КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра математичної інформатики

«До захисту допущено»
Завідувач кафедри
В. М. Терещенко _____
(підпис)

«___» _____20___ р.

Кваліфікаційна робота

на здобуття ступеня бакалавра
за спеціальністю122 Комп'ютерні науки
на тему:

ПРОБЛЕМА МАСШТАБОВАНОСТІ БЛОКЧЕЙНУ

Виконав студент 4 курсу
Черкашин Михайло Юрійович _____
(підпис)

Науковий керівник:
доктор фіз.-мат. наук, професор
Анісімов Анатолій Васильович _____
(підпис)

Засвідчую, що в цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2022

РЕФЕРАТ

Обсяг роботи 31 сторінок, 4 ілюстрацій, 2 таблиці, 59 джерел посилань.

БЛОКЧЕЙН, МАСШТАБОВАНІСТЬ БЛОКЧЕЙНУ, ТРИЛЕМА БЛОКЧЕЙНУ, LAYER 1, LAYER 2.

Об’єктами дослідження у роботі є проблеми масштабованості блокчейну, його властивості, підходи до її вирішення та технології, що реалізують ці підходи.

Результатами роботи є детальний опис основних властивостей блокчейну у контексті трилеми блокчейну, опис більшості існуючих на момент написання роботи підходів до вирішення проблеми масштабованості блокчейнів, визначення їх переваг та недоліків та висновки щодо їх застосування.

Розглянуті у роботі стратегії рішення трилогії блокчейну можуть бути застосовані відповідно до їх сильних та слабких сторін та сфери застосування для проектування і створення власного блокчейну, чи для адаптування, покращення вже існуючих рішень.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

Нода (від англ. node – «вузол») – клієнт мережі блокчейну.

Майнінг (від англ. mining – «видобуток корисних копалин») – процес підтримки роботи мережі, що базується на використанні алгоритму консенсусу Proof of Work.

Сайдчейн (від англ. sidechain) – технологія другого рівня; блокчейн суміжний з основним ланцюгом.

Смарт-контракт (smart-contract) – програмований протокол/алгоритм, що представляє певну угоду в блокчейні, зберігають її стан та забезпечують можливість взаємодіяти із нею та її станом за допомогою програмованих механізмів.

Стейкінг (від англ. stake – «ставка») – процес підтримки роботи мережі, що базується на використанні алгоритму Proof of Stake.

Шардінг (sharding) – сегментування мережі на окремі сегменти (“shard”).

DAG (Directed Acyclic Graph) – орієнтовний ациклічний граф; реалізація розподіленого реєстру на основі орієнтовного ациклічного графу.

DoS (Denial of Service – з англ. «відмова в обслуговуванні») – атака на комп’ютерну систему з метою зробити її недоступною для користувачів.

Peer-to-peer, p2p – однораногова комп’ютерна мережа з рівноправними вузлами.

PoS (Proof of Stake – з англ. «доказ частки») – алгоритм консенсусу блокчейну, що базується на ставках учасників мережі.

PoW (Proof of Stake – з англ. «доказ роботи») – алгоритм консенсусу блокчейну, що базується на виконанні певної обчислювальної роботи.

TPS (transactions per second – з англ. «кількість транзакцій на секунду») – показник пропускної можливості блокчейн мережі.

ВСТУП

Оцінка сучасного стану об'єкта дослідження. У відповідь на проблему масштабованості та відповідно до спрямованості застосування технології блокчейн виділилися інші типи мереж: приватні, консорціумні.

Проте найбільша кількість уваги зосереджена саме на публічних мережах, оскільки вони втілюють у собі максимально децентралізовані рішення – ідею, для якої і було створено блокчейн, - а також використовуються для криптовалют – першого і найпопулярнішого варіанту застосунку блокчейну.

Для таких мереж наразі існують технології надбудови над блокчейном, які прийнято називати рішеннями другого рівня. Серед таких: Bitcoin Lightning Network [4], Ethereum Plasma [5].

Рішення на кшталт шардінгу (Harmony [7], Ethereum 2.0 [8][9]), збільшення розміру блоків (BitcoinCash [11]) чи структури блоків (SegWit [10]), альтернативні алгоритми консенсусу (Tendermint [12], Stellar [13]) – представляють рішення першого рівня, тобто такі, що змінюють початкову структуру блокчейн мережі.

Також було запропоновано альтернативні блокчейну технології розподіленого реєстру, які замість структури ланцюга використовують орієнтовні ациклічні графи: Tangle, Hashgraph [14].

Серед великої кількості існуючих рішень, які мають свої особливості, переваги та недоліки, важко вибрати варіант, що найкраще підходить у конкретному випадку застосування блокчейну.

Актуальність роботи та підстави для її виконання. Технологія блокчейн здійснила мрії людей про децентралізовану утопію, разом із реалізованою мережею *Bitcoin* змогла втілити у життя ідеї й концепції незалежних децентралізованих цифрових валют, які активно зароджувалися наприкінці двадцятого століття. Першою серед подібних система *Bitcoin*

привернула багато уваги, а блокчейн став однією з найінноваційніших технологій початку двадцять першого століття. Зацікавленість технологією породила багато експериментів з нею, а також інших криптовалют та технологій. Загальнодоступність та безпека у купі з широким спектром можливих впровадження робить технологію універсальним рішенням для більшості проблем сьогодення. Застосування блокчейну поширилось на майже всі сфери життя, включаючи інтернет речей, медицину, штучний інтелект [15].

Разом з тим збільшення кількості користувачі криптовалют виявило проблеми масштабованості блокчейну. Вже у 2015 р. мережа *Bitcoin* почала досягати своїх лімітів пропускної можливості [16]. Ця проблема одразу породила дискусії щодо її вирішення [17]. За декілька років ситуація сильно погіршилась і деяким користувачі доводилось чекати підтвердження транзакцій декілька днів, а запропоновані рішення вимагали певних компромісів у системі – це й породило трилему блокчейну.

Хоча зараз існує багато стратегій і технологій для нівелювання проблеми масштабованості, важко назвати будь-яке з рішень ідеальним та застосовним для будь-якої мережі. Тому питання вибору якоїсь з них для практичного застосування (покращення існуючої блокчейн мережі чи створення нової) у будь-якій з численних сферах, де використовується блокчейн, потребує аналізу.

Мета й завдання роботи. Метою роботи є дослідження проблеми масштабованості блокчейн мереж, трилеми блокчейну, стратегій та технологій її вирішення. Для досягнення цієї мети було поставлено такі завдання:

- розглянути технологію блокчейн;
- простежити витоки блокчейну, розглянути технології та ідеї, що лягли в його основу, концепції, які були закладені в нього початково;
- розглянути типи блокчейн мереж;

- дослідити проблематику трилеми блокчейну та описати основні властивості блокчейн мереж;
- проаналізувати та визначити особливості наявних рішень масштабованості блокчейну у контексті трилеми блокчейну.

Об’єкт дослідження. Об’єктом досліджень у цій роботі є технології, створені для вирішення проблеми масштабованості блокчейну, а також самої технології блокчейн, її властивостей.

Можливі сфери застосування. Розглянуті у роботі стратегії вирішення проблеми масштабованості блокчейн мереж разом з конкретними прикладами їх реалізацій можуть бути використані для проектування і створення власної блокчейн мережі, чи для адаптування, покращення вже існуючих рішень відповідно до сфери застосування блокчейну.

РОЗДІЛ 1 ТЕХНОЛОГІЯ БЛОКЧЕЙН

1.1 Витоки концепції блокчейну

Блокчейн (англ. Blockchain) – незмінна розподілена база даних, одна із реалізацій ідеї розподіленого реєстру (distributed ledger), що була вперше запропонована Сатоші Накамото як основа криптовалютної мережі Bitcoin у 2008 р. [18], як розвиток ідеї Стюарта Габера, У. Скотта Сторнетта та Дейва Байєра [19][20], а також Вей Дайя та Ніка Сабо.

Оригінальна стаття Габера та Сторнетта '*How to Time-Stamp a Digital Document'* [19], що була надрукована у 1991 р., описує метод створення цифрових часових міток для документів у розподіленій мережі користувачів, який:

а) забезпечує приватність та непідробність інформації, а також зменшує навантаження на пропускну та обробну здатність мережі за допомогою використання підписаного хешу певного файлу чи інформації замість використання оригіналу як при передачі, так і на самому сервері, який видає часові мітки користувачам, – таким чином можна перевірити і дійсність оригіналу, і приналежність його певному користувачеві;

б) забезпечує непідробність міток:

1) у *централізованій схемі* за допомогою використання у кожній новій мітці певної поєднуючої інформації, що містить хеш попередньої, її час, ідентифікатор та іншу інформацію – таким чином неможливо зробити мітку наперед чи видати мітку, що передую останній, які були б дійсні, адже для цього треба в першому випадку знати попередні мітки, в другому – змінити попередні;

2) у *децентралізованій схемі* мітка часу формується із підписів, що містять час, ідентифікатор і хеш інформації, інших k клієнтів мережі, які обираються випадковим чином генератором псевдовипадкових послідовностей з хешем інформації в якості початкового числа – складність підробки базується на знаходженні початкового числа, відмінного від оригінального, такого, що генератором псевдовипадкових чисел буде згенерована така послідовність довжини k, що містить тільки тих клієнтів, що змовилися на підробку.

Обидві схеми мали свої недоліки і розглядались авторами порізно, проте обидві лягли в основу технології блокчейн та мережі Bitcoin:

- учасники розподіленої мережі зберігають інформацію про транзакції у вигляді ланцюгу з блоків з часовими мітками, що містять мітки попереднього блока;
- для досягнення згоди – консенсусу – щодо вірності інформації між учасниками мережі використовується певного роду голосування з підтвердженням інформації багатьма учасниками мережі.

Голосування у мережі Блокчейн, щоправда, відбувається за рахунок обчислювального часу процесорів для розв’язання певної алгоритмічної задачі, і цим самим більше походить на концепції *B-Money*, яку описав у переписці шифропанків Вей Дай у 1998 р. [21]:

1) для участі у емісії (об’єм якої наперед визначається всіма власниками рахунків валюти) кожен учасник, що має бажання, транслює в мережу певну математичну задачу з пулу невирішених раніше задач (обчислювальні зусилля для якої можна чітко визначити) і ставку, яку сподівається отримати за вирішення задачі;
2) всі учасники обчислюють вибрані задачі і транслюються у мережу, де перевіряються іншими учасниками мережі;

3) з усіх рішень приймаються і оплачуються лише найвигідніші з розрахунку номінальної вартості задачі.

Також Вей Дай у контексті вищезазначеного концепту запропонував використовувати цифрові псевдоніми – відкриті ключі – для ідентифікації користувачів, кожне повідомлення яких має підписуватись та шифруватись, при цьому у перевірці правильності транзакцій беруть участь усі користувачі, так само як і кожен з них має свою копію бази даних. В його розумінні система має не залежати від влади та інших інституцій, на які покладена роль посередника у розрахунках та обміні валютою.

Варто окремо відзначити Ніка Сабо, який у 1998 р. незалежно від автора *B-Money* запропонував схожі ідеї щодо створення децентралізованої цифрової валюти *Bit gold* [22]. Сабо був шифропанком, піонером криптовалют, автором концепції смарт-контрактів та прихильником криптоанархізму. Концепція *Bit gold* частково спиралася на попередні спроби створити електронні гроші та комбінувала деякі попередні підходи. Запропонована ним система мала відповідати Візантійській відмовостійкості: функціонувати правильно без додаткових арбітрів, навіть якщо в ній є певна кількість недоброчесних серверів. Вона використовувала ланцюжок із хешів, що й були доказом роботи. Якщо ж кількість недоброчесних серверів буде достатньо велика і у них вийде дискредитувати систему, то доброчесна меншість зможуть відділитися та функціонувати окремо.

Появі технології блокчейн передували багато різних концепцій та ідей, які вплинули на його появу блокчейну, проте представлені концепції децентралізованих систем цифрових грошей мали недоліки і так і не були реалізовані. Найголовнішою інновацією статті Сатоші Накамото і, відповідно, структури блокчейн було вирішення проблеми подвійних витрат.

1.2 Типи блокчейн мереж

Попри те що блокчейн задумувався для створення загальнодоступної, неконтрольованої та цілком децентралізованої системи, захищеної механізмами заохочувань та криптоекономіки, існують блокчейни, доступ до яких контрольований.

Блокчейн мережі можна поділити на такі типи [1][2]:

- Публічні – блокчейни повністю децентралізовані та неконтрольовані: не мають обмежень щодо приєднання до мережі та прав у ній; безпека у таких мережах базується на алгоритмах консенсусу таких, як PoW (альтернативами є PoS та інші, які будуть розглянуті далі), які гарантують високий рівень безпеки за таких умов, та криптоекономіці; найпопулярнішим застосуванням таких мереж є криптовалюти.
- Приватні – блокчейни, що контролюються певною організацією; всі права контролюються певним централізованим органом, який вирішує, що буде записано до ланцюгу.
- Консорціумні – блокчейни, що контролюються певною групою організацій чи суб’єктів; більш децентралізовані, аніж повністю приватні мережі, адже консенсус контролюється не одним органом, а обраним набором суб’єктів, водночас право на перегляд ланцюгу може бути загальнодоступним; такі блокчейни використовуються, наприклад, у сфері ланцюгів доставок.

РОЗДІЛ 2. ТРИЛЕМА БЛОКЧЕЙНУ

2.1 Опис проблематики

Трилема блокчейну (або трилема масштабованості) запропонована Віталіком Бутеріним, винахідником та співзасновником *Ethereum* [23]. Згідно неї, компроміси між трьома основними властивостями блокчейну – безпекою, масштабованістю, децентралізацією – неминучі (рисунок 1). Вдаючись до простих технік, блокчейн може задовольняти лише двом з них [6]. Розглянемо ці властивості детально.

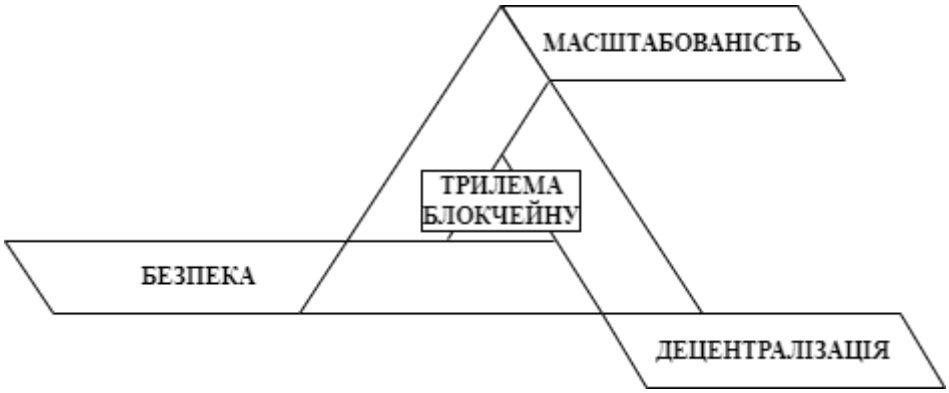

Рисунок 1 – Трилема блокчейну

Примітка. За трилемою можна досягти властивостей лише з однієї сторони трикутника

Децентралізація характеризує можливість блокчейну функціонувати у розподіленій мережі не покладаючись на верифікацію з боку одного чи декількох довірених суб'єктів, тобто функціонувати без будь-якої довіри між нодами.

На децентралізацію також впливають вимоги до запуску ноди (об'єм пам'яті, обчислювальна потужність, пропускну здатність), оскільки цей фактор впливає на загальну кількість власників нод, які будуть брати участь у перевірці ланцюга, проте не обов'язково будуть задіяні у процес майнінгу (PoW) чи стейкінгу (PoS) чи у будь-якому іншому процесі консенсусу. Наявність великої кількості користувачів, які будуть відхиляти блоки, що порушують протокол,

навіть при переважаючій кількості майнерів, які будуть ці блоки підтримувати, унеможливлює чистий виграш для нечесних нод: відбудеться розгалуження блокчейну, при цьому гілка недоброчесних нод буде лише незначною частиною мережі, або відбудеться паніка на ринку через тимчасове, але значне розгалуження – це все може значно знизити прибутки недоброчесних гравців і їм буде невигідно порушувати правила [24][25].

Відсутність такого «пасивного» захисту робить систему більш вразливою до атаки «51%». Це ж і зробило можливим розділ мережі Ethereum після зламу DAO [26] [27].

Децентралізація лежить в основі створення блокчейну як структури, на якій базується незалежна від третіх довірених осіб система цифрових грошей Bitcoin (див. розділ 1.1). Ця властивість притаманна більшості криптовалютам та публічним блокчейн мережам, проте у інших типах мереж нею можуть нехтувати (див. розділ 1.2).

Безпека – властивість блокчейну, що полягає у Візантійській відмовостійкості системи [28], здатність системи протистояти атакам значного відсотка нод і зберігати цілісність й непідмінність блокчейну, що забезпечується алгоритмом консенсусу блокчейну разом із системою заохочень для учасників консенсусу: нагороди за блок та податків з транзакцій. Ідеальний алгоритм разом із системою заохочень забезпечують рівновагу Неша: так що порушники протоколу не отримають чистого виграшу [29][30]. Хоча все ще залишається можливість атаки Голдфінгера, метою якої є дискредитація мережі та руйнування економіки усієї системи [31]. Це важлива і невід’ємна властивість децентралізованих мереж з низькою довірою до учасників.

Масштабованість полягає у здатності мережі збільшувати свою пропускну здатність із ростом кількості нод та транзакцій, підтримувати кількість обробки транзакцій у секунду (TPS – transaction per second). Масштабованість блокчейну залежить від двох показників:

- *максимальної пропускної здатності* блокчейну – максимальної швидкості, з якою блокчейн може підтверджувати транзакції;
- *затримки* – часу між створенням транзакції та її підтвердженням у мережі.

Проблема полягає у знаходженні рішення збільшення пропускної здатності мережі без шкоди для безпеки та децентралізації системи.

Серед розглянутих типів мереж (див. розділ 1.2) тільки публічні можуть претендувати на володіння усіма трьома властивостями, адже приватні та консорціумні блокчейни за умовою нехтують першою із характеристик – децентралізацією, – яка була ключовою ще за часів виникнення концепції блокчейну (див. розділ 1.1), і можуть легко добитися високого рівня масштабованості не прибігаючи до складних стратегій. Тому й розглянуті далі стратегії та технології стосуються саме публічних блокчейн мереж та криптовалют, які є одним із найпоширеніших застосунків блокчейну.

Існуючі рішення трилеми масштабованості поділяються на два рівні (рисунок 2):

а) *рішення першого рівня (layer 1, L1)* – рішення, які безпосередньо вносять зміни самого ланцюга:
   1) зміна структури блоків;
   2) зміна розміру блоків;
   3) вибір альтернативного консенсусу;
   4) шардінг (сегментування);

б) *рішення другого рівня (layer 2, L2)* – надбудови до блокчейн мережі, які не змінюючи мережу знижують навантаження на неї та забезпечують високий показник TPS для користувачів, виконуючи основну роботу поза межами основного ланцюга:

1) платіжні канали;
2) розгалужені блокчейни;
3) згортки (rollups);
4) сайдчейни.

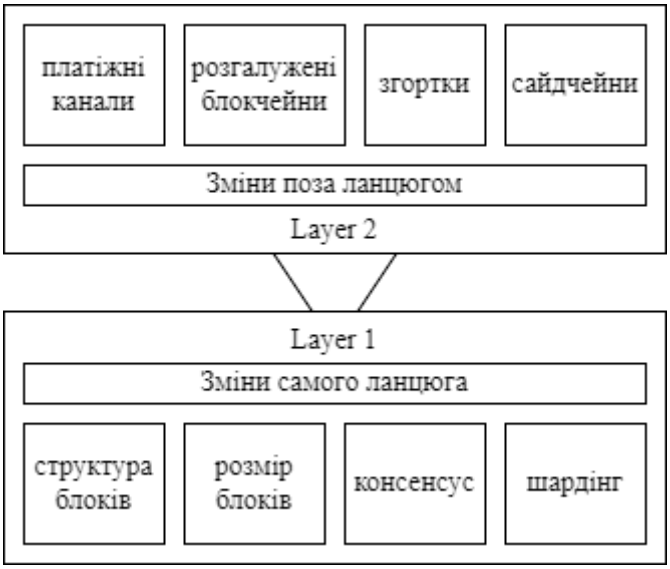

Рисунок 2– Стратегії вирішення проблеми масштабованості, згруповані за рівнями

Далі розглянемо деякі із стратегій детально.

2.2 Зміна розміру блоків

Обмеження на розмір блоку та відповідно кількості транзакцій у ньому в мережі Bitcoin, як і у інших мережах, пов’язане з питаннями безпеки і децентралізації. Від цього параметра залежить навантаження на p2p мережу блокчейну при поширенні нового блока між нодами, кількість обчислювального часу, затраченого на обробку та перевірку транзакцій у блоці. Занадто високе значення параметру чи відсутність обмеження взагалі створює загрозу для проведення DoS атак: одна чи декілька нод можуть навмисно розсилати великі блоки із набором «сміттєвих» транзакцій, тим самим завантажуючи мережу системи. Також таку мережу зможуть підтримувати лише ноди, що здатні забезпечити значні мережеві та обчислювальні можливості, а ще можливість зберігати більшу за розмірами локальну копію блокчейну. Варто зазначити, що у результаті технічного прогресу, появи нових рішень і здешевлень технологій рівень цих можливостей зростає.

Як спосіб упередження можливих DoS атак та створення деякими майнерами блоків більших, ніж інші майнери могли б прийняти, у мережі Bitcoin у 2010 р. було введене обмеження на максимальний розмір блоку у 1 МБ – більші за розміром блоки просто не приймалися нодами. Також таке обмеження гарантує повільне і прогнозоване збільшення блокчейну в розмірах, що дозволяє будь-кому зберігати та підтримувати мережу. Оскільки складність рішення PoW контролюється мережею та формування блоків відбувається через майже однакові проміжки часу, обмеження на розмір блоку обмежує TPS та може викликати значні затримки при високому навантаженні на систему.

На початку 2015 р., коли із розширенням мережі та досить різким збільшенням кількості транзакцій, розмір блоку Bitcoin почав досягати своєї граничної межі у 1 МБ [16]. У 2016 р. проблеми із пропускною здатністю блокчейну почали викликати вже реальні складнощі для користувачів, адже черга із непідтверджених транзакцій сягала значення у 50000, а затримки до підтвердження транзакції могли сягати дні, податки за транзакції зросли [50].

Для вирішення проблеми масштабованості у Bitcoin було запропоновано два підходи:

1) застосування Segregate Witness;
2) збільшення розміру блоку транзакції.

Розбіжності поглядів на ці підходи серед нод призвели до розділення мережі Bitcoin у 2017 р.: основна мережа впровадила софтфорк із Segregate Witness та утворився хардфорк Bitcoin Cash із збільшеним максимальний розмір блоку (спочатку 8 МБ, а потім 32 МБ) [32].

Технологія SegWit (Segregate Witness) змінює структуру блоків (рисунок 3): в основний блок транзакцій записуються лише входи та виходи транзакцій, підписи та скрипти, які можуть займати аж до 65% розміру транзакції, виносяться у окрему структуру – witness data – і не враховуються у обчисленні ID транзакції.

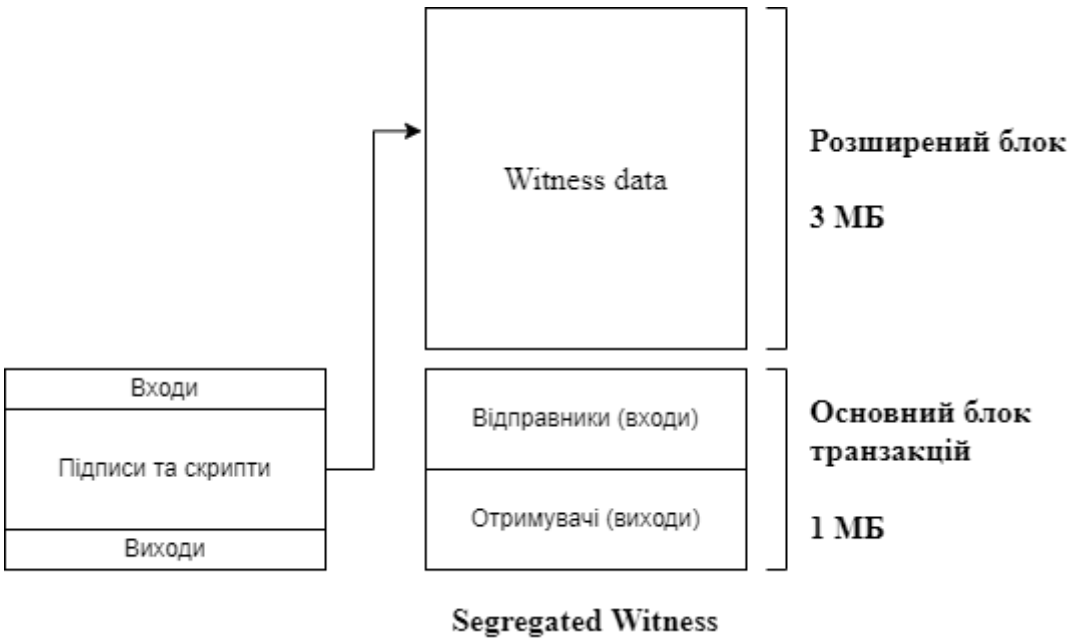

Рисунок 3 – Структура блоку у SegWit

SegWit дозволяє розміщати у блоці того ж розміру більше транзакцій і за рахунок цього підвищує показник мережі, проте насправді не зменшує

навантаження на мережу та ноди і в цьому не відрізняється від звичайного збільшення розміру блоку. Менше з тим, застосування SegWit не потребує хардфорку, адже модифікована структура залишається сумісною з основним блоком транзакцій. Водночас SegWit має обмежений потенціал прискорення TPS, що диктується розміром основного блоку.

Відокремлюючи скрипти та підписи, SegWit також вирішує проблему пластичності транзакцій (malleability problem), яка полягає у тому, що транзакції можуть бути частково змінені, проте залишатися дійсними. У Bitcoin ID транзакції, за яким її можна розрізнити і відстежити, формується хешування її підписів та інших даних, зміна яких призведе до зміни підписів. Разом з тим можна змінити ID транзакції видозмінюючи підписи, наприклад, додавши нулі на початку, які не вплинуть на перевірку підписів та їх валідність, проте змінять хеш. Насправді ця проблема є недоліком програмної реалізації Bitcoin і може бути виправлена. Усі методи зміни ID транзакції та варіанти їх вирішення описані у BIP 0062 [53], який так і не було прийнято. В Bitcoin Cash ця проблема частково виправлена [54]: зовнішні суб’єкти не можуть змінювати хеш транзакції, яку вони не створювали, однак особа, яка створила транзакцію, все ще може змінити підпис і хеш транзакції. Відсутність цієї проблеми дозволяє реалізовувати рішення другого рівня, такі як платіжні канали та сайдчейни, які вже у свою чергу дозволяють значно пришвидшити Bitcoin.

Обмеження блоку є необхідною вимогою для безпеки, децентралізації, прогнозованості блокчейну. Фактично збільшення розміру блоку не вирішує проблему масштабованості, проте є скоріше тимчасовою адаптацією до потреб відносно можливостей. Архітектура блокчейну має гнучко підлаштовуватись до сьогочасних потреб у пропускній здатності системи, не вдаючись до хардфорків, які складно провести без розколу блокчейн мережі. Важливо розробляти такі рішення, які б зберігали усі переваги малих блоків при збільшенні показника TPS.

Ethereum, замість обмеження на розмір блоку, має обмеження на розмір газу у блоці – одиниці, яка вимірює кількість обчислювальних зусиль та пам’яті, необхідних для виконання конкретних операцій у мережі Ethereum. Такий підхід дозволяє гнучко використовувати можливості мережі, не упираючись у її фізичні можливості або навпаки у фіксований розмір блоку.

Блокчейни із фіксованим максимальним розміром блоку, особливо меншим за спроможності мережі, та створенням нових блоків через регулярні проміжки часу більш вразливі до DDoS атак флудом транзакцій. Загроза спам атаки не є чимось чисто теоретичним: 14 вересня 2021 відбулися атаки на Solana та Arbitrum One. Цьому може зарадити розподіл мережі на сегменти – шардінг.

2.3 Згортки

Згортки (rollups) представляють «гібридну» схему другого рівня: обробка транзакцій, як і у інших рішеннях другого рівня, винесені за межі основної мережі, проте всі дані про транзакції зберігаються на основному блокчейні. Ідея полягає у компонуванні та стисненні («згортанні») великої кількості транзакції до однієї («пакетна транзакція» або «беч транзакція» від англ. «batch transaction»), яка буде записана на основному ланцюзі. Така схема об'єднує переваги платіжних каналів та сайдчейнів, покладаючись на безпеку головної мережі та забезпечуючи швидке багатоцільове використання. Публікуючи усі необхідні для локальної валідації дані транзакцій на основному ланцюзі можна запобігти *проблемі доступності даних* [39], а також атак, пов'язаних із цією проблемою, яка є притаманною для «легких» клієнтів («light clients») [40] та вищезгаданих рішень другого рівня, які покладаються у зберіганні та видачі за запитом даних на окремих суб'єктів. Записуючи транзакції на основний ланцюг, згортки забезпечують будь-якому користувачу можливість виявити шахрайство, ініціювати вивід коштів або особисто почати створювати бечі – пакети транзакцій.

Вміст бечу може відрізнятися залежно від реалізації, та загалом він містить стиснуті дані про транзакції, хеш нового стану, представлений корнем дерева Меркла стану згортки після обробки цих транзакцій, а також хешем стану системи після попереднього блока, який для нового бечу має відповідати поточному стану. Самі дерева Меркла стану не записуються для зменшення розміру бечу, оскільки їх можна обчислити та перевірити із інформації на основному ланцюзі. Згортки за допомогою смарт-контрактів зберігають хеш свого поточного стану – стану запропонованого останнім підтвердженим бечем. Новий беч публікується в якості даних виклику беч транзакції – транзакції виклику функції смарт-контракту згортки, який перевіряє відповідність хешу поточного стану у бечі із власним, і у разі збігу замінює власний на новий. Загальна схема згорток подана на рисунку 4.

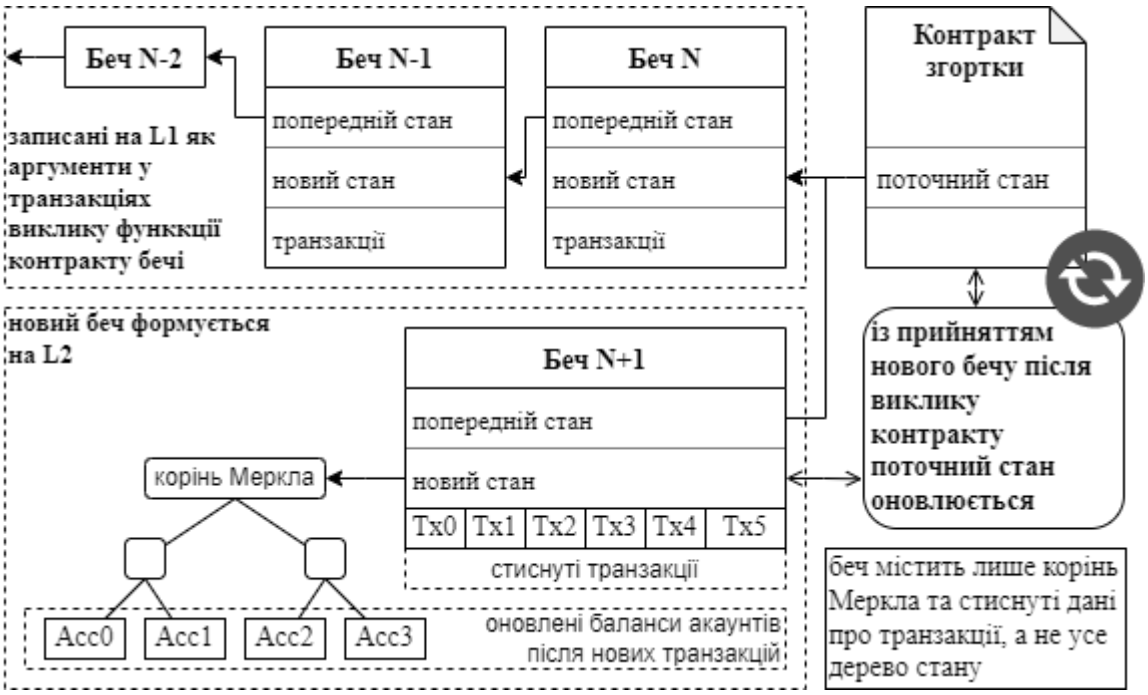

Рисунок 4 – Загальна схема згорток

Транзакції обробляються на другому рівні, де вартість газу набагато дешевша, ніж на першому. Зазвичай, використовуються модифіковані варіанти засобів першого рівня, щоб забезпечувати максимальну сумісність з основним блокчейном та зручність для користувачів. Згортки на мережі Ethereum використовують модифікації EVM – віртуальної машини Ethereum – і забезпечують таким чином більшість різноманітних можливостей Ethereum, як, наприклад, використання смарт-контрактів, зберігання даних, побудова dApp та інше.

Зазвичай згортки підтримуються секвенсорами (sequencer) - суб’єктами, які відстежують стан ланцюга згортки, обробляють надіслані користувачами транзакції у порядку їх надходження, обраховують новий стан згортки, об’єднують оброблені транзакції та роблять беч транзакцію, як тільки новий блок згортки сформований. Згортки також забезпечують у контрактах відповідний функціонал для самостійної публікації транзакцій, вводу активів до мережі другого рівня та виведення їх з неї до основного блокчейну, що унеможливлює цензурування секвенсором.

Кількість даних на основному ланцюзі про транзакції у згортці є мінімальною для забезпечення їх валідації: певні обов'язкові для звичайних транзакцій поля можна значно скоротити, а певні прибрати взагалі – це, разом із використанням оптимальної серіалізації та стисканням даних, дозволяє зберігати в рази більше транзакцій в одній (таблиця 1). За потребою початковий вигляд даних про транзакцію може бути легко відновлений для перегляду користувачами.

Таблиця 1 – Можливе стиснення полів транзакції [37]

Поле	Ethereum, байт	Згортка, байт	Подробиці
Nonce	~3	0	У згортці можна повністю прибрати значення nonce (порядковий номер транзакції акаунту), яке можна відновлювати із попереднього стану мережі. Повторне відтворення транзакції із попереднім значенням nonce не буде успішним, оскільки підпис буде перевірятися разом із даними, які містять актуальне значення nonce.
Gas price	~8	0-0,5	Значення розміру податку можна замінити фіксованим діапазоном значень, або використовувати фіксовані рівні податку для кожного пакету.
Gas limit	3	0-0,5	Ліміт газу може бути зазначеним на рівні усього пакету транзакцій, а не для кожної з них.
To	21	4	Замість збереження повної адреси можна вказувати більш короткий індекс у

Поле	Ethereum, байт	Згортка, байт	Подробиці
			додатковому дереві адрес, яке буде зберігатися у смарт-контракті.
Value	~9	~3	Значення для звичайних транзакцій можна подавати експоненціальним записом.
Signature	~68	~0,5	Для підписів транзакцій може бути застосована BLS [46] агрегація, таким чином значно зменшуючи кількість байтів на підписи для кожної транзакції.
From	0	4	Адреса відправника зазвичай відновлюється із його підпису, проте із використанням методів агрегації підписів, її потрібно зберігати явно. Тут можна застосувати стратегію з індексом у дереві, як і для адреси отримувача.
Разом	~112	~12	Використовуючи ці та схожі техніки можна досягти масштабування у більш ніж сто разів, не залежно від застосування згорток, самих транзакцій та даних у них.

Примітка. Оскільки Ethereum – поки що єдина мережа, де розповсюджені згортки, то поля транзакцій, а також технології, розглянуті у цьому розділі, стосуються саме Ethereum.

Наприклад, згортка Optimism [49] використовує базові методи для стискання даних про транзакції разом із Gzip [47]. Проте досліджуються і більш складні стратегії стискання даних транзакції, які можуть досягати лінійного стиснення даних у більш ніж два рази [48]. Стиснення даних і зменшення їх на першому рівні (тобто на основному ланцюзі) є одним із ключових параметрів ефективності згорток, від якого залежить показник TPS та податки для користувачів за транзакцію: чим більше стиснення, тим більше транзакцій

можна згрупувати до однієї на основному ланцюзі, і тим менше газу (податку), який розподіляється між усіма транзакціями у бечі, доведеться за неї сплачувати на основній мережі. Секвенсер також стягає податок з транзакцій за виконану роботу на другому рівні. Мережі зазвичай достатньо одного секвенсора, для уникнення зайвої роботи, проте, як згадувалось у розділі 2.2 секвенсер згортки Arbitrum піддався DDoS атаці і не міг підтримувати роботу мережі. Загалом згортки не мають механізмів захисту від зловмисного секвенсору, який може затримувати або не обробляти певні транзакції та отримати значний прибуток за рахунок цього.

Оскільки транзакції виконуються поза межами основної мережі, а додавання нового блоку до згортки загалом може бути ініційоване будь-ким, згортки мають реалізовувати певний механізм захисту від шахрайства. Для гарантування коректності нових бечів використовуються два різних підходи, за якими технології згорток можна розділити на два типи:

- оптимістичні згортки (optimistic rollups) – базуються на принципі доказу шахрайства (fraud proof)*;*
- згортки із нульовим розголошенням (zero-knowledge rollups) – використовують доказ валідності (validity proof), який забезпечується криптографічними методами доказів із нульовим розголошенням.

При цьому в кожній із схем достатньо хоча б одного чесного активного валідатора для доведення коректності нового бечу. Коректність усього ланцюга блоків згортки виходить із транзитивного припущення про коректність кожного попереднього блока. Серед запропонованих нових блоків приймається найперший коректний.

Оптимістичні згортки приймають новий беч із припущенням про його коректність та відсутність шахрайських маніпуляцій у ньому. Нові бечі публікуються без будь-якого доказу дійсності хешу нового стану, проте із

певною ставкою в токенах основної мережі. Впродовж певного часу (в оптимістичних згортках Optimism і Arbitrum він дорівнює приблизно семи дням) – «випробувального терміну» ("challenge window") – блок вважається неопрацьованим. У цей період будь-хто, хто помітив некоректну транзакцію чи невідповідність хешів стану, може оскаржити беч опублікувавши доказ шахрайства із запропонованими корекціями та ставкою. Згортка виконує перевірку бечу із виконанням спірних транзакцій за наданим доказом Меркла: спірними станами та проміжними вершини дерева. Якщо опрацювання згорткою доводить некоректність бечу, суб'єкта, що її опублікував, позбавляють його ставки, частина з якої йде на оплату виконаних на основній мережі перевірок, а іншу частину отримує суб'єкт, що надав доказ. За протилежного результату стягненню підлягає суб'єкт, що надав невірний доказ, таким чином запобігаючи спаму некоректними доказами шахрайства. В будь-якому разі в якості поточного стану приймається коректний. Якщо впродовж випробувального терміну не було надано жодного доказу шахрайства, беч автоматично приймається за коректний.

Згортка Arbitrum використовує інтерактивний метод доведення шахрайства, який полягає у зворотному зв'язку між суб'єктом, який опублікував беч, і суб'єктом, надавшим доказ шахрайства. На кожному кроці відсіюється половина кроків доказу, з якою обидві сторони згодні, поки вони не дійдуть до одного суперечливого кроку, який і буде перевірений на основній мережі, що зводить зайві обчислення на ній до мінімуму.

Складною задачею є підтримання повного актуального стану на основній мережі. Проте оптимістичні згортки через свою простоту можуть реалізовувати повний спектр EVM можливостей без особливих змін.

У згортках із нульовим розголошенням бечі мають містити доказ із нульовим розголошенням, який може бути швидко перевірений контрактом згортки на основній мережі, а некоректні бечі одразу ж відхиляються контрактом. В якості доказу використовується ZK-SNARK, перевірка якого

доводить коректність вирахування нового стану. Такий підхід дозволяє прибрати ще більше інформації з бечу, значно скоротивши його. На відміну від оптимістичних згорток, згортки через складнощі пов’язані із обчислення доказу стану мають сильно обмежену функціональність. Виключення є zkSync [56], який повністю сумісний з EVM та може виконувати смарт-контракти на Solidity.

SNARK потребує довіреного початкового налаштування для створення за наданими правилами доказуючої та верифікуючої сторін. Технологія STARK [58], не потребує етапу такого налаштування, хоча доказ у ній набагато більший.

Згортки із нульовим розголошенням є більш безпечними: вони спираються на математику, і вони не потребують криптоекономічних стимулів.

Порівняння основних властивостей різних типів згортки наведено у таблиці 2.

Таблиця 2 – Порівняння основних властивостей різних типів згортки

Властивості	Оптимістичні згортки	Згортки із нульовим розголошенням
Період виводу коштів	У розглянутих оптимістичних згортках остаточне підтвердження бечу займає приблизно тиждень для забезпечення достатнього проміжку часу на перевірку іншими суб’єктами.	Залежить лише від формування наступного нового блоку;
Кількість обчислень на	Невелика: згорткам потрібно лише обробляти нові	Значно більше, оскільки до цього додається обчислення

другому рівні	транзакції та підтримувати актуальний стан.	ZK-SNARK.
Складність реалізації	Оптимістичні згортки прості у реалізації.	Алгоритми ZK-SNARK доволі складні у реалізації.
Сумісність	Оптимістичні згортки сумісні з EVM і реалізують смарт-контракти.	Через складнощі із застосуванням доказів із нульовим розголошенням до виконування смарт-контрактів, більшість згорток цього типу мають дуже обмежену сумісність із можливостями основної мережі.
TPS	Максимальний TPS серед оптимістичних згорток у 146 транзакцій демострує Arbitrum One. Хоча згортки із нульовим розголошенням демонструють більший TPS, оптимістичні згортки користуються більшою популярністю, що відображається у більшому співвідношенні середніх показників TPS за місяць.	Серед згорток із нульовим розголошенням Loopring показує рекорд у 576 TPS. ZKSync, яка реалізує обширний функціонал має власний рекорд у 48,75 TPS.

Примітка. Значення TPS відображені в середньому на блок; дані актуальні станом на 20.06.2022 [59].

Згортки виділяються серед інших рішень другого рівня тим, що загалом повністю сумісні із основною мережею, наслідують її обширний функціонал і

тим самим надають можливість багатоцільового використання. По при це варто зауважити, що контракти не можуть бути перенесені із одного рівня на інший. Згортки також нівелюють проблему доступності даних, притаманну всім іншим рішенням другого рівня і цим значно виграють. Попри це згортки забезпечують не найбільший TPS – найбільші рекорди демонструють сайдчейни із PoS. Серед проблем, притаманних згорткам, можна виділити атаки із сповільненням у оптимістичних згортках та проблему централізації секвенсера.

Згортки реалізовані у мережі Ethereum і спираються на використання смарт-контрактів для контролювання стану системи другого рівня. Окрім Ethereum та інших блокчейнів із моделлю облікових записів (account model), такі ж властивості можуть мати блокчейни із моделлю eUTxO – розширенням звичайної моделі UTxO [41][42], що зберігає певні переваги базової моделі [43], хоча є складною у реалізації та не надто ефективною технологією. Попри це використання такого підходу поки неможливе у звичайних UTxO блокчейнах, таких як Bitcoin, хоча відповідні спроби створити згортки для таких мереж мають місце у 2022 р. [44][45].

ВИСНОВКИ

У цій роботі було розгорнуто оглянуто трилему блокчейну, описано залежності між властивостями блокчейну в контексті трилеми, які роблять неможливим знаходження просто рішення проблеми масштабованості децентралізованих систем не шкодячи іншим властивостям.

Були розглянуті лише декілька підходів до вирішення цієї проблеми. На прикладі розміру блоку було наглядно досліджено проблематику масштабованості та неможливість знаходження простого рішення трилеми, яке б не вимагало компромісів.

Наразі серед багатьох технологічних рішень більшість розробники блокчейн мереж схиляються до впровадження шардінгу (sharding), як універсальне рішення проблеми, що є найменш компромісним. Проте реалізація останнього є комплексною, надскладною задачею.

Серед рішень другого рівня було детально розглянуто згортки (rollups) – принципово новий підхід, вперше представлений у 2021 р. на мережі Ethereum. Його інноваційність полягає у нівелюванні проблеми доступності даних, що притаманна іншим рішенням другого рівня та забезпечує більшу безпеку користувачів, реалізації повного функціоналу основної мережі на другому рівні, що забезпечує багатоцільове використання згорток з набагато меншою комісією. Було порівняно два види згорток як теоретично, так і за реальними показниками роботи і застосування у блокчейні.

Як і кожна нова технологія, згортки знаходяться на етапі пошуку нових застосувань та розширення функціоналу. Недослідженим напрямком є використання згорток у блокчейну з моделлю UTxO, таких як Bitcoin. Наразі з актуальних досліджень є використання доказів із нульовим розголошенням як у згортках, так і в інших блокчейн технологіях. Вони забезпечують високий рівень захисту та децентралізації, оскільки не покладаються повністю на криптоекономіку. Тим не менш реалізація повного функціоналу першого рівня

мережі Ethereum, смарт-контрактів у згортках із нульовим розголошенням потребує подальшого дослідження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Vitalik Buterin. On Public and Private Blockchains [Електронний ресурс] – Режим доступу до ресурсу: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

2. Kathleen E. Wegrzyn Eugenia Wang. Types of Blockchain: Public, Private, or Something in Between [Електронний ресурс] – Режим доступу до ресурсу: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

3. Bitcoin [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoin.org/uk/

4. Lightning Network [Електронний ресурс] – Режим доступу до ресурсу: https://lightning.network/

5. Ethereum Plasma [Електронний ресурс] – Режим доступу до ресурсу: https://ethereum.org/en/developers/docs/scaling/plasma/

6. Vitalik Buterin. Why sharding is great: demystifying the technical properties https://vitalik.ca/general/2021/04/07/sharding.html

7. Harmony [Електронний ресурс] – Режим доступу до ресурсу: blockchain https://www.harmony.one/

8. What Is Ethereum 2.0 And Why Does It Matter? [Електронний ресурс] – Режим доступу до ресурсу: https://academy.binance.com/en/articles/what-is-ethereum-2-0-and-why-does-it-matter

9. Ethereum Shard-Chains upgrade [Електронний ресурс] – Режим доступу до ресурсу: https://ethereum.org/en/upgrades/shard-chains/

10. Jake Frankenfield. Segregated Witness (SegWit) [Електронний ресурс] – Режим доступу до ресурсу: https://www.investopedia.com/terms/s/segwit-segregated-witness.asp#

11. Bitcoin Cash [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoincash.org/

12. Jae Kwon. Tendermint: Consensus without Mining [Електронний ресурс] – Режим доступу до ресурсу: https://tendermint.com/static/docs/tendermint.pdf

13. David Mazieres. Stellar Consensus Protocol: A Federated Model for Internet-level Consensus [Електронний ресурс] – Режим доступу до ресурсу: https://www.stellar.org/papers/stellar-consensus-protocol

14. Are there better, decentralized alternatives to blockchain? [Електронний ресурс] – Режим доступу до ресурсу: https://blog.fasset.com/blockchain-alternative/

15. Joe Abou Jaoude, Raafat George Saad. Blockchain Applications – Usage in Different Domains [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/331460008_Blockchain_Applications_-_Usage_in_Different_Domains

16. Bitcoin Network Capacity Analysis – Part 1: Macro Block Trends [Електронний ресурс] – Режим доступу до ресурсу: https://blog.tradeblock.com/blog/bitcoin-network-capacity-analysis-part-1-macro-block-trends/

17. On Scaling Decentralized Blockchains [Електронний ресурс] – Режим доступу до ресурсу: https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf

18. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf

19. How to time-stamp a digital document [Електронний ресурс] – Режим доступу до ресурсу: https://www.anf.es/pdf/Haber_Stornetta.pdf

20. Improving the Efficiency and Reliability of Digital Time-Stamping [Електронний ресурс] – Режим доступу до ресурсу: https://www.math.columbia.edu/~bayer/papers/Timestamp_BHS93.pdf

21. Wei Dai (1998). "B-Money"1998 [Електронний ресурс] – Режим доступу до ресурсу: http://www.weidai.com/bmoney.txt

22. Nick Szabo. Bit Gold [Електронний ресурс] – Режим доступу до ресурсу: https://unenumerated.blogspot.com/2005/12/bit-gold.html

23. About Ethereum [Електронний ресурс] – Режим доступу до ресурсу: https://ethereum.org/uk/whitepaper/

24. Vitalik Buterin. The Limits to Blockchain Scalability [Електронний ресурс] – Режим доступу до ресурсу: https://vitalik.ca/general/2021/05/23/scaling.html

25. Vitalik Buterin. A Philosophy of Blockchain Validation [Електронний ресурс] – Режим доступу до ресурсу: https://vitalik.ca/general/2020/08/17/philosophy.html

26. Ethereum Classic and the Ethereum hard fork [Електронний ресурс] – Режим доступу до ресурсу: https://help.coinbase.com/en/coinbase/getting-started/crypto-education/eth-hard-fork

27. David Siegel. Understanding The DAO Attack [Електронний ресурс] – Режим доступу до ресурсу: https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

28. Vincent Tabora. The Byzantine General's Problem Solution Using The Blockchain [Електронний ресурс] – Режим доступу до ресурсу: https://medium.datadriveninvestor.com/the-byzantine-generals-problem-solution-using-the-blockchain-31eb5318f37f

29. How Bitcoin Works, Featuring Nash Equilibrium [Електронний ресурс] – Режим доступу до ресурсу: https://blogs.cornell.edu/info2040/2021/09/22/how-bitcoin-works-featuring-nash-equilibrium/

30. Kendra Staggs. Game Theory and Bitcoin: the Miners' Perspective [Електронний ресурс] – Режим доступу до ресурсу: https://saltlending.com/game-theory-and-bitcoin/

31. Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries [Електронний ресурс]

– Режим доступу до ресурсу: https://asset-pdf.scinapse.io/prod/2188530018/2188530018.pdf

32. SegWit [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

33. Jimmy Song. Transaction Malleability Explained [Електронний ресурс] – Режим доступу до ресурсу: https://bitcointechtalk.com/transaction-malleability-explained-b7e240236fc7

34. Segregated Witness Activates On Bitcoin: This Is What To Expect [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoinmagazine.com/technical/segregated-witness-activates-bitcoin-what-expect

35. Segregated Witness Costs and Risks [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoincore.org/en/2016/10/28/segwit-costs/

36. Joseph Poon, Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [Електронний ресурс] – Режим доступу до ресурсу: https://lightning.network/lightning-network-paper.pdf

37. Vitalik Buterin. An Incomplete Guide to Rollups [Електронний ресурс] – Режим доступу до ресурсу: https://vitalik.ca/general/2021/01/05/rollup.html

38. https://forklog.com/chto-takoe-resheniya-masshtabirovaniya-vtorogo-urovnya/

39. The Data Availability Problem - Vitalik Buterin [Електронний ресурс] – Режим доступу до ресурсу: https://youtu.be/OJT_fR7wexw

40. Mustafa Al-Bassam, Alberto Sonnino, and Vitalik Buterin. Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities, 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://arxiv.org/pdf/1809.09044.pdf

41. Understanding the Extended UTXO model [Електронний ресурс] – Режим доступу до ресурсу: https://docs.cardano.org/plutus/eutxo-explainer

42. Manuel Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Michael Peyton Jones, Philip Wadler. The Extended UTXO Model, 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://api.zotero.org/groups/478201/items/T24L95MI/file/view?key=QcjdK4erSuUZ8jvAah59Asef
43. UTXO VS. ACCOUNT MODEL [Електронний ресурс] – Режим доступу до ресурсу: https://academy.horizen.io/technology/expert/utxo-vs-account-model/
44. ZK-Rollups for Bitcoin research fellowship announce - https://twitter.com/gladstein/status/1501655418153570305
45. Bitcoin / ZK-Rollup Research Fellowship - https://hrf.org/zkrollups
46. Pragmatic signature aggregation with BLS [Електронний ресурс] – Режим доступу до ресурсу: https://ethresear.ch/t/pragmatic-signature-aggregation-with-bls/2105
47. Optimism The Canonical Transaction Chain Format [Електронний ресурс] – Режим доступу до ресурсу: https://community.optimism.io/docs/protocol/compressed-ctc/#ctc-transaction-type-zero
48. Rollup diff compression - application level compression strategies to reduce the L2 data footprint on L1 – Ethreserch topic [Електронний ресурс] – Режим доступу до ресурсу: https://ethresear.ch/t/rollup-diff-compression-application-level-compression-strategies-to-reduce-the-l2-data-footprint-on-l1/9975
49. Optimism [Електронний ресурс] – Режим доступу до ресурсу: https://community.optimism.io/
50. Bitcoin Transactions Confirmation Delays [Електронний ресурс] – Режим доступу до ресурсу: https://cointelegraph.com/news/bitcoin-transactions-confirmation-delays
51. Transaction malleability [Електронний ресурс] – Режим доступу до ресурсу: https://en.bitcoin.it/wiki/Transaction_malleability

52. What is Segwit? Segregated Witness Explained Simply [Електронний ресурс] – Режим доступу до ресурсу: https://youtu.be/f3CFUbeehc8
53. BIP-0062 [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki
54. Daniel Phillips. Transaction Malleability: What Is It And Why Is It Still A Problem? [Електронний ресурс] – Режим доступу до ресурсу: https://beincrypto.com/transaction-malleability-what-is-it-and-why-is-it-still-a-problem/
55. Rob Behnke. How Blockchain Ddos Attacks Work [Електронний ресурс] – Режим доступу до ресурсу: https://halborn.com/how-blockchain-ddos-attacks-work/
56. zkSync [Електронний ресурс] – Режим доступу до ресурсу: https://zksync.io/
57. Dimitar Bogdanov. Optimistic Rollups vs ZK Rollups: Examining Six of the Most Exciting Layer 2 Scaling Projects for Ethereum [Електронний ресурс] – Режим доступу до ресурсу: https://limechain.tech/blog/optimistic-rollups-vs-zk-rollups/
58. STARKEx [Електронний ресурс] – Режим доступу до ресурсу: https://starkware.co/starkex/
59. ETHTPS.info [Електронний ресурс] – Режим доступу до ресурсу: https://ethtps.info/