Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз світового досвіду реалізації Блокчейн-застосунків

Виконав: студент IV курсу, групи СТс-42
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

_____ Сидорук В.Ю.
(підпис) (прізвище та ініціали)

Керівник _____ Пасічник В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Гащин Н.Б.
(підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«17» _червня_ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)

Студенту Сидоруку Віталію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз світового досвіду реалізації Блокчейн-застосунків

Керівник роботи Пасічник Володимир Володимирович, д.т.н., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » березня 2022 року № 4/7-162

2. Термін подання студентом завершеної роботи 17 червня 2022р.

3. Вихідні дані до роботи Наукові публікації про Блокчейн-застосунки та особливості їх інформаційно-технологічної реалізації

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Стан та перспективи досліджень щодо інтеграції Блокчейн в інноваційні застосунки. 1.1 Інтеграція Блокчейн та інформаційних технологій. 1.2 Інформаційно-технологічний концепт Блокчейн. 1.3 Узагальнена структура Блокчейн-фреймворків. 2 Аналіз світового досвіду реалізації Блокчейн-застосунків. 2.1 Використання Блокчейну для Інтернету речей. 2.2 Блокчейн та великі за обсягом колекції даних. 2.3 Блокчейн в царині хмарних та крайових обчислень. 2.4 Блокчейн для управління ідентифікацією. 2.5 Блокчейн, криптовалюта, економіка та ринки. 2.6 Бізнес-рішення, розумні контракти та автоматизація на основі Блокчейн. 2.7 Блокчейн для відстежування сутностей в логістиці. 2.8 Блокчейн та медична інформатика. 2.9 Блокчейн та комунікаційні мережі. 2.10 Інші категорії Блокчейн-застосунків. 3. Безпека життєдіяльності, основи охорони праці. Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Тема та мета роботи. 3 Завдання роботи. 4 Актуальність роботи. 5 Блокчейн та інформаційні технології. 6 Узагальнена структура Блокчейн-фреймворків. 7 Блокчейн рівень даних. 8 Дерево Меркла. 9 Цифровий підпис. 10 Мережевий рівень Блокчейн. 11 Прикладний рівень Блокчейн. 12 Особливості Блокчейна. 13 Категорії Блокчейн-застосунків. 14 Блокчей та хмарна інфраструктура. 15 Блокчейн для персональної ідентифікації. 16 Блокчейн, криптовалюта, економіка та ринки. 17 Блокчейн для відстежування сутностей в логістиці. 18 Висновки. 19. Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик Олег Ярославович, доцент	04.04.2022	01.05.2022

7. Дата видачі завдання 24 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Підбір джерел про Блокчейн-застосунки та	04.01.2022-30.01.2022	*Виконано*
	особливості їх реалізації		
3.	Переклад та опрацювання джерел про Блокчейн-	31.01.2022-06.02.2022	*Виконано*
	застосунки та особливості їх реалізації		
4.	Виконання дослідження щодо світового досвіду	07.02.2022-13.02.2022	*Виконано*
	реалізації Блокчейн-застосунків		
5.	Оформлення розділу «Стан та перспективи	14.02.2022-06.03.2022	*Виконано*
	досліджень щодо інтеграції Блокчейн в інноваційні		
	застосунки»		
6.	Оформлення розділу «Аналіз світового досвіду	07.03.2022-03.04.2022	*Виконано*
	реалізації Блокчейн-застосунків»		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	04.04.2022-17.04.2022	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	18.04.2022-01.05.2022	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат	06.06.2022	*Виконано*
12.	Попередній захист кваліфікаційної роботи	07.06.2022	*Виконано*
13.	Захист кваліфікаційної роботи	20.06.2022	

Студент _____ Сидорук В.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Пасічник В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз світового досвіду реалізації Блокчейн-застосунків // Кваліфікаційна робота освітнього рівня «Бакалавр» // Сидорук Віталій Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТс-42 // Тернопіль, 2022 // С. 47, рис. – 16, табл. – 0, кресл. – 19, бібліогр. – 50.

Ключові слова: аналіз, безпека, блокчейн, використання, застосунок, Інтернет речей.

Кваліфікаційна робота присвячена аналізу світового досвіду реалізації Блокчейн-застосунків. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є проведення аналізу світового досвіду інтеграції Блокчейн з інноваційними інформаційними технологіями та практичної реалізації застосунків.

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» розглянута інтеграція Блокчейн та інформаційних технологій. Описано інформаційно-технологічний концепт Блокчейн. Проаналізовано узагальнену структуру Блокчейн-фреймворків. Зокрема, описано рівень даних, мережевий рівень та особливості Блокчейну.

В другому розділі кваліфікаційної роботи описано використання Блокчейну для Інтернету речей. Проаналізовано інтеграцію Блокчейну та великих за обсягом колекцій даних. Розглянуто Блокчейн в царині хмарних та крайових обчислень. Описано Блокчейн для управління ідентифікацією. Висвітлено інформацію про Блокчейн, криптовалюти та економіку. Проаналізовано бізнес-рішення, розумні контракти та автоматизацію на основі Блокчейн. Описано Блокчейн для відстежування сутностей в логістиці. Проаналізовано інтеграцію Блокчейну та медичної інформатики тощо.

ANNOTATION

Analysis of the world experience of Blockchain applications implementation // Qualification work of the educational level "Bachelor" // Sydoruk Vitalii Yuriiovych // Ternopil Ivan Pulyuy National Technical University, Computer information systems and software engineering faculty, Computer science department, Group STs-42 // Ternopil, 2022 // P. 47, fig. - 16, tabl. - 0, chair. - 19, ref. - 50.

Keywords: analysis, security, blockchain, use, application, Internet of Things.

Qualification work is devoted to the analysis of world experience in the implementation of Blockchain applications. The purpose of this qualification work of the educational level "Bachelor" is to analyze the world experience of integration of Blockchain with innovative information technologies and practical implementation of applications.

In the first section of the qualification work of the educational level "Bachelor" the integration of Blockchain and information technologies is considered. The information technology concept of Blockchain is described. The generalized structure of Blockchain frameworks is analyzed. In particular, the data level, network layer and features of Blockchain are described.

The second section of the qualification describes the use of the Blockchain for the Internet of Things. The integration of Blockchain and large data collections is analyzed. Blockchain in the field of cloud and boundary computing is considered. Describes Blockchain for Identity Management. Information on Blockchain, cryptocurrencies and the economy is covered. Business solutions, smart contracts and Blockchain-based automation are analyzed. Blockchain for tracking entities in logistics is described. The integration of Blockchain and medical informatics, etc. is analyzed.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних.

ВДТ – відео-дисплейний термінал.

ЕОМ – електронно-обчислювальна машина.

ПЕОМ – персональна електронно-обчислювальна машина.

ПК – персональний комп’ютер.

IoT (англ. internet of things, IoT) – Інтернет речей.

IP (англ. Internet Protocol) – Інтернет протокол.

P2P (англ. Peer-to-Peer) – рівний до рівного – варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів.

PBFT (англ. Practical Byzantine Fault Tolerance) – Практична візантійська відмовостійка система – це перший новий алгоритм консенсусу, заснований на теорії BFT, що поєднується з реальністю.

PoET (англ. Proof of the past) – Доказ минулого часу – — це механізм консенсусу мережі блокчейн, який запобігає високому використанню ресурсів і енергоспоживанню; це робить дію більш ефективною, дотримуючись чесної системи лотереї.

PoS (англ. Proof-of-Stake) – «підтвердження частки» – метод захисту в криптовалютах, заснований на необхідності доказу зберігання певної кількості коштів на рахунку.

PoW (англ. Proof-of-Work) – доказ виконання роботи – система захисту систем від DoS-атак або зловживання послугами.

TEE (Trusted Execution Environment) – довірене середовище виконання.

ЗМІСТ

ВСТУП

Актуальність теми. Блокчейн, як механізм децентралізації послуг, безпеки та перевірки, пропонує однорангову систему, в якій розподілені вузли спільно підтверджують походження транзакції. Він забезпечує безперервне зберігання історії транзакцій, захищене цифровим підписом і підтверджене консенсусом. На даний час присутній підвищений інтерес до Блокчейну, як альтернативи традиційним централізованим системам. Тому аналіз можливостей застосування Блокчейну в інноваційні інформаційно-технологічні платформи та застосунки є актуальним напрямком досліджень.

Мета і задачі роботи. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є проведення аналізу світового досвіду інтеграції Блокчейн з інноваційними інформаційними технологіями та практичної реалізації застосунків. Для досягнення поставленої мети потрібно:

– Подати огляд інформаційної технологій Блокчейну.

– Описати структуру високого рівня Блокчейн та виділити її критичні функції і характеристики.

– Провести ретельний аналіз різних областей по категоріях, у яких застосовувався Блокчейн або в яких тривають дослідження щодо застосування Блокчейна для розроблення інноваційних застосунків.

Практичне значення одержаних результатів. Подано огляд інформаційної технологій Блокчейн. На основі аналізу сучасних наукових публікацій висвітлено структуру високого рівня Блокчейн, виділено та описано її критичні функції і ключові характеристики. Прокласифіковано та проаналізовано різні області запровадження Блокчейн-застосунків. Зокрема розглянуто запровадження Блокчейн для Інтернету речей, великих даних, хмарних та периферійних обчислень, управління ідентифікацією, криптовалют, економіки та ринків, бізнес-застосунків, смарт-контрактів та автоматизації, відстеження в логістиці, медичної інформатики, комунікаційних мереж та ін.

РОЗДІЛ 1. СТАН ТА ПЕРСПЕКТИВИ ДОСЛІДЖЕНЬ ЩОДО ІНТЕГРАЦІЇ БЛОКЧЕЙН В ІННОВАЦІЙНІ ЗАСТОСУНКИ

1.1 Інтеграція Блокчейн та інформаційних технологій

Системне запровадження інформаційних технологій, розвиток Інтернету речей (IoT) [1], хмарних і граничних обчислень [2] та великих за обсягом даних [3] формує потребу щодо розроблення та запровадження інноваційних програмно-алгоритмічних рішеннях управління розподіленими та децентралізованими системами. Водночас першорядне значення має формування безпечних, надійних і перевірених служб, оскільки обсяг підключених до мережі пристроїв та даних безпрецедентно збільшується.

Блокчейн – це розподілений і незмінний реєстр транзакцій, в якому кожна транзакція невідступно пов’язана з попередньою. Основна мета блокчейну – робота в ненадійних децентралізованих середовищах, може бути забезпечена записом транзакцій та децентралізованим консенсусом щодо дійсності запису транзакцій. Транзакції реалізують операційний код, що забезпечує обслуговування програмного забезпечення між ненадійними користувачами. Відколи вони були вперше використані в криптовалютах [4], інтерес до цієї інформаційної технології невпинно зростає. Промислові фахівці та наукова спільнота позитивно оцінюють застосування та роботу основних елементів інформаційної технології Блокчейн. Блокчейн активно розглядається як ефективне інформаційно-технологічне рішення для обширного переліку потреб інноваційних застосунків, зокрема для:

– Інтернет речей (IoT) [5];
– великі дані [6];
– хмарні та граничні обчислення [7];
– управління ідентифікацією тощо.

Одночасно в промисловості тривають активні розробки щодо оцінки ефективності Блокчейну для різних категорій бізнес-застосунків. Для реалізації потенційних майбутніх потреби розвиваються фреймворки.

Незважаючи на інноваційний потенціал, який створює Блокчейн, він явно збалансований на користь захисту конфіденційності даних користувачів і залишає невирішеними багато питань щодо використання інформаційно-технологічної платформи з точки зору постачальника послуг, внутрішніх обчислювальних витрат на консенсус та масштабованість, які залишаються критичними. Незважаючи на потенціал Блокчейну революціонізувати розподілені та децентралізовані архітектури, на даний час опубліковано результати практичних досліджень [8], які потребують подальшого вирішення. В будь-якій програмній системі, зокрема Блокчейні, вразливості в закодованій реалізації або базовій операційній системі можуть створити потенціал для зловмисного компроментування користувачів або всієї системи. Більше того, деякі теоретичні аспекти самої системи можуть дозволити зловмисне використання. Тому важливо провести ретельну оцінку актуального стану запровадження Блокчейн, щоб всесторонньо оцінити наслідки запровадження та інтеграції інформаційної технології.

1.2 Інформаційно-технологічний концепт Блокчейн

Інформаційно технологічний концепцт Блокчейн з’явився відносно недавно та досить загадково, з появою «білої книги» про Біткоїн у 2008 році [4]. Він не є унікальним в царині програмного забезпечення з відкритим кодом. З моменту першої реалізації Біткоїн приблизно в 2009 році [9], Блокчейн постійно перевіряється в реальній практиці, як доказ ефективності роботи відповідні концепції. Проте на даний час не відомо, чи ці інформаційні технології повністю безпечні [10]. Вони практично функціонують та демонструють стійкість і передбачувану функціональність.

Нещодавній значний інтерес до Блокчейну можна безпосередньо пов’язати з великим обсягом баз даних користувачів криптовалют, сформованих на основі Біткоїн та багатьох інших. Також це зумовлено диверсифікацією Блокчейн-застосунків розробниками, які вже прагнуть застосувати децентралізований консенсус для інших класів завдань. Наприкінці 2017 року криптовалюти досягли найвищої на даний час оцінки [11]. З 2018 року відбулася інституціалізація положення щодо раніше нерегульованих фінансових технологій та ринків [12].

В контексті зростаючого інтересу до інформаційної технології Блокчейн, доцільно оцінити їх запровадження для використання в обширному переліку інноваційних сфер людської діяльності. На даний час накопичена обширна історія запровадження інформаційних систем криптографічного захисту, зокрема, аукціонів [13]. Зважаючи на перспективи розвитку ненадійних централізованих систем та наявність зловмисників необхідно розглянути принципи роботи блокчейну та пов’язаних з ним інформаційно-технологічних механізмів:

– цифровий підпис;
– криптографія відкритого ключа;
– алгоритми консенсусу;
– смарт-контракти тощо.

Потрібно проаналізувати наукові публікації про поточні практичні реалізації Блокчейн-застосунків та особливості їх функціонування.

1.3 Узагальнена структура Блокчейн-фреймворків

Блокчейн можна розглядати як послідовність пов’язаних блоків даних, кожен з яких залежить від попереднього блоку, утворюючи безперервну ланцюжкову структуру даних. Однак у ширшому сенсі Блокчейн можна розглядати як базову структуру, яка включає ряд необхідних компонентів, зокрема середовище взаємодії та програми.

Розглянемо узагальнене подання Блокчейн-фреймворків. Зокрема його можна умовно поділити на мережевий рівень, рівень даних та рівень застосунків [14] (див. рисунок 1.1).

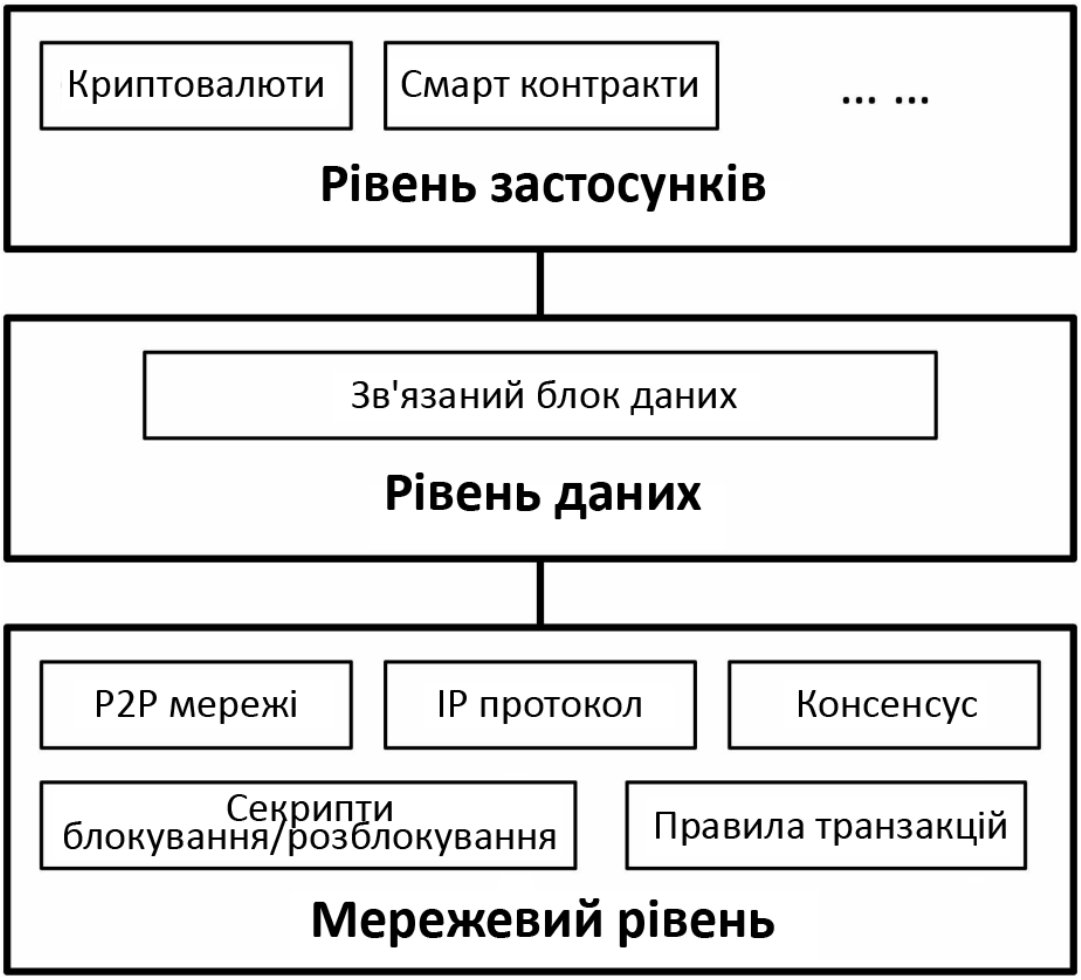

Рисунок 1.1 – Узагальнена структура Блокчейн-фреймворків

На рівні даних розміщено фундаментальні сутності Блокчейну, які сформовано на основі різнотипових структур даних та алгоритмів, зокрема:

– хеш;

– хеш-покажчик;

– дерево Меркла;

– цифровий підпис тощо.

Дизайн структур даних і алгоритмів дозволяє забезпечити загальновідомі функції Блокчейну, зокрема:

– прозорість;

– стійкість;

– децентралізація тощо.

Мережевий рівень використовується для забезпечення взаємодії елементів Блокчейн-середовищ [14]. Сюди входять:

– децентралізована мережа на основі IP-протоколів;

– однорангова P2P-мережа;

– сценарії блокування та розблокування;

– механізм консенсусу, що використовується для реалізації розподіленої угоди щодо дійсності блоків.

Мережевий рівень додатково дозволяє оновлювати та розподіляти Блокчейн серед користувачів.

Прикладний рівень представляє різні програми, які можуть інтегрувати Блокчейн для:

– використання його безперервної книги;

– консенсусу між недовіреними вузлами;

– розумних контрактів;

– криптографічних компонентів.

Будучи відносно новим за межами «світу» криптовалют, Блокчейн все ж використовується в багатьох сферах, щоб задовольнити зростаючі вимоги конфіденційності та безпеки користувачів, а також розподіленого та децентралізованого контролю. Використовуючи представлення високого рівня, наведене на рис. 1.1, розглянемо детальніше рівні даних і мережі, виділивши важливі компоненти та їх варіації.

1.3.1 Рівень даних

З точки зору структури даних, Блокчейн – це зростаючий список пов’язаних записів даних або блоків, які пов’язані та захищені застосуванням криптографічних хешів. Кожен блок містить набір нових записів даних або

транзакцій, а також хеш-значення попереднього блоку [14]. Цей хеш пов’язує поточний блок з попереднім і разом із міткою часу ускладнює зміну записів, оскільки вони залежать від попереднього валідності структури запису та поточного часу. Ключові компоненти та детальні структури, які утворюють блок – це записи даних, хеш і хеш-покажчик.

Записи даних (Транзакції). Як основне корисне навантаження в блокчейні, легкі транзакції зберігаються як записи даних [14]. Ці транзакції є свідченням певних взаємодій, наприклад, переказу коштів або зберігання даних у БД, що відбуваються в певний час.

Хеш і хеш-покажчик. Хеш-функція використовується для відображення вихідних даних – повідомлення у набір даних фіксованого розміру – хеш-значення [14]. Криптографічні хеш-функції повинні мати:

– стійкість до атак;

– стійкість до попереднього зображення;

– стійкість до другого попереднього зображення;

– зручність головоломки.

Завдяки цим властивостям хеш-функції можна застосовувати для перевірки цілісності вихідного повідомлення або як хеш-показники, в якому покажчик містить хеш повідомлення, на яке він вказує. На рисунку 1.2 показана структура зв’язаного списку, яка використовує хеш-покажчики [14].

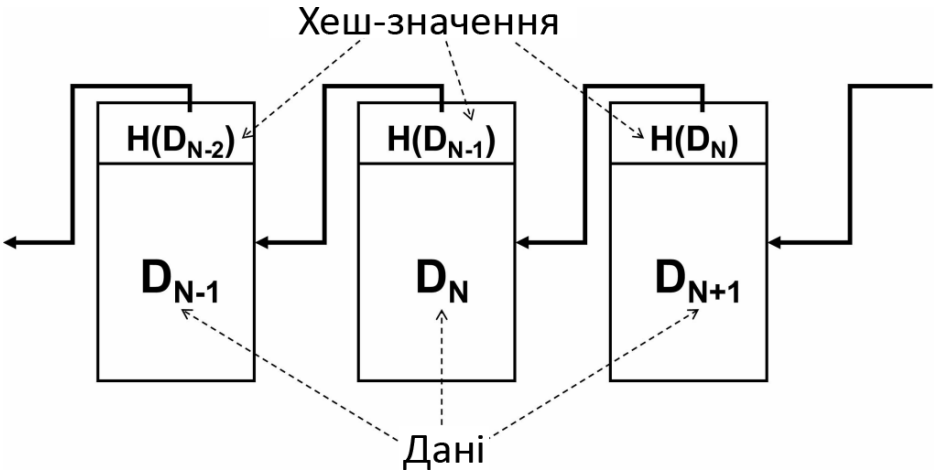

Рисунок 1.2 – Хеш-покажчик

У наведеному прикладі кожен блок даних містить хеш-значення попереднього блоку, щоб можна було перевірити цілісність усіх попередніх даних. У Блокчейні хеш-покажчики пов’язують кожен блок даних, запобігаючи зміні записів транзакцій.

Асиметрична криптосистема та цифрові підписи. Асиметрична криптосистема використовує схему відкритих секретних ключів, використовуючи математичні проблеми, для яких не існує ефективного рішення [14]. У цій криптосистемі відкриті ключі широко доступні всім для шифрування повідомлення, яке може розшифрувати лише власник ключа. Крім того, цифрові підписи також використовують схему публічного секретного ключа. Зовнішній користувач може перевірити повідомлення, закодовані за допомогою приватного ключа, декодуючи його відкритим ключем.

Для Блокчейну використання цифрових підписів забезпечує передачу транзакцій від одного користувача до іншого, оскільки кожна транзакція пов’язана з попередньою транзакцією. Основою Блокчейну є безперервна історія транзакцій, зібрана в більші блоки, звідси походить назва «блокчейн». Приклади транзакцій, виконання довільного коду або, у випадку з біткоїнами, записи переказів монет між користувачами. На рисунку 1.3 проілюстровано транзакції з цифровими підписами в Блокчейні [14].

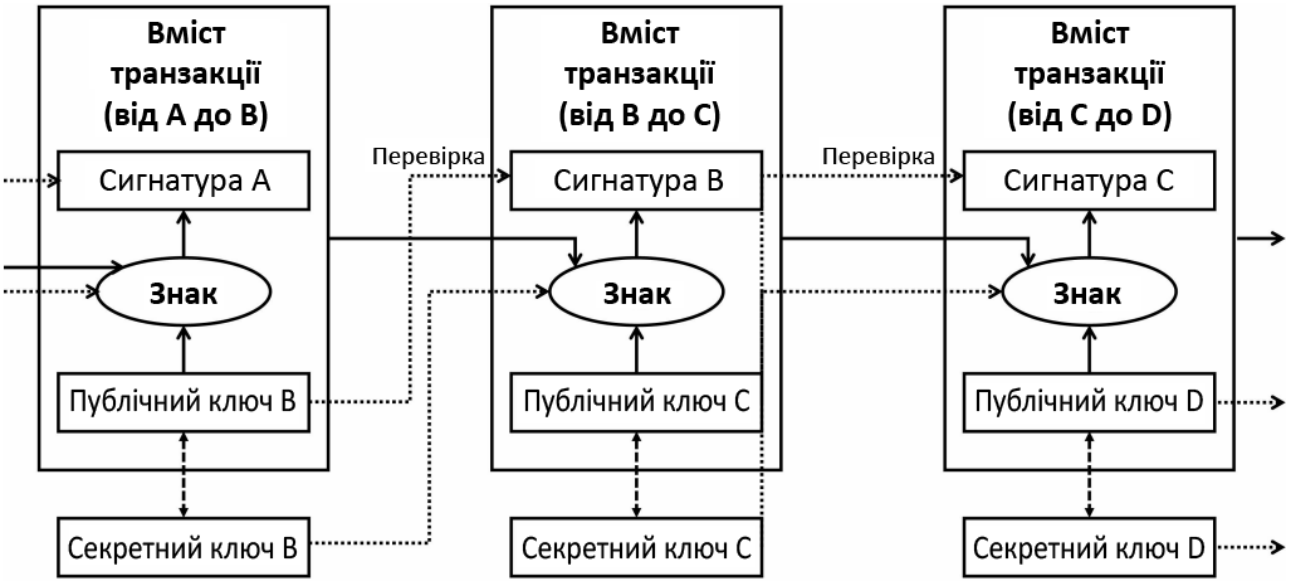

Рисунок 1.3 – Транзакція з цифровим підписом

Транзакція в Блокчейні вимагає від емітента цифрового підпису хеша попередньої транзакції та відкритого ключа одержувача. Потім емітент транзакції може бути перевірений, а одержувач – єдиний, кому належить транзакція. У випадку з валютними операціями, одержувач – єдиний, хто може здійснити наступну транзакцію в цьому ланцюжку транзакцій [15].

Дерево Меркла. На рисунку 1.4 подано ілюстрацію структури дерева Меркла [14]. Оскільки хеш-значення кожного з батьків у дереві Мекла залежить від його дочірніх листків – блоків даних у нижній частині, то практично неможливо маніпулювати одним лиском без зміни інших.

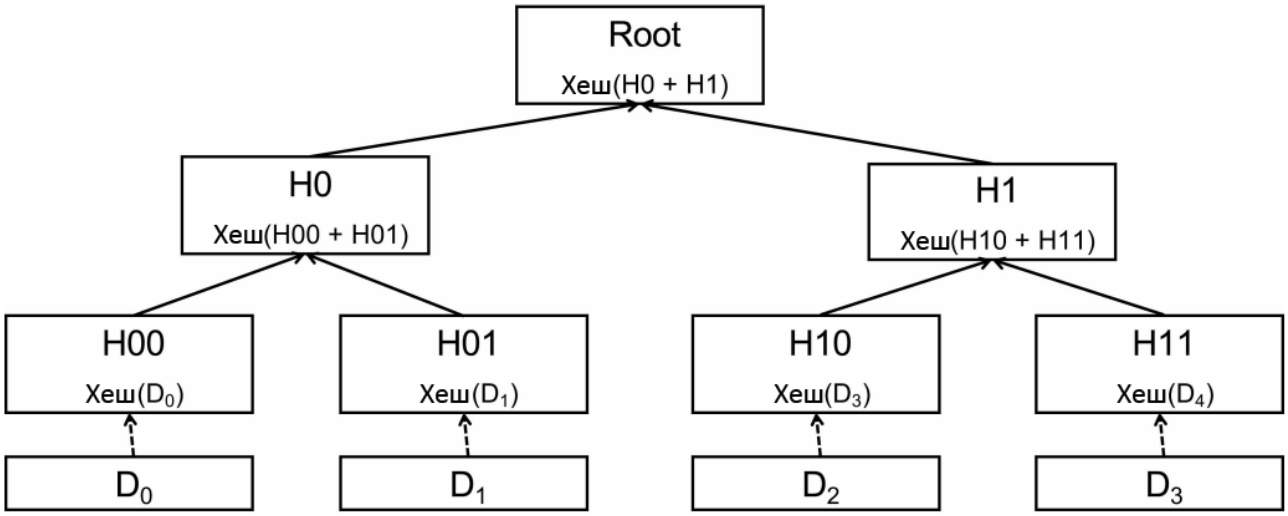

Рисунок 1.4 – Дерево Меркла

Будь-яка зміна транзакції вплине на хеш-значення аж до кореня дерева Меркла. Корінь (Root) можна використовувати як ідентифікатор. В Блокчейні, транзакції – корисне навантаження даних, записуються за допомогою дерева Меркла для підтримки цілісності даних.

Блоки даних. Блок – це контейнерна структура даних фіксованого розміру. У випадку з криптовалютами блоки зазвичай містять багато тисяч транзакцій, а типовий розмір блоку становить декілька Мб – це безпосередньо впливає на кількість транзакцій, що обробляються за одиницю часу. Блок зазвичай складається із заголовка блоку та тіла блоку [14] (див. рисунок 1.5).

Рисунок 1.5 – Структура блоків даних

Хоча реалізація може відрізнятися в залежності від інформаційно-технологічної платформи або залежно від програмно-алгоритмічних застосунків, заголовок блоку зазвичай містить:

– правила ідентифікації версії блоку, яких Блокчейн має дотримуватися;
– хеш попереднього блоку;
– хеш кореня дерева Меркла, що агрегує всі хеші включених транзакцій;
– мітку часу для відстеження;
– nBits – поточна мета хешування;
– Nonce, що використовується для консенсусу.

Тіло блоку зазвичай містить лічильник транзакцій та всі транзакції. Кількість транзакцій, які може мати блок, залежить від розмірів блоку та кожної транзакції.

Блокчейн. Наступним кроком після розгляду транзакції та блоків є збір блоків, щоб сформувати Блокчейн – незмінну книгу, яка забезпечує відстеження [14]. Блок містить:

– хеш попереднього блоку, що впливає на ланцюжок;
– набір транзакцій, хешованих через дерево Меркла;
– позначку часу;

– одноразовий номер [4].

В структурі дерева Меркла транзакції представляють листові вузли, кожен з яких хешується окремо. Кожен набір дочірніх хешів об’єднується і знову хешується вгору по дереву, поки не буде досягнуто кореня. Це використовується для зменшення розміру Блокчейн-сховища шляхом відкидання старих транзакцій, а також ефективне для перевірки блоку [16].

Після створення трансакції транслюються по всій мережі для збору та об’єднання в дійсні блоки. Мітка часу перевіряє транзакції, що існували на момент створення блоку. Одноразове число – це одноразове значення, яке необхідно обчислити, щоб під час хешування поточного блоку хешове значення відповідало певним довільним критеріям. Наприклад, починалося з певної фіксованої кількості нулів. Потім цей критерій можна використовувати для посилення труднощів у обчисленні хешування блоку [17]. Оскільки рішення важко знайти, але легко перевірити, воно підходить для визначення правильності блоку в Блокчейні [16].

1.3.2 Мережевий рівень

Розглянемо мережевий рівень Блокчейн-фреймворків, який представляє P2P-мережу, а також викладаємо консенсус і різні його реалізації.

P2P-мережа. У P2P користувач одночасно використовує і створює основу мережі, хоча надання ресурсів є цілком добровільним [14]. Кожен одноранговий партнер вважається рівним і зазвичай називається вузлом. Незважаючи на те, що всі вузли рівні, вони можуть виконувати різні ролі в Блокчейн-екосистемі. Наприклад, «майнер» та «повний вузол». До повного вузла, поки він підключений до мережі, копіюється весь Блокчейн. Це означає, що інформація, що зберігається в Блокчейні, не може бути втрачена або знищена, оскільки це потребувало б знищення кожного повного вузла мережі. Доки існує один вузол з копією блокчейну, всі записи залишаться недоторканими, надаючи можливість перебудувати мережу.

Консенсус. Щоб забезпечити децентралізацію блокчейну, вузли, які беруть участь у проведенні транзакцій і створенні блоків, також повинні мати можливість підтверджувати дійсність блоків, коли вони додаються до ланцюжка [14]. У цьому випадку консенсус між вузлами є необхідністю, оскільки немає довіреної централізованої системи, щоб зробити таке визначення. Для досягнення такої угоди були розроблені різні механізми консенсусу, зокрема PoW, PoS, PBFT тощо [18]. Ці варіанти повинні досягати однієї мети – точного визначення того, які блоки в Блокчейні є коректними, шляхом перевірки роботи кожного доданого блоку на дійсність. Відмінності полягають у тому, хто може додавати блоки і з якою швидкістю, і яка головоломка використовується для реалізації консенсусу. Консенсус зазвичай має на увазі «майнинг» або вирішення якоїсь складної проблеми, яку легко перевірити, але нелегко подолати.

Окреслимо основні приклади механізму консенсусу та відзначимо існуючі обмеження. Концепція PoW використовує криптографічні обчислення і в загальному випадку це визначення належного одноразового номера, що призводить до хешування блоку, що починається з певної кількості нулів. Тільки майнер, який вирішує цю проблему, може додати блок до ланцюжка, а іншим потрібно перевірити, чи робота виконана правильно. Крім того, різні рішення можуть призвести до форка в блокчейні, з унікальним рішенням у кожному форку. Дійсно, робота майнерів у мережі передбачається візантійською – довільною, і має бути досягнута відмовостійкість. Однак одним із недоліків цього механізму є те, що, керуючи підмножиною майнерів, можна підтвердити незаконні або неправильні блоки. Крім того, складність задачі знаходження одноразового значення не може бути як завгодно малою, оскільки в результаті буде створено багато форків на великому обсязі, що потенційно також призведе до «подвійних витрат». Хоча існують ефективніші механізми PoW, вони за своєю природою вимагають значних обчислювальних витрат для забезпечення точності та перевірки.

У PoS вартість частки майнера в мережі – залишок його рахунку заблоковано. Відповідно до зміни ставки, змінюється складність головоломки – стає легшою зі збільшенням ставки. Результатом є кілька майнерів з високими ставками, які забезпечують ефективний консенсус. Незважаючи на те, що це має проблему «нічого на карті», у якій бідні майнери змовляються розколоти Блокчейн, існує декілька рішень, включаючи систему, яка вимагає «бай-ін» або депозит, який вилучається, якщо майнінг є помилковим [19]. PoS-механізм використовувався у «Tendermint», «Etherium Casper» та «Tezos».

Механізм PBFT, на відміну від PoW, є детермінованим – тобто включення блоку в Блокчейн є остаточним. Він працює в три фази та вимагає для реалізації мережевого зв'язку [18]. На етапі попередньої підготовки лідер транслює вузлам передбачувану цінність, яка буде передана в блокчейн. Далі, на етапі підготовки, вузли передають значення, які вони мають намір зафіксувати. На На етапі підтвердження більше двох третин відповідей вузла повинні узгоджувати значення на етапі підготовки для значення, яке буде зафіксовано. Оскільки консенсус вимагає декількох раундів комунікації, цей механізм у своїй початковій формі погано масштабується. Додаткові варіанти включають зміну голосуючої сили вузлів на основі окремих критеріїв.

PoET – надійні апаратні механізми для досягнення консенсусу, забезпечують життєздатну альтернативу для зменшення накладних витрат на майнинг і потенційно стійкішими до відмов. Проте їх безпека, як правило, залежить від надійної бази коду і вимагає спеціального обладнання, наприклад довірене середовище виконання (TEE) Intel [19]. Всі надійні апаратні механізми використовують пару ключів, записану в апаратне забезпечення, яка встановлює корінь довіри, і весь код вимірюється шляхом хешування вмісту одного з ключів перед виконанням. Це використовується для дистанційної атестації, щоб засвідчити те, що виконується на пристрої [19]. Хоча вони можуть бути більш енергоефективними, їх впровадження не так перевірено, як інші конкуруючі системи.

Варто згадати два інших консенсусних алгоритми: Proof-of-Authority (PoA) і Proof-of-Burn (PoB) [19]. У PoA повноваження призначаються певним майнерам, що дозволяє їм пропонувати нові блоки. Це додатково обмежується призначенням часових вікон кожному вузлу повноважень у схемі «RoundRobin», таким чином, що нові блоки можна пропонувати лише всередині вікна. У PoB вузол знищує певну валюту, монету або вартість, якими він володіє, щоб запропонувати нові блоки для прийняття мережею Блокчейнів. Це схоже на концепцію «бай-ін» в модифікованому PoS.

1.3.3 Особливості Блокчейна

Похідний від вищеописаних компонентів даних і мережевих рівнів Блокчейн надає декілька ключових функцій, які дозволяють використовувати унікальні програми на прикладному рівні.

Відмовостійкість. З точки зору вищерозглянутого мережевого рівня, Блокчейни за своєю суттю є децентралізованими системами з низкою різних учасників [14]. Дії цих учасників залежать від наявних стимулів та інформації. При отриманні нової трансакції кожен вузол, який представляє учасника децентралізованої мережі Блокчейнів має можливість або визнати транзакцію – додаючи її до локальної копії книги, або ігнорувати її. Потім можна досягти консенсусу, коли більшість вузлів прийме рішення щодо одного стану. У результаті помилки, які можуть виникнути в невеликій кількості вузлів, навряд чи змінять стан загальнодоступної книги і будуть відновлені після оновлення стану консенсусу. За звичайних обставин Блокчейн толерантний навіть до однієї помилки, що виникає на багатьох вузлах, якщо загальна їх кількість менше половини всіх вузлів.

Стійкість до атак. В централізованих системах компроментування центру обробки даних внаслідок вторгнення або злому є фатальним. На противагу цьому, на основі децентралізованої P2P-мережі, Блокчейн має здатність протистояти хакерству [20]. Доки кожен вузол мережі зберігає копію

Блокчейну, скомпрометовані вузли не можуть вводити шахрайські транзакції або блоки в ланцюжок. Тому цілісність записів у Блокчейні захищена. Так само, як і відмовостійкість, це залишається вірним до тих пір, поки кількість скомпрометованих вузлів залишається меншою. Консенсус більшості копій Блокчейну забезпечує надійне резервне копіювання для системи, а також для перезапису будь-якої зламаної версії. Іншою загрозою в P2P-мережі є подвійні витрати [20]. Тобто, коли одна і та ж монета використовується для здійснення декількох платежів. Коли трансакції, що очікують на розгляд, транслюються в мережу, можуть виникати затримки, які призводять до отримання непідтверджених транзакцій в різний час. У Блокчейні PoW-механізм вирішує проблему, дозволяючи вузлам вирішувати складну математичну задачу – майнінг, для перевірки транзакції. Оскільки в Блокчейн можна додати лише блоки з правильними відповідями на складну математичну задачу, повторити роботу по зміні транзакції в блоці важко. Крім того, блоки мають часову мітку, і все, що має значення, найперша транзакція з монетою та її власник. Інші платежі з тим же фондом будуть ігноровані, що запобігає дворазовому використанню коштів.

Прозорість. Як публічна книга, блокчейн забезпечує високий рівень прозорості [14]. За механізмом консенсусу кожен запис транзакції перевіряється більшістю. Спроби змінити або видалити попередні транзакції вимагатимуть консенсусу більшості вузлів системи, що малоймовірно. В результаті кожна первісна транзакція може бути перевірена.

РОЗДІЛ 2. АНАЛІЗ СВІТОВОГО ДОСВІДУ РЕАЛІЗАЦІЇ БЛОКЧЕЙН-ЗАСТОСУНКІВ

Завдяки зростаючій видимості біткоїн та інших криптовалют, різноманітності інформаційно-технологічних платформ, доступних для запровадження Блокчейну, а також децентралізації та перевірки, які надають Блокчейни, дослідження різко зросли, зачіпаючи різноманітний спектр застосунків. Їх можна розділити на категорії [14]:

– Інтернет речей (IoT);
– великі за обсягом набори даних;
– хмарні та крайові обчислення;
– управління ідентифікацією;
– криптовалюта;
– економіка та ринки;
– бізнес-застосунки;
– розумні контракти та автоматизація;
– відстеження в логістиці;
– медична інформатика;
– комунікаційні мережі тощо.

Проаналізуємо особливості застосовувався Блокчейн для різних інформаційно-технологічних областей на основі опублікованих даних про дослідження щодо застосування блокчейну для нових застосунків.

2.1 Використання Блокчейну для Інтернету речей

Розвиток інформаційних технологій Блокчейн та їх зростання в цілому призвели до спроб їх застосування для IoT. Децентралізована та розподілена система для забезпечення довіри – це дійсно приваблива можливість.

Інтернет речей і пов’язані з ним системи «розумного світу» (див. рисунок 2.1) [2], які впроваджують масово розгорнуті:

– давачі;
– виконавчі механізми;
– розумні електронні пристрої.

Рисунок 2.1 – Інтернет речей

Тим не менш, масове розгортання пристроїв з дуже обмеженими обчислювальними можливостями для збору та передачі даних викликає серйозні проблеми з безпекою та конфіденційністю. Таким чином, ретельний розгляд та оцінка Блокчейну в застосуванні до Інтернету речей має здійснюватися з аналізом усіх можливих точок зору (див. рисунок 2.2).

З цією метою було проведено дослідження щодо вирішення аспектів Блокчейну для IoT. Наприклад, Доррі [21] запропонував БД на Блокчейні для розумних будинків, реалізуючи багаторівневу систему, що складається з розумного дому, хмарного сховища та засобів інтеграції. Розумний дім складається з:

– локального сховища;
– розумного домашнього майнера;
– IoT- пристроїв.

Рисунок 2.2 – Блокчей та IoT

Він підтримує локальний приватний Блокчейн, обробляючи локальні компоненти. Ху [22] досліджує БД на Блокчейні для систем управління ресурсами хмарних центрів обробки даних (DC). Розроблена система уникає PoW, PoS та інших механізмів підтвердження. Замість цього реалізовано систему, в якій хмарні центри обробки даних, виконуючи функції майнерів, сортують список майнерів і видаляють зі списку λ-попередніх майнерів. А перший DC, що залишився у списку, видобуває наступний блок.

Консценті [23] провів систематичний огляд літератури про Блокчейн для IoT. Оцінка мала на меті дослідити випадки використання та відмінності впровадження, а також цілісність, анонімність та адаптивність Блокчейну.

Полізос та Фотіо [24] оцінили проблеми безпеки та конфіденційності, стійкості та довіри, пов’язані з IoT, і розглянули модель, в якій завдання, пов’язані з Блокчейном, передаються на сумісний з платформою «Etherium» мережевий шлюз для подолання обчислювальних обмежень. IoT- пристроїв.

2.2 Блокчейн та великі за обсягом колекції даних

Великі за обсягом колекції даних мають надзвичайно великі показники:

– обсягу;

– різноманітності;

– швидкості;

– правдивості;

– цінності тощо.

Тому традиційні послуги зберігання, обслуговування та аналізу даних не можуть бути використані для їх обробки [3]. З розвитком обчислювальної техніки, інтелекту даних і машинного навчання [25] великі дані отримали значне поширення, як основу для сучасних систем аналітики даних і стають все більш сформованою галуззю в царині інформаційних технологій.

Механізми, що підвищують здатність систем великих даних обробляти й оцінювати великі дані, а також створювати та збирати великі дані, стають все популярнішими. Керовані IoT інформаційні системи «розумного» світу передбачають масове ґенерування безпрецедентно великих колекцій даних [3]. Тому, розглядаючи застосування інформаційної технології Блокчейн, розподіл і управління даними, а також децентралізацію обробки та атестації пропонують можливі шляхи для просування технологій великих за обсягом даних (див. рисунок 2.3). З цією метою Карафілоскі та Мішев [26] розглянули Блокчейн-застосунки, які з’явилися для вирішення проблем великих даних, у тому числі у сферах:

– захисту персональних даних;

– цифрової власності;

– Інтернету речей.

Сміт [27] запропонував три основних критерії для оцінки потенціалу управління даними на основі блокчейну:

– надійність;

– безпеку;

– довіру.

Рисунок 2.3 – Блокчей та великі за обсягом дані

Що втілює таксономію, розроблену на основі аналізу та комбінації різних таксономій з досліджуваних робіт. Потім розроблені критерії та підкритерії були застосовані до групи проектів та застосунків під управлінням Блокчейн.

2.3 Блокчейн в царині хмарних та крайових обчислень

Хмарні обчислення та нова парадигма крайових/туманних обчислень пропонують розподілені незалежні від пристроїв обчислення та послуги зберігання даних [2]. Хмарні обчислення вважаються напівцентралізованою архітектурою, яка залежить від великих центрів обробки даних. Крайові обчислення реалізують розподілену хмарну структуру на межі мережі, поблизу користувачів. Застосування Блокчейну до хмарних і периферійних обчислень є логічним. Основні застосування Блокчейну до хмарної та периферійної інфраструктури (див. рисунок 2.4) призначені для безпеки на основі здатності Блокчейну забезпечувати консенсус та підтримувати історію підписаних транзакцій.

Рисунок 2.4 – Блокчей та хмарна інфраструктура

Застосування Блокчейну для механізму керування контрактами на обслуговування є привабливим для хмарних і периферійних обчислень, оскільки дозволяє користувачам автономно виконувати контракти.

Враховуючи потреби майбутньої хмарної інфраструктури, Шарма [28] запропонував архітектуру на основі Блокчейна для хмарних обчислень, яка інтегрує програмно визначену мережу (SDN) і крайові обчислення, щоб зменшити потребу в надійних платформах сторонніх розробників та зменшити витрати на хмарні обчислення. Автори окреслили:

– надання послуг на основі Блокчейну в хмарі;
– підключені до Блокчейну SDN-контролери в туманних кластерах;
– базові станції з підтримкою SDN на межі
– консенсус Блокчейну з двома стрибками – «Proof-of-Service».

2.4 Блокчейн для управління ідентифікацією

Управління ідентифікацією можна розглядати з точки зору користувачів та цифрових сутностей:

– пристроїв;
– апаратного забезпечення;
– віртуальних машин тощо.

В обох випадках, оскільки для використання різних послуг і продуктів, зокрема, електронної пошти, соціальних мереж, програмного забезпечення тощо, необхідні критерії ідентифікації, що зберігаються в електронному вигляді, безпека ідентичності залежить від базових програмних систем, які містять дані ідентифікації, та від засобів комунікації, за допомогою якої необхідно підтвердити особу. У контексті контролю доступу цифровий підпис забезпечує безпечний засіб для перевірки користувача. Завдяки застосуванню Блокчейну може бути додатково покращена криптографічно захищена ідентичність шляхом децентралізації консенсусу щодо транзакцій доступу та перевірки. Наприклад, розглядаючи системи атестації та управління ідентичностями, Ясін і Лю [29] розробили систему управління ідентифікацією на основі блокчейну та управління розумними контрактами, яка окремо оцінює особисту, професійну та онлайн-репутацію (див. рисунок 2.5).

Рисунок 2.5 – Блокчейн для персональної ідентифікації

Система призначена для захисту особистості користувача за допомогою Блокчейну, одночасно забезпечуючи атестацію користувача шляхом аналізу даних інституцій та соціальних мереж. Аналогічно, Ян [30] запропонував сховище персональних даних на основі Блокчейн (BC-PDS) на існуючій платформі «OpenPDS/SafeAnswers», щоб діючи як нотаріус для безпечного зберігання та контролю доступу на основі автономності. Блокчейн був застосований для покращення бази даних «OpenPDS», а система контролю доступу була впроваджена для покращення системи «SafeAnswers» на основі відносин між авторизованими користувачами та власниками даних.

2.5 Блокчейн, криптовалюта, економіка та ринки

Перше застосування Блокчейну – це механізм для запису транзакцій цифрових валют, і це залишається найбільшим застосунком цієї концепції на даний час. Біткоїн був першою криптовалютою, яка отримала широку популярність [4]. Відтоді численні варіації інформаційної технологій Блокчейн призвели до появи багатьох різноманітних криптовалют, а також застосування Блокчейну на міжнародних цифрових ринках та в економіці (див. рисунок 2.6).

Рисунок 2.6 – Блокчейн, криптовалюти та економіка

Згідно з дослідженням глобального порівняльного аналізу криптовалют [31] на різних цифрових ринках торгуються сотні криптовалют. Хоча більшість цих криптовалют класифікуються як «альткоїни» і, по суті, є клонами біткоїнів або інших монет з реалізацією різних параметрів, невелика частина нових пропозицій внесла значні інновації.

Наприклад, «Litecoin» застосував перший новий алгоритм консенсусу після «PoW Bitcoin», який називається «Scrypt». Це зменшує часовий інтервал генерації блоків до 2,5 хвилин і вважається найкращим для роздрібної торгівлі. Інші криптовалюти, які впровадили інновації щодо механізму консенсусу:

– «Peercoin», який поєднує PoW і PoS;
– «Myriad» – перша валюта, яка підтримує п’ять алгоритмів;
– «NXT» – застосовує лише PoS.

Ще одне нововведення – це використання PoW, крім простого захисту Блокчейну, для вирішення складних наукових проблем. Наприклад, система PoW у «Primecoin» шукає ланцюжки простих чисел, а «Curecoin» використовує свій PoW для дослідницьких розрахунків у згортанні білків. Ці нововведення заслуговують на особливу увагу, оскільки вони представляють потенційне застосування накладних витрат на видобуток для позитивного глобального зиску, а не просто споживання енергії, а також потенційно пропонують подвійні стимули у формі майнингу монет та цінних математичних даних.

2.6 Бізнес-рішення, розумні контракти та автоматизація на основі Блокчейн

Спричинивши хвилю збурень в біржових та інвестиційних спільнотах, інформаційні технології Блокчейн почали поширюватися в бізнес-застосунках завдяки концепції смарт-контрактів [32]. Оскільки реєстр Блокчейну може зберігати та перевіряти транзакції, можливість виконувати повні сценарії та складні смарт-контракти є доволі привабливою (див. рисунок 2.7).

Рисунок 2.7 – Блокчейн та смарт контракти

Можна запровадити можливість арбітражного розгляду таких контрактів, оскільки запис трансакцій можна легко розглянути. Одна з труднощів у цьому напрямку, однак, полягає в тому, як прив’язати розумні контракти до зовнішніх послуг, даних або навіть реального обміну товарами, які вони можуть представляти. Нат [33] запропонував унікальний бізнес-додаток – БД на Блокчейні – структуру для обміну інформацією про страхування між агентствами для боротьби з шахрайством. Застосунок розглядає:

– попередні спроби обміну даними розвідки;

– процес страхових відшкодувань;

– залежність структури від співпраці кількох компаній різного розміру та конкуренції.

Аналогічно, використовуючи автоматизацію розумних контрактів, Зоу [34] запропонував схему управління контрактом на обслуговування з протоколом арбітражного розгляду спорів.

2.7 Блокчейн для відстежування сутностей в логістиці

Логістичні ланцюги постачання є необхідним взаємозв’язком підприємств для виведення продукції на ринок, часто залучаючи повністю відокремлені організації або підрозділи, які залежать від взаємної чесності та порядності, дотримуються правил і надають безпечні продукти та послуги. Тим не менш, ця система сприйнятлива до корупції, фальсифікації, фальсифікації та

може бути монополістичною, коли одна організація володіє всім ланцюгом поставок, непрозорою та асиметричною щодо кінцевих споживачів. Щоб подолати ці труднощі, особливо в світлі різноманітних скандалів з безпекою та якістю в регульованих галузях, було сформовано запит щодо впровадження Блокчейну для забезпечення відстеження та цілісності відповідності нормативним вимогам ланцюга поставок (див. рисунок 2.8).

Рисунок 2.8 – Блокчейн та логістика

Тіан [35] розглянув нещодавні скандали з безпечністю та якістю харчових продуктів у Європі та Китаї і запропонував систему відстеження ланцюга постачання для виробництва сільськогосподарської продукції на основі Блокчейну. Водночас він запропонував оновлену систему відстеження ланцюга постачання, засновану на Інтернеті речей та Блокчейні, щоб забезпечити вищий рівень безпеки харчових продуктів загалом [36]. Лу і Сю [37] розробили «originChain» – консорціумну Блокчейн-платформу для надання послуг щодо відстеження та автоматизації дотримання вимог регулятора. Зазначена

платформа зберігає лише хеші сертифікатів простежуваності та невеликі обсяги організаційних даних та даних про відстеження, завантажуючи необроблені файли відстеження в централізовану MySQL БД з резервними копіями, які також можливі для локального зберігання бізнесових даних.

2.8 Блокчейн та медична інформатика

Медичні послуги, як галузь із суворим регулюванням, надзвичайно зацікавлені в захисті даних, зібраних від пацієнтів, особливо в контексті державного нагляду та повноважень. Через дуже чутливу та конфіденційну природу таких даних було проведено значну роботу над розробкою високостійких систем безпеки медичних даних. Будучи відносно новою інформаційною технологією, Блокчейн може забезпечити управління та передачу медичних даних безпосередньо пацієнтам (див. рисунок 2.9), завдяки чому історія хвороби зберігається та доступна для пошуку, і лише авторизовані постачальники послуг можуть її переглядати та зберігати. Тим не менш, це створює ряд проблем, оскільки потреба в швидких і своєчасних даних історії хвороби може бути критично-важливою в надзвичайній ситуації.

Рисунок 2.9 – Блокчейн в медичній галузі

Маючи широкий погляд на системи медичних даних, Маг'яр [38] розглядає прикладну модель на основі Блокчейну для захисту медичних даних, зважуючи витрати та стимули різних реалізацій. Шае і Цай [39] запропонували інформаційно-технологічну Блокчейн-архітектуру для застосунків обміну та зберігання медичних даних, що вимагає розробки:

– структур управління з підтримкою Блокчейну;
– підсистеми управління обміном даними;
– системи управління анонімною ідентифікацією;
– підсистеми управління зберіганням даних;
– компонентів для розподілених паралельних обчислень.

Хоча попередні роботи були зосереджені на високорівневих концептуальних архітектурах, дослідники також впровадили декілька фреймворків для окремих підрозділів та інформаційно-технологічних платформ. Зокрема, Азарія [40] використав «Etherium» для розробки «MedRec» – блокчейн-фреймворку для зберігання, аутентифікації та обміну електронними медичними записами (EMR). А Xia [41] розробив «MedShare» – інформаційну систему обміну медичними записами для розпорядників медичних даних.

2.9 Блокчейн та комунікаційні мережі

Використання Блокчейну для зв'язку та управління мережею, тісно пов'язане з Інтернетом речей і хмарними обчисленнями, має потенціал, щоб дозволити безпечну та трансакційно-перевірену мережеву взаємодію. Оскільки майнинг, необхідний для роботи та перевірки Блокчейну, є дорогим ресурсом, реалізація вузлів і компонентів Блокчейну на краю мережі забезпечує:

– збагачене ресурсами середовище для підтримки транзакцій і атестації блоків;
– безпечний зв'язок;
– зашифроване зберігання даних;
– реалізація контракту на розумне обслуговування.

Це додаткові переваги, які можна реалізувати за допомогою мережевих інфраструктур на основі Блокчейну (див. рисунок 2.10).

Рисунок 2.10 – Блокчейн та комунікаційні мережі

Ча [42] запропонував шлюз «Blockchain Connected» (BC) з підтримкою Блокчейн-конфіденційності для захисту IoT-пристроїв за допомогою платформи «Etherium» для реалізації смарт-контрактів. Інформаційна система використовує політику конфіденційності, що зберігається в JSON-об’єкти, і створює смарт-контракти як для IoT-пристроїв, підключених за допомогою Bluetooth Low Energy (BLE), та для BC-шлюзів, які зберігаються в Блокчейні.

2.10 Інші категорії Блокчейн-застосунків

На додаток до описаних вище категорій, розглядаємо інші інноваційні сфери використання Блокчейн. У цих галузях застосування Блокчейну тільки починає з’являтися, і мало що розглядається поза запропонованими теоретичними рамками. Зокрема, це Блокчейн для:

– управління інтелектуальною власністю (див. рисунок 2.11);
– управління авторськими правами;
– «розумних» державних рішень тощо.

Рисунок 2.11 – Блокчейн та інтелектуальна власність

Ху [43] запропонував схему управління цифровими правами мережевого медіа за допомогою Блокчейну. Хоу [44] розглянув практичні застосування та обмеження технологій Блокчейн для використання в ініціативах електронного уряду. Зокрема, блокчейн надає перспективний механізм підвищення якості та інтеграції державних послуг, а також створення індивідуалізованої системи ідентифікації та кредитування.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1 Природне середовище і його забруднення

В кваліфікаційній роботі освітнього рівня «бакалавр» проведено аналіз світового досвіду реалізації Блокчейн-застосунків. На даний час ця інформаційна технологія активно розвивається та запроваджується практично в усі сфери людської діяльності. Запровадження інноваційних інформаційних технологій тісно пов’язане зі збереженням навколишнього середовища. Тому в даному розділі доцільно розглянути природне середовище, як основу безпеки життєдіяльності людини та його забруднення.

Кінець двадцятого та початок двадцять першого століття – це час усвідомлення кризи цивілізації, негативних її наслідків при підкоренні природи. Технічний прогрес породжує серйозні екологічні проблеми. Природа Землі під натиском людської діяльності на даний час опинилася на межі екологічної катастрофи. Понад сім мільярдів людей на планеті користуються природними ресурсами, часто зловживаючи ними. Це призводить до вимирання видів, забруднення води та повітря токсичними речовинами, незворотну втрату природних екосистем і, як наслідок, погіршення здоров'я людей та якості їх життя. Екологія набула особливого значення як наукова основа раціонального природокористування й оохорони живого світу нашої планети [45].

Поряд із виснаженням природних ресурсів збільшення чисельності населення планети створює небезпеку глобального забруднення середовища мешкання, яке призводить до непередбачуваних катаклізмів: епідемій, погіршення якості води, їжі та людського життя в цілому.

За статистикою, серед усіх джерел забруднення на першому місті – відпрацьовані гази автотранспорту, які спричиняють до 70% усіх хвороб у містах. На другому місці викиди теплових електростанцій. На третьому – хімічна промисловість.

Швидкими темпами відбувається забруднення атмосфери. Оскільки поки що основним способом отримання енергії залишається спалювання викопного палива, то з кожним роком зростає споживання кисню, а на його місце надходить велика кількість вуглекислого газу, оксидів азоту, чадного газу, сажі, пилу та шкідливих аерозолів [46].

Щороку в світі спалюється понад десять мільярдів тон умовного палива. При цьому в повітря викидається більше мільярда тон різних завислих часток, серед яких багато канцерогенних речовин. За останні 100 років в атмосферу потрапило більше мільйона тон кремнію, 1.5 мільйона тон миш'яку, 900 тисяч тон кобальту. Тільки в атмосферу США щорічно викидається понад 200 мільйонів тон шкідливих речовин. Серед них 100 мільйонів тон оксидів вуглецю, 37 мільйонів тон оксидів сірки, 30 мільйонів тон вуглеводнів, 20 мільйонів тон оксидів азоту і 30 мільйонів тон різноманітного пилу.

Забруднення атмосфери шкідливе не тільки для дихання населення планети, воно водночас зменшує прозорість атмосфери, через яку відбувається взаємодія планети з космосом, передусім з випромінюванням Сонця. Вважають, що сьогодні в атмосфері перебуває близько 20 мільйонів тон завислих часток. Катастрофічних розмірів набуло забруднення океану нафтопродуктами, отрутохімікатами, синтетичними миючими засобами, нерозчинними пластиками. Зараз в океан потрапляє близько 30 мільйонів тон нафтопродуктів за рік. Зважаючи на повільні темпи розчинення нафти у воді, значна частина поверхні океану вкрита нафтовою плівкою. Деякі спеціалісти вважають, що її загальна площа складає 1/5 від площі океану. Нафтова плівка таких розмірів дуже небезпечна, тому що вона порушує газо- і водообмін між атмосферою і гідросферою, пригнічує розвиток життя, особливо планктону [47].

Антропогенна міграція хімічних елементів стала основним чинником змін у навколишньому середовищі. Природне надходження хімічних елементів з надр здебільшого досягає 1% від антропогенних надходжень. Якщо приріст світового виробництва сталі залишиться на сучасному рівні – близько 5% на рік то вміст оксидів заліза в ґрунті та воді через 50 років подвоїться. За цей час за

відсутності регулювальних заходів концентрація свинцю в навколишньому середовищі зросте в 10 разів, ртуті – у 100, миш'яку – в 250 разів. Досліджено, що вміст свинцю в кістках сучасної людини приблизно в 50 разів вищий, ніж у рештках наших давніх пращурів, а концентрація ртуті в сьогоднішніх організмах у 100-200 разів перевищує її вміст у навколишньому середовищі.

На стан природного середовища земної поверхні великий вплив справляє теплове забруднення [48]. При спалюванні палива людство вивільняє в рік 34-1015 кКал тепла, яке розсіюється в навколишньому просторі, змінюючи температурний режим середовища і динаміку процесів, які в ньому відбуваються. Особливо інтенсивно при цьому змінюються темпи процесів окислення. Тому вміст кисню в середовищі істотно змінюється залежно від перепадів температури. Різка зміна температурного балансу середовища внаслідок теплового забруднення починає помітно відбиватися на погоді і навіть на кліматі в цілому, що особливо помітно в районі великих міст і великих промислових центрів. Перепад температури між; центром великого міста і околицею становить 2-4 °С.

До серйозних чинників забруднення середовища, крім зазначених, належить підвищення фону електромагнітного випромінювання від численних електротехнічних пристроїв, підвищення звукового фону в середовищі, інфра- та ультразвуки, шуми. А також підвищення радіоактивного фону.

Забруднення середовища негативно відображається на здоров'ї людей і на житті всього населення планети. При всіх безперечних успіхах медицини і санітарного обслуговування збільшується кількість хворих на серцево-судинні, онкологічні захворювання, а також; хвороби шлунку, печінки і нирок. Зростає чисельність вроджених патологій. Від хвороб, спричинених забрудненням води, щорічно вмирає близько 5 мільйонів немовлят. У промислово розвинутих країнах зафіксовані нові захворювання, викликані різними забрудненнями. Зокрема, в Японії стала відома хвороба під назвою «ітай-ітай», яка виникає при отруєнні кадмієм і вражає майже всі внутрішні органи.

3.2 Заходи, що покращують умови праці оператора

В даній кваліфікаційній роботі освітнього рівня «бакалавр» подано аналіз світового досвіду реалізації Блокчейн-застосунків. Блокчейн-застосунки інтегруються на основі інноваційних інформаційних технологій, котрі використовуються операторами різнотипової комп’ютерної техніки. Тому в даному параграфі доцільно розглянути заходи, що покращуюють умови праці оператора ПК. Організація робочого місця оператора повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам, характеру та особливостям трудової діяльності [49]. Площа, виділена для одного робочого місця з ВДТ, повинна складати не менше 6 м^2, а об'єм – не менше 20 м^3. Базовими елементами комп'ютеризованого робочого місця вважається відеотермінал, клавіатура – основне обладнання та пюпітр – тримач для документів – допоміжне обладнання.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом – 30° від лінії зору користувача. Найкращі зорові умови і можливість розпізнавання знаків досягається такою геометрією розміщення, коли верхній край відеотерміналу знаходиться на висоті очей, а погляд спрямований вниз на центр екрана. Оскільки при роботі за ВДТ найбільш сприятливим вважається нахил голови вперед, приблизно на 20° від вертикалі, при такому положенні голови м'язи шиї розслабляються, то екран відеотерміналу також повинен бути нахиленим назад на 20° від вертикалі. Екран відеотерміналу та клавіатура розташовуються на оптимальній відстані від очей користувача, але не ближче 600 мм.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв та обладнання для обслуговування та налагоджування Е0М виконується як окрема групова трьохпровідникова мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників.

Нульовий захисний провідник використовується для заземлення, занулення електроприймачів і прокладається до стійки групового розподільчого

щита, розподільчого пункту до розеток живлення. Не допускається підключення ЕОМ, периферійних пристроїв ЕОМ до звичайної двопровідної електромережі, в тому числі з використанням перехідних пристроїв.

Для споруд та приміщень, в яких експлуатуються відеотермінали та ЕОМ, крім загальних вимог пожежної безпеки, здійснюються спеціальні протипожежні заходи, визначені Правилами пожежної безпеки в Україні ДНАОП 0.00-1.31-99 та іншими нормативними документами.

Згідно санітарних правил для нормальної організації праці працівників, які обслуговують ВДТ ЕОМ та ПЕОМ слід передбачити внутрішньозмінні регламентовані перерви для відпочинку, які передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності [50]. При виконанні протягом дня робіт, які належать до різних видів трудової діяльності, за основну роботу з ВДП ЕОМ і ПЕОМ слід вважати таку, що займає не менше 50 відсотків часу впродовж робочої зміни чи робочого дня.

Відповідно до санітарних правил встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

– для розробників програм із застосуванням ЕОМ, слід призначити регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи;

– для операторів із застосуванням ЕОМ, слід призначити регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні 2 години роботи;

– для операторів комп'ютерного набору, слід призначити регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр»:

– Розглянута інтеграція Блокчейн та інформаційних технологій.

– Описано інформаційно-технологічний концепт Блокчейн.

– Проаналізовано узагальнену структуру Блокчейн-фреймворків. Зокрема, описано рівень даних, мережевий рівень та особливості Блокчейну.

В другому розділі кваліфікаційної роботи:

– Описано використання Блокчейну для Інтернету речей.

– Проаналізовано інтеграцію Блокчейну та великих за обсягом колекцій даних.

– Розглянуто Блокчейн в царині хмарних та крайових обчислень.

– Описано Блокчейн для управління ідентифікацією.

– Висвітлено інформацію про Блокчейн, криптовалюти та економіку.

– Проаналізовано бізнес-рішення, розумні контракти та автоматизацію на основі Блокчейн.

– Описано Блокчейн для відстежування сутностей в логістиці.

– Проаналізовано інтеграцію Блокчейну та медичної інформатики.

– Розглянуто взаємодію Блокчейну та комунікаційних мережі.

– Висвітлено дані про інші категорії Блокчейн-застосунків.

У розділі «Безпека життєдіяльності, основи охорони праці» подано опис природнього середовища і його забруднення. Висвітлено заходи, що покращують умови праці оператора.

ПЕРЕЛІК ДЖЕРЕЛ

1 J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125– 1142, Oct 2017.

2 W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang. A survey on the edge computing for the Internet of Things. *IEEE Access*, 6:6900–6919, 2018.

3 F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao. A survey on big data market: Pricing, trading and protection. *IEEE Access*, 6:15132– 15154, 2018.

4 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http: //bitcoin.org/bitcoin.pdf.

5 Matsiuk O., Kunanets N., Pasichnyk V., Rzheuskyi A., Bilak Y., Formation of Hypercubes Based on Data Obtained from Systems of IoT Devices of Urban Resource Networks, International Journal of Sensors, Wireless Communications and Control (2020) 10: 1. ISSN 2210-3287.

6 Matsiuk O., et al, Selection of Effective Methods of Big Data Analytical Processing in Information Systems of Smart Cities. CEUR Workshop Proceedings 2631, pp. 68-78. 2020.

7 Bodnarchuk I., Duda O., Kharchenko A., Kunanets N., Matsiuk O., Pasichnyk V. Choice method of analytical information-technology platform for projects associated to the smart city class. ICTERI 2020 ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume I: Main Conference p.317-330.

8 Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle. A quantitative analysis of the impact of arbitrary blockchain content on Bitcoin. In *Proceedings of the 22nd International Confer-ence on Financial Cryptography and Data Security (FC)*, 2018.

9 Bitcoin core integration/staging tree. https://github.com/bitcoin/bitcoin/.

10 O., Kunanets, N., Martsenko, S., Matsiuk, O., Pasichnyk, V., Building secure Urban information systems based on IoT technologies. CEUR Workshop Proceedings 2623, pp. 317-328. 2020.

11 Cryptocurrency market capitalizations. https://coinmarketcap.com/.

12 Oscar Williams-Grut. Here are all the theories explaining the crypto market crash. http://www.businessinsider.com/ bitcoin-cryptocurrency-market-crash-explained-causes-2018-1.

13 D. An, Q. Yang, W. Yu, D. Li, Y. Zhang, and W. Zhao. Towards truthful auction for big data trading. In *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, pages 1–7, Dec 2017.

14 Gao, Weichao, William G. Hatcher, and Wei Yu. "A survey of blockchain: Techniques, applications, and challenges." 2018 27th international conference on computer communication and networks (ICCCN). IEEE, 2018.

15 K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4:2292–2303, 2016.

16 Minhaj Ahmad Khan and Khaled Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395 – 411, 2018.

17 J. Göbel, H.P. Keeler, A.E. Krzesinski, and P.G. Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104:23 – 41, 2016.

18 D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen. Untangling Blockchain: a data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, PP(99):1–1, 2018.

19 Alyssa Hertig. Intel is winning over blockchain critics by reimagining bitcoin’s dna. https://www.coindesk.com/ intel-winning-blockchain-critics-reimagining-bitcoins-dna/, dec 2016.

20 Jennifer J. Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):25, Dec 2016.

21 A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.

22 C. Xu, K. Wang, and M. Guo. Intelligent resource management in blockchain-based cloud datacenters. *IEEE Cloud Computing*, 4(6):50– 59,Nov. 2017.

23 M. Conoscenti, A. Vetrò, and J. C. De Martin. Blockchain for the Internet of Things: a systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–6, Nov 2016.

24 G. C. Polyzos and N. Fotiou. Blockchain-assisted information distribution for the Internet of Things. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 75–78, Aug 2017.

25 W. G. Hatcher and W. Yu. A survey of deep learning: Platforms, applications and emerging research trends. *IEEE Access*, pages 1–1, 2018.

26 E. Karafiloski and A. Mishev. Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, pages 763–768, July 2017.

27 T. D. Smith. The blockchain litmus test. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2299–2308, Dec 2017.

28 P. K. Sharma, M. Y. Chen, and J. H. Park. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access*, 6:115–124, 2018.

29 A. Yasin and L. Liu. An online identity and smart contract management system. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 192–198, June 2016.

30 Z. Yan, G. Gan, and K. Riad. BC-PDS: protecting privacy and selfsovereignty through BlockChains for OpenPDS. In *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 138–144, April 2017.

31 Garrick Hileman and Michel Rauchs. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, 2017.

32 A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 839–858, May 2016.

33 I. Nath. Data exchange platform to fight insurance fraud on blockchain. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pages 821–825, Dec 2016.

34 J. Zou, Y. Wang, and M. A. Orgun. A dispute arbitration protocol based on a peer-to-peer service contract management scheme. In *2016 IEEE International Conference on Web Services (ICWS)*, pages 41–48, June 2016.

35 Feng Tian. An agri-food supply chain traceability system for china based on RFID blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pages 1–6, June 2016.

36 Feng Tian. A supply chain traceability system for food safety based on HACCP, blockchain Internet of Things. In *2017 International Conference on Service Systems and Service Management*, pages 1–6, June 2017.

37 Q. Lu and X. Xu. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software*, 34(6):21–27, November 2017.

38 G. Magyar. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In *2017 IEEE 30th Neumann Colloquium (NC)*, pages 000135–000140, Nov 2017.

39 Z. Shae and J. J. P. Tsai. On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 1972– 1980, June 2017.

40 A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. MedRec: using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Aug 2016.

41 Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.

42 S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access*, PP(99):1–1, 2018.

43 R. Xu, L. Zhang, H. Zhao, and Y. Peng. Design of network media 2019s digital rights management scheme based on blockchain technology. In *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pages 128–133, March 2017.

44 H. Hou. The application of blockchain technology in e-government in china. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–4, July 2017.

45 Основні екологічні проблеми людства, їх глобальний характер та суть. URL: https://osvita.ua/vnz/reports/bjd/23700/.

46 Актуальні питання забруднення атмосферного повітря. URL: https://ecolog-ua.com/news/aktualni-pytannya-zabrudnennya-atmosfernogo-povitrya.

47 Нафтова плівка. URL: https://www.eionet.europa.eu/gemet/uk/concept/5848.

48 Теплове забруднення навколишнього середовища – джерела і види, наслідки | Доповідь. URL: https://nrv.org.ua/teplove-zabrudnennya-navkolyshnogo-seredovyshha-dzherela-i-vydy-naslidky-dopovid/.

49 Організація праці операторів комп 'ютерів. URL: https://pidru4niki.com/92832/bzhd/organizatsiya_pratsi_operatoriv_komp_yuteriv.

50 Заходи для покращення умов праці операторів комп'ютерів. URL: https://pidru4niki.com/92831/bzhd/zahodi_pokraschennya_umov_pratsi_operatoriv_kompyuteriv.