнительный анализ. *Финансы: теория и практика*. 2019. №6. С.36-49.

76. Стаття «Десять барьеров на пути распределенных реестров» від 28.08.2018. URL: <https://www.osp.ru/os/2018/03/13054407> (дата звернення 26.04.2021).

77. Стаття «Как в разных странах регулируют криптовалюту: обзор законов в 2020 году» від 15.10.2020. URL: <https://habr.com/ru/company/moneypipe/blog/523354/> (дата звернення 26.04.2021).

78. Мелиховский В.М. Причины возникновения криптовалюты и экономические свойства блокчейна в цифровой экономике. *Теоретическая экономика*. 2019. № 7. С. 109-121.

79. Стаття «Війна з готівкою: наступна фаза» від 13.04.2021. URL: <https://goldenfront.ru/articles/view/vojna-s-nalichnymi-sleduyushaya-faza/> (дата звернення 26.04.2021).

80. Доклад Департамента макроэкономической политики Евразийской экономической комиссии «Криптовалюты и блокчейн как атрибуты новой экономики. Разработка регуляторных подходов: международный опыт, практика государств-членов ЕАЭС, перспективы для применения в Евразийском экономическом союзе». 2019. 90 с.

81. Morten Bech, Rodney Garratt. Central bank cryptocurrencies. URL: [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.pdf](https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf) (дата звернення 26.04.2021).

82. Стаття «Цифрова валюта центрального банку: що це таке, чому всі про це говорять та як працюватиме е-гривня» від 12.04.2021. URL: <https://ucap.io/czyfrova-valyuta-czentralnogo-banku-shho-cze-take-chomu-vsi-pro-cze-govoryat-ta-yak-praczuivatyme-e-gryvnya/> (дата звернення 26.04.2021).

83. Стаття «Крохотный блокчейн на Python в 50 строк» від 22.05.2020. URL: <https://lambda-it.ru/post/krokhotnyi-blokchein-na-python-v-50-strok> (дата звернення 26.04.2021).

## ДОДАТОК А

## Код програмної моделі «блокчейну»

```

import hashlib as hasher
import datetime as date

class Block:
    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = self.hash_block()

    def hash_block(self):
        sha = hasher.sha256()
        prehash = (
            str(self.index)
            + str(self.timestamp)
            + str(self.data)
            + str(self.previous_hash)
        )
        sha.update(prehash.encode("utf-8"))
        return sha.hexdigest()

def create_genesis_block():
    return Block(0, date.datetime.now(), "Genesis Block", "0")

def next_block(last_block):
    this_index = last_block.index + 1
    this_timestamp = date.datetime.now()
    this_data = "Hey! I'm block " + str(this_index)
    this_hash = last_block.hash
    return Block(this_index, this_timestamp, this_data, this_hash)

blockchain = [create_genesis_block()]
previous_block = blockchain[0]

num_of_blocks_to_add = 30

for i in range(0, num_of_blocks_to_add):
    block_to_add = next_block(previous_block)
    blockchain.append(block_to_add)
    previous_block = block_to_add
    print("Block #{ } has been added to the blockchain!".format(block_to_add.index))
    print("Hash: { }\n".format(block_to_add.hash))

```