Міністерство освіти і науки України
Харківський національний університет ім. В. Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

"Допущено до захисту"
В.о. завідувача кафедри БІСТ
Мелкозьорова О.М._____
"_____" червня 2024р.

**Пояснювальна записка**
до кваліфікаційної роботи бакалавра
на тему: « Дослідження та застосування технологій блокчейн для підвищення кібербезпеки в мережах Інтернету речей (IoT)»

оцінка « » Керівник ст. викладач Шеханін К. Ю.
Голова ЕК
Лемешко О. В._____ Рецензент Родінко М.Ю_____
Виконавець: студентка групи КБ-41

_____ Ільченко К. Ю.

Харків – 202

# РЕФЕРАТ

Пояснювальна записка до дипломного проекту містить 56 сторінок, 27 рисунків, 4 таблиць та 35 посиланнь на джерела.

Метою даної дипломної роботи є дослідження потенціалу технології блокчейн для підвищення кібербезпеки в мережах Інтернету речей. Робота охоплює аналіз існуючих загроз та вразливостей в IoT-системах, вивчення принципів роботи блокчейну та його можливостей у сфері кібербезпеки, а також розробку та впровадження рішень на основі блокчейну для забезпечення належного рівня захисту IoT-пристроїв та даних, що передаються між ними.

Предметом дослідження є застосування технології блокчейн для підвищення кібербезпеки в мережах Інтернету речей (IoT). В рамках дослідження було проведено аналіз можливостей і переваг використання блокчейн технології для захисту даних, що обмінюються між пристроями IoT, а також розроблено ефективні стратегії впровадження цієї технології з метою підвищення рівня кібербезпеки в контексті Інтернету речей.

Об'єктом роботи є створена програма , яка демонструє, як такі технології можуть бути застосовані на практиці, забезпечуючи безпеку та достовірність даних у мережі IoT.

Створена програма демонструє, як такі технології можуть бути застосовані на практиці, забезпечуючи безпеку та достовірність даних у мережі IoT.

У результаті створення програми було досліджено та продемонстровано як технологія блокчейн може бути застосована на практиці, забезпечуючи безпеку та достовірність даних у мережі IoT.

Результати дослідження можуть бути використанні для покращення алгоритмів автоматизації та безпеки. Саме тому дослідження є актуальним і в подальшому може бути основою нових робіт.

Ключові слова: BLOCKCHAIN, IDS, IOT, JSON, PYTHON, БЛОК, КІБЕРАТАКА, КІБЕРБЕЗПЕКА, МЕРЕЖІ, СМАРТ-КОНТРАКТ .

# ABSTRACT

The explanatory note to the diploma project contains 56 pages, 27 figures, 4 tables and 35 references to sources.

The purpose of this thesis is to study the potential of blockchain technology to improve cyber security in Internet of Things networks.

The work covers the analysis of existing threats and vulnerabilities in IoT systems, the study of the principles of blockchain operation and its opportunities in the field of cyber security, as well as the development and implementation of blockchain-based solutions to ensure an adequate level of protection of IoT devices and the data transmitted between them.

The subject of the study is the application of blockchain technology to improve cyber security in Internet of Things (IoT) networks.

As part of the study, an analysis of the possibilities and advantages of using blockchain technology to protect data exchanged between IoT devices was carried out, as well as effective strategies for the implementation of this technology were developed in order to increase the level of cyber security in the context of the Internet of Things.

The object of the work is the created program, which demonstrates how such technologies can be applied in practice, ensuring the safety and reliability of data in the IoT network.

The created program demonstrates how such technologies can be applied in practice, ensuring the safety and reliability of data in the IoT network.

As a result of the creation of the program, it was investigated and demonstrated how blockchain technology can be applied in practice, ensuring the security and reliability of data in the IoT network.

Research results can be used to improve automation and security algorithms. That is why the research is relevant and can be the basis of new works in the future.

Keywords: BLOCKCHAIN, IDS, IOT, JSON, PYTHON, BLOCK, CYBER ATTACK, CYBER SECURITY, NETWORKS, SMART CONTRACT.

ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

BLE - Bluetooth Low Energy

DPoS - Делеговане підтвердження ставки

DDoS - Розподілене заподіяння послуг

IDS - Системи виявлення вторгнень

IIoT - Індустріальний Інтернет речей

IoT - Інтернет речей

JSON - JavaScript Object Notation

LPWAN - Мережа малої потужності та широкого діапазону

LTE-M - Long-Term Evolution for Machines

M2H - Людина до машини

M2M - Машина до машини

MITM - Атака посередника

NFC - Ближньодійова комунікація

PBFT - Practical Byzantine fault tolerance

PoA - Підтвердження повноважень

PoS - Підтвердження ставки

PoW - Підтвердження роботи

RFID - Радіочастотна ідентифікація

TCP - Протокол управління передачею

UDP/IP - Протокол без з'єднання

USB - Універсальна послідовна шина

WiFi - Бездротовий стандарт

ZigBee - Бездротова мережа

Брутфорс-атака - Атака грубої сили

# ВСТУП

У світі, де чисельність з'єднаних пристроїв зростає експоненційно, проблеми безпеки стають набагато складнішими і вимагають інноваційних підходів. Один із найбільш прогресивних напрямків у цьому контексті - технологія блокчейн.

Блокчейн, спочатку був розроблений для криптовалют, відомий він своєю надійністю та несхильністю до змін. Ці характеристики роблять його ідеальним інструментом для забезпечення кібербезпеки в мережах IoT. Використання технології блокчейн може допомогти вирішити проблеми централізованих місць вразливості та забезпечити безпеку, конфіденційність та цілісність даних, що передаються між підключеними пристроями.

Розвиток цифрових технологій та поширення концепції Інтернету речей (IoT) в різних галузях життєдіяльності людини призвів до стрімкого зростання кількості підключених пристроїв та обсягів даних, що передаються між ними. IoT-системи знаходять велике застосування у промисловості, транспорті, медицині, енергетиці, а також у побутовій сфері, забезпечуючи автоматизацію процесів, моніторинг, збір та аналіз даних. Однак, поряд із численними перевагами, широке впровадження IoT-систем супроводжується підвищеним ризиком для сфери кібербезпеки.

Багато IoT-пристроїв мають обмежені можливості захисту через низьку обчислювальну потужність, малий обсяг пам'яті та енергозалежність, що робить їх вразливими для різноманітних кіберзагроз. Крім того, децентралізована природа IoT-мереж, де дані передаються між численними пристроями без належного контролю та захисту, створює додаткові ризики для конфіденційності та цілісності даних.

Одним із перспективних рішень для підвищення рівня безпеки в IoT-мережах є застосування технології блокчейн. Блокчейн являє собою децентралізовану, розподілену базу даних, що забезпечує високий рівень надійності, прозорості та захищеності інформації. Завдяки використанню

криптографічних алгоритмів та консенсусних протоколів, блокчейн гарантує цілісність даних, їх незмінність та відстежуваність операцій, тим самим підвищуючи рівень довіри та безпеки в системі.

Ця робота важлива не лише з академічного погляду, але й з практичного – вона може сприяти розробці нових підходів та рішень для забезпечення кібербезпеки в мережах Інтернету речей, що є актуальною проблемою в сучасному цифровому світі.

Метою даної дипломної роботи є дослідження потенціалу технології блокчейн для підвищення кібербезпеки в мережах Інтернету речей. Робота охоплює аналіз існуючих загроз та вразливостей в IoT-системах, вивчення принципів роботи блокчейну та його можливостей у сфері кібербезпеки, а також розробку та впровадження рішень на основі блокчейну для забезпечення належного рівня захисту IoT-пристроїв та даних, що передаються між ними.

Предметом дослідження є застосування технології блокчейн для підвищення кібербезпеки в мережах Інтернету речей (IoT). В рамках дослідження буде проведено аналіз можливостей і переваг використання блокчейн технології для захисту даних, що обмінюються між пристроями IoT, а також розроблено ефективні стратегії впровадження цієї технології з метою підвищення рівня кібербезпеки в контексті Інтернету речей. Отримані результати будуть корисними, як для користувачів , які хочуть убезпечити себе, так і для різних установ, адже фінальні рекомендації допоможуть покращити рівень безпеки застосунків. Саме тому дослідження є актуальним і в подальшому може бути основою нових робіт.

Завдання дослідження включають: аналіз сучасного стану кібербезпеки в мережах Інтернету речей ; вивчення принципів та технічних особливостей технології блокчейн ; дослідження можливостей застосування блокчейн для забезпечення безпеки та конфіденційності в мережах IoT ; визначення переваг і недоліків використання блокчейн технології в контексті кібербезпеки IoT ;

розробку рекомендацій щодо оптимального впровадження технології блокчейн для підвищення кібербезпеки в мережах Інтернету речей.

# 1 СУТЬ ТА СТРУКТУРНІ ОСОБЛИВОСТІ ТЕХНОЛОГІЇ INTERNET OF THINGS , ПРОБЛЕМА ПРИВАТНОСТІ

## 1.1 Загальна характеристика Інтернету речей

З успіхом Інтернету і його потужною здатністю задовольняти потреби різних людей і суспільства в цілому виникла новітня епоха, відома як Інтернет речей (IoT). Ця революція спостерігається перед людськими очима і продовжує розвиватися зі швидкістю, що здається експоненційною, стимулюючи спритну взаємодію між фізичними об'єктами (M2M)[1] та між людиною та об'єктами (M2H).

Створення такої мережі, яка призначається для спілкування об'єктів на рівні одного користувача, має значні масштаби в ринковому аспекті і може помітно покращити якість нашого життя. У минулому було важко передбачити повний масштаб і довгостроковий вплив додатків Інтернету речей, особливо у вузьких галузях, як охорона здоров'я, сільське господарство, міська автоматизація та автоматизація будинку/офісу, промислове управління та управління енергоспоживанням, але вже зараз легко уявити конкретне застосування. Найважливішим для успішного розвитку Інтернету речей є розробка стандартів і архітектури , що забезпечують сумісність і інтероперабельність між різними пристроями і додатками. Проте, як і у багатьох інших областях, IoT може зіткнутися з викликами, такими як потреба в глобальному консенсусі щодо стандартів. У цьому розділі ми широко розглянемо Інтернет речей, простежимо його еволюцію та розглянемо різноманітні сфери його застосування.

Інтернет речей (IoT) здійснив революцію в обчисленнях і датчиках у різних сферах, пропонуючи повсюдне підключення та обмін даними [2]. З промисловими мережами, які широко використовують IoT, взаємозв’язок мільярдів пристроїв створює як можливості, так і проблеми [3]. Таке розповсюдження посилює потенціал уразливостей і вторгнень, значно розширюючи поверхню атаки. Отже, постійний моніторинг і контроль стає

обов’язковим для швидкого виявлення та пом’якшення загроз безпеці. Оскільки розгортання Інтернету речей продовжує розвиватися, забезпечення стійкості мереж проти кібератак вимагає пильного спостереження та профілактичних заходів для захисту конфіденційних активів і критичної інфраструктури [4]

Інтернет речей  є значним прогресом у підключенні завдяки з’єднанню мільярдів пристроїв з підтримкою Інтернету, сприянню розумній взаємодії та інтеграції фізичної інфраструктури з цифровими системами. IoT розширився, щоб охопити різноманітні галузі, включаючи розумні заводи, охорону здоров’я, розумні міста та транспорт [5]. Кількість пристроїв, підключених до Інтернету речей, у 2021 році перевищила 10 мільярдів, а до 2027 року очікується, що кількість пристроїв, підключених до Інтернету речей, досягне 41 мільярда.[6]. Датчики та виконавчі механізми є життєво важливими для Інтернету речей, оскільки вони збирають дані та маніпулюють реальним середовищем. Однак IoT стикається з такими проблемами, як уразливість безпеки, що виникає через обмеження ресурсів у сенсорних вузлах і проблеми сумісності, спричинені різними протоколами зв’язку. Незважаючи на ці перешкоди, конвергенція IoT з аналітикою даних і штучним інтелектом дозволяє приймати рішення в режимі реального часу та проводити прогнозне технічне обслуговування, що призводить до значного вдосконалення процесів. Щоб визначити потенціал IoT, необхідно розглянути питання конфіденційності, безпеки, неоднорідності даних і сумісності.

Поширення пристроїв Інтернету речей, різноманітність цих пристроїв та еволюція протоколів зв’язку призвели до сплеску нових технологій з інженерної точки зору [7]. Технології штучного інтелекту та машинного навчання ще більше розширили потенціал IoT шляхом вилучення інформації з неоднорідних даних датчиків, тим самим змінюючи бізнес-операції [8]. Модульна конструкція систем IoT, абстрагує ці системи на окремі компоненти, покращує їх адаптивність і уточнює їхню архітектуру [9]. Як на рисунку 1.1, багаторівнева структура IoT включає рівні сприйняття,

транспортування, обробки, застосування та аналітики. Рівень сприйняття охоплює фізичні пристрої, які відчувають навколишнє середовище та передають дані на вищі рівні, а транспортний рівень полегшує зв'язок між пристроями та хмарними службами. Рівень обробки, переважно розміщується на периферійних або хмарних платформах, надає можливості зберігання та обчислення, забезпечуючи масштабованість і взаємодію. Прикладний рівень управляє системними операціями, взаємодіє з користувачами та керує логічними процесами. Зрештою, аналітичний рівень пропонує користувачам практичну інформацію, що полегшує процес прийняття рішень. Проте проблеми з безпекою залишаються, особливо в пристроях IoT з обмеженими ресурсами та хмарному проміжному програмному забезпеченні, що підкреслює потребу в надійних заходах безпеки [9].

Туманні обчислення є протилежним трендом сучасних мережевих технологій до хмарних обчислень. В хмарних обчисленнях значні централізовані ресурси для зберігання та опрацювання даних надаються розподіленим користувачам через хмарні мережі для порівняно невеликої кількості споживачів (див. Таблиця 1.1).

Таблиця 1.1 – Порівняння хмарних та туманних обчислень

| | Хмарні обчислення | Тумані обчислення |
|---|---|---|
| Розташування ресурсів, зберігання / обробки | У центрі | Крайні |
| Затримка | Від низької до високої | Низька |
| Доступ | Фіксований або бездротовий | В основному безпровідний |
| Підтримка мобільності | Не застосовується | Застосовується |
| Контроль | Централізований /ієрархічний (повний контроль) | Розподілений ієрархічний або частковий контроль |
| Доступ до служб | Через ядро | З портативного пристрою (смартфон і тп.) |

Продовження таб. 1.1

| | | |
|---|---|---|
| Доступність | 99,99% | Висока нестабільність /високий рівень резервування |
| Число користувачів / пристроїв | Десятки і сотні мільйонів | Десятки мільярдів |
| Основний генератор контенту | Люди і пристрої | Пристрої / сенсори |
| Генерація контенту | У центральному розташуванні | Скрізь |
| Споживання контенту | На кінцевих пристроях | Скрізь |
| Віртуальна програмна інфраструктура | Корпоративні центральні сервери | Призначені для користувачів пристрої |

Концептуальна основа IoT зв’язує мільярди пристроїв із доступом до Інтернету, дозволяючи даним взаємодіяти один з одним та їх середовищем. Розвиток Інтернету речей призвів до доступу до даних по всьому світі , що забезпечує підключення в реальному часі та взаємодію між фізичними та цифровими системами в різних доменах. З самого початку, підтримуючи технологію радіочастотної ідентифікації (RFID), IoT розширився до різноманітних програм охорони здоров’я, транспорту та розумних заводів/міст. Останні статистичні дані свідчать про значне зростання кількості підключених пристроїв IoT, за прогнозами, до 2027 року їх кількість досягне 41 мільярда, що означає понад 152 000 нових підключень за хвилину до 2025 року . Це зростання відображає бурхливий ринок, коли світовий ринок Інтернету речей сягнув 157,9 мільярдів доларів США в 2021 році, головним чином завдяки промисловим додаткам і інтелектуальним пристроям [10].

IoT відкриває можливості для підвищення продуктивності завдяки моніторингу та контролю активів у реальному часі. Галузі приймають обґрунтовані рішення, використовуючи дані з IoT-пристроїв, таких як сенсори

та актуатори, підвищуючи ефективність роботи. Крім того, IoT полегшує розробку інтелектуальних програм у різних секторах, таких як фабрики, будинки, міста та сільське господарство, що сприяє підвищенню зручності та ефективності щоденних операцій (див. Рисунок1.1).

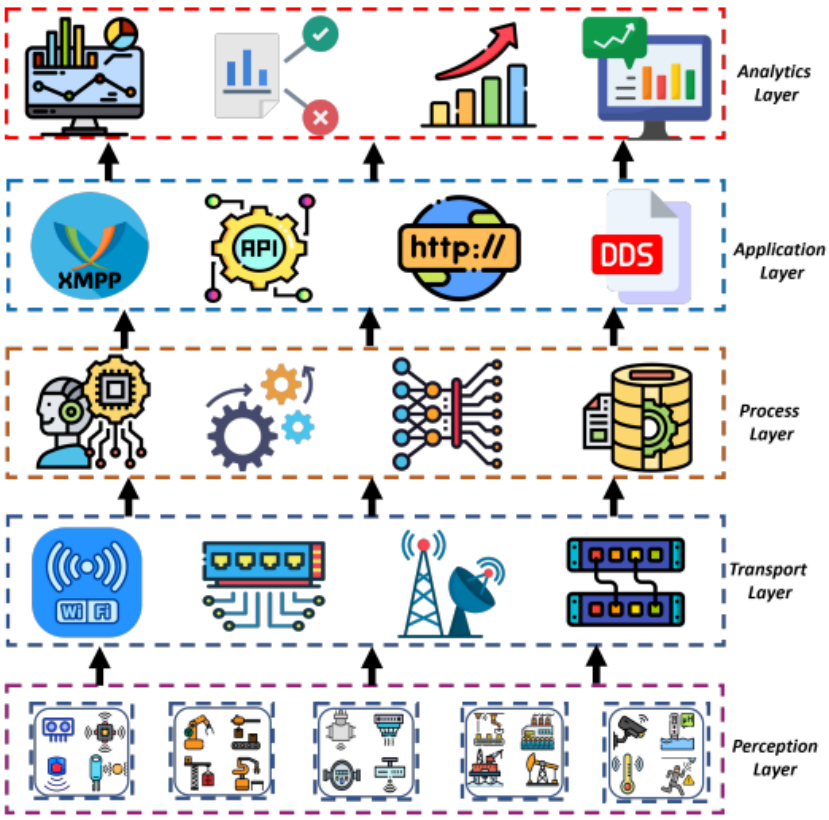


Рисунок 1.1 – Архітектурні рівні IoT

## 1.2 Базові визначення в мережі IoT

Інтернет речей (IoT) впроваджує ідею повсюдних обчислень. Це явище, також відоме як усюдисущі обчислення, полягає в тому, що обчислювальна потужність, зазвичай у вигляді мікропроцесорів, вбудовується в повсякденні предмети для їхньої ефективної комунікації та виконання корисних завдань, мінімізуючи потребу у взаємодії з комп'ютерами з боку кінцевого користувача. Ці обчислювальні пристрої підключені до мережі й завжди активні. Основна мета усюдисущих обчислень полягає в тому, щоб зробити ці пристрої "розумними", створивши сенсорну мережу, яка може збирати, обробляти та

передавати дані, а також обмінюватися ними, пристосовуючись до контексту та діяльності даних. Іншими словами, це мережа, яка може розуміти оточення та покращувати людський досвід та якість життя.[11]

Важливо зазначити, що існує багато різних архітектур для Інтернету речей (IoT), і вони варіюються за складністю та кількістю шарів в залежності від конкретних бізнес-потреб. Наприклад, прикладна модель, представлена на Всесвітньому форумі IoT 2014 компаніями Cisco, IBM та Intel, має сім рівнів. За словами Cisco, мета цієї архітектури полягає в тому, щоб навчати IT-професіоналів та розробників проектів IoT та сприяти їх швидшому впровадженню (див. Рисунок1.2).


Рисунок 1.2- Рівнева модель IoT

Незалежно від конфігурації та кількості шарів, основні компоненти будь-якої структури IoT залишаються незмінними:

- Умілі пристрої
- Мережі та шлюзи, які дозволяють пристроям з низьким енергоспоживанням підключатися до великої мережі Інтернету
- Платформи проміжного програмного забезпечення IoT для зберігання даних, покращених обчислювальних ресурсів та аналітичних можливостей

• Додатки для кінцевих користувачів, які надають можливість отримувати переваги від IoT та управляти фізичним оточенням (див. Рисунок1.3).


Рисунок 1.3- Базова структурна архітектура IoT

Основа системи IoT включає ряд ключових компонентів, що можуть формувати ефективну многорівневу структуру. Ці рівні включають:

- Рівень сприйняття: де розумні речі збирають дані.
- Транспортний рівень: для передачі даних між фізичними пристроями та хмарою через мережі і шлюзи.
- Рівень обробки: використовується для зберігання та управління потоками даних за допомогою IoT платформ.
- Прикладний рівень: надає рішення для аналітики, звітування та управління пристроями для кінцевих користувачів.
- Додаткові компоненти можуть включати:
- Шар обчислення на краю: для передпопередньої обробки даних біля джерела збору.
- Діловий рівень: де на основі даних приймаються бізнес-рішення.
- Рівень захисту: що охоплює всі інші рівні з метою забезпечення безпеки.

Ці додаткові компоненти, хоча й розглядаються як необов'язкові, відіграють важливу роль у забезпеченні сучасних бізнес-потреб.

Рівень сприйняття :

На початковому етапі системи IoT розумні пристрої діють як містки між реальним та цифровим світами, збираючи дані з різних "речей", від малих сенсорів до великих транспортних засобів. Ці пристрої, такі як датчики, перетворюють фізичні параметри, наприклад температуру, в електричні сигнали та передають їх у систему IoT.

Рівень підключення :

Цей рівень відповідає за комунікацію між пристроями, мережами та хмаровими службами. Зв'язок може бути здійснений безпосередньо за допомогою протоколів TCP або UDP/IP або через шлюзи, які транслюють різні протоколи та забезпечують шифрування даних (див. Рисунок1.4).

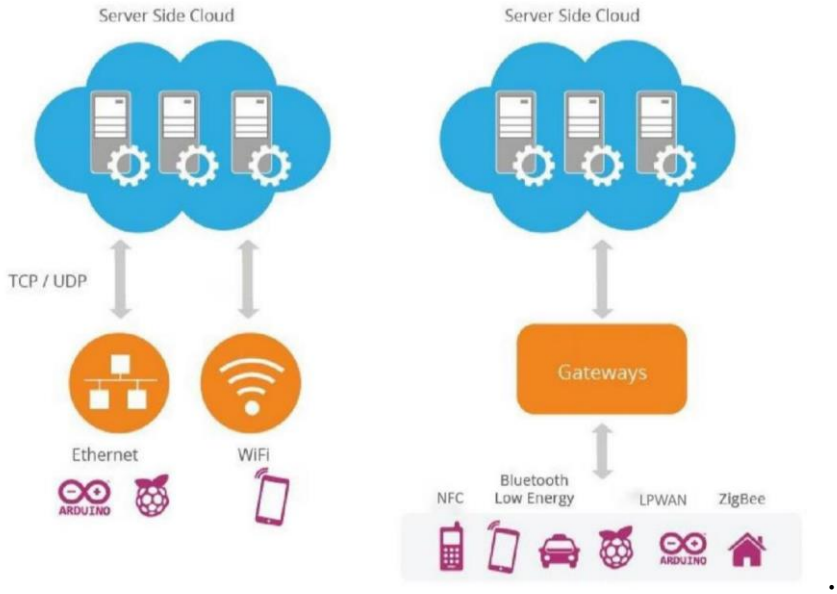


Рисунок 1.4 - Зв'язок між фізичним рівнем та хмарою

Взаємодія пристроїв з хмарними послугами або шлюзами охоплює різноманітні мережеві технології. Ethernet з'єднує постійні пристрої IoT, такі як відеокамери та обладнання, зокрема промислове, а також гральні консолі.

WiFi, як найбільш популярний бездротовий стандарт, ідеально підходить для IoT рішень з великим обсягом даних, які працюють на

обмеженій площі. Розумні девайси в домі, підключені до мережі, є хорошим прикладом цього підходу.

NFC (Ближньодійова комунікація) дозволяє простий і безпечний обмін інформацією на відстані до 10 см.

Bluetooth зазвичай використовується для короткодійових з'єднань між портативними пристроями. Для малопотужних IoT пристроїв розроблено стандарт Bluetooth Low-Energy (BLE), який передає невеликі об'єми даних.

LPWAN (мережа малої потужності та широкого діапазону) оптимізована для IoT, забезпечуючи бездротове підключення з низьким споживанням енергії і тривалою автономною роботою. Ця технологія ідеально підходить для моніторингу у розумних містах, будівлях і сільському господарстві.[12]

ZigBee - це бездротова мережа для передачі малих обсягів даних на короткі відстані. Особливістю ZigBee є здатність до підтримки до 65,000 вузлів із фокусом на домашню автоматизацію, а також на промислових і наукових застосуваннях.

Стільникові мережі забезпечують надійність і майже глобальне охоплення. Існують два стандарти LTE-M і NB-IoT, які спеціально розроблені для IoT, забезпечуючи передачу великих або малих пакетів даних відповідно.

## 1.3 Нормативно-правове регулювання технології Інтернет речей в Україні

Згідно з актами законодавства 2024 року, ключовими нормативно-правовими документами, які контролюють розробку та застосування сучасних інформаційно-комунікаційних технологій у впровадженні електронного урядування, є такі: Стратегія розвитку інформаційного суспільства в Україні, Стратегія сталого розвитку "Україна – 2020"[13], Стратегія реформування державного управління України на період 2016-2020 років, Концепція розвитку електронного урядування в Україні, а також Концепція розвитку цифрової економіки та суспільства України на період 2018-2020 років. Ці

документи покликані розв'язувати питання цифрової трансформації, стимулювання економіки, скорочення цифрового розриву, зміцнення співпраці з Європейським Союзом і розвитку інноваційної інфраструктури.

Особливу увагу приділяємо аналізу Концепції розвитку цифрової економіки та суспільства України на період 2018-2020 років, що має на меті реалізацію ініціатив "Цифрового порядку денного України 2020"[14] для усунення перешкод на шляху цифрової трансформації. Це передбачає заходи зі стимулювання економіки, залучення інвестицій, подолання цифрового розриву та розвиток інноваційної інфраструктури. Реалізація цієї концепції сприятиме стимулюванню економіки, перетворенню індустрій на конкурентоспроможні за допомогою цифровізації, розвитку експорту цифрових продуктів та послуг, та іншому.

У контексті впровадження електронного урядування, особливу увагу приділяємо питанням захисту персональних даних та приватності. Ці аспекти регулюються відповідними законодавчими актами, зокрема "Про інформацію" та "Про захист персональних даних". Згідно зі ст. 11 Закону України "Про інформацію"[15], інформація про фізичну особу включає особисті дані, які охоплюють різні аспекти, від освіти до місця народження. Збір такої інформації без згоди особи забороняється, крім випадків, передбачених законом. Закон "Про захист персональних даних" встановлює обов'язок реєстрації баз даних, що містять інформацію про громадян, та регулює питання захисту цих даних.

Питання захисту приватності стають особливо актуальними з розвитком Інтернету речей. В проекті нового Цивільного кодексу України відзначається, що право на приватність є особистим немайновим правом, яке тотожне праву на особисте життя та його конфіденційність.

Згідно з Конституцією України, жодна особа не може піддаватися втручанню у її особисте і сімейне життя, крім випадків, передбачених Конституцією. Збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди допускається лише у визначених законом

випадках і в інтересах національної безпеки, економічного добробуту та прав людини.

### 1.4 Сучасна ситуація в області інтернету речей

Швидкість підключення фізичних пристроїв до Інтернету стрімко зростає, і це тенденція не зупиниться. IoT відіграє ключову роль у нашому повсякденному житті, і це означає, що в майбутньому його використання буде набагато важливішим у технологічній інфраструктурі. Прогнозується, що до 2025 року загальна кількість підключених пристроїв у світі перевищить 75,44 мільярди (див. Рисунок1. 5).

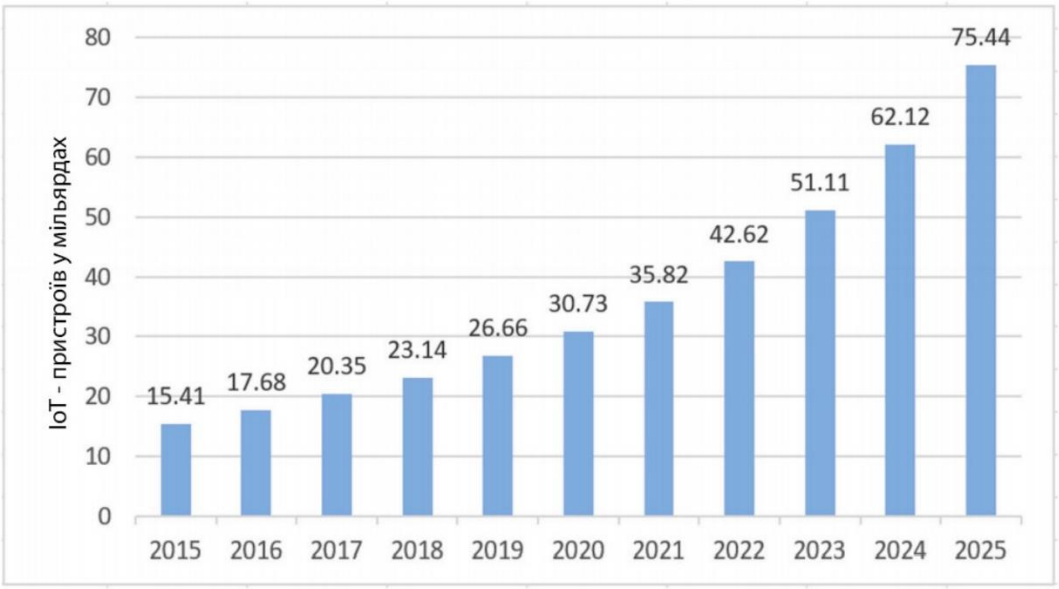


Рисунок 1.5 - Прогноз Інтернету речей з 2014 по 2025 рік (у мільярдах).

У той час як компанії поспішають розробляти нові IoT-пристрої з інноваційними додатками, безпека залишається проблемою. Багато компаній можуть використовувати застарілі стандарти безпеки.

Використання IoT-додатків росте у всьому світі, з основними лідерами, такими як Західна Європа, Північна Америка та Китай. Цей зріст свідчить про те, що Інтернет речей стане одним із ключових ринків майбутнього, що сприятиме розширенню цифрової економіки. Прогнозується, що доходи від

галузі IoT зростуть з 892 мільярдів доларів у 2018 році до 4 трільйонів доларів до 2025 року.[16]

Зв'язок машин досягає широкого кола застосувань, включаючи розумні міста, розумне середовище, розумні мережі, розумну роздрібну торгівлю, розумне сільське господарство та розумне здоров'я. Архітектура Інтернету речей відображає минуле, сучасне та майбутнє розвитку (див. Рисунок 1.6).


Рисунок 1.6- Сучасна та майбутня архітектура IoT

Крім підключених пристроїв, з'являється концепція соціального IoT (SIoT), яка дозволяє користувачам соціальних мереж підключатися до пристроїв та обмінюватися ними через Інтернет.

Проте з усім цим ростом IoT виникають проблеми безпеки та конфіденційності. Без надійної екосистеми IoT додатки не зможуть задовольнити високий попит та ризикують втратити свій потенціал. Окрім того, існують унікальні проблеми безпеки, такі як проблеми конфіденційності, аутентифікації та управління, які становлять загрозу для цього середовища.

Кіберфізичні системи (CPS) також використовуються у IoT і мають важливе значення, оскільки вони відслідковують фізичні об'єкти та реагують на фізичні зміни. Уразливості безпеки у таких системах можуть мати серйозні наслідки, оскільки вони охоплюють критично важливі активи, наприклад, електричні мережі та транспортні системи.

Усі елементи IoT мають свої власні проблеми безпеки, включаючи рівні використання датчиків та механізмів виконання, мережу зв'язку, проміжний шар та наскрізні додатки. Ці проблеми потребують уваги, оскільки загрози кібербезпеці не зупиняються і можуть мати серйозні наслідки для користувачів та компаній.

## 1.5 Загрози у сфері кібербезпеки для технології Internet of Things (проблема приватності)

Технологія, яка стоїть за розвитком Інтернету речей, дозволяє підключати до мережи не лише комп'ютери, але й різні предмети реального світу. Швидкий темп її розвитку ускладнює створення повного списку можливих пристроїв. Це підкреслює важливість забезпечення безпеки використання цієї технології. Засоби масової інформації часто акцентують увагу на захисті особистої інформації, оскільки використання роутерів, маршрутизаторів та відеокамер є поширеним.

Технічні експерти вже ідентифікували ризики безпеки. У мережі існує ряд пристроїв, що співпрацюють на рівні "машина-машина" (M2M), де окремі пристрої можуть бути також контрольовані людьми. Така взаємодія може формувати різні системи, включаючи ті, що використовують штучний інтелект. Однак існує ризик вразливості даних цих пристроїв в мережі Інтернет.

Більшість пристроїв раніше взаємодіяли лише в локальних мережах, але з часом їх функціонал розширився. Це часто відбувалося без врахування потреби в безпеці даних. Наприклад, проблема "Диявольського плюща"[17] виникла через недоліки в архітектурі пристроїв для зберігання даних. Ці технічні помилки можуть мати серйозні наслідки через поширення мереж Інтернету речей.

Інші загрози включають втрату контролю над пристроями через технічні проблеми або зловмисні дії. Проблеми можуть вплинути на сфери, такі як транспорт, зв'язок та управління. Пристрої в мережі Інтернет стають ціллю для

хакерів, які можуть використовувати різні методи для втручання в їх роботу. Це може призвести до ускладнення управління пристроями або навіть до підміни даних.

Особливий ризик існує для медичних пристроїв, які використовують технологію Інтернету речей. Втручання в їх роботу може бути смертельним для пацієнтів. Також важливо враховувати ризики для безпілотних літальних апаратів, які можуть впливати на M2M пристрої і передавати невірні дані геолокації.

Такі проблеми добре відомі у військовій сфері, де безпілотники розробляються з урахуванням сучасних можливостей радіо-електронної боротьби. Однак комерційне використання безпілотників може призвести до конфліктів між технологією і суспільними потребами. Недавні дослідження показують ризики використання комерційних безпілотників, такі як небезпека для публіки та можливість втручання в операції критичної важливості.

Розповсюджені атаки на IoT :

Щоб захистити пристрої IoT від атак, спершу необхідно ознайомитися з поширеними видами атак, які кіберзлочинці можуть застосовувати для досягнення своїх цілей.

DDoS-атака: виникає, коли ботнет – мережа заражених комп'ютерів – постійно надсилає величезну кількість запитів до системи. Така надмірна активність може спричинити значні затримки у роботі системи або навіть призвести до її повної зупинки. Добре налаштована DDoS-атака може викликати системну помилку компонента безпеки, приховуючи реальні шкідливі дії. Крім того, заражені пристрої IoT також можуть стати частиною ботнета і допомагати зловмисникам проводити ще більш руйнівні атаки в межах локальної мережі, які зазвичай мають більше довіри з боку систем інформаційної безпеки.

Не всі пристрої IoT стають цілями хакерів — невеликі гаджети, такі як датчики, що працюють з невеликими обсягами даних, використовують зашифровані протоколи зв'язку, такі як Z-Wave та Zigbee, і часто потребують

об'єднання з'єднань, подібних до NFC, у системах "Розумний дім" або управління будівлями, не можуть бути використані в бездротових мережах. Метою зловмисників стають пристрої, які підключаються безпосередньо до Інтернету і мають виділені IP-адреси. Саме вони становлять реальну загрозу.

Експлойт програмного забезпечення: багато кіберзлочинців використовують відомі уразливості в програмному забезпеченні пристроїв для проведення атак. Розробники зазвичай виправляють ці "дірки" в оновленнях, але нові версії ПЗ часто не завантажуються на пристрої вчасно, залишаючи їх уразливими для експлойтів. Додатковою загрозою є те, що не всі виробники інформують користувачів про реальний технологічний стек ПЗ, мотивуючись ринковими стимулами, такими як використання конкурентоспроможних бібліотек, що можуть бути перевагою на ринку.

MITM-атака (атака посередника): хакери можуть перехоплювати мережевий трафік, вставши посеред каналу передачі між відправником і отримувачем, отримуючи таким чином облікові дані або конфіденційну інформацію, яку пристрої IoT передають через корпоративні мережі.

Оскільки багато смарт-пристроїв не використовують шифрування, зловмисники можуть легко використовувати отримані дані для несанкціонованого доступу до системи.Фізичне втручання: достатньо просто підключення кіберзлочинцем USB-флешки з шкідливим кодом до зовнішнього пристрою IoT, щоб розповсюдити шкідливе ПЗ через мережу та шпигувати за проходячими в ній комунікаціями.

Брутфорс-атаки: це тип кібератаки, при якій зловмисник намагається отримати доступ до захищених ресурсів шляхом систематичного випробування всіх можливих комбінацій паролів або ключів шифрування до тих пір, поки не знайде правильну. Недостатня увага до безпеки паролів для пристроїв IoT у компаніях робить їх вразливими до атак грубої сили, або "брутфорс". Часто паролі залишаються незмінними після встановлення їх користувачами і використовують стандартні значення, що дозволяє зловмисникам легко їх зламати.

Перехоплення прошивки: якщо оновлення мікропрограми пристрою не було криптографічно підписано або прошивка передається по не захищеному каналу зв'язку – це дозволяє зловмисникам перехопити її та завантажувати шкідливе ПЗ на пристрій під видом оновлень. Також за допомогою викраденої прошивки у кіберзлочинців з'являється (див. Таблиця 1.2).

Таблиця 1.2 – Атаки на IoT і їх потенційний вплив

| Атаки | Впливи (потенційні впливи) |
|---|---|
| Фізичні атаки | Несправність/Знищення пристрою |
| Атаки бічного каналу | Крадіжка даних |
| Криптоаналіз | Крадіжка даних |
| | Введення помилкових даних |
| | Маніпулювання даними/модифікація |
| Мережа та протокол | Крадіжка даних |
| | Введення помилкових даних |
| | Знищення даних |
| | Маніпулювання даними/модифікація |
| | Порушення/знищення служби |
| Програмні атаки | Крадіжка даних |
| | Введення помилкових даних |
| | Знищення даних |
| | Маніпулювання даними/модифікація |
| | Порушення/знищення служби |
| Соціальна інженерія | Крадіжка даних |
| | Порушення/знищення служби |
| | Несправність/Знищення пристрою |

Вразливість програм та відсутність криптографічного захисту роблять IoT пристрої цілью для хакерських атак(див Таблиця 1.3). Використання технології блокчейну може розв'язати деякі з цих проблем, зокрема проблеми з аутентифікацією та безпекою з'єднань.

Реєстрація кожного пристрою IoT у децентралізованому реєстрі, а також управління доступом за допомогою блокчейн-транзакцій, дозволяють всім учасникам мережі перевіряти легітимність підключень та запитів. Це ускладнює несанкціонований доступ та можливість перехоплення або зміни даних[18].

Таблиця 1.3 – Порівняльна характеристика загроз в IoT

| Технологія | Загрози | Рішення |
|---|---|---|
| RFID | Десинхронізація, витік інформації, DoS, MITM. | Використовувати захищені канали зв’язку. |
| NFC | Relay-атака, підміна приймача. | Автентифікація, блокчейн |
| WSNs | MITM | Автентифікація, блокчейн |
| IoT-пристрій | Брутфорс, зараження шкідливим програмним забезпеченням. | Міжмережеве екранування, стійка автентифікація, захист ПЗ |
| Інтернет | MITM, підміна IP-адрес та всі загрози притаманні для Інтернет. | Використання традиційних методів захисту, шифрування трафіку. |

# 2 ТЕХНОЛОГІЯ BLOCKCHAIN ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1 Загальна характеристика технології Blockchain

Блокчейн - інноваційна технологія, що викликала значний інтерес разом із зростанням популярності криптовалют. В основі криптовалюти лежать результати обчислень, представлені у вигляді електронних реєстрів, які орієнтуються на кількість коштів користувачів та їхні трансакції. Ці дані зберігаються на електронних гаманцях і передаються за допомогою криптографічних методів, базованих на технології блокчейн.

Блокчейн є децентралізованим журналом запису транзакцій, який є частиною ширшої обчислювальної інфраструктури, що також включає функції зберігання, комунікації, обслуговування файлів і архівування. Це послідовний ланцюжок блоків, побудований за певними правилами, що містять інформацію про транзакції. На рисунку 2.1 представлена структурна схема блоків у мережі блокчейн.

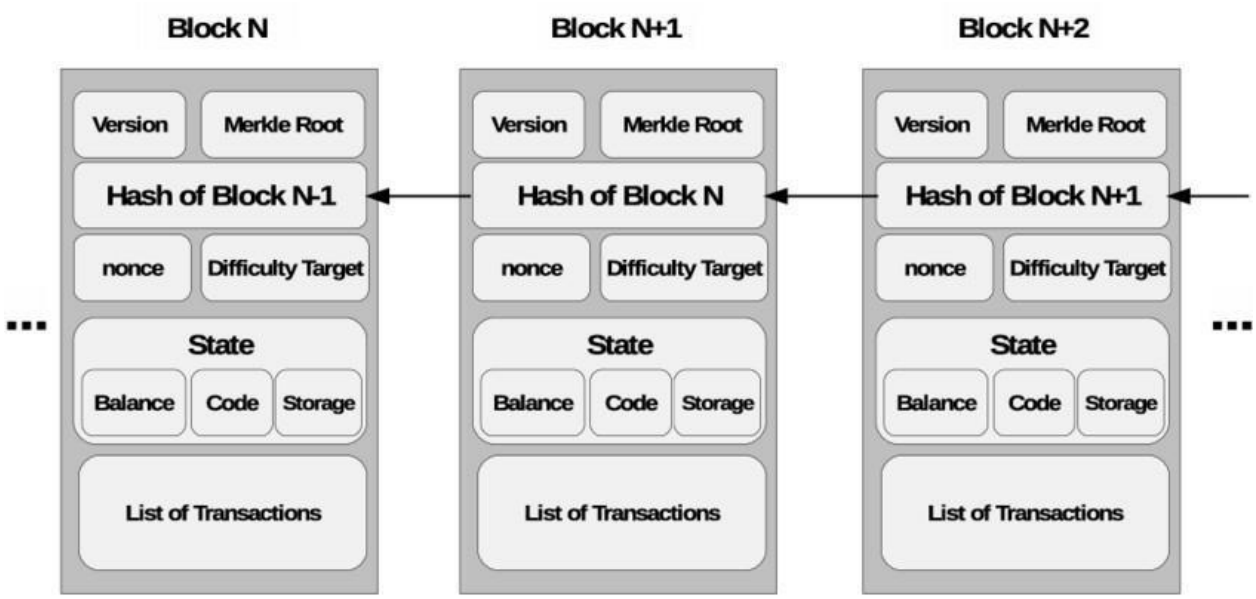


Рисунок 2.1 – Послідовність блоків у блокчейн мережі

Блокчейн представляє собою послідовний ланцюжок блоків, що містять інформацію, і зазвичай зберігається на безлічі комп'ютерів. Вона може мати різні конфігурації в залежності від застосування, від відкритих мереж до приватних систем з обмеженим доступом.

Блок — це структура даних, яка об'єднує транзакції для включення у ланцюг. Кожен блок складається з заголовка, який містить метадані, і довгого списку транзакцій. Ідентифікувати блок можна за допомогою хешу блоку або посилання на його висоту. Також в кожній блокчейн-мережі існує генезисний блок, який є унікальним і не посилається на попередній блок.

Кожен блок блокчейну ідентифікується своїм хешем (так званий хеш блоку або хеш заголовка блоку). Наступний блок орієнтований на попередній блок, який називається батьківським блоком, включаючи хеш батьківського блоку в спеціальному полі в його заголовку. Це означає , що кожен блок має у своєму заголовку хеш батьківського блоку , який об’єднується в його основний хеш. Коли батьківський блок змінюється, його хеш змінюється, внаслідок чого змінюється хеш блоку потоку. Це означає, що як тільки блок має багато наступних блоків у ланцюжку, якщо його змінити, це призведе до автоматичного перерахунку всіх наступних блоків і для кожного наступного блоку потрібно буде надати нове підтвердження роботи. Для цього знадобиться обчислювальна потужність, яка перевершить потужність окремих вузлів, навіть якщо вони працюють разом. Ця функція є ключем до безпеки блокчейну, що забезпечує цілісність і безпеку транзакцій.

Блок у блокчейн-мережі має дві основні частини: заголовок (head) і тіло (payload). У заголовку міститься інформація, що забезпечує стабільність і незмінність мережі. Тіло містить список усіх транзакцій, які потрібно зберегти в даному блоку та включити до блокчейну. На рисунку 2.2 зображено структуру блока в блокчейні.

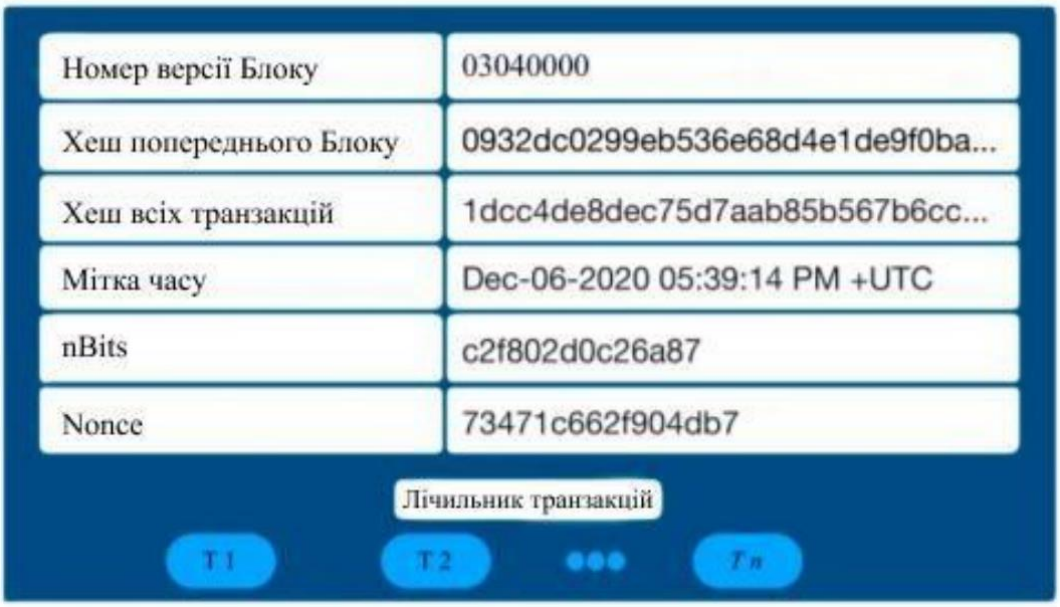


Рисунок 2.2 – Структура блоку

Потенціал блокчейну для забезпечення безпеки IoT полягає у його децентралізованості, незмінності, прозорості та можливостях розумних контрактів. Інтеграція блокчейну з системами машинного навчання, шифруванням та управлінням ідентифікацією зміцнює структуру безпеки IoT . Хоча інтерес промисловості та розвиток блокчейну відповідають сучасним дослідницьким пріоритетам, існують прогалини в розумінні його повного потенціалу та масштабованості . Аналіз поточного стану та майбутніх тенденцій блокчейну дозволяє приймати обґрунтовані рішення та сприяти прогресу, що робить його важливим елементом розвитку безпеки Інтернету речей [19]. Це дослідження розглядає взаємодію блокчейну та IDS для кібербезпеки IoT, оскільки можливості блокчейну підвищують рівень захисту IoT. [20]

Блокчейн, спочатку створений для підтримки криптовалют, перетворився на революційну технологію в різних секторах. Він виступає децентралізованою книгою, що забезпечує безпечний та прозорий запис транзакцій. Його розподілена архітектура та криптографічні принципи гарантують цілісність даних і стійкість до втручань [21].

## 2.2 Типи блокчейн мереж

Розглядаючи розвиток блокчейна з точки зору додатків в державному секторі, кількість таких розробок і продуктів, що використовуються в реальному процесі, все ще невелика, в той же час очікується, що більшість цих блокчейнів також будуть закритими (приватними).

Другим за важливістю показником є те, що будь-який користувач може вільно підключатися до мережі без отримання дозволу. Це вирішальна різниця між публічним блокчейном та приватним блокчейном. Більшість відомих на даний момент блокчейнов відкриті для публіки — щоб підключитися до них, досить завантажити клієнтський програмний додаток, сумісний з поточною версією протоколу, і встановити зв'язок з іншими одноранговими вузлами мережі.

Для повноцінної участі в роботі мережі, зокрема для перевірки і ретрансляції транзакцій інших користувачів, або для участі в створенні блоків, вам необхідно запустити клієнтське програмне додаток з повними можливостями вузла. В іншому випадку буде достатньо клієнтського програмного додатка з обмеженою функціональністю. Однак в публічному блокчейні рівень участі користувача завжди визначається незалежно і залежить тільки від його власних (фінансових або апаратних) ресурсів. Крім того, ніхто не може відключити користувачів від розподіленої мережі, оскільки всі учасники публічного блокчейна рівні. У деяких випадках ми можемо, наприклад, ігнорувати або блокувати користувачів, які надсилають неправильні транзакції або намагаються надіслати інформацію, яка не відповідає протоколу, але такі ініціативи мають суто саморегульований характер і не встановлюються на рівні протоколу.

У приватному блокчейні певний довірений вузол або група вузлів з вищим рівнем привілеїв порівняно з іншими користувачами, але новий користувач - це мережа, приватний блокчейн - це ієрархічна структура, що складається з 2 або більше рівнів. Пара ключів, що забезпечує доступ до системи, видається і управляється спеціальним вузлом управління і при

необхідності може бути відкликана. В результаті приватні блокчейни не в повній мірі реалізують основні принципи технології-децентралізацію і рівність учасників, оскільки існування корпоративних систем може бути пов'язано зі значними ризиками.

Наступним критерієм, який створює ще один ступінь в класифікації блокчейнів, є рівень управління блокчейном. Згідно з цим критерієм, блокчейн можна розділити на 4 групи:

- Публічний децентралізований блокчейн.
- Публічний блокчейн з делегованим управлінням.
- Приватний контрольований блокчейн.
- Урядовий блокчейн.

Більшість сучасних публічних блокчейнів мають однорівневу структуру. У них всі учасники рівні, а консенсус досягається за рахунок непрямого голосування вузлів, що виконують функцію створення блоків. Публічні децентралізовані мережі не накладають обмежень на участь в управлінні, а можливості учасників визначаються тільки відсотком ресурсів від загального числа.

За більш ніж 10-річну історію розвитку блокчейну можна зробити висновок, що повна децентралізація в саморегульованої, а точніше, стихійно регульованою мережі практично неможлива.

Кожен публічний блокчейн рано чи пізно стикається з однією з форм централізації. У зв'язку з цим були зроблені спроби впровадити елементи централізації для поліпшення функцій управління та інших показників блокчейна. Це призвело до появи першого публічного блокчейна зі структурою рівня 2 2015 року[22], в якій вузли з розширеними привілеями відігравали провідну роль. Це ознака того, що в блокчейн-мережі існує 2 або більше рівнів управління, кожен з яких має різний ступінь повноважень і є основною функцією публічного блокчейна з делегованим управлінням.

Блокчейн приватного контролю (Корпоративний) - це технічне рішення для потреб компаній. У такій системі кожен вузол має заздалегідь призначений рівень доступу, і, на відміну від публічного блокчейна, дані не завжди загальнодоступні навіть для читання. Управління таким блокчейном здійснюється за допомогою спеціальних вузлів з підвищеними привілеями, які відповідають за підтвердження політики поширення даних і ідентифікацію користувача, а також за введення даних в блокчейн.

Децентралізовані реєстри для державних установ, як правило, трохи відрізняються від корпоративних блокчейнів і також вимагають контрольованого доступу до інформації. Однак Державні установи висувають особливі вимоги до блокчейну - максимальний рівень незмінності вже доданої інформації і найсуворіший контроль за її додаванням. У той же час інформація, що вже міститься в блокчейні, часто може бути оприлюднена, оскільки державні установи повинні прагнути до підвищення прозорості своєї роботи. Таким чином, ми можемо сказати, що урядовий блокчейн - це окремий випадок корпоративного блокчейна зі своїми специфічними особливостями, але в той же час він відноситься до іншої групи.

Таким чином, класифікацію блокчейна, засновану на рівні доступу до інформації, можна представити у вигляді структури з двох рівнів, де 1-й рівень визначає критерії просування, а 2-й рівень визначає рівень управління блокчейном. Схематично ця структура відображена на рисунку 2.3[23]

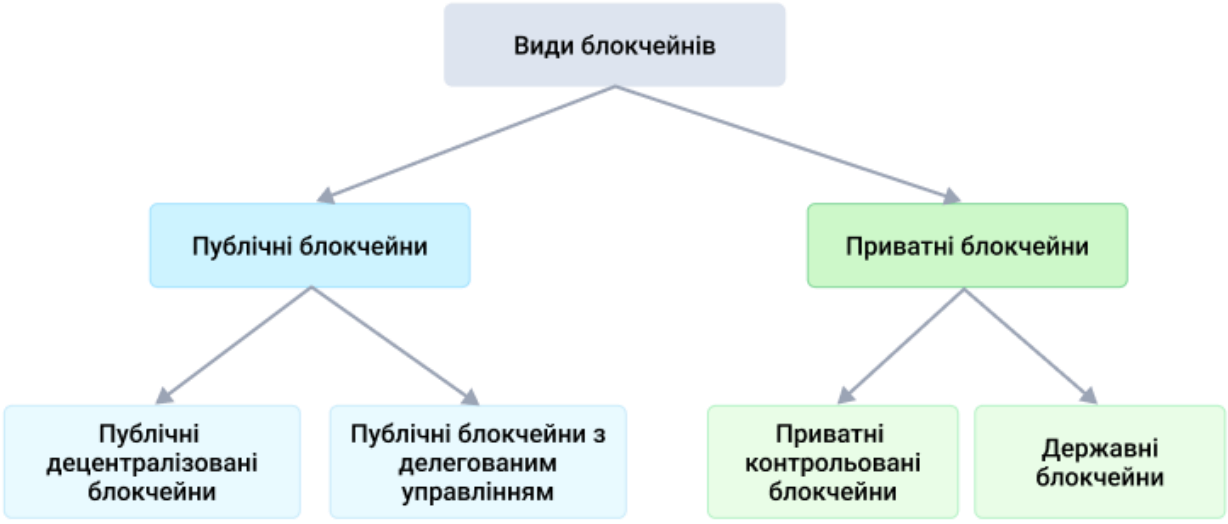


Рисунок 2.3 – Класифікація блокчейнів

Підсумовуючи розгляд технологічних аспектів блокчейну, варто відзначити, що це нова технологічна парадигма. Вона поєднує кілька різних концепцій: розподілені реєстри зберігання даних, алгоритми консенсусу та криптографічні механізми захисту даних. Блокчейн працює за принципом зберігання даних без залежності від централізованого сервера або групи серверів, створюючи та зберігаючи послідовний список записів, відомих як блоки. Кожен блок містить позначку часу та унікальний хеш попереднього блоку, що забезпечує зв’язок між блоками та унеможливлює зміну даних у вже створених блоках без зміни всієї послідовності блоків.

Таблиця 2.1 – Порівняльний аналіз видів блокчейну

| | Публічний | Приватний | Урядовий |
|---|---|---|---|
| Загальнодоступність (Permissionless) | Так | Ні | Ні |
| Записи читальні для | Усіх | Виняткова для запрошених | Залежно від потреб мережі |

Продовження таб. 2.1

| | | | |
|---|---|---|---|
| Хто може робити записи? | Хто завгодно | Затверджені учасники | Затверджені учасники |
| Хто володіє мережею? | Ніхто | Одне обличчя | Декілька осіб |
| Чи доступна інформація про користувачів? | Ні | Так | Так |
| Швидкість транзакції | Повільна | Швидка | Швидка |

2.3 Основні функції безпеки блокчейну

1) Незмінність і цілісність даних: незмінність блокчейну гарантує, що записані дані залишаються незмінними без консенсусу в мережі, що робить його ідеальним для захисту важливих даних IoT, таких як показання датчиків, деталі ланцюжка поставок і журнали пристроїв. Ця функція має вирішальне значення для підтримки цілісності даних, головного пріоритету в системах IoT, які вимагають точних і незмінених даних під час зберігання та передачі [24].

2) Децентралізація та прозорість: діючи як децентралізовані та розподілені реєстри, транзакції реєструються на численних вузлах, гарантуючи, що жодна особа не контролює мережу. Децентралізована архітектура в пристроях IoT зменшує залежність від центральних органів влади та сприяє прозорим і захищеним від втручання транзакцій. Він усуває одиничні точки відмови та підвищує стійкість системи проти кіберзагроз .

3) Розумні контракти: Ці самовиконувані угоди, закодовані в блокчейні, автоматично виконують дії на основі умов, зменшуючи залежність від посередників у транзакції Інтернету речей . Завдяки автоматизації попередньо

визначених завдань, таких як сповіщення про технічне обслуговування або перевірка даних, смарт-контракти підвищують ефективність і мінімізують потребу в посередниках і потенційні вразливості в транзакціях Інтернету речей [25].

4)Механізми консенсусу: механізми консенсусу — це набори правил і протоколів, які використовуються в мережах блокчейнів для досягнення згоди між учасниками мережі щодо дійсності транзакцій і стану розподіленої книги [26]. Це гарантує, що всі вузли в мережі досягнуть консенсусу або спільного рішення щодо поточного стану блокчейну. Кожен з механізмів консенсусу сприяє згоді та довірі в децентралізованих мережах, запроваджуючи правила додавання нових транзакцій до блокчейну та вирішення конфліктів між учасниками.

Ось деякі з цих механізмів:

- Підтвердження роботи (PoW): вимагає вирішення складних головоломок для перевірки транзакцій і створення блоку; ідеально підходить для високозахищених систем IoT, таких як промислові системи керування.
- Підтвердження ставки (PoS): вибирає валідаторів на основі поставлених монет; забезпечує енергоефективність, що підходить для пристроїв IoT з обмеженими ресурсами, таких як системи розумного дому. Делеговане підтвердження ставки (DPoS): використовує обрані вузли для підтвердження транзакцій, забезпечуючи високу швидкість і масштабованість для реальних додатків IoT, таких як розумні міста.
- Підтвердження повноважень (PoA): валідатори перевіряють особу; підходить для корпоративних розгортань IoT, таких як управління ланцюгом поставок, забезпечуючи підзвітність.
- Practical Byzantine fault tolerance (PBFT): фокусується на низькій затримці та високій пропускній здатності, що робить його придатним

для фінансових систем IoT або автономних транспортних засобів, які потребують швидкого консенсусу.

Ці механізми забезпечують цілісність даних, безпеку та довіру в IoT, пристосовуючись до конкретних потреб і обмежень додатків IoT.

5) Управління ідентифікацією та автентифікація: Рішення ідентифікації на основі блокчейну забезпечують безпечне та надійне управління ідентифікацією в IoT, гарантуючи, що лише авторизовані пристрої беруть участь у мережі.

6) Шифрування: транзакції та дані, що зберігаються в блокчейні, шифруються за допомогою сучасних криптографічних алгоритмів, що гарантує їх конфіденційність і безпеку, захищаючи конфіденційні дані IoT від уразливостей.

7) Конфіденційність і контроль доступу: приватні блокчейни забезпечують контрольований доступ до даних, що гарантує конфіденційність, що робить їх придатними для сценаріїв, де конфіденційна інформація потребує безпечного обміну. IoT використовує приватні блокчейни для безпечного обміну критично важливими даними, такими як записи про стан здоров’я пацієнтів або дані промислових процесів.

Функції блокчейну значно сприяють кібербезпеці IoT, забезпечуючи довіру, прозорість і надійність. Проте масштабованість залишається проблемою для широких впроваджень IoT через енергоємні консенсусні механізми. Крім того, необхідна сумісність між різними блокчейнами та протоколами IoT для безперебійної інтеграції пристроїв. Дослідники продовжують шукати інноваційні рішення для вирішення цих проблем і підвищення синергії між блокчейном та IoT. Рисунок 2.4 пояснює інтеграцію блокчейну з ШІ для виявлення вторгнень.

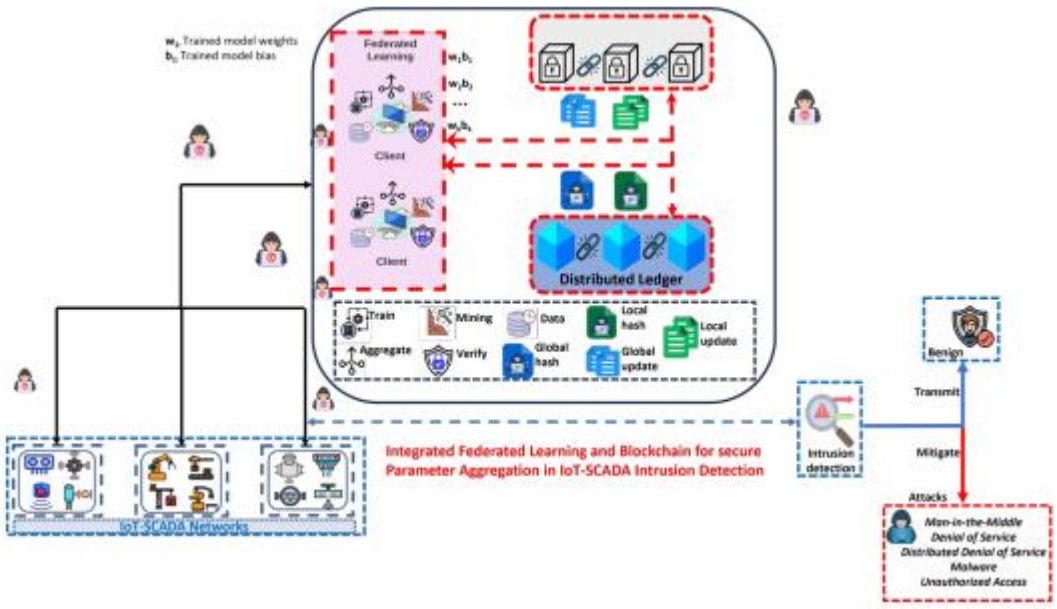


Рисунок 2.4 – Діаграма прикладу поєднання блокчейну та IDS, що наочно демонструє переваги виявлення вторгнень

Блокчейн-технологія нещодавно була застосована дослідниками в системах виявлення вторгнень (IDS) для покращеного моніторингу та виявлення, запобігання зловмисним діям або атакам, а також для захищеного зберігання і обробки транзакцій в пристроях та мережах Інтернету речей (IoT). Незмінність блокчейну сприяє підвищенню безпеки та ефективності зберігання даних у системах з обмеженими ресурсами. Однак, незважаючи на децентралізацію, масштабованість, прозорість та незмінність, цей метод має деякі недоліки у порівнянні з існуючими підходами IDS. Протягом останнього десятиліття зросла увага до IDS для захисту IoT/IIoT через необхідність суворого контролю, забезпечення роботи в реальному часі, цілісності даних та сумісності з обмеженими телекомунікаційними протоколами . Наявна література розглядає питання безпеки та моніторингу, але ця стаття пропонує комплексне дослідження інтеграції блокчейну та штучного інтелекту для підсилення підходів IDS в IoT/IIoT.

## 2.4 Застосування Blockchain в IoT

Впровадження блокчейну має великий потенціал для покращення функціональності та безпеки IoT, зокрема в розумних фабриках і містах, підвищуючи довіру, прозорість та ефективність. Ключові блокчейн-додатки в системах Інтернету речей включають забезпечення цілісності і безпеки даних за допомогою незмінних розподілених реєстрів, що зберігаються на кількох вузлах. Це є критично важливим для керування великими обсягами даних, створюваними інтелектуальними системами [27]. Управління ідентифікацією на основі блокчейну забезпечує безпечний доступ до пристроїв і послуг шляхом присвоєння унікальних криптографічних ідентифікаторів, що зберігаються в блокчейні, створюючи надійну основу для управління об'єктами екосистеми IoT. Розумні контракти автоматизують транзакції та процеси в розумних містах, підвищуючи ефективність і прозорість у таких сферах, як торгівля енергією та управління ланцюгом постачань [28]. Блокчейн-мережі IoT з децентралізованою інфраструктурою та взаємозв'язками зменшують кількість посередників і єдиних точок відмови, що підвищує безпеку, надійність та стійкість промислових додатків [29]. Крім того, блокчейн підтримує мікроплатежі та обмін цінностями між IoT-пристроями, спрощуючи транзакції в таких сценаріях, як автоматизовані процеси на розумних фабриках [30]. Попри потенціал для революції у промислових процесах, масштабованість, сумісність і управління залишаються важливими питаннями для широкомасштабного впровадження IoT. Прозорість даних та потреба в безпеці, доступності та надійності стимулюють використання блокчейну в IoT.

Зростання кількості кібератак створює серйозну проблему для захисту мереж Інтернету речей через їхню вразливість та обмежені ресурси. Інтеграція IoT зі штучним інтелектом стає все більш популярною для підвищення безпеки завдяки аналітичним можливостям ШІ для виявлення атак у мережевому трафіку. Однак централізовані підходи на основі ШІ стикаються з проблемами довіри та масштабованості, що робить їх несумісними з

децентралізованою природою IoT. Блокчейн, забезпечуючи безпечний потік даних між ненадійними вузлами та пропонуючи децентралізовані стратегії захисту, обіцяє підвищити безпеку IoT. Незважаючи на свій потенціал, блокчейн-рішення стикаються з такими проблемами, як обмежене розуміння мереж IoT та проблеми з масштабованістю [31]. Необхідні більш ефективні та інтелектуальні децентралізовані рішення для подолання цих перешкод, і поєднання аналітичної потужності ШІ з децентралізованою архітектурою блокчейну стає перспективним шляхом до цього.

## 2.5 Проблема безпеки Блокчейн/IoT

Проблеми безпеки, пов'язані з пристроями IoT, блокчейном і підключенням IoT-пристроїв до блокчейн-мереж, є значною кібербезпековою загрозою для систем IoT на основі блокчейну. Блокчейн функціонує як відкрита цифрова книга в одноранговій мережі, записуючи транзакції з мітками часу в незмінні блоки. Кожен блок пов'язаний з наступним і зашифрований, що забезпечує прозорість та цілісність без централізованого контролю. Існують загальнодоступні та приватні варіанти блокчейнів: загальнодоступні дозволяють універсальний доступ, тоді як приватні обмежують доступ лише для авторизованих осіб . Транзакції підписуються цифрово, групуються та зберігаються в розподіленій електронній базі даних, що забезпечує консенсус і перевірку, запобігаючи підробці. Цей децентралізований підхід гарантує узгодженість даних у всіх копіях книги. Рисунок 2.5 ілюструє блокчейн-підхід до передачі даних у мережах IoT.

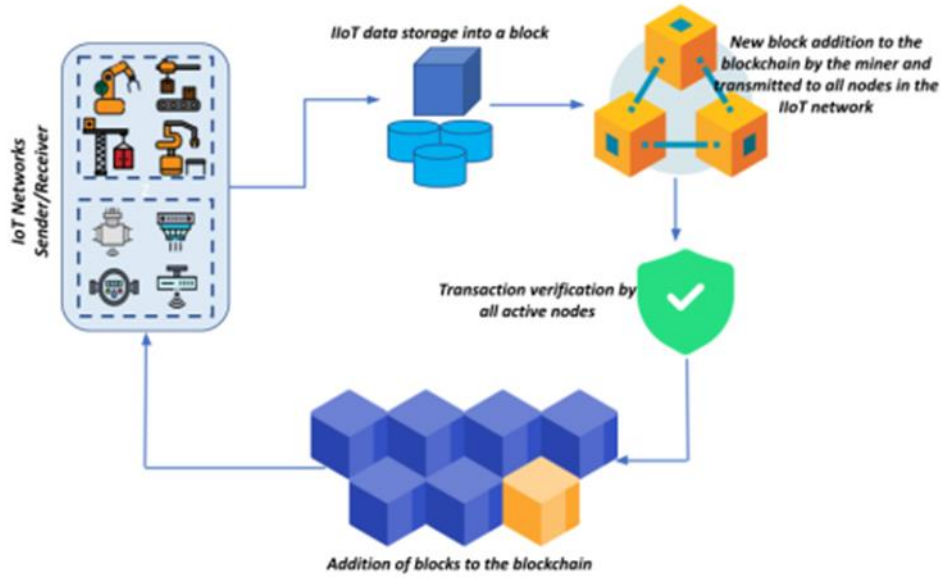


Рисунок 2.5 – Процес транзакцій блокчейну.

## 2.6 Випадки використання смарт-контрактів

У сучасну цифрову епоху, коли довіра та ефективність мають вирішальне значення, смарт-контракти на блокчейні пропонують нове рішення для оптимізації та автоматизації складних бізнес-процесів. Оскільки організації все частіше прагнуть використовувати можливості блокчейн-технології для створення децентралізованих додатків, розуміння практичних наслідків смарт-контрактів стає критичним для впровадження інновацій та отримання конкурентних переваг. Завдяки серії глибоких тематичних досліджень і реальних прикладів, смарт-контракти сприяють розвитку додатків на основі блокчейн-технологій, які відрізняються від традиційних додатків.

Важливо висвітлити трансформаційний потенціал смарт-контрактів, пропонуючи розуміння їх прийняття, впровадження та впливу на сучасні бізнес-практики. У блокчейн-мережі смарт-контракт - це електронний договір, який автоматично вступає в силу при виконанні певних умов. Коли умови цифрової угоди, підписаної та збереженої в блокчейні, виконуються, контракт негайно набуває чинності. Умови прописані мовами програмування, розробленими спеціально для блокчейну, такими як Solidity.

Смарт-контракти є потужною інфраструктурою для автоматизації, оскільки вони не контролюються центральним адміністратором і не вразливі до окремих точок атаки зловмисників. Використовуючи смарт-контракти в багатосторонніх цифрових угодах, можна зменшити ризик контрагента, підвищити ефективність, знизити витрати та забезпечити новий рівень прозорості процесів.

Смарт-контракти можна також розглядати як програми на блокчейні, які дозволяють кожній стороні виконати свою частину транзакції. Додатки на основі смарт-контрактів зазвичай називають "децентралізованими додатками" або "dapps". Одним зі способів реалізації протоколу Біткоїн є використання смарт-контрактів для представлення системи; специфіка цієї моделі, як з технічної, так і з юридичної точки зору, ще потребує доопрацювання. План передбачає перетворення окремих положень контрактів на цифрові коди, які можуть виконуватися самостійно в блокчейн-системі, натхненій біткойном [32].

Смарт-контракти вперше були запропоновані американським вченим-комп'ютерником Ніком Сабо в 1994 році. У своїй фундаментальній праці він визначив смарт-контракт як "комп'ютеризований протокол транзакцій, який виконує умови контракту", з метою "задовольнити загальні договірні умови, мінімізувати винятки, як зловмисні, так і випадкові, і зменшити потребу в довірених посередниках".

У 2012 році блокчейн Біткоїн еволюціонував і запропонував ще один важливий тип смарт-контрактів, відомий як транзакції з декількома підписами. Транзакція з мультипідписом вимагає, щоб певна кількість осіб (публічні ключі) підписали транзакцію своїми приватними ключами, перш ніж вона буде вважатися дійсною. Це підвищує безпеку коштів користувачів, зменшуючи ймовірність збоїв, таких як крадіжка або втрата приватного ключа. Рисунок 2.6 пояснює процес транзакції за допомогою блокчейна .

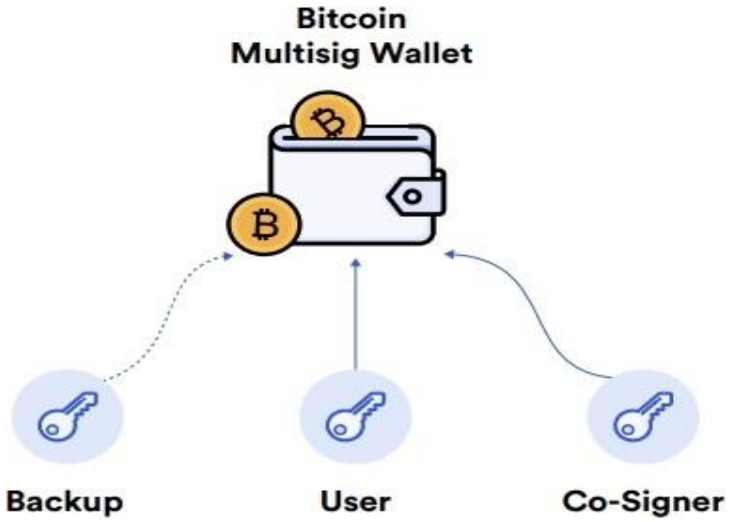


Рис 2.6 – Транзакція Multisig на блокчейні

2.7 Опис роботи смарт контракта

Як і будь-який інший контракт, смарт-контракт - це обов'язковий до виконання договір між двома сторонами. Він використовує код, щоб скористатися перевагами технології блокчейн, тим самим забезпечуючи більшу ефективність, відкритість і конфіденційність. Виконання смарт-контрактів контролюється відносно простими реченнями "якщо/коли...то...", записаними в коді на блокчейні.

Це кроки, необхідні для функціонування смарт-контрактів

1)Угода: Сторони, які бажають вести бізнес або обмінюватися продуктами чи послугами, повинні домовитися про умови угоди. Крім того, вони повинні визначити, як буде працювати смарт-контракт, включаючи критерії, які повинні бути виконані для того, щоб угода була виконана.

2)Створення контракту: Учасники транзакції можуть створювати смарт-контракти різними способами, в тому числі створювати їх самостійно або співпрацювати з постачальником смарт-контрактів. Положення контракту кодуються мовою програмування. На цьому етапі дуже важливо ретельно перевірити безпеку контракту.

3)Розгортання: Коли контракт завершено, його потрібно опублікувати в блокчейні. Смарт-контракт завантажується в блокчейн так само, як і звичайні

криптовалютні транзакції, з кодом, що вставляється в поле даних біржі. Після перевірки транзакції вона вважається активною в блокчейні і не може бути скасована або змінена.

4)Моніторинг умов: Смарт-контракт працює, відстежуючи блокчейн або інше надійне джерело за заздалегідь визначеними умовами або підказками. Такими тригерами може бути будь-що, що піддається цифровій перевірці, наприклад, досягнута дата, здійснений платіж тощо.

5)Виконання: Коли параметри тригера досягнуті, смарт-контракт активується відповідно до твердження "якщо/коли...то...". Це може реалізовувати лише одну або декілька дій, наприклад, передачу коштів продавцю або реєстрацію права власності покупця на актив.

6)Запис: Результати виконання контракту оперативно публікуються в блокчейні. Система блокчейн перевіряє виконані дії, реєструє їх завершення у вигляді обміну та зберігає укладений договір у блокчейні. Цей документ доступний у будь-який час.[33]

Підсумовуючи, можна сказати, що розвиток нових технологій є багатогранним, і кожна з них спрямована на задоволення конкретних потреб і вирішення конкретних проблем. Смарт-контракти на блокчейні розвиваються завдяки його унікальним характеристикам, таким як децентралізація та прозорість, що робить блокчейн ідеальним для додатків, де довіра та безпечне управління даними є важливими. Інтеграція блокчейну з іншими новітніми технологіями є постійною тенденцією, що стимулює інновації та відкриває нові можливості в різних галузях.

# 3 ПРОГРАМНА РЕАЛІЗАЦІЯ

## 3.1 Створення IOT системи

У рамках даної кваліфікаційної роботи буде створено додаток тобто IOT систему використовуючи мову програмування python, та її вбудовані бібліотеки.

Python — це інтерпретована об’єктно-орієнтована мова програмування високого рівня з динамічною семантикою. Його високорівневі вбудовані структури даних у поєднанні з динамічною типізацією та динамічним зв’язуванням роблять його дуже привабливим для швидкої розробки додатків, а також для використання як мови сценаріїв або з’єднувальної мови для з’єднання існуючих компонентів.[35]

Python – це мова програмування котра використовується в багатьох напрямках розробки, веб розробка, аналіз даних, нейро-мережі і тд. За допомогою цієї мови була зімітована IOT система в котрій було створено три пристрої, котрі будуть керуватися з комп’ютеру адміністратора.

Для початку було створено основні python файли котрі контролюють стани пристроїв, та повертають цю інформацію головній системі (рис. 3.1).

Клас Camery.py зберігає у собі, інформацію про пристрій Камера. Він має наступний функціонал (рис. 3.1):

Метод start_recording – цей метод повертає логічне значення True, коли адміністратор натискає на кнопку Почати запис.

Метод stop_recording – повертає значення False якщо адміністратор натиснув на кнопку Закінчити запис.

Метод download_records – повертає повідомлення у термінал, при цьому перевіряючи властивість recording.

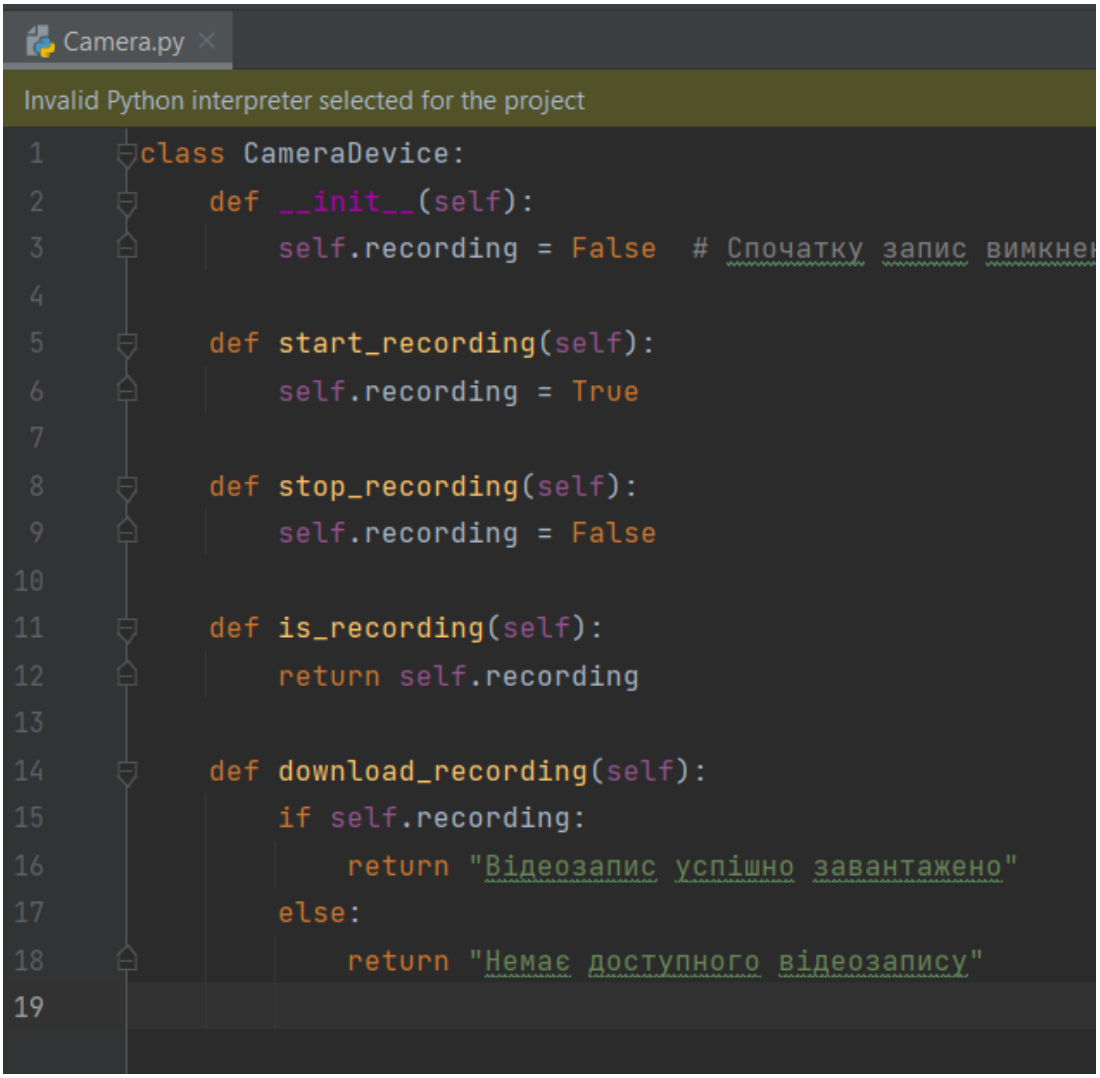


Рисунок 3.1 – Клас пристрою Камера

Далі було додано пристрій Світло, цей пристрій у даній IOT системі відповідав за світло котре можливо були увімкнути або вимкнути використовуючи адмін панель (рис. 3.2). Було створено клас для цього пристрою котрий мав наступні методи:

get_state – метод котрий повертав поточне значення світла для адміністратора.

turn_on – функція котра виставляло значення світла у True.

turn_off - функція котра виставляло значення світла у False.

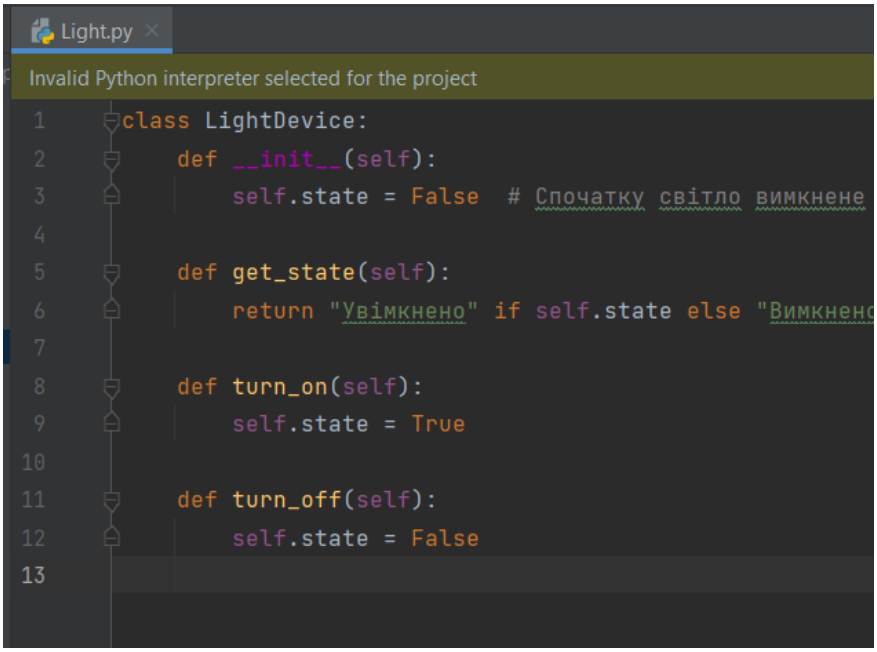


Рисунок 3.2 – Клас пристрою Світло

Останнім кроком для створення пристроїв для нашої IOT системи став крок створення пристрою Телевізор, котрий має схожі за логікої базові методи як для пристрою Світло (рис. 3.3). Використовуючи адмін панель, людина котра працює з даною системою може вмикати та вимикати пристрій Телевізор, та переглядати поточний стан пристрою. Тобто адміністратор може побачити ввімкнений телевізор чи ні.

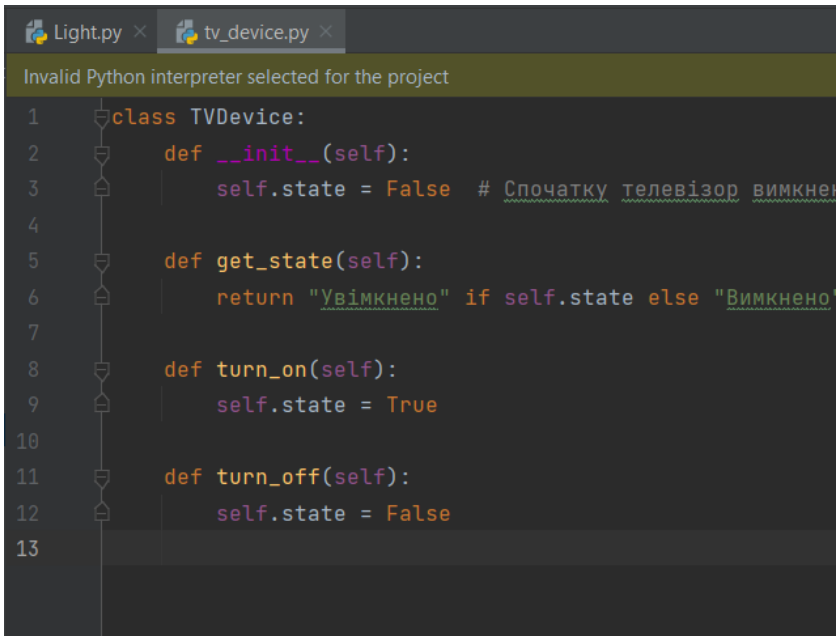


Рисунок 3.3 – Клас пристрою Телевізор

Після того як всі пристрої були створені, було розпочато роботу що до створення панелі адміністратора та розширення функціоналу деяких пристроїв. Створення панелі було зроблено за допомогою бібліотеки tkinter вона дозволяє створювати візуальні панелі використовуючи мову програмування python. До цієї панелі було додано назви пристроїв та дії коті можливо виконувати для кожного з пристроїв. Спочатку було створено глобальний об’єкт класу Tk, за допомогою котрого було зрегенеровано панель у котрій міститься вся інформація про девайси, ця панель імітування IOT системи (рис. 3.4).

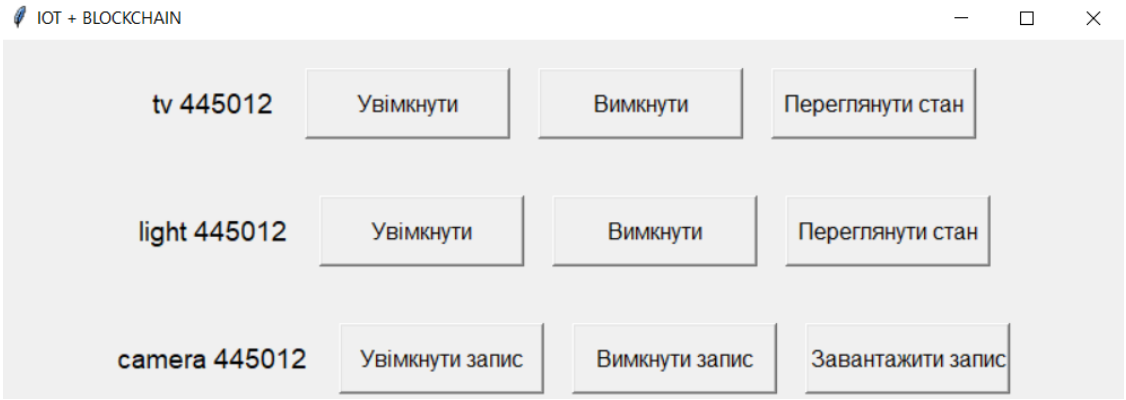


Рисунок 3.4 – Адміністративна панель IOT системи для керування пристроями

Коли панель була створена можливо було розпочато роботу над розширенням функціоналу для деяких пристроїв щоб зробити IOT систему більш продуманою. Для пристрою Світло було додано перевірку та автоматичне ввімкнення світла, дивлячись на поточний час. Тобто за допомогою цього було додано автоматизовану частину в нашу IOT систему. Данна перевірка перевіряє якщо поточний час на комп’ютері адміністратора більше шостої вечора та менше десятої, і якщо так то система автоматично показує користувачеві що світло вмикається, без всяких дій користувача. Для роботи системи у реальному часі було додано обробники дій котрі кожні 15 хвилин, викликають цю частину функціоналу для перевірки часу щоб вимкнути а ввімкнути світло (рис. 3.5).

```
def check_auto_light():
    current_hour = datetime.now().hour
    if 18 <= current_hour < 22 and light.get_state() == "Вимкнений":
        light.turn_on()
        verify_light_block("light 445012", "Увімкнути")
        print("Світло увімкнено автоматично")

    elif current_hour == 22:
        light.turn_off()
        verify_light_block("light 445012", "Вимкнути")
        print("Світло вимкнено автоматично")
```

Рисунок 3.5 – Приклад автоматичної роботи пристрою Світло у IOT системі

Також розширена функціональність була додана для пристрою Камера. Коли адміністратор тисне на кнопку Почати запис, система починає додавати випадкові дані у масив кожні три секунди. Коли адміністратор натискає на кнопку Вимкнути запис система автоматично виключає процес генерації та заповнення масиву (рис. 3.6).

```
def start_recording():
    global recording_data
    recording_data = []
    root.after(3000, generate_random_data)  # Запуск генерації даних кожні 3 секунди

def stop_recording():
    root.after_cancel(generate_random_data)  # Зупинка генерації даних

def generate_random_data():
    global recording_data
    random_number = random.randint(0, 100)
    recording_data.append(random_number)
    root.after(3000, generate_random_data)  # Повторна генерація даних через 3 секунди

def save_recording_data():
    filename = "recording_data.json"
    with open(filename, "w") as file:
        json.dump(recording_data, file)
    print(f"Дані запису збережено у файл: {filename}")
```

Рисунок 3.6 – Приклад автоматичної роботи пристрою Світло у IOT системі

Фінальним кроком цього пристрою є Завантаження створеного запису. Котрий записує створений масив у JSON. Та зберігає усі створені дані у масив.

Таким чином було зімітовано IOT систему котра має вигляд панелі адміністратора, котрий може керувати, отримувати дані з пристроїв. Також були додані автоматизаційні процеси до системи, котрі дозволяють змінювати стан пристроїв дивлячись на час, або на дії котрі обрав адміністратор.

## 3.2 Імітування блокчейну та смарт-контрактів

Наступним та важливим кроком котрий був впроваджений до IOT системи було налаштування та імітація блокчейну та його інтеграція. Ця частина відповідає за впровадження безпеки до системи IOT. За допомогою блокчейну буде створюватися сховище даних, а саме дій котрі виконувалися під час роботи із системою. Також було передбачено випадки коли систему будуть взламувати або атакувати. За допомогою блокчейн технології, адміністратор зможе побачити ланцюг дій, та проаналізувати чи були у системі шахраї. Великою перевагою блокчейну є те що дані записані у блоки неможливо змінити або видалити. Це гарантуватиме IOT безпеку, за допомогою використання смарт-контрактів.

Для створення блоків та відображення їх візуально було створено клас BlockChain, котрий імітував роботу реального блокчейну та співпрацював із створеною адміністративною панеллю (рис. 3.7). Створений клас має наступні методи:

Конструктор __init__ – ініціалізує новий екземпляр класу Blockchain. Створює перший блок (блок генезису) і додає його до другого блоку блоків.

Метод save_to_json – Зберігає блокчейн у файл blockchain.json. Зчитує існуючий ланцюг з файлу, якщо він існує, і додає нові щойно створені блоки до цього ланцюга. Якщо файл не знайдено, буде виконуватися процес створення нового ланцюга. Зберігає оновлений ланцюг блоків у файлі у форматі JSON.

Метод createGenesisBlock – Створює генезис-блок (перший блок у ланцюзі блоків). Повертає блок з фіксованими значеннями timestamp, data, previousHash та hash.

Метод getLatestBlock – Повертає останній блок у ланцюзі. Використовується для отримання попереднього хеша при додаванні нового створеного блоку.

Метод addBlock – Додає новий блок до ланцюга блоків. Встановлює previousHash нового блоку на хеш останнього блоку в ланцюзі. Обчислює новий хеш для блоку за допомогою методу calculateHash.

Метод calculateHash – Обчислює хеш для блоку. Об'єднує timestamp, data (якщо існує) та previousHash блоку у строку. Кодує цю строку у форматі SHA-256 для отримання хеша. Повертає отриманий хеш у вигляді шістнадцяткового рядка. Додає новий блок до ланцюга.

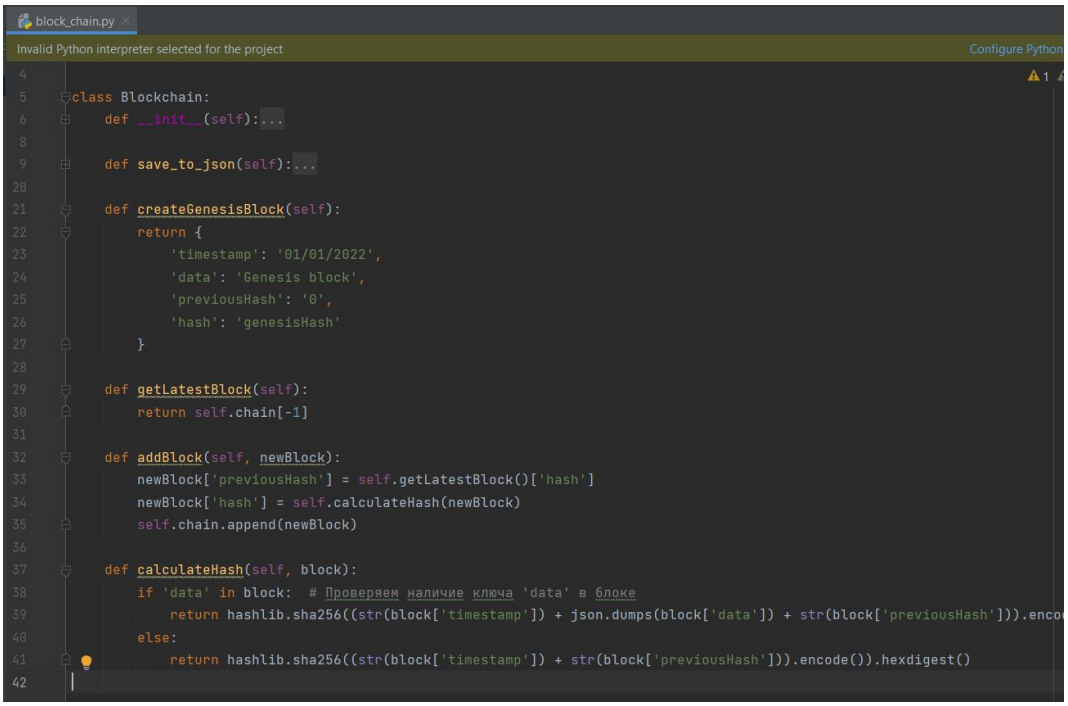


Рисунок 3.7– Клас блокчейну

Після того як основний клас блокчейну було створено була розпочата робота над інтегруванням дій адміністратора із смарт-контрактами, у даному випадку смарт-контракт буде виконувати роль частини продукту котра перевіряє те що усі вимоги можливих дій виконані, та після того як перевірка пройшла, буде виконуватися запис та створення нових блоків до блокчейну. До створеного пристрою Телевізор була розроблена перевірка на те що

виконання дій відбувається із компьютера адміністратора, якщо ні запис до блокчейну також виконується але з помилкою , котра вказує на те що, дії котрі були виконані під час використання системи були не з очікуваного просторою, та робиться запис ай-пі адреси системи з котрої була спроба взламуваня IOT системи (рис. 3.8).

Програмна частина системи, зчитує ім’я компьютера за допомогою бібліотеки socket. Та перевіряє що якщо, зчитане ім’я не співпадає з очікуваним, тоді відбувається запис блоку помилки. Якщо значення співпали йде запис дії котру зробив адміністратор, час коли це було зроблено, ім’я пристрою.

```
import socket
from datetime import datetime
from blockChain.block_chain import Blockchain

def verify_and_add_block(device, action):
    expected_computer_name = 'DESKTOP-U0PC9VM'
    expected_device = 'tv 445012'

    computer_name = socket.gethostname()
    ip_address = socket.gethostbyname(computer_name)

    blockchain = Blockchain()
    if computer_name == expected_computer_name and device == expected
        new_block = {
            'timestamp': datetime.now().strftime('%Y-%m-%d %H:%M:%S')
            'data': {'device': device, 'action': action},
            'previousHash': '',
            'hash': ''
        }
        blockchain.addBlock(new_block)
        blockchain.save_to_json()
        print("Блок успішно додано до блокчейну.")
    else:
        # Запис помилки в блок
        error_block = {
            'timestamp': datetime.now().strftime('%Y-%m-%d %H:%M:%S')
            'data': {'device': device, 'action': action},
            'error': "Дія відбувалася не з пристрою адміністратора",
            'ip_address': ip_address,
```

Рисунок 3.8 – Контракт до пристрою Телевізор

Наступним кроком стало створення контракту для пристрою Світло. За допомогою цього контракту була реалізована не тільки частина перевірки того

що дії над системою виконуються із компьютера адміністратора, а й те що автоматизовані дії програми працюють правильно. Окрім програмної частини системи котра перевіряє час, перевірки також були додані й до контракту, для того щоб перевіряти правильність роботи системи у декількох місцях. Якщо час не співпадає із правилами котрі задані у контрактні запис до блокчейну не виконується. Та автоматична дія системи також ігнорується. У даному контракті реалізовано три правила (рис. 3.9):

1) Перевірка адміністративного компьютера у випадку якщо системою захочуть скористуватися зловмисники.
2) Перевірка часу для ввімкнення світла
3) Перевірка часу для вимкнення світла.

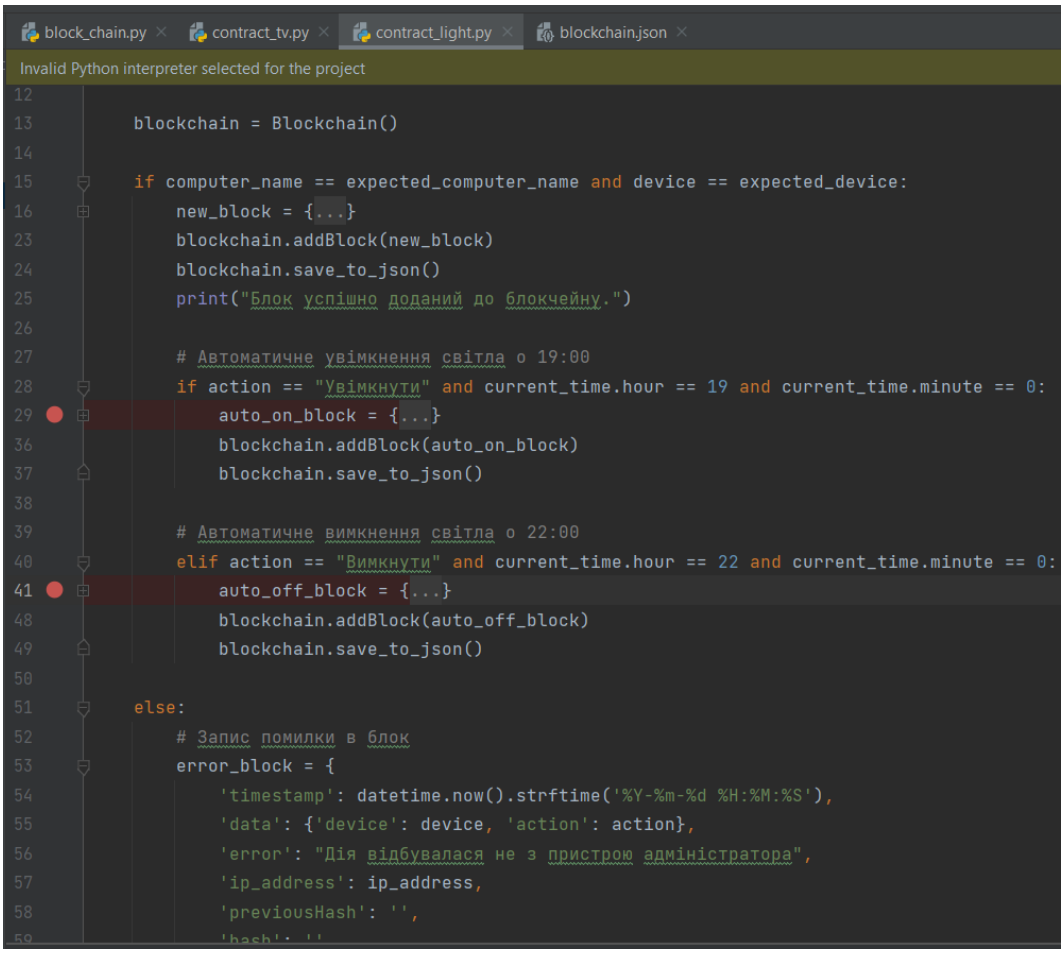


Рисунок 3.9 – Контракт до пристрою Світло

Останнім контрактом котрий був створений був контракт для пристрою Камера. Він має у собі тільки частину перевірки того що компьютер є

адміністративним, адже даний пристрій є відображенням роботи функціональності системи IOT, коли головний пристрій може брати інформацію із інших пристроїв котрими він керує (рис. 3.10).

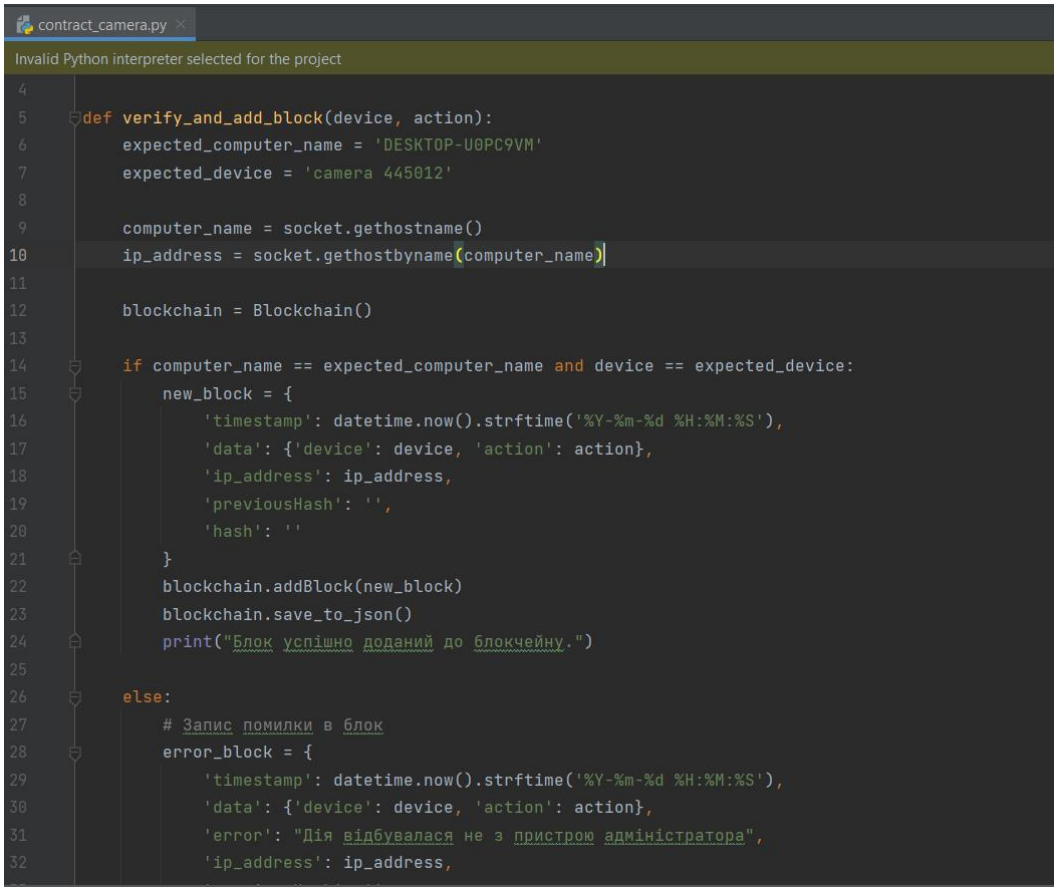


Рисунок 3.10 – Контракт до пристрою Камера

Отже, було зімітовано та створено віртуальний блокчейн, котрий імітує поведінку реальних ланцюгів. Були додані смарт-контракти котрі виконують функцію перевірки умов за котрих система робить записи до ланцюгів. Основною метою даної реалізації до системи IOT є збільшення безпеки системи, запис усіх дій у блокчейн запобігає несанкціонованим змінам даних. Децентралізована природа блокчейна створює захист від злому та збоїв центральних серверів. Блокчейн гарантує, що дані не можуть бути підроблені або змінені заднім числом, що є особливо важливим для критично важливих систем. Модульний підхід до розробки дозволяє легко додавати нові пристрої та функціональність. Блокчейн забезпечує єдиний стандарт зберігання даних всім пристроїв у системі.

3.3 Тестування системи

Починаючи тестування системи нам необхідно запустити адміністративну панель, це можливо зробити за допомогою команди python device_controller.py (рис. 3.11).

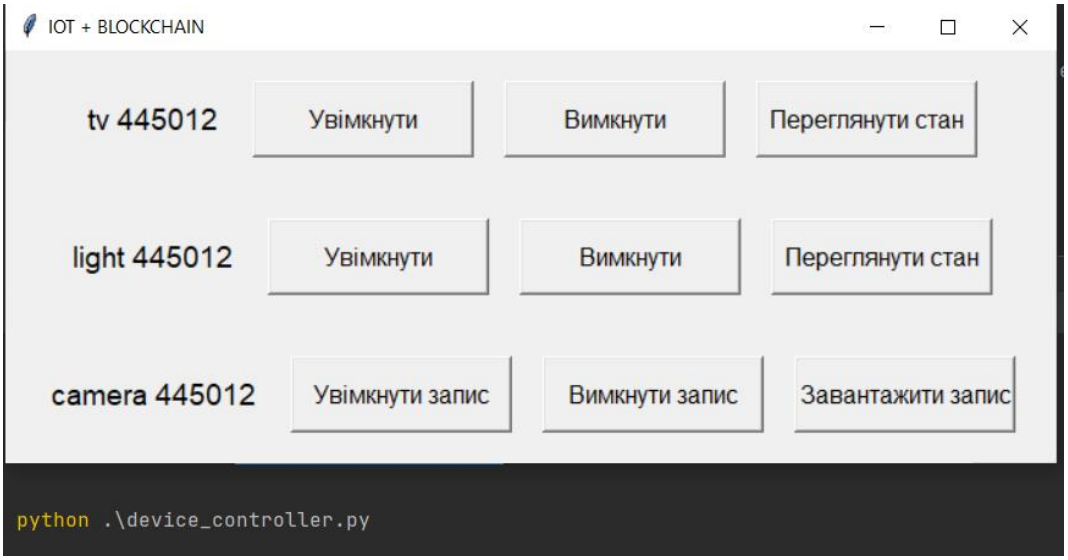


Рисунок 3.11 – Запуск адміністративної панелі

Після того як головний інтерфейс запущено було запущено були виконані основні дії для пристрою Телевізор. За результати цих дій було додано необхідну інформацію до ланцюгу блокчейн (рис. 3.12).

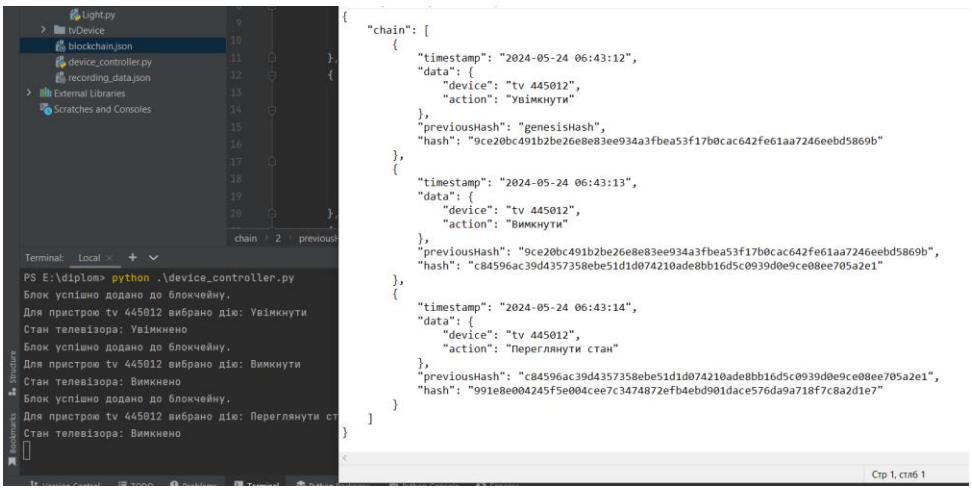


Рисунок 3.12 – Обробка всій дій пристрою Телевізор та запис у блокчейн

Далі було перевірено дії для пристрою Камера. Їх запис до блокчейну та завантаження файлу котрий автоматично генерується коли користувач

натискає на кнопку Завантажити запис. Запис було запущено на 15 секунд, тому очікуваний результат буде масив із 5 елементами (рис. 3.13).

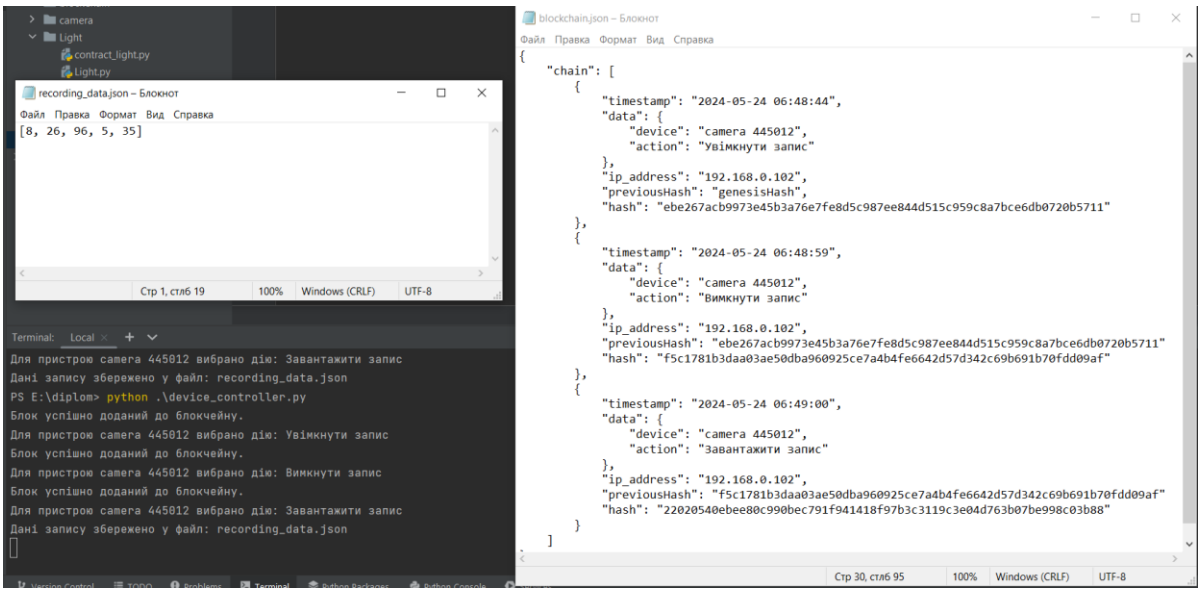


Рисунок 3.13 – Обробка всій дій пристрою Камера та запис у блокчейн

Наступним кроком перевірки є перевірка пристрою Світло. Було перевірено випадки коли адміністратор може вимкнути та ввімкнути світло (рис 3.14).

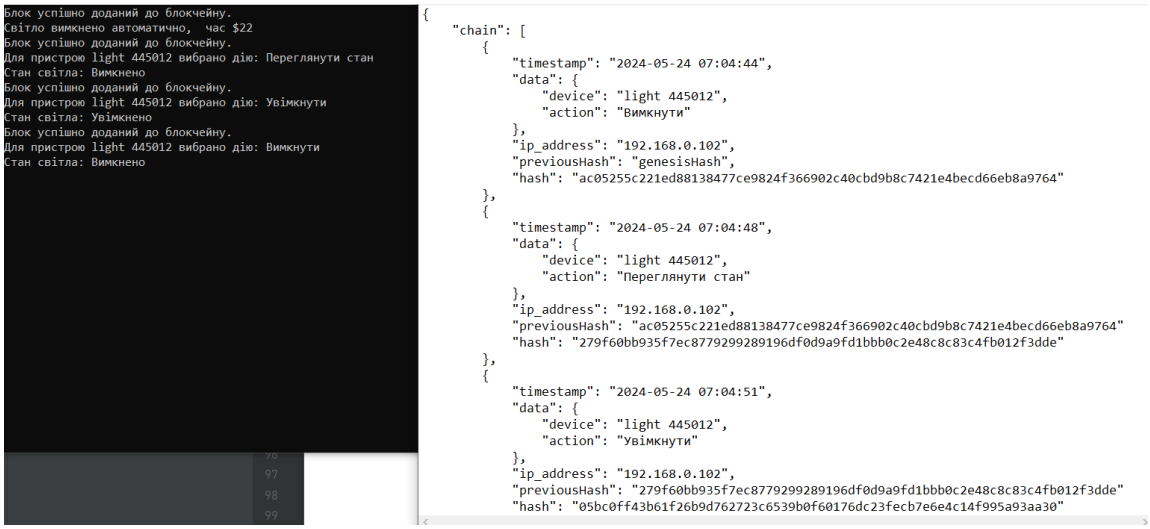


Рисунок 3.14 – Обробка всій дій пристрою Світло та запис у блокчейн

Також для тестування було змінено програмну частину додатку щоб перевірити випадки коли система автоматично включає або вимикає світло. Останнім етапом перевірки стало тестування, випадку коли систему

намагаються взламати, це робилося шляхом підміни очікуваного ім’я адміністративного компьютера (рис. 3.15).


Рисунок 3.15 – Перевірка спроби несанкціонованого користування IOT системи

Загалом можливо сказали що всі цілі даної роботи були реалізовані. Інтеграція IoT систем з блокчейном відкриває нові можливості для створення безпечних, прозорих та надійних систем керування пристроями. Створена програма демонструє, як такі технології можуть бути застосовані на практиці, забезпечуючи безпеку та достовірність даних у мережі IoT. Надалі можна розширювати функціональність, додаючи нові типи пристроїв та покращуючи алгоритми автоматизації та безпеки.

# ВИСНОВКИ

У сучасному світі, де інтернет грає ключову роль у всіх сферах життя, кібербезпека стає надзвичайно важливою, особливо в контексті розширення Інтернету речей (IoT). У даній дипломній роботі було ретельно досліджено можливості застосування технологій блокчейн для підвищення рівня кібербезпеки в мережах IoT.

Основні результати дослідження показали, що інтеграція технологій блокчейн може ефективно захищати споживачів та пристрої IoT від різних кіберзагроз, забезпечуючи надійну інфраструктуру для обміну даними та управління. Це вказує на необхідність активного впровадження таких рішень у майбутніх проектах розробки та реалізації IoT.

На основі отриманих результатів у дипломній роботі були сформовані рекомендації щодо оптимальних стратегій впровадження технологій блокчейн для забезпечення кібербезпеки в мережах IoT. Та було проведено імітацію реальних пристроїв з впровадженням блокчейну і смарт конрактів з метою посилення кібербезпеки . На основі наведених фактів можна зробити висновок, що цілі даної роботи були успішно досягнуті. Інтеграція IoT систем з блокчейном дозволила створити безпечні, прозорі та надійні системи керування пристроями. Розроблена програма показала ефективність застосування цих технологій на практиці, забезпечуючи безпеку та достовірність даних у мережі IoT.

Функціональність створеної системи можна розширювати шляхом додавання нових типів пристроїв та вдосконалення алгоритмів автоматизації та безпеки. В процесі тестування було змінено програмну частину додатку для перевірки сценаріїв, а також протестовано стійкість системи до атак шляхом підміни очікуваного ім'я адміністративного комп'ютера. Ці перевірки підтвердили надійність і безпеку системи. Важливим аспектом є розробка

стандартів та протоколів, які б сприяли інтеграції цих технологій у вже існуючі й майбутні мережі IoT.

Отже, результати цієї роботи підкреслюють важливість подальших досліджень у цьому напрямі та активного співробітництва між академічною та промисловою спільнотами для створення безпечніших та надійних інтернет-рішень.

У зв'язку з постійним розвитком та ускладненням методів кібератак, ця робота є важливим внеском у сферу кібербезпеки. Вона може бути корисною для фахівців, які працюють над забезпеченням безпеки інтернету речей , а також для тих, хто розробляє нові методи захисту від кібератак, сприяючи подальшій еволюції сучасних технологій з метою створення більш безпечного інтернет-середовища.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Що таке M2M (Machine-to-Machine) та IoT (Internet of Things) та як з їх допомогою можна автоматизувати бізнес-процеси? [Електронний ресурс]. – Режим доступу: https://business.diia.gov.ua/handbook/tehnologii-dla-avtomatizacii-biznesu/so-take-m2m-machine-to-machine-ta-iot-internet-of-things-ta-ak-z-ih-dopomogou-mozna-avtomatizuvati-biznes-procesi

2. Алайлан, Р.; Альхумам, Н.; Фріха, М. Кібербезпека для систем IoT на основі блокчейну – Режим доступу: Applied Sciences | Free Full-Text | Cybersecurity for Blockchain-Based IoT Systems: A Review (mdpi.com)

3. Ахаконьє, LAC; Нваканма, CI; Лі, Дж.М.; Кім, DS Агностична техніка CH-DT для високовимірної системи виявлення вторгнень мережі SCADA.IEEE Internet Things – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S2542660522001573?via%3Dihub

4. Ахаконьє, LAC; Нваканма, CI; Лі, Дж.М.; Кім, DS SCADA Схема виявлення вторгнень, що використовує поєднання модифікованого дерева рішень і вибору ознак хі-квадрат. – Режим доступу: http://dx.doi.org/10.3390/s18082575

5. Скаллі, П. Топ-10 IoT-додатків у 2020 році. IoT Analytics: Market Insights for the Internet of Things. 2020. – Режим доступу: https://iot-analytics.com/top-10-iot-applications-in-2020/

6. Ельгаззар, К.; Халіл, Х.; Альгамді, Т.; Бадр, А.; Абделькадер, Г.; Елева, А.; Буйя, Р. Перегляд Інтернету речей: нові тенденції, можливості та великі виклики. – Режим доступу: https://www.frontiersin.org/articles/10.3389/friot.2022.1073780/full

7. Бугетайя, А.; Шен, QZ; Бенаталла, Б.; Ніат, А.Г.; Містрі, С.; Ghose, A.; Непал, Ю.; Яо, Л. Дорожня карта служби Інтернету речей. – Режим доступу: https://dl.acm.org/doi/10.1145/3464960

8. Blockchain Integration for Trustworthy IIoT Communications Author: Joseph [Електронний ресурс] /ResearchGate. – Режим доступу: https://www.researchgate.net/publication/380181116_Blockchain_Integration_for_Trustworthy_IIoT_Communications

9. Лін, Дж.; Ю, В.; Чжан, Н.; Ян, Х.; Чжан, Х.; Чжао, В. Опитування про Інтернет речей: архітектура, передові технології, безпека та конфіденційність, а також програми. . – Режим доступу: https://ieeexplore.ieee.org/document/7879243

10. . Вегнер, П. Розмір глобального ринку Інтернету речей зросте на 19% у 2023 році — Інтернет речей демонструє стійкість, незважаючи на економічний спад. IoT Analytics. – Режим доступу: https://iot-analytics.com/iot-market-size/

11. 7. Manohar H. L. T. Data Consumption Pattern of MQTT Protocol for IoT Applications. In: Venkataramani G., Sankaranarayanan K., Mukherjee S., Arputharaj K., Sankara Narayanan S. (eds) Smart Secure Systems – IoT and Analytics Perspective. ICIIT 2017. Communications in Computer and Information Science, vol 808. Springer, – Singapur, 2018 – P. 97 – 99;

12. Конвергенція технологій LPWAN: багатофункціональність – це тренд! [Електронний ресурс] . – Режим доступу: https://www.dusuniot.com/uk/blog/the-convergence-of-lpwan-technologies-multi-connectivity-is-the-trend/

13. Про схвалення Концепції розвитку електронного урядування в Україні.– Режим доступу: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

14. Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року.– Режим доступу: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

15. Закон України від 02.10.92 N 2657-XII "Про інформацію" .– Режим доступу: https://tax.gov.ua/dlya-gromadskosti/dpa-i-gromadskist/normativno-pravova-baza-u-sferi/arhiv-normativno-pravova-baza/53366.html

16. Цікава статистика та факти про Інтернет речей (IoT): розмір ринку, використання та прогнози [Електронний ресурс] . – Режим доступу: https://cases.media/en/article/cikava-statistika-ta-fakti-pro-internet-rechei-iot-rozmir-rinku-vikoristannya-ta-prognozi

17. Hack Brief: 'Devil's Ivy' Vulnerability Could Afflict Millions of IoT Devices [Електронний ресурс] . – Режим доступу: https://www.wired.com/story/devils-ivy-iot-vulnerability/

18. Поширені атаки на IoT та захист від них. [Електронний ресурс] . – Режим доступу: https://corewin.ua/blog/attacks-on-iot-how-protect/

19. Альфанді, О.; Ханджі, С.; Ахмад, Л.; Хаттак, А. Опитування щодо підвищення безпеки та конфіденційності Інтернету речей через блокчейн: дослідження, вимоги та відкриті питання. – Режим доступу: https://link.springer.com/article/10.1007/s10586-020-03137-8

20. Хемашрі, П.; Кавіта, В.; Махалакшмі, С.; Правіна, К.; Таруніка, Р. Підходи до машинного навчання в безпеці Інтернету речей на основі технології блокчейн: дослідження поточних розробок і відкритих викликів. вТрансформації блокчейну: навігація в епоху децентралізованих протоколів; Springer: Cham, Швейцарія, 2024; С. 107–130.

21. . Принц, В.; Роуз, Т.; Урбах, Н. Технологія блокчейну та міжнародні простори даних. Проектування просторів даних; Springer: Cham, Швейцарія, 2022– Режим доступу: https://link.springer.com/chapter/10.1007/978-3-030-93975-5_10

22. Блокчейн, управління інноваціями та руйнівні технології. – Режим доступу: http://elar.kpnu.edu.ua/xmlui/bitstream/handle/123456789/6345/Nikolashyn-A.O.-Blokchein-upravlinnia-innovatsiiamy-ta-ruinivni-tekhnolohii.pdf?sequence=1&isAllowed=y

23. Класифікація блокчейнів [Електронний ресурс] . – Режим доступу: https://www.bitbon.space/ua/knowledge-base/distributed-ledger-technologies-blockchain/technological-aspects-of-blockchain/classification-of-blockchains

24.Лі, В.; Він, М.; Хайцюань, С. Огляд технології блокчейн: застосування, виклики та майбутні тенденції. У матеріалах 11-ї міжнародної конференції IEEE 2021 з електронної інформації та зв'язку в надзвичайних ситуаціях (ICEIEC) – Режим доступу: https://ieeexplore.ieee.org/document/9463842

25. Хрістідіс, К.; Девецікіотіс, М. Блокчейни та розумні контракти для Інтернету речей. – Режим доступу: https://ieeexplore.ieee.org/document/7467408

26. Діксіт, П.; Бансал, А.; Rathore, PS; Payal, M. Огляд технології блокчейн: архітектура, алгоритм консенсусу та його виклики. в Технологія блокчейн та Інтернет речей; – Режим доступу: . https://ieeexplore.ieee.org/document/8977439

28. Ферраг, М.А.; Шу, Л. Оцінка ефективності систем безпеки та конфіденційності на основі блокчейну для Інтернету речей: підручник.IEEE Internet Things J.2021 рік,8, 17236–17260 – Режим доступу:

https://ieeexplore.ieee.org/document/9424688

29. Аббасі, Ю.; Benlahmer, H. IoT та Blockchain Combined: For Decentralized Security.Procedia Comput. Sci.2021 рік,191, 337–342 ) – Режим доступу:

https://www.sciencedirect.com/science/article/pii/S1877050921014423?via%3Dihub

30. Icca, B.; Мустафа, Н.; Тернбулл, Б.; Сохрабі, Н.; Тарі, З. Федеративне навчання на основі блокчейну для захисту Інтернету речей: Всебічне опитування.ACM Comput. Surv.2023 рік,55, 1–43. ) – Режим доступу: https://dl.acm.org/doi/10.1145/3560816

31. Альхарбі, С.; Аттіа, А.; Альгазаві, Д. Інтеграція блокчейну зі штучним інтелектом для захисту мереж IoT: майбутні тенденції. – Режим доступу: https://www.mdpi.com/2071-1050/14/23/16002

32. Smart Contracts: A Preliminary Evaluation – Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2729548

33. Що таке смарт-контракти? [Електронний ресурс] . – Режим доступу: https://klona.ua/uk/blog/blockchain-smart-contract/shho-take-smart-kontrakty

34. Про сутність смарт-контрактів: їх переваги й ризики, застосування у різних сферах [Електронний ресурс] . – Режим доступу: https://pozovna.in.ua/pro-sutnist-smart-kontraktiv-iih-perevagi-j-riziki-zastosuvannya-u-riznix-sferax/

35. Що таке Python? [Електронний ресурс] . – Режим доступу: https://www.python.org/doc/essays/blurb/