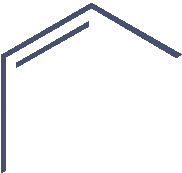
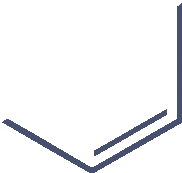
[електроніка](http://www.mdpi.com/journal/electronics)



*Стаття*

**Імітаційна модель для блокчейн-систем з використанням теорії масового обслуговування**

# Рахіл Ахмед Мемон 1,2,\* , Цзянь Пін Лі 1 і Джунаїд Ахмед 3

1. Школа комп'ютерних наук, Університет електронних наук і технологій , Ченду 611731, Китай;  [jpli2222@uestc.edu.cn](mailto:jpli2222@uestc.edu.cn)
2. Кафедра комп'ютерних наук, Університет Суккур IBA, Суккур 65200, Пакистан
3. кафедра електротехніки, Університет Суккур IBA, Суккур 65200, Пакистан;  [j.bhatti@iba-suk.edu.pk](mailto:j.bhatti@iba-suk.edu.pk)

**\*** Листування: [raheelmemon@iba-suk.edu.pk](mailto:raheelmemon@iba-suk.edu.pk)

Отримано: 26 січня 2019 року; прийнятий: 13 лютого 2019 року; Опубліковано: 19 лютого 2019

[Перевірте Рор](http://www.mdpi.com/2079-9292/8/2/234?type=check_update&version=1)

**[Оновлення](http://www.mdpi.com/2079-9292/8/2/234?type=check_update&version=1)**

**Анотація:** В останні роки блокчейни привернули стільки уваги з боку дослідників, інженерів та установ, а впровадження блокчейнів почало відроджувати велику кількість додатків, починаючи від електронних фінансів, електронної охорони здоров'я, розумного будинку, Internet of Things, соціального забезпечення, логістики тощо . У літературі про блокчейни виявлено, що більшість статей були зосереджені на їх інженерній реалізації, в той час як мало уваги було приділено дослідженню теоретичних аспектів system, однак існуюча робота обмежується лише моделюванням процесу видобутку. У даній роботі пропонується модель, заснована на теорії черги для розуміння робочих і теоретичних аспектів блокчейна. Ми підтверджуємо запропоновану нами модель, використовуючи фактичну статистику двох популярних криптовалют, Bitcoin та Ethereum, проводячи моделювання протягом двох місяців транзакцій. Отримана продуктивність вимірює такі параметри, як кількість транзакцій на блок, час майнінгу кожного блоку, пропускна здатність системи, кількість пам'яті, час очікування в Memorypool, кількість непідтверджених транзакцій у всій системі, загальна кількість транзакцій та кількість згенерованих блоків; Ці значення порівнюються з фактичною статистикою. Було встановлено, що результати, отримані від запропонованої нами моделі, добре узгоджуються з реальною статистикою. Хоча моделювання в цій роботі представляє моделюваннялише криптовалют на основі blockcha, запропонована модель може бути використана для представлення широкого спектру систем на основі блокчейну.

**Ключові слова:** моделювання блокчейну; Теорія блокчейн-черг; Імітація біткоїну; Моделювання Ethereum; Симуляції криптовалюти

# Введення

У 2008 році невідома особа або група під псевдонімом «Сатоші Накамото» ввела революційну концепцію систем електронних грошових коштів Peer-to-Peer (P2P) і назвала її «Bitcoin» (цифрова валюта ). Ця система цифрових валют P2P була спрямованана те, щоб запобігти залученню третіх сторін до фінансових операцій між невідомими надійним та перевіреним способом [[1](#_bookmark20)]. У січні 2009 року ця ж група або особа зробили програмне забезпечення доступним у вигляді відкритого вихідного коду і запустилипершу в історії цифрову валюту [[2](#_bookmark21)]. Основною технологією Bitcoin є блокчейн, який забезпечує послідовний і незмінний впорядкований список блоків транзакцій, пов'язаних між собою, з усіма аналогами в Мережа P2P, що підтримує власну копію блокчейну, відому як розподілена книга. Основним протоколом валюти Bitcoin є консенсус, який вимагає від усіх аналогів у мережі узгодження кожного окремого запису блоку в розподіленій книзі [ 1,3].

Останнім часом блокчейнам приділяється величезна увага з боку декількох дослідників. Поява технології блокчейн у вигляді цифрових валют вплинуло на багато інших

*Електроніка* **2019**,  *8*, 234; doi:[10.3390/electronics8020234](http://dx.doi.org/10.3390/electronics8020234) [www.mdpi.com/journal/electronics](http://www.mdpi.com/journal/electronics)

такі сфери, як електронна охорона здоров'я, електронне фінансування, нерухомість, електронне голосування, ланцюги поставок, розумні будинки, розумні міста , розумні галузі , Інтернет речей тощо [[3](#_bookmark22)–[6](#_bookmark23)]. Популярність блокчейнів природна, оскільки вони мають потенціал надати бажані функції, замінивши централізовані архітектури зв'язку. Але проблема біткойна полягає в тому, що він вимагає трудомістких процесів для досягнення безпеки та цілісності системи, а Bitcoin mining вважається процедурою, що забирає багато часу та ресурсів [7,8 ].

Було кілька спроб скоротити необхідний час і підвищити продуктивність за рахунок модифікації характеристик базових алгоритмів. Нові криптовалюти, подібні до біткойна, називаються альт-монетами; в даний час Ethereum, BitShares, Dash, DogeCoin, LiteCoin, PeerCoin і Ripple є найвідомішими валютами, які були натхненні біткойнами [[9](#_bookmark26)–[15](#_bookmark27)]. Сьогодні існує 2116 криптовалют [[16](#_bookmark28)], і більшість з них створені на одній і тій же розподіленій технології блокчейн , хоча і зі зміненим набором принципів і поліпшені характеристики [[15](#_bookmark27)].

Оскільки більшість додатків реалізують блокчейн, аналітичне моделювання та моделювання блокчейн-систем мають важливе значення для оцінки ефективності таспостереження за поведінкою d . На жаль, менше зусиль було приділено імітаційному моделюванню блокчейнів [[17](#_bookmark29)]; статей в літературі дуже мало, і майже всі вони тільки аналітичного моделювання біткоіни. Quan-Lin Li et al. [[17](#_bookmark29)] описав цілий блокчейн, зокрема лише операції з видобутку, використовуючи єдину чергу; транзакції в черзі передбачалися для процесу генерації блоків, а транзакції в обслуговуванні припускалися для процесу побудови блоків. Йошіакі Кавасе [[18](#_bookmark30)] надав дослідження з теорії масового обслуговування, щоб повторитичас підтвердження транзакцій для біткойна. Деяка робота також була виконана з теорії ігор Бісіасом та ін. [[19](#_bookmark31)], Левенберг та ін [[20](#_bookmark32)] і Хоуй та ін [[21](#_bookmark33)].

У цьому папер ми зробили імітаційне моделювання системи блокчейн з використанням теорії масового обслуговування. Запропонована модель може бути використана для спостереження за реалістичною поведінкою як пам'яті, так і пулу майнінгу для будь-якої системи блокчейну. На відміну від попередньої роботи, наш процес посилюється кількома способами; він забезпечує спрощене моделювання для моделювання як пулу пам'яті за допомогою M/M/1, так і пулу майнінгу за допомогою черги M/M/c, а також надає більш детальні спостереження за обома. Використовуючи запропоновану модель, ми представляємо observations для таких важливих показників, як кількість транзакцій на блок, час майнінгу кожного блоку, кількість транзакцій в секунду, кількість memorypool, час очікування в пулі пам'яті, кількість непідтверджених транзакцій у всій системі, загальна кількість транзакцій і кількість згенеровані блоки.

Запропонована модель для нашого блокчейну вперше була використана для отримання ідеальної статистики в симуляції Bitcoin. А потім він використовувався для перевірки даних з блокчейн-додатків Bitcoin і Ethereum в режимі реального часу. Статистика із запропонованої моделі порівнюється з фактичною статистикою, і було встановлено, що запропонована модель змогла оцінити сценарії в реальному часі лише з незначними помилками.

Решта статті впорядкована як follows: розділ [2](#_bookmark0) охоплює фони Bitcoin, Ethereum та їх базових технологій блокчейну. У розділі [3](#_bookmark3) йдеться про запропоновану еталонну модель; У розділі [4](#_bookmark6) представлені деталі налаштування моделювання пулу пам'яті і процесу майнінгу з використанням моделі теорії масового обслуговування в JMT, JSIMgraph, і представлені отримані результати. Розділ [5](#_bookmark11) підтверджує наш model, моделюючи 60-денну фактичну статистику як для Bitcoin, так і для Ethereum, і порівнює отримані результати з фактичною статистикою; У розділі [6](#_bookmark18) наведена запропонована імітаційна модель для декількох типів реалізацій блокчейнов. Висновок наведено в розділі [7](#_bookmark19).

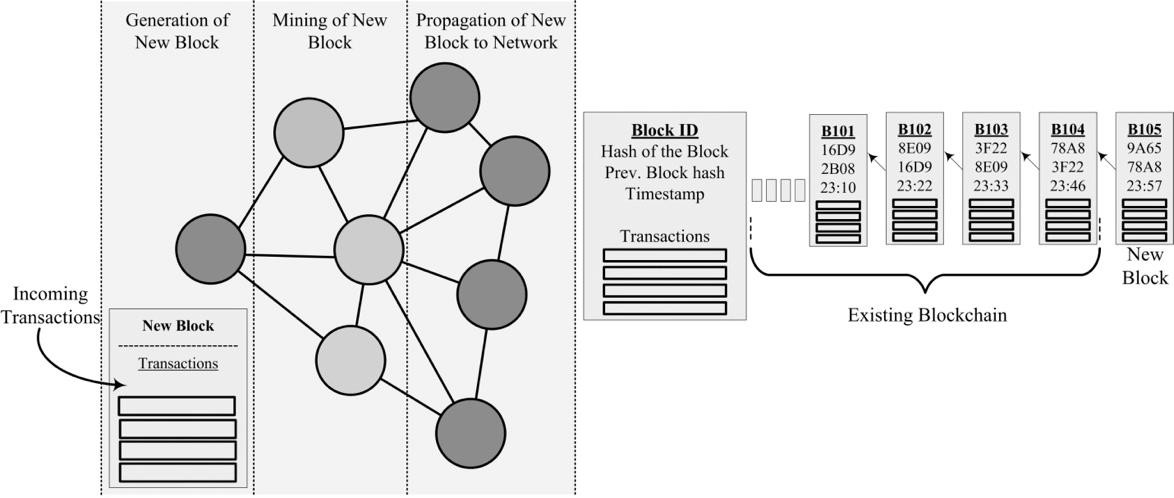
# Попередні

Щоб зрозуміти блокчейни, ми встановлюємо Bitcoin як наше посилання в цьому розділі. Bitcoin - це система електронних грошових коштів P2P, основною технологією якої є блокчейн. Біткойн перешкоджає залученню третіх сторін (наприклад, банків), поширюючи кілька копій блоків транзакцій серед аналогів мережі [[1](#_bookmark20)]. Кожен учасник мережі блокчейн веде своє власне сховище даних для зберігання транзакцій, відоме як розподілена книга [[19](#_bookmark31)]. Як і в P2P-мережах, всі бенкети рівні, т. Е. Кожен вузол в мережі здатний надавати і споживати послуги. Аналогічно, в мережі Bitcoin P2P транзакції можуть ініціюватися будь-ким у мережі та поширюватися в неструктурованих

децентралізовані мережі для надання послуг, де будь-хто інший може виконувати функції майнера [[1](#_bookmark20)]. В даний час біткойн володіє максимальною часткою ринку криптовалют, т. Е. 52, 5% [[16](#_bookmark28)].

У біткоіни транзакції записуються за допомогою криптографічного підпису відправника і транслюються в мережу. Ініційована транзакція залишається непідтвердженою в тимчасовому заповнювачі на вузлах мережі, відомому як пул пам'яті [[22](#_bookmark34)]. Як тільки пул досягне певного розміру або визначеного часу для створення блоку , будь-хто в мережі може вибрати ці транзакції та об'єднати їх для створення нового блоку; потім блок сигнед за допомогою кореня Меркле, який містить інформацію про всі транзакції в ньому [[1](#_bookmark20)]. Потім новий блок перевіряється на валідність шляхом вирішення трудомісткої математичної головоломки для пошуку правильного nonce майнером; дійсний блок, що містить дійсні транзакції, потім додається до локального блокчейну, і далі поширюється в мережі з тією ж головоломкою і виявленим нонсом, який використовувався для вирішення головоломки, як доказ роботи шахтаря [1,23].

Отримані вузли перевіряють, чи справедливий знову видобутий блок. Якщо так, він додається до їхнього локального блокчейну та пересилається до подальших мереж, що призводить до його остаточного поширення по всій мережі. Майнер, який виявив нонс для блоку, отримає винагороду за свіжий випуск біткоіни [[20](#_bookmark32)], [[24](#_bookmark36)]. На рисунку [1](#_bookmark1) показаний повний процес майнінгу нового блоку транзакцій і додавання його до блокчейну.



**Малюнок 1.** Транзакції в мережі Біткойн.

Кожен окремий блок являє собою пакет даних із заголовком і корисним навантаженням. Заголовок містить метадані: ідентифікатор блоку, хеш блоку, хеш попереднього блоку та позначку часу. Розділ корисного навантаження містить тільки транзакції. Блокчейн - це незмінна книга transactions; кілька копій усіх транзакцій записуються як книга і розподіляються по однорангових вузлах у мережі, відомій як "розподілена книга". Не існує жодної головної або свинцевої копії розподіленої книги для зміни блоків після того, як вони будуть додані бджолоюn [[25,26](#_bookmark37)]. У цій книзі блоки пов'язані з попереднім блоком за допомогою хешу попереднього блоку. Цей ланцюжок зв'язку з попередніми блоками піднімається до блоку Буття (першого блоку), видобутого Сатоші Накамото 3 січня 2009 року [[27](#_bookmark39)].

Символічно, що блокчейни можна розглядати як впорядковану пару (*G*, *B*); де G represents

Блок Генезису і В є основним ланцюгом блоків:

*В* = [б 1, б 2, *б*3. . . б н*−*1, *бн*]

Додавання нового блоку b n вимагає перевірки його істинного зв'язку з попереднім блоком *b n−*1; Після того, як блок перевірений, він appзакінчується на ланцюжку. У біткоіни нові блоки are генеруються з частотою кожні 10 хвилин [[1](#_bookmark20)]. Порушити цілісність блокчейну шляхом внесення змін до bn*−*m математично є дуже diffi культовим завданням, яке r equires величезна кількість обчислювальної потужності

в порівнянні навіть з тим, що потрібно в процесі видобутку [[1](#_bookmark20)]. Прибуття кожної транзакції та додавання нещодавно видобутих блоків у блокчейн є 5-етапним процесом, як показано на рисунку [2](#_bookmark2).



**КРОК-1**

Надходження нових транзакцій



**КРОК-2**

Пул пам'яті



**КРОК-3**

генерація блоків



**КРОК-4**

Гірничі процеси



**КРОК-5**

Новий блок для блокчейну

* 1. *Надходження нових транзакцій*

**Малюнок 2.** Новий потік процесу додавання блоків .

Всі вузли мережі можуть ініціювати транзакції з передачі цифрових активів в доступні аналоги в мережі [[28](#_bookmark40)]. Прихід нових транзакцій є незалежним фактором, і він змінюється з кожним днем, в біткойнах кількість транзакцій варіюється від 200 000 до 350 000 в день.

* 1. *Пул* пам'яті

Пул пам'яті являє собою тимчасовий заповнювач або загальний простір, який доступний всій мережі для накопичення транзакцій, де вони чекають, коли їх підберуть майнери для майнінгу [[29](#_bookmark41)]. Транзакції очікування in пулу називаються непідтвердженими транзакціями. У випадку з біткоіни через кожні 10 хвилин майнер вибирає обмежену кількість транзакцій накопиченого розміру в 1 Мб для формування блоку для Майнінг [[30](#_bookmark42)]. Після видобутку блоку ці транзакції більше не залишаються непідтвердженими, а стають частиною блоку в блокчейні [[28](#_bookmark40)]. На момент написання статті в мережі Біткойн існує 5000+ непідтверджених транзакцій ([https://www.blockchain.com](https://www.blockchain.com/)). Цей розмір пулу пам'яті дуже динамічний і постійно зростає або скорочується відповідно до кількості вхідних unconfirmed і залишають підтверджені транзакції.

* 1. *генерація* блоків

Через дорогі обчислювальні ресурси в минулому робочі місця тримали на паузі для операцій обробки, які повинні виконуватися партіями. Аналогічно, в системах блокчейн транзакції зберігаються on hold до досягнення певного часу і розміру з двох причин: одна, процес майнінгу дорогий, і дві, поширення вже видобутого блоку в мережі [[31](#_bookmark43)]. Після того, як час і розмір дотримані, майнерам дозволяється формувати партію. У блокчейн-системах партія відома як блок. Один блок варіюється за кількістю транзакцій; у біткойнах кількість транзакцій на блок становить від 1000 до 25001.

* 1. *процес* видобутку

Видобуток блоків- це процес пошуку одного правильного цільового значення шляхом ітерації через мільярди значень, відомих як "nonce" [[32](#_bookmark44)]. Вузли мережі з можливостями майнінгу починають знаходити цільове значення шляхом ітерації та збільшення nonce в кожному циклі. Цей процес складний і вимагає величезних обчислювальних потужностей, щоб знайти правильний нонсенс. Знаходження правильного nonce можна представити у вигляді:

*Хеш* (*BlockHeader ∪ nonce*) *≤ D*

де *Hash*  - криптографічна хеш-функція (наприклад, SHA256), Blockheader - це новий набір транзакцій, що вимагають додавання над книгою як нового блоку, *∪*  - операція об'єднання, а *D* - глобальний параметр, який визначає головоломку.

Після того , як nonce небуде охоплений, новий блок додається до локального блокчейну самого майнера, тоді як метадані блоків та виявлені як Proof-of-Work транслюються іншим аналогам у мережі для перевірки та оновлення їх локальної копії розподіленої книги блокчейну [[23](#_bookmark35)]. Результат цього процесу видобутку двоякий; по-перше, він вводить в економіку нові криптовалютні монети у вигляді винагород для майнерів; а по-друге, він здійснює криптоплатіж

система сильна, надійна і безпечна завдяки потужним комп'ютерам. Теоретично майнер(и) час майнера (-ів) на видобуток блоку становить 600 секунд, і за добу по всій мережі Біткойн може бути видобуто 144 блоки [[1](#_bookmark20)]. Однак фактична кількість блоків, що генеруються щодня, і середній час, витрачений блоком, є нестабільним через додавання нової потужності майнінгу щодня, яку можна розрахувати як:

*Вn* = *Т*

*Бт*

Для підтримки часового проміжку між блоками, видобутими майнерами, існує рівень складності математичної головоломки, який регулюється відповідно до наявних ресурсів видобутку. Рівень складності математичної головоломки регулюється, іпрограмне забезпечення Bit coin відстежує новостворені блоки протягом двох тижнів або блоків 2016 року, як жорстко закодовані (https://github.com/trottier/original-bitcoin) в системі Bitcoin, ( 144 *×* 14 = 2016) для визначення рівня складності [[19,33](#_bookmark31)]

*Ціль* = *Ціль*  *t*

*нові старі·*

2016 *×* 600

де *t* - загальний час , витрачений в процесі видобутку за попередні блоки 2016 року.

Якщо частота генерації блоків більше 2016 року за два тижні, рівень складності математичних головоломок зростає. В даний час включення графічних процесорів (GPUs) і прикладних специфічних інтегральних мікросхем (ASIC) майнерів підвищило рівень складності математичних головоломок таким чином, що звичайному комп'ютеру знадобилося б більше року, щоб вирішити головоломку пошуку nonce для одного блоку [[34](#_bookmark46)].

Таким чином, видобуток біткойнів - це гонка між майнерами; тим швидше один отримає винагороду, а інші підуть з порожніми руками [[35](#_bookmark47)]. Таким чином, майнер з більшою хеш-потужністю має можливість вирішувати доказ роботи більш quickly, ніж будь-хто інший. Це, як правило, об'єднує майнерів у групи, відомі як Mining-Pools; ці угруповання підвищують ймовірність виграшу свіжозібраних біткоїнів [[36](#_bookmark48)]. Майнінг-пул - це мережа майнерів; Майнінгова мережа = [A, B, C, D, E] де

А = [а 1, а 2, а 3, а 4. . . an] - сукупність майнерів, що утворюють групу.

Винагорода - це спосіб випустити нові біткойни в економіку та запропонувати компенсацію за зусилля майнерів. Спочатку винагорода за майнінг блоку становила 50 біткоіни. За правилом, ця винагорода зменшується вдвічі кожні 4 роки або кожні 210 000 блоків (ще одне правило з жорстким кодуванням у програмному забезпеченні Bitcoin)2. До цього часу було 2 половинки; у 2013 році винагорода за блок становила 25 біткоїнів, а в 2016 році стала

12.5 біткоїни.

* 1. *Новий блок для блокчейну*

Після того, як блок видобувається майнером, він додається до їх локального блокчейну і транслюється в мережу з тією ж головоломкою і виявленим нонсом, що і його PoW. Всі інші в мережі тепер більше не намагатимуться вирішити цей блок, натомість вони поганоперевіряють блок, вирішуючи головоломку з наданим недоліком. Якщо він дійсний, то вони також додадуть блок до свого локального блокчейну. Цей процес відомий як «Консенсус», коли всі або більшість вузлів досягають угоди про додавання нового block до свого блокчейну [[37,38](#_bookmark49)].

* 1. *Ефіріум*

Ethereum є найвідомішою блокчейн-платформою після Bitcoin, з цифровою валютою під назвою «Ефір» [[39](#_bookmark51)]. Криптовалюта Ether використовується для виконання смарт-контрактів між невідомими сторонами для транзакцій. The базова технологія Ethereum використовує блокчейн, але вона носить більш універсальний характер [[40,41](#_bookmark52)]. Смарт-контракт в Ethereum надає послугу довіри між невідомими сторонами. А прикладнііони, що використовують смарт-контракт Ethereum, варіюються від розумної системи голосування, реєстрації доменних імен, контрактів та угод, операцій з нерухомістю та розподілених автономних організацій [[39,42](#_bookmark51)]. Ethereum відрізняється від біткойна кількома способами; на відміну від Bitcoin, він розраховує обчислення та зберігання за допомогою газової метрики; Газ має обмеження для мережі, яке може бути

споживається однолітками в мережі. Ставлячи обмеження на мережу з точки зору використання газу, вона захищає від перевантаження. Також частота генерації блоків в Ethereum зустрічається дуже часто [[9,38,43](#_bookmark50)]. Граничний обсяг газу і частота генерації блоків детально розглянуті далі в розділі  [4](#_bookmark6).

* 1. *Теорія* масового обслуговування

Теорія масового обслуговування - це математичний метод аналізу різних типів систем і спостереження за їх поведінкою, пов'язаним з продуктивністю системи і якістю обслуговування. Вона варіюється від аналізу ланцюгів обслуговування до довільних складних черг величезних мережевих систем. Зазвичай він використовується для аналізу розподілу ймовірностей в просторі безперервного стану [[44,45](#_bookmark56)]. Кілька моделей систем масового обслуговування представлені нотацією Кендалла для класифікації типів систем і подій їх черг. Всі типи уявлень описуються за допомогою трьох факторів, т. Е. A/S/c, де A - прибуття, S - розмір роботи і c - число станції обслуговування [[46](#_bookmark58)]. Популярними альтернативними позначеннями є M/M/c, і в решті статті ми будемо використовувати цю номенклатуру. У цій статті ми зосередимося на двох варіаціях типів черг і парі станцій Fork-Join в об'єднанні для запропонованої нами моделі M/M/1 і M/ М/бл. Модель M/M/1 використовується для моделювання пулу пам'яті блокчейну. У цій моделі прибуття є Poisson-Distributed і час обслуговування розподілено в геометричній прогресії, в той час як кількість станцій обслуговування тільки одна. Майнінг-пул моделюється за моделлю M/M/c; У даній моделі кількість серверів більше одного. У реальних сценаріях майнери працюють у величезній мережевій групі для вирішення єдиної блокової головоломки. Аналогічно, в нашій моделі в системі є кілька майнерів для вирішення

єдиний блок Транзакцій.

Fork-Join - це дві станції, такі як черги, які використовуються для досягнення швидкої обробки та мінімізації часу обслуговування; у багатьох випадках робоче навантаження системи абстрагується як робочі місця і розбивається на кілька керованих завдань. Всі завдання синхронізуються і пересилаються для обробки p arallel (можливо, різнорідними серверами) і знову об'єднуються як завдання після завершення всіх супутніх завдань [[47](#_bookmark59)]. При паралельній обробці це поняття також відоме як «нитки».

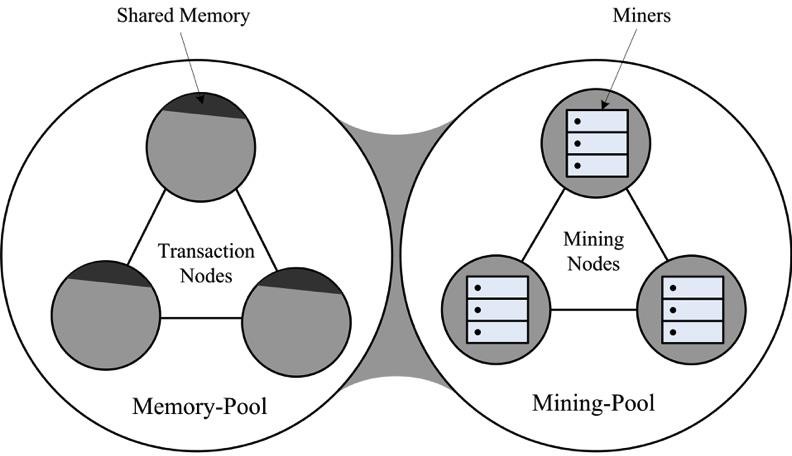
Як правило, c розмірні станції Fork-Join є частиною системи масового обслуговування , яка управляється  *за номером c*

паралельних серверів; Сервери синхронізовані для потоку приходу і вильоту завдань з черги. Замовник надходить в систему партіями розміром J розміром не більше кількості серверів  *J ≤ c*. У форк-примітивах *J* число клієнтів відразу присвоюється c номеру Серверів для паралельної обробки. Після того, як *J* кількість клієнтів, задіяних в партії, завершить обслуговування, партія негайно формується на станції Join. Станція Join синхронізована зі станцією Fork і володіє тимчасовим буфером пам'яті нескінченної ємності, де обслуговуються клієнтичекають возз'єднання з клієнтами, обслуговування яких ще не завершено [[48](#_bookmark60)].

Черги Fork-Join вивчаються в області моделювання дискових масивів, паралельної обробки і розподілених систем [[49](#_bookmark61)]. Для отримання додаткової інформації про аналітичне моделювання черг For-Join, будь ласка, зверніться до книги Геленбе [[50](#_bookmark62)] та Cheeha Kim And Ashok K. Стаття Агували для аналізу черги вилкового приєднання [[51](#_bookmark63)]. Аналіз черг, використаних у статті, тобто М/М1 та М/М/с, наведено у книзі Лазівської Едуарда та ін.[[52](#_bookmark64)].

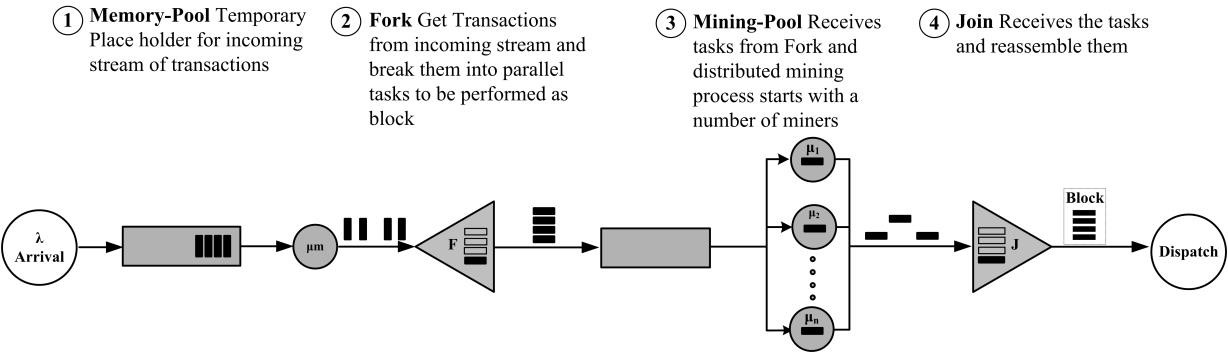
# Пропонована модель

Як зображено на рисунку [3](#_bookmark4), ми розділилимережу блокчейн на два типи пулів: один тип вузлів має справу з непідтвердженими транзакціями в Memory-pool, де транзакції, згенеровані різними користувачами, накопичуються для відправки майнерам. Другий - мережа вузлів Майнінг (Mining-pool); ці бенкети мереж вибирають транзакції з пулу пам'яті, щоб згенерувати блок і почати їх видобуток. У будь-який момент часу в майнінг-пулі може бути тільки один блок. Однак всередині майнінг-пулу майнінг-завдання можна розділити на численні множинні завдання або потоки для паралельної обробки в декількох вузлах видобутку в мережі. Але всі ці робочі місця повинні бути частиною одного блоку, як тільки робота з видобутку блоку буде виконана, всі частини знову об'єднуються на станції приєднання і відправляються до решти мережі.



**Малюнок 3.** Мережа блокчейн розділена на два типи пулів.

На рисунку [4](#_bookmark5) представлена запропонована модель нашої системи блокчейн; Ми розглядаємо пул пам'яті як єдину чергу з одним сервером, а пул майнінгу з кількома номерами серверів або майнерів, як правило, на кілька більше, ніж розмір блоку. Однак справжня мережа блокчейн складається з сотень мільйонів користувачів і майнерів, і запропонована модель також може бути масштабована для цієї мети. Але для простоти ми вибрали найпростішу модель для обговорення тут. Пул пам'яті налаштовується за допомогою M/M/1, а майнінг-пул з чергою M/M/c. Майнінг-пул розміщується між набором станцій Fork і Join. Вилка використовується для двох цілей; Перший полягає в тому, щоб накопичити транзакції для управління заданим розміром блоку заnd раз, а другий - генерувати потоки, які будуть видобуватися кількома майнерами паралельно. Ємність форка обмежується одним розміром блоку, як тільки досягається необхідна кількість транзакцій. Кожна транзакція перетворюється в один потік (однак, потоків для однієї транзакції може бути багато) і передається в пул майнінгу, де ряд майнерів з пулу можуть отримати потоки для виконання операції майнінгу на всіх потоках одночасно. Після завершення майнінгу всі транзакції повинні бути приєднані до станції, де всі потоки блоку накопичуються, утворюючи блок, який потім перенаправляється в мережу.



**Малюнок 4.** Робочий процес запропонованої моделі для систем на основі блокчейну.

Для досягнення ідеального часового проміжку між блоками майнінг-пул налаштовується на сервіс час, еквівалентний 600 секундам для майнінгу кожного блоку. Наприклад, якщо угод 2000 В a блокувати грн. необхідний Гірничо Час є 600-і роки і грн. нуMber з Гірничо Вузлів В грн. Гірничо пул є 2100; то служба Час для a Гірничо Вузол Можете бути Обчислювані як: 2100/600 = 0.0015873.

2000

Вилкова станція не отримує нових робочих місць, якщо вже досягла максимальної потужності. В якості

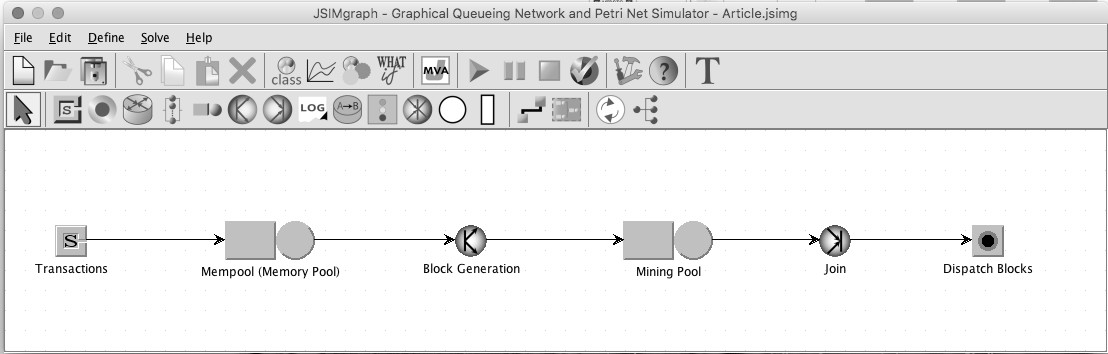
форк-станція налаштована з кінцевою ємністю для розміру блоку, надлишкові транзакції можуть бути відкинуті, а в мережі Blockchain пакет або транзакція не можуть бути втрачені через трансляцію вхідних транзакцій в кілька вузлів однорангової мережі. Щоб подолати проблему падіння в нашій моделі, ми використовували правило Block After Service (BAS) на форк-станції , так що якщо кількість транзакцій вже досягла розміру блоку b, пул пам'яті не зможе відправити подальші операції; натомість ці транзакції накопичуються в пулі пам'яті.

У нашій запропонованій моделі ми використовували політику черги першого приходу (FCFS) для моделювання всіх станцій, включаючи пул пам'яті, вилку та майнінг-пул. Однак політика масового обслуговування може бути змінена під конкретний тип моделювання. Прихід транс-ctions слідує за Poisson-Distribution, і після майнінгу та приєднання транзакцій блок транзакцій залишає систему.

# Налаштування та результати моделювання

Ми змоделювали запропоновану нами модель в Java Modeling Tools (JMT, Politecnico di Milanano, 1.0.3, Мілан, Італія), наборі інструментів з відкритим кодом. Це дискретний симулятор подій для оцінки продуктивності; набір включає інструменти для загального призначення моделювання сіткиnd Petri, ідентифікації вузьких місць, характеристики робочого навантаження та моделей ланцюга Маркова. Він також надає такі функції, як вилка-з'єднання, область кінцевої ємності та кілька типів розподілів для прибуття та обслуговування на будь-якій станції. На додаток до цього, він має опцію аналізу  *whatif* для повторення сценаріїв протягом декількох разів шляхом зміни тарифів на прибуття або обслуговування [[53](#_bookmark65)].

Моделювання запропонованої моделі складається з малогабаритноїсистеми Blo ckchain, про що йшла мова в більш ранньому розділі. На рисунку [5](#_bookmark7) представлена настройка моделювання в JSImgraph. Запропонована модель складається з вихідної станції під назвою «Транзакції», двох станцій черги, M/M/1 під назвою «Mempool» та M/M/c під назвою «Майнінг пул», одного набору станцій для приєднання до вилки під назвою «Block-Generation» та «Join», і, нарешті, станції раковини під назвою «Диспетчерські блоки».



**Малюнок 5.** Імітаційна модель для системи блокчейн з використанням JSImgraph.

* 1. *Розрахунок параметрів моделювання*

На запропонованій нами моделі було проведено три різні імітаційні експерименти; перший - з синтаксично ідеальною статистикою біткойна за один день, тоді як два інших моделювання були виконані для фактичної статистики Bitcoin та Ethereum, отриманої від надійних дослідників протягом 60 днів транзакцій (для Bitcoin [www.blockchain.com](http://www.blockchain.com/); Для Ethereum [www.etherscan.io](http://www.etherscan.io/); та [www.etherchain.org](http://www.etherchain.org/);). Однак там, де це потрібно, параметри розраховуються за формулами, розглянутими в цьому розділі.

На момент написання статті в біткоіни середня кількість транзакцій на блок - 2002 рік, середня кількість підтверджених транзакцій в секунду - 3, 056, а середня кількість блоків в день - 1333. Однак середній розмір транзакції можна розрахувати за розміром блокчейну/загальною кількістю транзакцій, яка зросла з 308 тo 560 байт з 2011 по 2018 рік [[www.blockchain.com](http://www.blockchain.com/)]. Крім того, зберігаючи обмеження Біткойна, що розглядаються, як жорстко закодовані в блокчейні Сатоші для Біткойн:

* Розмір блоку не повинен перевищувати 1 Мегабайт
* Час генерації блоку та майнінгу має становити 600 секунд (10 хвилин)

Ми взяли щедрі цифри для симуляційних цілей. Ми розглянули, що одна транзакція розміром 500 байт і 1 Мегабайт дорівнює 1048576 байтам; таким чином, 1048576 ÷ 500 *≈*  2100 транзакцій на блок, тому 2100 *÷* 600 = 3,5 - це середня кількість підтверджених транзакцій в секунду, а

Всього видобуто 144 блоки, при цьому 2100 *×* 144 = 302400 - загальна кількість транзакцій за день. Кількість блоків,  *βn*, можна розрахувати за допомогою:

*T*

*βn* = *βт*

де *T* - загальний час , *а βt* - час блок-майнінгу. Для імітації одного дня *T* становить 86400 секунд,  *а* в ідеалі β *t* - 600 секунд. Середня кількість транзакцій на блок *βTx* можна розрахувати як:

*Тхдобу*

*βTx* = *βn*

*де Txday* – кількість Транзакцій за день, яку можна обчислити:

*Тхдень* = *Тх × T*

*Сек*

Коефіцієнт прибуття *λ*(*ів*) можна розрахувати як:

*λ*(*и*) =

*Тх* добу + *Удобу Т*

*де Uдень* - кількість непідтверджених операцій на кінець кожного дня:

*U день* = Граф *пам'ятіпул* + *Графмайнінгпул − Uдень−*1

А середній час майнінгу  *μ*(*ів*) розраховується як:

*μ*(*и*)

=  *βТх ÷* 600

*m*

де, *m* - кількість майнерів в добувному басейні.

У таблиці [1](#_bookmark9) наведені параметри моделювання криптовалюта біткоіни. Ми встановлюємо, що кількість вхідних транзакцій буде трохи вище, ніж ємність майнінгу для спостереження за непідтвердженими транзакціями в пулі пам'яті.

**Таблиця 1.** Параметр моделювання одноденних транзакцій Bitcoin.

|  |  |  |
| --- | --- | --- |
| **Станцій** | **опис** параметрів | **Значення** |
| Target | Швидкість прибуття транзакції | 3.55 (λ(с)) |
|  | Кількість транзакцій, відправлених з Mempool | 0,2856 (1/μ(и)) |
| Пул пам'яті | Політика | ФКФС |
|  | Пропускна здатність черги | ∞ |
|  | Кількість робочих місць | 2100 (Тх/Блок) |
|  | Кількість завдань (блок) | 1 |
| Вилка/приєднання | Політика | ФКФС |
|  | Скінченна ємність | 2100 |
|  | Правило падіння | БАС |
|  | Швидкість видобутку | 0,0016 (1/μ(и)) |
|  | Кількість шахтарів | 2200 |
| Гірничодобувний басейн | Політика | ФКФС |
|  | Пропускна здатність черги | 2100 |
|  | Правило падіння | БАС |

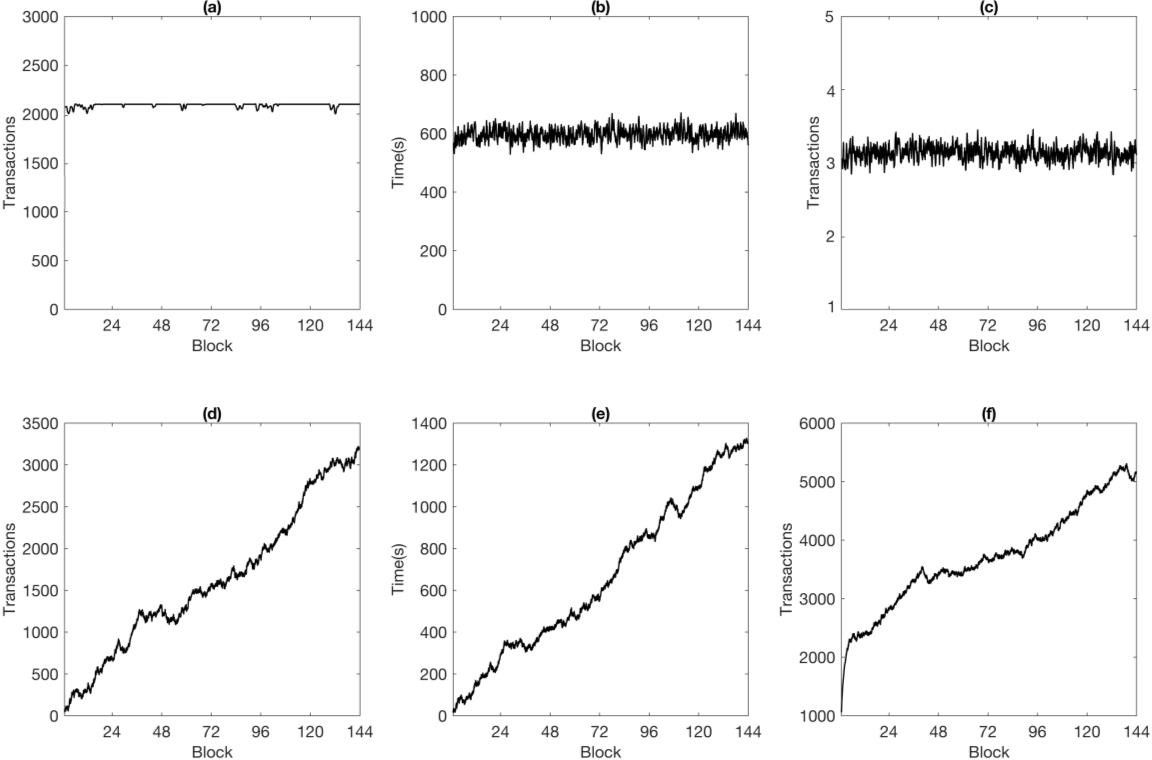
Число з Підсумок Угоди 306720

параметри виконання

Час моделювання 86400-ті

* 1. *Результатів*

Метою даного дослідження є перше надання імітаційної моделі для вивчення поведінки блокчейн-системи з використанням теорії масового обслуговування. Запропонована модель може бути застосована до малих і великомасштабних систем, а також для коротко- і довгострокового моделювання будь-якої такої системи. У цьому розділі ми представляємо результати короткострокового моделювання криптовалюти Bitcoin за один день. Результати наведені на рисунку [6](#_bookmark10)a–f, підсумовуючиспостереження під час одноденних транзакцій з криптовалютою Bitcoin. Моделювання проводилося з урахуванням параметрів, зазначених у таблиці [1](#_bookmark9). Із запропонованої імітаційної моделі отримані важливі індекси, які розглядаються Bitcoin explorer3 to для оцінки повсякденних транзакцій. Показники ефективності, наведені на рисунку [6](#_bookmark10), такі: (**a**) Кількість транзакцій на блок (**b**) Час майнінгу кожного блоку (**c**) Кількість транзакцій в секунду (**d**) Кількість memorypool (**e**) Час очікування в Memorypool ( **е**) Кількість непідтверджених транзакцій у всій системі.



**Малюнок 6.** Моделювання одноденної ідеальної статистики біткойна в запропонованому режиміl. (a) Кількість транзакцій на блок; (**b**) час видобутку кожного блоку; (**c**) Середня кількість транзакцій в секунду;

(**г**) Кількість пам'яті; (**e**) Час очікування в Memorypool; (**f**) Кількість непідтверджених транзакцій у всій системі.

* + 1. Кількість транзакцій на блок

В ідеальних теоретичних припущеннях біткоіни кількість транзакцій на блок не повинна перевищувати ліміт розміру в 1 Мб, і, як обговорювалося в розділі [4](#_bookmark6), ми припускали, що існує 2100 Тх/блоків. Однак тенденція на рисунку [6](#_bookmark10) а показує, що спочатку починається блок з 1400 транзакцій, а потім збільшується, в певний момент система стає стабільною і забезпечує 2100 для залишок згенерованих блоків.

* + 1. Час майнінгу кожного блоку

Зверніться до розділу [4.1](#_bookmark8) для жорстко закодованих правил блокчейну, які передбачають, що в ідеалі блокування повинно зайняти близько 10 хвилин (або 600 секунд), щоб бути виявленим майнером. Однак t його часове обмеження не може точно спостерігатися в реальних ситуаціях; завжди є варіації часу видобутку, і один блок відрізняється від іншого за складністю видобутку. На цьому графіку ми бачимо, що час

Видобувати блок варіюється від блоку до блоку, що дуже реально. Коливання часу видобутку було між 587-ми і 609-ми роками, а середній час видобутку всього дня становив 600-х/блок.

* + 1. Кількість транзакцій в секунду

Кількість підтверджених транзакцій в секунду на блок, або пропускна здатність системи, є найбільш критикованим параметром Bitcoin, коли справа доходить до порівняння його з Visa та іншими платіжних систем [[54,55](#_bookmark66)]. Цей графік показує середню кількість підтверджених транзакцій в секунду на блок, що означає час, необхідний для успішного видобутку транзакції.

* + 1. Кількість Мемпул

Ми припустили, що кількість прибуттів в систему трохи більше, ніж тих, що обслуговуються на Майнінгової станції. Наприклад, якщо кількість транзакцій, що надходять в систему, становить 3,55/с, а загальна потужність майнінгу - 3,5, то в якийсь момент транзакції почнуть накопичуватися в Mempool. Це впливає на систему Біткойн, і кількість накопичених непідтверджених транзакцій може спостерігатися для збільшення протягом дня.

* + 1. Час очікування в Мемпулі

Кожна транзакція, що надходить до системи Біткойн, повинна почекати деякий час, перш ніж буде обрана будь-яким майнером. І в міру зростання кількості пам'яті час очікування транзакцій, які будуть обрані майнером, також збільшується. Ця тенденція відображається як у кількості пам'яті poo l, так і в часі очікування пулу пам'яті. Поки кількість продовжує збільшуватися, час очікування новоприбулої транзакції в системі також буде зростати.

* + 1. Кількість непідтверджених транзакцій у всій системі

Надходження транзакцій в день непопередньодиктується; в даний момент часу в систему може потрапити велика кількість транзакцій , в той час як в наступний момент кількість прибуттів може бути нижче, ніж зазвичай. Таким чином, вхідні запити транзакцій від користувачів не фіксуються, а час обробки і ємність системи мають кілька обмежень, змушуючи систему вести себе певним і прописаним чином, т. Е. Обробка системи є незалежною від навантаження. У нашому моделюванні кількість прибуттів була встановлена трохи вище, ніж необхідно, тобто, від тих, що чекають в Мемпулі, тоді як це не єдині транзакції присутній в системі в даний момент часу.

Процес видобутку біткойнів ніколи не переходить у непрацюючий стан; Так що можна сказати, що в будь-який момент часу на розвилці накопичується певна кількість транзакцій, а деякі чекають возз'єднання на станціях приєднання, щоб завершити блок. Транзакції всередині Майнінг-станції і пулу Mem в сукупності відповідають кількості непідтверджених транзакцій у всій системі. Цей індекс ефективності зазвичай не обговорюється в статистиці Біткойн, але це один з найважливіших факторів, який також слід враховувати при оцінці будь-яка система.

# Валідація запропонованої моделі

Через відсутність бенчмаркінгу для Blockchain [[56,57](#_bookmark68)], нам знадобилося 60 днів фактичної статистики з двох найпопулярніших валют, Bitcoin та Ethereum, щоб підтвердити запропоновану нами модель. Фактичні стани обох в основному є статусом транзакцій , що відбуваються в їх системах щодня. Як обговорювалося в розділі [2](#_bookmark0), на відміну від Біткойн, обчислення та зберігання Ethereum використовує газову метрику та обмеження мережі, які можуть споживатися його користувачами, шляхом введення обмеження на мережу в терміни використання газу, фактично є механізмом захисту від перевантаження. Як правило, у звичайний час доби the розмір Ethereum становить близько 1500 000 газів, а його основна складність становить 21000 газів. Таким чином, в блок могли поміститися 1500 000 *÷* 21000 = 71, 428 транзакцій. За розміром даних він також відрізняється від Bitcoin; 1 блок Ethereum має розмір менше 2КБ; також Ethereum базується на рахунку, а не на транзакціях. Ми взяли дві різні реалізації блокчейнів, щоб підтвердити гнучкість нашої моделі з багатообіцяючими результатами.

У цьому процесі перевірки ми взяли 60 днів фактичної статистики, з періоду з 26 жовтня 2018 року по 24 грудня 2018 року, від надійних дослідників обох валют. Для біткойнів ми використовували [www](http://www.blockchain.com/).  [blockchain.com](http://www.blockchain.com/), а для Ethereum зібрані дані були з двох ресурсів: [www.etherscan.io](http://www.etherscan.io/) і [www.etherchain.org](http://www.etherchain.org/). У таблиці [2](#_bookmark12) наведено середнє значення зібраних параметрів за 60 днів.

**Таблиця 2.** Актуальна статистика Bitcoin і Ethereum за останні 60 днів.

**No тх /добу**

**Кількість** Мемпул

**Tx/блок Час міни підтверджено**

**Біткоїн (60-денний Середній)**

**Tx/Сек**

**No блоків**

264197.016 5641 2003 626.139 3.057 133.77

**Ethereum (середній показник за 60 днів )**

557478.783 66523.5\*Н/Д 14.096 Н/Д6055.233

Для всіх необхідних параметрів Bitcoin дані легко доступні, тоді як для Ethereum *β* tx і  *Ctx* і кількість пулу пам'яті становить в середньому 4 дні (з 20 грудня по 24 грудня). Крім того, середні значення зібраних даних для Bitcoin не знаходяться в рівнозначномулібріумі; таким чином, нам потрібно було змінити параметри, тому ми налаштували *Ctx*, *Txday* і *βn*. У таблиці [3](#_bookmark13) наведені модифіковані параметри для моделювання:

**Таблиця 3.** Параметри, розглянуті для моделювання.

**Ні. з Тх/добу Мемпул**

**Рахувати**

**Tx/block Час майну підтверджений біткойн (середній показник за 60 днів )**

**No блоків**

275247 5641 2003 626.139 3.1857 137

**Tx/Сек**

**Ethereum (середній показник за 60 днів )**

570274,56 66523,5 93,03 14,096 6,6 6129,398

Таблиця [4](#_bookmark14). Показує вхідні параметри і відповідні їм значення; налаштування моделювання виконується 60 разів з різною швидкістю обслуговування у всіх ітераціях  *аналізу WhatIF*.

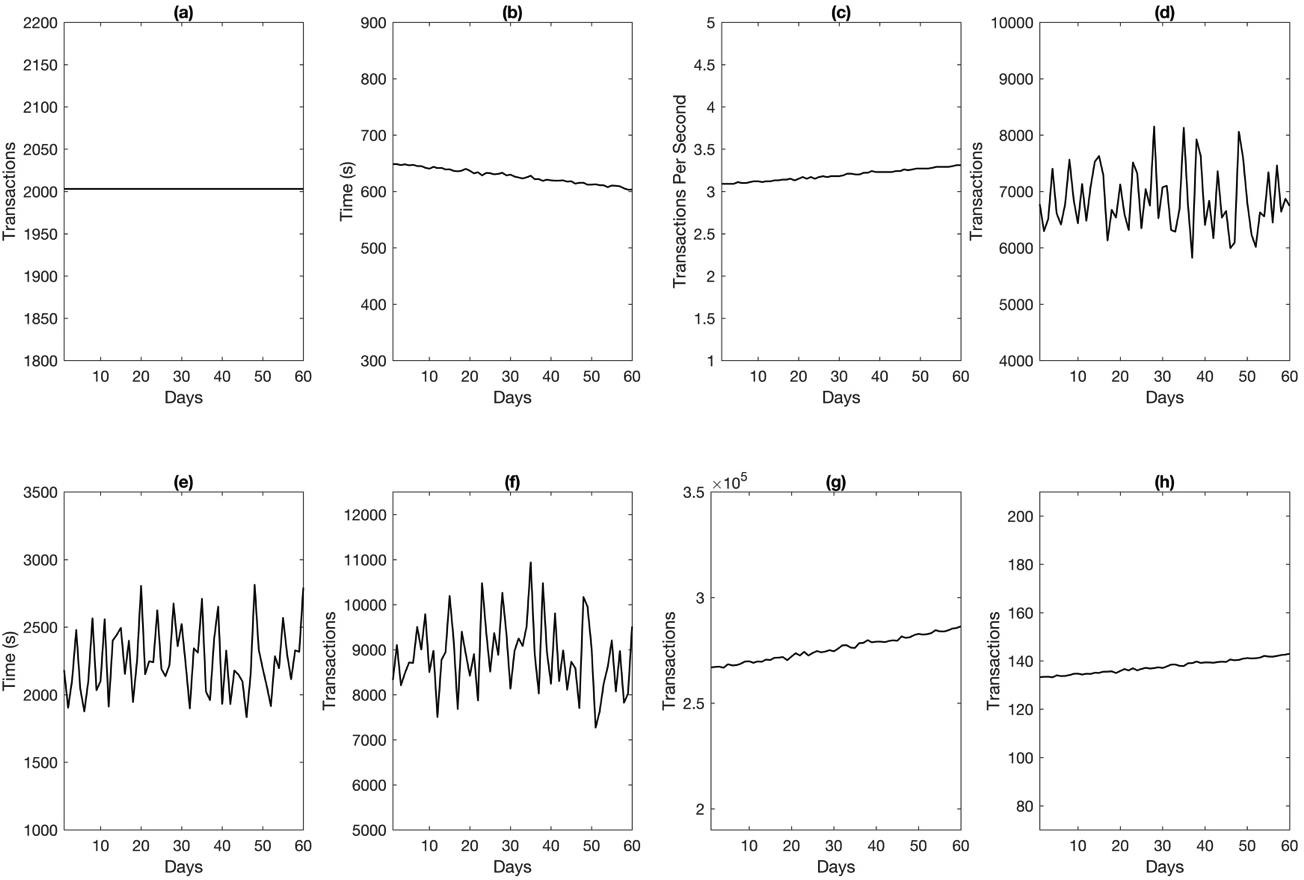
**Стіл 4.** Вводу Параметри для Моделювання з Біткоїн і Ефіріум.

|  |  |  |  |
| --- | --- | --- | --- |
| **Станцій** | **опис параметрів** | **Біткоїн** | **Ефіріум** |
| Ціль | Швидкість прибуття транзакції | 3.432 (λ(и)) | 6.57 (λ(и)) |
|  | Транзакції , відправлені з Мемпул | 0.2941 | 0.1503 |
| Пул пам'яті | Політика | ФКФС | ФКФС |
|  | Пропускна здатність черги | ∞ | ∞ |
|  | Кількість робочих місць | 2003 (Тх/Блок) | 93 (Тх/Блок) |
|  | Кількість завдань (блок) | 1 | 1 |
| Виделка | Політика | ФКФС | ФКФС |
|  | Скінченна ємність | 2003 | 93 |
|  | Правило падіння | БАС | БАС |
|  |  | від 0,001546 до 0,001650 | від 0,07137 до 0,07082 |
|  | | (1/μ(и)) | (1/μ(и)) |
| Кількість майнерів у черзі в пулі майнерів | | 2200 | 100 |
| Політика | | ФКФС | ФКФС |
| Пропускна здатність черги | | 2003 | 93 |
| Правило падіння | | БАС | БАС |
| Кількість загальних транзакцій | | 275247 | 570274 |
| Початкові транзакції Мемпул | | 5641 | 66523 |
| Параметри виконання початкових транзакцій у форку | | 2003 | 93 |
| Час моделювання | | 86400-і роки | 86400-і роки |
| Повторення насіння (днів) | | 60 | 60 |

Швидкість видобутку

*Результатів*

Блокчейн-системи Bitcoin і Ethereum були змодельовані за допомогою запропонованої моделі для цілей валідації. На рисунках [7](#_bookmark15) і [8](#_bookmark16) показані результати нашого моделювання для обох валют. Графіки на рисунках зображують (**а**) кількість транзакцій на блок (**б**) час майнінгу кожного блоку (**в**) кількість транзакцій В секунду (**d**) Memorypool підраховує (**e**) Час очікування в Memorypool, як обговорювалося в попередньому розділі. Однак, крім того, були також обчислені ще два параметри, тобто (f) загальна кількість транзакцій і (**g**) середня кількість блоків. Загальна кількість tra nsactions - це кількість загальних підтверджених транзакцій щодня, а середня кількість блоків - це кількість блоків, видобутих щодня. На рисунку [7](#_bookmark15) a–g показано моделювання біткоїну за 60 днів , а на рисунку [8](#_bookmark16)a–g показано моделювання Ethereum протягом 60 днів.

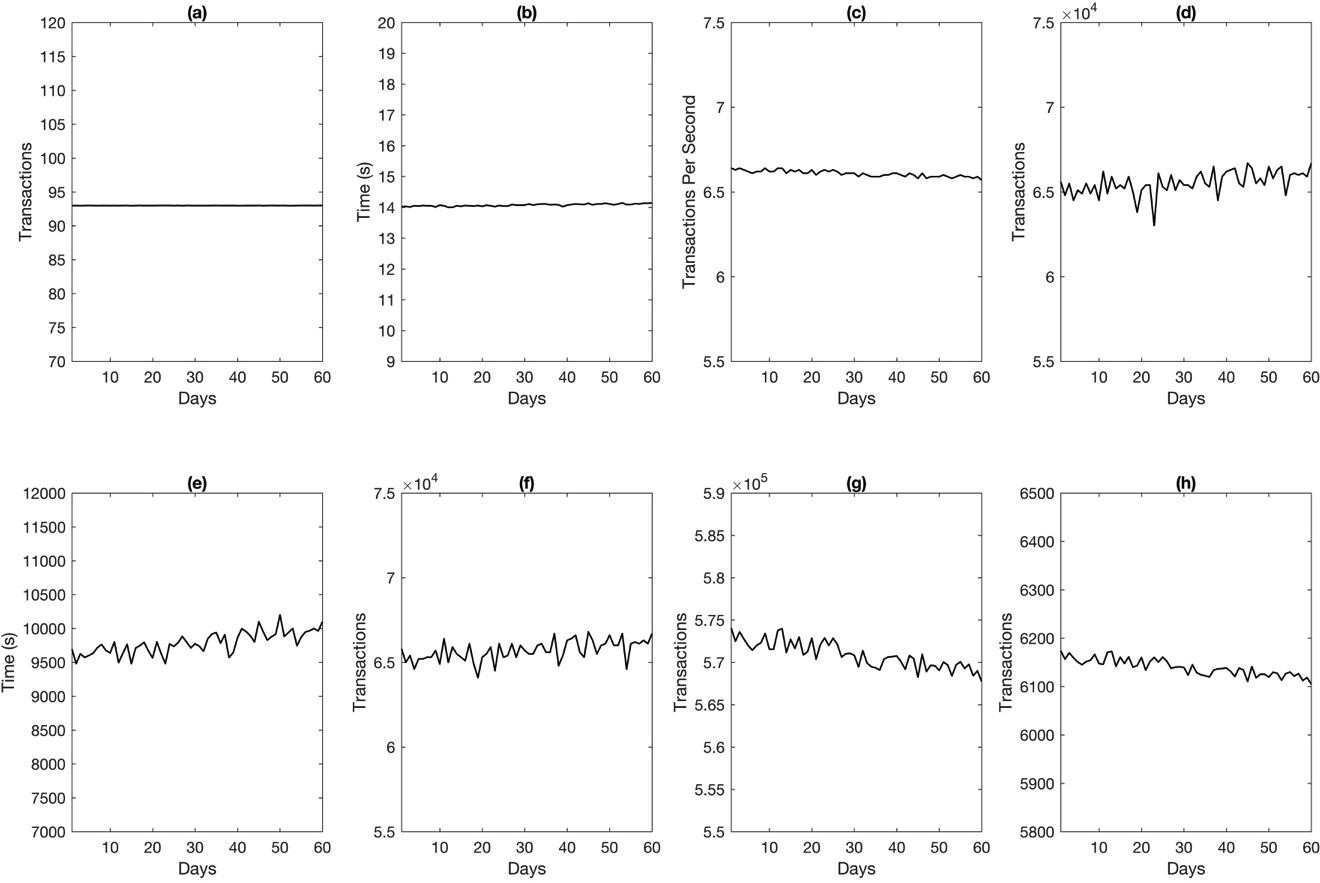


**Малюнок 7.** Моделювання шістдесяти днів фактичної статистики для Bitcoin із запропонованою моделлю (**a**) Кількість транзакцій на блок (**b**) Час майнінгу кожного блоку (**c** ) Середня кількість транзакцій в секунду

(**г**) Кількість memorypool (**e**) Час очікування в Memorypool (**f**) Кількість непідтверджених транзакцій у всій системі (**g**) Загальна кількість транзакцій (**h**) Середнє значення Кількість блоків.

Проведене моделювання має час обслуговування як змінну in кожної ітерації як для Bitcoin, так і для Ethereum; Можна припустити, що кожен день тариф на обслуговування майнерів трохи змінюється; наприклад , у випадку з біткойнами, перший день мав курс обслуговування 0,001536, другий день 0,001537, третій день 0,0015397, до 0,00165016 на 60-й день моделювання. Ефект від цього можна побачити у варіації кількості транзакцій, кількості транзакцій в секунду, часу майнінгу та кількості згенерованих блоків, наведених на рисунку [7](#_bookmark15)b,c,f,g,h. Зі збільшенням кількості транзакцій кількість блоків, що генеруються щодня, також збільшувалася, як і пропускна здатність або транзакції в секунду, в той час як час майнінгу зменшувався. Аналогічно, при збільшенніse в кількості вхідних транзакцій, кількість накопичених елементів в пулі пам'яті також збільшилася, як показано на рисунку [7](#_bookmark15)d, тому що вхідні транзакції були вище в число, ніж число , яке можна було б прочесати. Таким чином, якщо вхідні транзакції накопичуються в пулі пам'яті, середній час очікування транзакцій в Mempool також збільшується з кожним днем. Як обговорювалося раніше, кількість непідтверджених транзакцій, показаних на рисунку 7 f, вище, ніж кількість Mempool , показана на рисунку [7](#_bookmark15) d, тому що кількість

транзакції в Mempool не тільки непідтверджені в системі, але і транзакції, включаючи форк, Майнінг-пул і станції об'єднання , всі разом складають кількість непідтверджених транзакцій.



**Малюнок 8.** Моделювання шістдесяти днів фактичної статистики Ethereum із запропонованою моделлю (**а**) Кількість транзакцій на блок; (**b**) час видобутку кожного блоку; (**c**) Середня кількість транзакцій в секунду; (**d**) Кількість пам'яті; (**e**) Час очікування в Memorypool; (**f**) кількість непідтверджених транзакцій у всій системі; (**g**) Загальна кількість транзакцій; (**h**) Середня кількість блоків.

Крім того, слід зазначити, що моделювання має деякі обмеження у роботі з кількістю транзакцій у блоці. Як показано на рисунку [7](#_bookmark15)а, це був 2003 рік за всі дні; однак у реальних сценаріях це різниться. Але через фіксований розмір вилки кількість транзакцій склала 2003 рік протягом усього моделювання. Однак на рисунку [6](#_bookmark10)цей параметр продемонстрував різну поведінку. Причина f або це полягала в тому, що моделювання ідеального сценарію не мало залишкових транзакцій в Mempool з попереднього дня, т. Е. Воно починалося з нуля, в той час як моделювання, яке ми проводили для фактичної статистики, мало деякі початкові значення для параметрів fork і Mempool, як наведено в таблиці [4](#_bookmark14). Таким чином, коли симуляція почалася, всередині пулу пам'яті і форку вже накопичився ряд транзакцій, з яких накопичення вилки миттєво відправлялося у вигляді партії для Майнінг-пулу без будь-яких затримок.

З набором нових значень параметрів, наведених у таблиці [4](#_bookmark14), на рисунку [8](#_bookmark16)a–h показано моделювання для Ethereum. Існує величезна різниця в параметрах Bitcoin і Ethereum. В Ethereum кількість транзакцій щодня вдвічі більше, ніж у Bitcoin, кількість транзакцій на блок дуже мала, а частота генерації блоків вище, а середня кількість накопичених транзакцій в Mempool становила десять times, ніж у Bitcoin протягом вибраних днів. Слід припустити, що визначення індексів моделювання для Ethereum було тим, що обговорювалося раніше для Bitcoin.

Для подальшої валідації запропонованої нами моделі в таблиці [5](#_bookmark17) наведено порівняння результатів моделювання та фактичних значень. Оскільки моделювання проводилося за середніми значеннями за 60 днів транзакцій у Bitcoin та Ethereum, длясередніх значень також був проведений c omparison. Досягнуті результати добре узгоджуються з фактичними значеннями; А відсоток похибки склав менше 1% за всіма параметрами. Похибка відсотка обчислюється як абсолютна різниця змодельованих і фактичних значень, поділена на

фактичні значення і помножені на 100. Значення, позначені знаком "Недоступно" (N/A) для фактичної статистики у випадку очікування пулу пам'яті та загальної кількості непідтверджених транзакцій результатів from, ці значення не надаються жодним провідником; таким чином, порівняння помилок таких тут не застосовується. А кількість транзакцій на блок фіксується в запропонованій нами моделі за рахунок використання вилки для фіксованого розміру пакетної генерації. При цьому отриманий результат від моделювання також фіксується з нульовою процентною похибкою.

**Таблиця 5.** Порівняння фактичних і змодельованих результатів.

**Параметри (середній) Bitcoin Ethereum**

**Фактичний Моделюється Відсотків Фактичний Моделюється Відсотків**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | **Помилка** |  |  | **Помилка** |
| Тх На блок (*βТх* ) | 2003 | 2003 | 0% | 93 | 93 | 0 |
| Час видобутку (*βт*) | 626.139 | 627.2323 | 0.174% | 14.096 | 14.073 | 0.163% |
| Tx/Сек (*Тхs*) | 3.18 | 3.1930 | 0.409% | 6.6 | 6.60770 | 0.116% |
| Граф Мемпул (*U*) | 6847.441 | 6849.1740 | 0.025% | 66523.5 | 65540 | 1.478% |
| Мемпул Вайт (*Мемпw*) | Н/Д | 2257.7936 | Н/Д | Н/Д | 9787.944 | Н/Д |
| Непідтверджений Тх в системі (*Uдень*) | Н/Д | 8876.95 | Н/Д | Н/Д | 65688.33 | Н/Д |
| Загальна кількість Tx/день (*Тхдень*) | 275247 | 275876.78 | 0.228% | 570274 | 570906 | 0.11% |
| Кількість блоків (*βn*) | 137.4 | 137.731 | 0.241% | 6129.398 | 6139.5225 | 0.165% |

Однак кількість Mempool для Ethereum має рівень похибки 1.478%; причиною цього є те, що фактичні дані для підрахунку Mempool протягом цих 60 днів транзакцій були недоступні, тому ми припускали лише 4-денне середнє значення для виконання моделювання за період шістдесяти днів. Таким чином, різниця в фактичних і змодельованих даних неминуча. It також варто зазначити, що той самий параметр, Mempool count для Bitcoin, дуже добре узгоджується з фактичною статистикою.

# Застосування запропонованої моделі

Блокчейн - це книга записів, що тиражуються по вузлах всієї мережі; Він має можливість створювати різноманітні програми поверх своєї розподіленої архітектури. Ethereum розкрив потенціал блокчейну, запровадивши смарт-контракти, які існують для встановлення зв'язку (у прямому сенсі, тобто нерозривного ланцюга) між невідомими сторонами з певною метою. Контракти відбили необхідність залучення третіх сторін і забезпечили основу для нового покоління додатків online [[58](#_bookmark70)].

У даній роботі запропонована модель лежить в черзі на основі теорії, яка є одним з найбільш популярних інструментів оцінки і оптимізації продуктивності системи для виконання моделювання розподілених і паралельних syстебел. Запропонована модель може бути використана для представлення для різних блокчейн-додатків. Ми розділили застосування нашої моделі на дві великі категорії, тобто криптовалюти та нове покоління додатків через Інтернет, де новий генеруючийіон додатків включає системи розумного голосування, банківську та фінансову галузь, підвищену прозорість ланцюгів поставок, розумні системи охорони здоров'я та багато додатків IoT.

* 1. *Криптовалюти*

Як показано в цій роботі, ряд показників ефективності можна розрахувати для оптимізації існуючих криптовалют, а також прогнозування потужності майнінгу, винагороди, отриманої за майнінгову потужність, і проведення порівнянь різних типів валют. Оцінити використання потужності і необхідну потужність майнінгу можна буде за допомогою запропонованої моделі.

* 1. *Нове покоління додатків через Інтернет*

Широкий спектрpplications можна змоделювати, щоб виявити поведінку системи, наприклад, затримка, пов'язана з пошуком інформації, час очікування, час черги, час обробки, пропускна здатність, використання енергії та час відгуку.

# Висновок

Блокчейни залишаються відносно невивченими для теоретичного моделювання; У даній роботі ми пропонуємо модель моделювання блокчейна за допомогою теорії масового обслуговування. Запропонована модель побудована шляхом використання однієї черги M/M/1 як пулу пам'яті, набору вилкових з'єднань для пакетної генерації та черги M /M/c як пулу Майнінг. Запропонована модель є простим, але потужним середнімзначенням s для виявлення багатьох важливих індексів, таких як (a) Кількість транзакцій на блок (b) Час майнінгу кожного блоку (c) Пропускна здатність/транзакції системи в секунду (d) Кількість пулу пам'яті (e) Час очікування в пулі пам'яті (f) Кількість непідтверджених транзакцій у всій системі (g) Загальна кількість транзакцій та (h) Кількість згенерованих блоків. По-перше, запропонована модель використовувалася для оцінки ідеальної статистики транзакцій за один день в біткоіни. А потім модель була використана для моделювання 2 місяців фактичної статистики Bitcoin і Ethereum для перевірки. Отримані результати знаходяться в хорошій згоді, з незначним відсотком похибки. Незважаючи на те, що запропонована модель використовується для оцінки криптовалют у цій роботі, вона все ще здатна моделювати різноманітні системи на основі блокчейну для оцінки ефективності та оптимізації.

**Внесок автора:** концептуалізація, Р.А.М. д Дж.А.; Формальний аналіз, Р.А.М.; Методологія, Р.А.М.; Програмне забезпечення, Р.А.М.; Супервізія, Ж.П.Л.; Письмо-оригінальний проект, Р.А.М.; Написання—рецензування та редагування, Р.А.М. і Дж.А.

Фінансування: Ця робота була підтримана Національним фондом природничих наук Китаю (грант No. 61370073), Національна програма досліджень і розробок високих технологій Китаю (Грант No 2007AA01Z423), Відділ проектів науки і технологій провінції Сичуань; та Управління проектами цивільно-військової інтеграції Ченду Лтд.

**Conflicts of Interest:** Автори заявляють про відсутність конфлікту інтересів.

# Посилання

1. Накамото, Н. Біткойн: однорангова система електронних грошових коштів. Доступно онлайн: [https://bitcoin.org/bitcoin.](https://bitcoin.org/bitcoin.pdf)  [pdf](https://bitcoin.org/bitcoin.pdf) (доступ 20 січня 2019 року).
2. Рід, Ф.; Гарріган, М. Аналіз анонімності в системі біткойнов. У *безпеці та конфіденційності в соціальних мережах*

*Мережі*; Спрінгер: Нью-Йорк, штат Нью-Йорк, США, 2013; Пп. 197–223.

1. Чжу, Х.; Бадр, Ю. Системи управління ідентифікацією для Інтернету речей: опитування щодо блокчейн-рішень.  *Датчики* 2018,  *18*, 4215. [[CrossRef](http://dx.doi.org/10.3390/s18124215)] [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/30513733)]
2. Дьюіведі, А.Д.; Сривастава, Г.; Дхар, С.; Сінгх, Р. Децентралізований блокчейн охорони здоров'я, що зберігає конфіденційність, для IoT.  *Сенсорс* **2019**,  *19*, 326. [[CrossRef](http://dx.doi.org/10.3390/s19020326)] [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/30650612)]
3. Фігоріллі, С.; Антонуччі, Ф.; Коста, К.; Паллоттіно, Ф.; Расо, Л.; Кастільоне, М.; Пінчі, Е.; ВекЧіо, Д.Д.; Колле, Г.; Прото, А.Р. Прототип впровадження блокчейну для електронної простежуваності деревини з відкритим вихідним кодом по  всьому ланцюжку поставок.  *Датчики* 2018,  *18*, 3133. [[CrossRef](http://dx.doi.org/10.3390/s18093133)] [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/30227651)]
4. Ку, Ч.; Дао, М.; Юань, Р. Модель блокчейну на основі гіперграфів та застосування в Інтернеті розумних будинків з підтримкою речей.  *Датчики* **2018**,  *18*, 2784. [[CrossRef](http://dx.doi.org/10.3390/s18092784)] [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/30149523)]
5. Еял, І.; Дженсер, А.Е.; Сирер, Е.Г.; Ван Ренессе, Р. Bitcoin-NG: масштабований блокчейн-протокол. У працях 13-го симпозіуму USENIX з проектування та впровадження мережевих систем (NSDI '16), Санта-Клара,  Каліфорнія, США, 16 –18 березня 2016 р.; Пп. 45–59.
6. Міллер, А.; Джуелс, А.; Ши, Е.; Парно, Б.; Кац, Дж. Пермакоін: Перепрофілювання біткойн-роботи для збереження даних. У матеріалах симпозіуму IEEE з безпеки та конфіденційності 2014 року (SP), Берклі, Каліфорнія, США, 18–21 травня 2014 року;  Пп. 475–490.
7. Бутерін, В. Біла книга Ethereum, GitHub Repos., 2013. Доступно онлайн: [https://github.com/ethereum/ wiki/wiki/White-Paper](https://github.com/ethereum/wiki/wiki/White-Paper) (доступ 20 січня 2019 року).
8. BitShares 2.0-Децентралізована децентралізована (DPoS) еко-система промислового рівня на блокчейні. Доступно онлайн:  [https:](https://bitshares.org/)

[bitshares.org/](https://bitshares.org/) (доступ 20 січня 2019 року).

1. Dash Офіційний сайт| Криптовалюта Dash — тире. Доступно онлайн: [www.dash.org](http://www.dash.org/) (доступ 20 січня 2019 року).
2. Догекоін. Доступно онлайн:<https://dogecoin.com/> (доступ 20 січня 2019 року).
3. Litecoin, цифрова валюта P2P з відкритим вихідним кодом Litecoin , 2013. Доступно онлайн: <https://litecoin.org/> ( 20 січня 2019 року).
4. Головна—Піркоін. Доступно онлайн:<https://peercoin.net/> (доступ 20 січня 2019 року).
5. Ціаян, П.; Райканьова, М.; Kancs, D. Віртуальні відносини: коротко- та довгострокові докази з ринків BitCoin та altcoin.  *Дж.*  *Інт.*  *Фінансовий.*  *Марка.*  *Установи Гроші* **2018**,  *52*, 173–195. [[Перехресний реф](http://dx.doi.org/10.1016/j.intfin.2017.11.001)]
6. Ринкова капіталізація криптовалюти| CoinMarketCap. Доступно онлайн:<https://coinmarketcap.com/> (доступ 19 січня 2019 року).
7. Лі, К.Л.; Ма, Ж.-Й.; Чанг, Ю.-Х. Теорія черги блокчейну , 2018. Доступно онлайн: [https://arxiv.org/abs/](https://arxiv.org/abs/1808.01795) [1808.01795](https://arxiv.org/abs/1808.01795) (доступ 20 січня 2019 року).
8. Кавасе, Ю.; Касахара, С. Час підтвердження транзакцій для біткойнів: аналітичний підхід до черги до механізму блокчейну. У конспектах лекцій з  *інформатики (включаючи підсерії* «Конспекти лекцій  *зі штучного інтелекту*»  *та « Конспекти* лекцій  *з біоінформатики»);*  Спрінгер: Нью-Йорк, штат Нью-Йорк, США, 2017; Пп. 75–88.
9. Біаїс, Б.; Бісьєр, К.; Бувард, М.; Касаматта, С. Народна теорема про блокчейн, 2018. Доступно онлайн:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3108601> (доступ 20 січня 2019 року).
10. Левенберг, Ю.; Бахрах, Ю.; Сомполінський Ю.; Зохар, А.; Розеншейн, J.S. Пули майнінгу біткойнів: теоретичний аналіз кооперативних ігор . У матеріалах Міжнаціональної спільної конференції з автономних агентів та багатоагентних систем, Стамбул, Туреччина, 4–8 травня 2015 р.; стор. 919–927.
11. Хоуї, Н. Гра про видобуток біткойнів, 2014. Доступно онлайн: [https://papers.ssrn.com/sol3/papers.cfm?](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834)  [abstract\_id=2407834](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834) (доступ 20 січня 2019 року).
12. Бакер, К.; Хуан, Д.Й.; Маккой, Д.; Ткач, Н. Підкреслюючи: Біткойн "стрес-тестування". У *конспекті лекцій у*

*Комп'ютерні науки (включаючи підсеріали «Конспект лекцій зі штучного інтелекту» та «Конспекти лекцій з біоінформатики»*);  Шпрінгер: Берлін, Німеччина, 2016; Пп. 3–18.

1. Жерве, А.; Караме, Г.О.; Вюст, К.; Гліканцис, В.; Ріцдорф, Х.; Капкун, С. Про безпеку і виконання доказів роботи блокчейнов. У матеріалах конференції ACM SIGSAC з комп'ютерної та комунікаційної безпеки 2016 року  — CCS'16, Нью-Йорк, штат Нью-Йорк, США, 24–28 жовтня 2016 року; с. 3–16.
2. Карлстен, М.; Калоднер, Х.; Вайнберг, С.М.; Нараянан, А. Про нестабільність біткоіни без винагороди за блок. У матеріалах конференції ACM SIGSAC з комп'ютерної та комунікаційної безпеки 2016 року  — CCS'16, Нью-Йорк, штат Нью-Йорк, США, 24–28 жовтня 2016 року; с. 154–167.
3. Ісая, М.; Soldatos, J. Технологія розподіленого реєстру для децентралізації виробничих процесів. У працях промислових кіберфізичних систем IEEE 2018 року, Санкт-Петербург, Росія, 15–18 травня 2018 року ;  Пп. 696–701.
4. Майкл, Дж.В.; Кон, А.; М'ясник, J.R. Технологія блокчейн та регуляторні дослідження. 2018. Доступно онлайн:<https://www.steptoe.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf> (доступ 19 листопада 2018 року).
5. Рон, Д.; Шамір, А. Кількісний аналіз повного графіка транзакцій Bitcoin . У *конспекті лекцій* на  *комп'ютері*

*наука (включаючи підсерії «*Конспекти лекцій  *зі штучного інтелекту» та «Конспекти лекцій з біоінформатики»);* Шпрінгер: Берлін, Німеччина, 2013; Пп. 6–24.

1. Дрешер, Д.  *Основи блокчейну*; Шпрінгер: Берлін, Німеччина, 2017.
2. Атік, Дж.; Gerro, G. Хардфорки на блокчейні Bitcoin: оборотний вихід, продовження голосу.  *1 Стен.*  *Дж.*  *Блокчейн Л. Пол.*  *1* **2018** рік. Доступно онлайн: [https://stanford-jblp.pubpub.org](https://stanford-jblp.pubpub.org/pub/hard-forks-bitcoin)/[pub/hard-forks-bitcoin](https://stanford-jblp.pubpub.org/pub/hard-forks-bitcoin) (доступ 20 січня 2019 року).
3. Макгінн, Д.; Береза, Д.; Акройд, Д.; Моліна-Солана, М.; Го, Ю.; Ноттенбелт, В.Дж. Візуалізація динамічних моделей транзакцій Bitcoin.  *Великі дані* **2016**, *4*, 109–119. [[CrossRef]](http://dx.doi.org/10.1089/big.2015.0056) [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/27441715)]
4. Сапірштейн, А.; Сомполінський Ю.; Зохар, А. Оптимальні егоїстичні стратегії майнінгу в біткоіни. У *конспекті лекцій у*

*Комп'ютерні науки (включаючи підсеріали «Конспект лекцій зі штучного інтелекту» та «Конспекти лекцій з біоінформатики»*);  Шпрінгер: Берлін, Німеччина, 2017; Пп. 515–532.

1. Мелоун, Д.; О'Дуайер, K.J. Видобуток біткойнів та його енергетичний слід. У матеріалах 25-ї конференції IET Irish Signals & Systems Conference 2014 та 2014 Китайсько-Ірландська міжнародна конференція з інформаційних технологій та технологій спільнот (ISSC 2014/CIICT 2014),  Лімерік, Ірландія, 26–27 червня 2014 року; Пп. 280–285.
2. Грюнспан, К.; Перес-Марко, Р. Подвійні гонки. 2017. Доступно онлайн: [https://arxiv.org/abs/1702.](https://arxiv.org/abs/1702.02867)  [02867](https://arxiv.org/abs/1702.02867) (доступ 20 січня 2019 року).
3. Сомполінський Ю.; Зохар, А. Основні стимули біткойна.  *Комун.*  *ACM* **2018**,  *15*, 29–52. [[Перехресний реф](http://dx.doi.org/10.1145/3152481)]
4. Лашка, А.; Джонсон, Б.; Гроссклагс, Дж. Коли пули майнінгу біткойнів висихають: теоретико-ігровий аналіз довгострокового впливу атак між пулами майнінгу. У конспектах лекцій *з інформатики (включаючи підсерії «Конспекти лекцій зі штучного інтелекту» та «Нотатки ЛеКтуре в біоінформатиці»);* Шпрінгер: Берлін, Німеччина, 2015;  Пп. 63–77.
5. Джонсон, Б.; Лашка, А.; Гроссклагс, Дж.; Васек, М.; Мур, Т. Гейм-теоретичний аналіз DDoS-атак на пули майнінгу біткойнів. у *фінансовій криптографії та безпеці даних*; Шпрінгер: Берлін, Німеччина, 2014;  Пп. 72–86.
6. Андервуд, С. Блокчейн за межами біткойна.  *Комун.*  *ACM* **2016**,  *59*, 15–17. [[Перехресний реф](http://dx.doi.org/10.1145/2994581)]
7. Хао, Ю.; Лі, Ю.; Донг, Х.; Ікло, Л.; Чен, П. Аналіз продуктивності алгоритму консенсусу в приватному блокчейні. У працяхсимпозіуму IEEE Intelli gent Vehicles, Праці, Чаншу, Китай, 26–30 червня 2018 року; Пп. 280–285.
8. Азарія, А.; Екблав, А.; Вієйра, Т.; Ліппман, А. MedRec: Використання блокчейну для доступу до медичних даних та управління дозволами. У матеріалах 2016 року 2-ї Міжнародної конференції з відкритих та великих даних, OBD 2016,  Відень, Австрія, 22–24 серпня 2016 року ; Пп. 25–30.
9. Buterin, V. Ethereum White Paper: Смарт-контракт наступного покоління та децентралізована платформа додатків. 2014. Доступно онлайн: <https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf> (доступ 20 січня 2019 року).
10. Бутерін, В. Смарт-контракт нового покоління та децентралізована платформа додатків. 2013. Доступно онлайн: <https://s3.us-east-2.amazonaws.com/bci-static/downloads/ethereum_whitepaper.pdf>(доступ 20 січня 2019 року).
11. Крістідіс, К.; Девецікіотіс, М. Блокчейни та смарт-контракти для Інтернету речей.  *Доступ*  *до IEEE*

**2016**,  *4*, 2292–2303. [[Перехресний реф](http://dx.doi.org/10.1109/ACCESS.2016.2566339)]

1. Луу, Л.; Чу, Д.-Х.; Оліккель, Х.; Саксена, П.; Хобор, А. Зробити смарт-контракти розумнішими. У матеріалах CCS '16 Конференції ACM SIGSAC з комп'ютерної та комунікаційноїбезпеки 2016 року,  Відень, Австрія, 24–28 жовтня 2016 року; Пп. 254–269.
2. Цзян, Г.; Фан, Ю.; Цзян, Г.; Фан, Ю. Метод аналізу впливу внутрішньосистемних та міжсистемних перешкод на DME, заснований на теорії масового обслуговування.  *Датчики* **2019**,  *19*, 348. [[CrossRef](http://dx.doi.org/10.3390/s19020348)] [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/30654559)]
3. Мен, Т.; Лі, Х.; Чжан, С.; Чжао, Ю. Гібридна безпечна схема бездротових сенсорних мереж від атак хронометражу з використанням безперервно-часового марківського ланцюга і моделі черги.  *Датчики* **2016**, 16, *1606*. [[CrossRef](http://dx.doi.org/10.3390/s16101606)]  [[PubMed](http://www.ncbi.nlm.nih.gov/pubmed/27690042)]
4. Чжан, Дж.; Хань, Г.; Цянь, Ю. Теорія черг базується на підході до аналізу коканальних перешкод  для локальних мереж з високою щільністю .  *Датчики* **2016**,  *16*, 9.
5. Марін, А.; Россі, С.; Соттана, М. Упереджений розподіл процесорів у чергах на форк-приєднання. У матеріалах Міжнародної конференції з кількісної оцінки систем, Пекін, Китай, 4–7 вересня 2018 р.; с. 273–288. Доступно онлайн: <https://link.springer.com/chapter/10.1007%2F978-3-319-99154-2_17> (доступ 20 січня 2019 року).
6. Бакчеллі, Ф.; Маковський, А.М.; Шварц, А. Черга форк-з'єднання і пов'язана з нею systems з обмеженнями синхронізації: стохастичне упорядкування і обчислювальні межі.  *Адв.*  *Додаток.*  *Пробаб.*  **1989**,  *21*, 629–660. [[Перехресний реф](http://dx.doi.org/10.2307/1427640)]
7. Боксма, О.Я.; Куле, Г.; Лю, З. Черги-теоретико-розв'язувальні методи для mоделів паралельних і розподілених систем. *в оцінці ефективності паралельних і розподілених систем-рішень*; Боксма, О.Я.,  Куле, Г.М., ред.; CWI: Амстердам, Нідерланди, 1994; Пп. 1–24.
8. Геленбе, Е.  *продуктивність мультипроцесора*; Джон Вілі та сини, Inc.: Нью-Йорк , штат Нью-Йорк, США, 1989.
9. Кім, С.; Агравала, А.К. Аналіз черги форк-з'єднання.  *IEEE Trans.*  *Комп'ютер.*  **1989**,  *38*, 250–255. [[Перехресний реф](http://dx.doi.org/10.1109/12.16501)]
10. Лазовська, Є.; Загорян, Дж.; Грем, Г.; Севчик, К. *Кількісна продуктивність системи: аналіз комп'ютерних систем* *з використанням мережевих моделей черг;* Прентіс-Холл, Inc.: Верхнє Сідло-Рівер, Нью-Джерсі, США, 1984.
11. Бертолі, М.; Казале, Г.; Serazzi, G. JMT:Інструменти для моделювання систем для моделювання системи.  *ACM* *SIGMETRICS виконують.*  *Евал.*  *Об'явлення* **2009**,  *36*, 6. [[Перехресний реф](http://dx.doi.org/10.1145/1530873.1530877)]
12. Кокоріс-Когіас, Е.; Йовановіч, П.; Гейлі, Н.; Хоффі, І.; Гассер, Л.; Ford, B. Підвищення безпеки та продуктивності біткойнів із сильною послідовністю шляхом колективного підписання. У матеріалах 25-го симпозіуму з безпеки USENIX, Остін, Техас, США, 10–12 Auguest 2016; Пп. 279–296.
13. Патрон, Т.  *Біткойн-революція:* Інтернет  *грошей*; Дигіноміка: Утрехт, Нідерланди, 2015.
14. Б'юкенен, Б.; Накві, Н. Побудова майбутнього ЄС: рух вперед з міжнародною співпрацею на блокчейні.  *JBBA* **2018**, 1, *1*–4. [[Перехресний реф](http://dx.doi.org/10.31585/jbba-1-1-(7)2018)]
15. Тхаккар, П.; Натан, С.; Вішванатан, Б. Бенчмаркінг продуктивності та оптимізація блокчейн-платформи Hyperledger Fabric. 2018. Доступно онлайн:<https://arxiv.org/abs/1805.11390> (доступ 20 січня 2019 року).
16. Барнс, Д. Blockchain Manoeuvres: Застосування технології Bitcoin до банківської справи. 2015. Доступно онлайн:  [https:](https://pdfs.semanticscholar.org/11f3/3397d35fd4916f9fdf6c89b84ea50802bbd1.pdf)

[pdfs.semanticscholar.org/11f3/3397d35fd4916f9fdf6c89b84ea50802bbd1.pdf](https://pdfs.semanticscholar.org/11f3/3397d35fd4916f9fdf6c89b84ea50802bbd1.pdf) (доступ 20 січня 2019 року).

© 2019 за авторами . Ліцензіат MDPI, Базель, Швейцарія. Ця стаття є статтею у відкритому доступі, що розповсюджується відповідно до умов ліцензії Creative Commons Attribution (CC BY) (<http://creativecommons.org/licenses/by/4.0/>).