НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування

і спеціалізованих комп'ютерних систем

«На правах рукопису»
УДК 004.77

До захисту допущено:

Завідувач кафедри

_____Віталій РОМАНКЕВИЧ

«___»_____2021 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системне програмування та спеціалізовані комп'ютерні системи»

зі спеціальності 123 «Комп'ютерна інженерія»

на тему: «Способи забезпечення захисту інформації від несанкціонованого доступу на основі сучасних технологій Blockchain»

Виконала:
студентка ІІ курсу, групи КВ-01мп
Сміюн Інна Володимирівна _____

Науковий керівник:
доцент кафедри СПСКС к.т.н., доцент
Орлова Марія Миколаївна _____

Консультант з нормоконтролю:
доцент, с.н.с., к.т.н.,
Боярінова Юлія Євгенівна _____

Рецензент:
професор кафедри ОТ, доктор технічних наук, професор
Кулаков Юрій Олексійович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2021 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра системного програмування

та спеціалізованих комп‘ютерних систем

Рівень вищої освіти – другий (магістерський)

Спеціальність – 123 «Комп‘ютерна інженерія»

Освітньо-професійна програма «Системне програмування та спеціалізовані комп‘ютерні системи»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____Віталій РОМАНКЕВИЧ

«___»_____20___р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Сміюн Інна Володимирівна

1. Тема дисертації «Способи забезпечення захисту інформації від несанкціонованого доступу на основі сучасних технологій Blockchain», науковий керівник дисертації Орлова Марія Миколаївна, доцент кафедри СПСКС к.т.н., доцент, затверджені наказом по університету від «05» листопада 2021 р. № 3682 - С

2. Термін подання студентом дисертації. 10 грудня 2021р.

3. Об’єкт дослідження: методи та способи забезпечення інформаційної безпеки на основі технології блокчейн.

4. Вихідні дані. Розроблений смарт-контракт на основі гібридного блокчейну.

5. Перелік завдань, які потрібно розробити: аналіз технології блокчейн, дослідження переваг та недоліків, огляд видів блокчейн технології та їх оцінка для забезпечення інформаційної безпеки, розробка смарт-контракту для забезпечення інформаційної безпеки.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація.

7. Орієнтовний перелік публікацій. За тематикою проведених досліджень опубліковано 2 наукові праці, тези доповідей на конференціях.

8. Дата видачі завдання. 1 жовтня 2020р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Постановка мети та цілі роботи	01.11.2020	
2	Вивчення теоретичного матеріалу	01.03.2021	
3	Аналіз існуючих методів	01.05.2021	
4	Проєктування алгоритму	01.07.2021	
5	Реалізація нового алгоритму	01.09.2021	
6	Тестування програмного продукту	01.10.2021	
7	Написання дисертації	20.10.2021	
8	Попередній розгляд магістерської дисертації на кафедрі	30.11.2021	

Студент Інна СМІЮН

Науковий керівник Марія ОРЛОВА

РЕФЕРАТ

Актуальність теми. З розвитком засобів інформаційних комунікацій, та можливостей заподіяння шкоди інформації, яка зберігається і передається за їх допомогою, виникла інформаційна безпека. Забезпечення інформаційної безпеки допомагає захистити інформацію та інформаційну інфраструктуру від негативних впливів. Такі впливи можуть мати випадковий або навмисний, внутрішній або зовнішній характер, результатом їх утручань може стати втрата важливої інформації, її несанкціонована зміна чи використання третіми особами. Забезпечити повноцінну та надійну інформаційну безпеку можна лише за умови застосування комплексного та системного підходу. Система інформаційної безпеки має бути побудована з урахуванням усіх актуальних загроз та вразливостей, а також з урахуванням тих загроз, які можуть виникнути в майбутньому, тому важливо забезпечити підтримку безперервного та надійного контролю.

Технологія Blockchain розпочинала свій розвиток як основа криптовалюти Bitcoin, але згодом стала перспективною технологію для забезпечення інформаційної безпеки. Блокчейн пропонує широкі можливості для підтримки високого рівня безпеки даних завдяки надійним механізмам шифрування, цілісності даних, стійкості мережі та масштабованості. У результаті перехід з традиційної системи інформаційної безпеки на систему на основі блокчейну може бути вигідним організаціям практично в будь-якій галузі.

Враховуючи усі переваги технології Blockchain та існуючі загрози сучасних інформаційних систем, розробка нових методів забезпечення інформаційної безпеки на основі блокчейну є актуальною і важливою задачею, як з наукової, так і з практичної точки зору.

Об’єктом дослідження є методи та способи забезпечення інформаційної безпеки на основі технології блокчейн.

Предметом дослідження є способи захисту інформації від несанкціонованого доступу, а також уже реалізовані системи забезпечення інформаційної безпеки на основі технології блокчейн.

Мета роботи: підвищення інформаційної безпеки, за рахунок розробки модифікованого смарт-контракту на основі гібридної блокчейн-мережі.

Наукова новизна одержаних результатів роботи полягає у наступному.

- Запропоновано спосіб забезпечення безпечної передачі даних на основі гібридної блокчейн-мережі, який являється покращеним методом уже існуючих та дозволяє забезпечити швидшу та надійнішу передачу даних.
- Розроблено смарт-контракт на базі гібридної мережі Blockchain, який, на відміну від існуючих смарт-контрактів реалізованих на основі публічної мережі Blockchain дозволяє уникнути недоліків при передачі інформації та забезпечити надійний захист інформації.

Практична цінність отриманих в роботі результатів полягає в тому, що запропонований спосіб дає змогу забезпечити надійну передачу інформації, на основі технології блокчейн. Він може бути розширений та використовуватися в різноманітних сферах для забезпечення інформаційної безпеки.

Апробація роботи. Основні положення і результати роботи були представлені та обговорювались на:

- XIV-тій науковій конференції магістрантів та аспірантів «Прикладна математика та комп’ютинг» ПМК-2021 (Київ, 17-19 листопада 2021 р.).

- XIII-тій Міжнародній науково-практичній конференції «Інтегровані інтелектуальні робототехнічні комплекси» ІПРТК-2020 (Київ, 2020 р.)

Публікації. За тематикою проведених досліджень опубліковано 2 наукові праці, а саме тези доповідей на 2-х конференціях.

Структура та обсяг роботи. Магістерська дисертація складається з вступу, трьох розділів та висновків.

У вступі подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень.

У першому розділі розглянуто основні поняття захисту інформації, проблеми інформаційної безпеки та існуючі методи забезпечення, а також проведено аналіз, який дає змогу визначити основні переваги та недоліки цих методів.

У другому розділі наведено теоретичні відомості щодо технології блокчейн, досліджено його архітектуру, види, проаналізовано основні переваги та недоліки.

У третьому розділі розробляється метод захисту інформації на основі гібридного ланцюга блокчейну, проведено тестування та порівняльний аналіз отриманих даних з результатами існуючих методів.

У висновках представлені результати проведеної роботи.

Ключові слова: захист інформації, інформаційна безпека, несанкціонований доступ, кібербезпека, технологія Blockchain, інформаційна безпека, смарт-контракти, децентралізована база даних.

ABSTRACT

Actuality of theme. With the development of information communications, and the ability to harm the information stored and transmitted through them, there was information security. Ensuring information security helps protect information and information infrastructure from negative impacts. Such influences may be accidental or intentional, internal or external, and may result in the loss of important information, unauthorized alteration, or use by third parties. Full and reliable information security can be ensured only with the use of an integrated and systematic approach. The information security system must be built taking into account all current threats and vulnerabilities, as well as taking into account those threats that may arise in the future, so it is important to ensure the maintenance of continuous and reliable monitoring.

Blockchain technology began as the basis of the cryptocurrency Bitcoin, but later became a promising technology for information security. Blockchain offers ample opportunities to maintain a high level of data security through robust encryption mechanisms, data integrity, network resilience and scalability. As a result, the transition from a traditional information security system to a blockchain-based system can be beneficial to organizations in virtually any industry.

Given all the advantages of Blockchain technology and the existing threats of modern information systems, the development of new methods of information security based on blockchain is an urgent and important task, both from a scientific and practical point of view.

The object of research are methods and ways to ensure information security based on blockchain technology.

The subject of the study are ways to protect information from unauthorized access, as well as already implemented information security systems based on blockchain technology.

Purpose: to increase information security by developing a modified smart contract based on a hybrid blockchain network.

The scientific novelty of the obtained results is as follows.

- A method for ensuring secure data transmission based on a hybrid blockchain network has been proposed, which is an improved method of existing ones and allows for faster and more reliable data transmission.
- A smart contract based on the Blockchain hybrid network has been developed, which, unlike existing smart contracts implemented on the basis of the public Blockchain network, avoids shortcomings in the transfer of information and provides reliable protection of information.

The practical value of the results obtained in this work is that the proposed method allows to ensure reliable transmission of information based on blockchain technology. It can be expanded and used in various fields to ensure information security.

Approbation of work. The main provisions and results of the work were presented and discussed at:

- XIV Scientific Conference of Undergraduates and Postgraduates "Applied Mathematics and Computing" PMK-2021 (Kyiv, November 17-19, 2021).
- XIII International Scientific and Practical Conference "Integrated Intelligent Robotic Complexes" IIRTC-2020 (Kyiv, 2020)

Publications. Two scientific papers were published on the topic of the research, namely abstracts of reports at 2 conferences.

Structure and scope of work. The master's dissertation consists of an introduction, three chapters and conclusions.

The introduction presents a general description of the work, assesses the current state of the problem, substantiates the relevance of research.

The first section discusses the basic concepts of information security, information security issues and existing security methods, as well as an analysis that identifies the main advantages and disadvantages of these methods.

The second section provides theoretical information on blockchain technology, explores its architecture, types, analyzes the main advantages and disadvantages.

The third section develops a method of information protection based on a hybrid blockchain chain, testing and comparative analysis of the obtained data with the results of existing methods.

The conclusions present the results of the work.

Keywords: information protection, information security, unauthorized access, cybersecurity, Blockchain technology, information security, smart contracts, decentralized database.

Зміст

Перелік скорочень, умовних позначень, термінів

Blockchain	– вибудувана за певними правилами безперервна послідовна ланцюжків блоків, децентралізована база даних, яка містить інформацію про всі транзакції, проведені учасниками системи.
DDoS	– Distributed denial-of-service attack. Хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів (серверів), що надаються, або цей доступ буде ускладнений.
DNS	– Domain Name System
EVM	– Ethereum virtual machine
POS	– Proof of Stake
POW	– Proof of Work
SHA	– Secure Hashing Algorithm
ІБ	– інформаційна безпека
Смарт-контракт	– комп'ютерний алгоритм, що зберігається мережі Blockchain, призначений для формування, контролю та надання інформації про володіння чимось.
КС	– комп’ютерна система.
ПЗ	– програмне забезпечення.

ВСТУП

Сучасне життя неможливо уявити без Інтернету та інформаційних технологій. Вони міцно увійшли в наше життя, значно спростивши його. Сьогодні Інтернет - це одна з найвпливовіших речей в світі, це колекція різних послуг та ресурсів, з якими людина зіштовхується постійно.

З розвитком інформаційних технологій нам стають доступні нові інструменти, які роблять звичні нам процеси швидшими та зручнішими. Проте, сучасне життя стало наскільки залежним від комп'ютерних технологій, що виведення з ладу комп'ютерної мережі або програмного забезпечення може призвести до негативних наслідків.

Захист даних в комп'ютерних мережах чи не найголовніша проблема в сфері інформаційних технологій. Проблема захисту від нових видів небезпек і загроз, породжених інформатизацією, турбує дослідників сучасного суспільства. Над цим питанням пильно працюють тисячі фахівців і саме це призвело до необхідності виділити заходи щодо захисту інформації в комп'ютерних системах в окремий напрям, що отримав назву інформаційна безпека.

Інформаційна безпека (ІБ) - це збереження і захист інформації, а також її найважливіших елементів, в тому числі пристроїв, систем та обладнання, призначених для використання, заощадження та передачі інформації. Іншими словами, це набір технологій, стандартів і методів управління, які необхідні для захисту інформаційної безпеки [1].

Лише системний та комплексний підхід до захисту може забезпечити інформаційну безпеку. У системі інформаційної безпеки потрібно враховувати всі актуальні та ймовірні загрози та вразливості. Для цього необхідний безперервний контроль в реальному часі. Контроль повинен проводитися постійно та охоплювати весь життєвий цикл інформації - від моменту, коли вона надходить в організацію, і до її знищення або втрати

актуальності [2]. Всі вище наведені вимоги може вирішити технологія блокчейн.

Блокчейн - це новітня технологія, інтерес до якої зріс разом з популярністю криптовалют. Криптовалюта - це результат комп'ютерних обчислень, це електронні реєстри, що зберігають інформацію про те, скільки у користувача коштів і куди він їх переводить. Зберігається криптовалюта на спеціальних електронних гаманцях. Її створюють і передають за допомогою криптографічних методів, а саме на базі технології блокчейн.

Ідея створення блокчейну виникла 2008-го року та належить людині, відомій як Сатоші Накамото. Задум було втілено 2009-го року, а саме, було розроблено основну складову криптовалюти Bitcoin, де Blockchain являється відкритим реєстром обліку для всіх транзакцій в мережі. Завдяки блокчейну, Bitcoin став першою криптовалютою.

Блокчейн (blockchain або block chain) – це вибудуваний за певними правилами безперервний послідовний ланцюжок блоків, що містять певну інформацію. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного. Блокчейн може мати різні конфігурації в залежності від області застосування, починаючи з загальнодоступних мереж з відкритим вихідним кодом, закінчуючи приватними мережами, де потрібно явне регулювання прав доступу на читання і запис даних [4].

Систему Blockchain порівнюють з великою книгою, що містить всі записи про те, що відбувається з криптовалютою, у кожного власника цієї криптовалюти на руках є самостійна, але ідентична іншим копія цієї книги. Записи у всіх книгах - правдиві і однакові. Ні банки, ні уряд, ні власник криптовалюти не може підробити ці записи. Іншими словами, в блокчейні немає єдиного контролера, система управляється багатьма учасниками. Побудована на математичних обчисленнях система захищає цифрову валюту від підробки або ж злому.

Технологія знайшла своє застосування не лише у криптовалютах, а також являється основною для смарт-контрактів. Смарт-контракт – це комп'ютерний код, який виконує угоди, укладені між двома і більше сторонами, в результаті яких, при виконанні тих чи інших умов відбуваються певні дії. Тобто, коли виконуються раніше запрограмовані умови, смарт-контракт автоматично реалізує відповідну угоду. Принцип розумних контрактів виник значно раніше, аніж технологія блокчейн, проте, на той момент реалізація цього процесу була неможливою [5].

Поява блокчейну послужила поштовхом для розробки смарт-контрактів. Через п'ять років від появи технології, платформа Ethereum дозволила використовувати смарт-контракти на практиці. Ринок пропонує безліч платформ, які дозволяють використовувати смарт-контракти, але Ethereum залишається одним з найпоширеніших для їхньої реалізації.

Сьогодні блокчейн застосовується в багатьох сферах крім відправки та отримання цифрових грошей. Як показала криптовалюта Bitcoin, криптографія та продумані економічні стимули можуть створити безпечний спосіб зберігання і управління інформацією, включаючи особисту інформацію.

На жаль, існує цілий ряд галузей, що повільно розвиваються та вразливі до хакерських атак та витоку інформації, а загроз інформаційної безпеки стає все дедалі більше. Захист інформації потребує нових методів та підходів для забезпечення інформаційної безпеки.

Блокчейн та його властивості, забезпечують передачу даних безпечним способом та повністю підходять як один з методів забезпечення інформаційної безпеки. Враховуючи незмінність блоків блокчейну, криптографічне шифрування у децентралізованій структурі, він може стати ідеальною системою захисту даних, маніпулювання якою буде практично неможливим. Технологія блокчейн дозволить користувачам самостійно зберігати особисті дані і повністю контролювати їх передачу кому-небудь,

завдяки чому необхідність сліпо довіряти корпораціям в збереженні даних просто відпаде. При цьому особиста інформація буде зберігатися під захистом, забезпеченим методами криптографічного шифрування. Сама архітектура розподілених баз даних створює ідеальну комбінацію прозорості даних, їх незмінності, а також їх децентралізації.

З вищевказаних проблем та переваг технології, метою даної роботи є дослідження можливих варіантів та способів захисту інформації від несанкціонованого доступу на основі технології Blockchain.

1. ЗАГАЛЬНИЙ ОГЛЯД ІСНУЮЧИХ ПРОБЛЕМ ТА МЕТОДІВ ЇХ ВИРІШЕНЬ. ОБГРУНТУВАННЯ ТЕМИ МАГІСТЕРСЬКОЇ ДИСЕРТАЦІЇ

1.1 Актуальність проблеми та обґрунтування поставленої задачі

У сучасному світі бурхливо розвиваються технології обробки, зберігання та передачі інформації. Застосування інформаційних технологій вимагає підвищеної уваги до питань інформаційної безпеки. Знищення інформаційних ресурсів, їх недоступність або несанкціоноване використання внаслідок порушень інформаційної безпеки, викликають серйозні проблеми у громадян, соціальних груп, компаній і держав.

Ще 25-30 років тому завдання захисту інформації могло бути ефективно вирішено за допомогою організаційних заходів (виконання режимних заходів, використання засобів охорони і сигналізації) і окремих програмно-апаратних засобів обмеження доступу і шифрування. Поява персональних ЕОМ, локальних і глобальних комп’ютерних мереж, супутникових каналів зв'язку, ефективних засобів технічної розвідки і отримання конфіденційної інформації істотно загострило проблему захисту інформації [3].

Зростання кількості і якості загроз безпеки інформації в комп'ютерних системах не завжди призводить до відповідної реакції у вигляді створення надійних систем захисту інформації та безпечних інформаційних технологій. У більшості комерційних і державних організацій, не кажучи вже про окремих користувачів, в якості засобів захисту інформації застосовуються тільки антивірусні програми, не завжди своєчасно оновлюванні, і обмеження прав користувачів комп'ютерної системи на основі паролів. У зв'язку з цим слід не тільки збільшувати кількість

спеціалістів в області інформаційної безпеки і захисту інформації, а й розробляти нові сучасні методи і засоби захисту інформації.

З виникненням та розвитком нових технологій з’являється дедалі більше проблем інформаційної безпеки. Експерти захисту інформації припускають, що загрози стануть більш замкнутими і цілеспрямованими, а поширення новітніх технологій, таких як, наприклад, машинне навчання і нейромережі, виведуть складність кібератак на новий рівень. Зокрема, найближчим часом може виникнути небезпека витоків особливо цінної інформації - наприклад, біометричних даних людини. Персональна інформація користувачів допомагає зловмисникам удосконалювати свої методи соціальної інженерії і проводити більш переконливі атаки, так що їх інтерес до чужих особистих даних буде тільки зростати. Крім цього, кіберзлочинці цілком можуть почати застосовувати штучний інтелект для профілювання жертви і створення інформаційних підробок, які вже сьогодні досить широко обговорюються.

За останній рік технології, безумовно, піднялися на нові висоти. Пандемія COVID-19 має великий вплив на людей і спільноти, вона в короткі терміни трансформувала тренди інформатизації та організації процесів, звички користувачів. Інформаційна безпека не стала винятком. У зв'язку з переходом на віддалену роботу компанії перейнялися збереженням працездатності основних технологічних процесів, тому багато послабили правила безпеки, щоб співробітники могли звертатися до необхідних для роботи матеріалів і сервісів. Додатковим джерелом загроз стали пристрої віддаленого доступу - використовувані вдома комп'ютери і смартфони. А те, що співробітникам, як правило, не вистачає часу і кваліфікації на забезпечення їх безпеки, погіршує ситуацію.

Різке зростання використання хмарних додатків позначився на збільшенні числа DDoS-атак, які спрямовані на припинення доступу користувачів до хмарних ресурсів і маскують більш небезпечні впливи на

обчислювальні системи організацій. В опитуванні директорів з інформаційної безпеки, проведеному нещодавно компанією Microsoft, 73% респондентів повідомили про те, що за останні 12 місяців в організації мали місце проблеми витоку інформації, і компанії акцентують увагу на управління ризиками інсайдерських атак у зв'язку з пандемією COVID-19 [5].

Змінилися цілі кіберзлочинців. Раніше атаки фокусувалися переважно на фінансових організаціях, що пояснюється бажанням отримати максимальну вигоду. Цього року частка таких атак, за даними Positive Technologies, знизилася до 8%, що пов’язано із збільшеним рівню захисту фінансових організацій і відповідним зменшенням їх привабливості для зловмисників. Промислові підприємства раніше мало цікавили злочинців. Ситуація змінилася, число атак на цей сектор збільшується. Якщо в IV кварталі 2020 року фахівці PT Expert Security Center зафіксували 33 атаки на промислові підприємства, то в I кварталі 2021 го - вже 72 [5].

Тепер перша трійка галузей, які найбільше постраждали від хакерських атак, виглядає досить несподівано - державні організації (14% загального числа атак), промисловість та енергетика (11%), медичні установи (10%). Причому 50% атак скоєно з використанням вірусів-вимагачів.

Оскільки, в 2021 році ми продовжуємо стикатися з новими викликами інформаційної безпеки, а кіберзлочинці стають все більш компетентними в їх здібностях проникати в корпоративні мережі і компрометувати дані, необхідно знаходити нові методи та способи забезпечення інформаційної безпеки. Системний підхід в цьому питанні дозволить значно знизити кількість інцидентів ІБ як для користувачів, так і для організацій в цілому.

Забезпечення інформаційної безпеки - безперервний процес, який полягає в розвитку систем захисту, постійному контролі, виявлення її слабких місць, а також можливих каналів витоку інформації. Для боротьби

зі зростаючими кіберзагрозами існує новий метод – технологія блокчейн. У ряді областей (в першу чергу, захист пристроїв інтернету речей і децентралізована ідентифікація) блокчейн має серйозний потенціал і може змінити поточні підходи до безпеки, він може забезпечити інформаційний суверенітет безпечним методом [3].

1.2 Основні поняття захисту інформації та забезпечення інформаційної безпеки

У нашу інформаційну епоху питання безпеки даних стала одним з найбільш важливих. Здається, що все наше життя стало відслідковуватися через бази даних, а наша конфіденційна інформація стала вразливою як ніколи.

Захист інформації – це діяльність по запобіганню витоку інформації, сукупність методів і засобів, що забезпечують цілісність, конфіденційність, достовірність, автентичність і доступність інформації в умовах впливу на неї загроз природного або штучного характеру. Під витоком розуміють неконтрольоване поширення інформації шляхом її розголошення, несанкціонованого доступу до неї і отримання розвідками [2].

Розголошення – це доведення інформації, що захищається до неконтрольованої кількості одержувачів інформації (наприклад, публікація інформації на відкритому сайті в мережі Інтернет або у відкритому друці). Несанкціонованим доступом вважають отримання інформації, що захищається інформаційно зацікавленим суб'єктом з порушенням правил доступу до неї. Несанкціонований вплив на захищену інформацію – вплив з порушенням правил її зміни (наприклад, навмисне впровадження в захищені інформаційні ресурси шкідливого програмного коду або навмисна заміна електронного документа). Під ненавмисним впливом на захищену інформацію розуміють вплив на неї з-за помилок користувача, збою технічних або програмних засобів, природних явищ, інших не

цілеспрямовано впливів (наприклад, знищення документів в результаті відмови накопичувача на жорсткому диску комп'ютера).

Основними цілями захисту інформації є [1]:

- запобігання витоку, розкрадання, втрати, спотворення і підробки інформації (захисту підлягає будь-яка інформація, в тому числі і відкрита);
- запобігання загрозам безпеки особистості, суспільства і держави (тобто захист інформації є одним із способів забезпечення інформаційної безпеки держави);
- захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, наявних в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства.

Під ефективністю захисту інформації розуміють ступінь відповідності результатів захисту інформації до поставленої мети. Об'єктом захисту може бути інформація, її носій або інформаційний процес, щодо яких необхідно забезпечувати захист. Під якістю інформації розуміють сукупність властивостей, обумовлюють придатність інформації задовольняти виділені потреби її користувачів відповідно до призначення інформації.

Одним з показників якості інформації є її захищеність - підтримання на заданому рівні тих параметрів інформації, які характеризують установлений статус її зберігання, обробки та використання. Основними характеристиками, що захищається являють конфіденційність, цілісність і доступність.

Конфіденційність інформації – це поширення її змісту тільки тим суб’єктам, що мають відповідні повноваження. Конфіденційність є суб'єктивною характеристикою інформації, пов'язаної з об'єктивною необхідністю захисту законних інтересів одних суб'єктів від інших.

Цілісністю інформації називають незмінність інформації в умовах її випадкового і (або) навмисного спотворення або руйнування, а доступністю інформації розуміють здатність забезпечення безперешкодного доступу суб'єктів до необхідної інформації.

Всі вище перераховані поняття, утворюють систему захисту інформаційної безпеки.

1.3 Основні загрози інформаційної безпеки

Під загрозою безпеки інформації в комп'ютерній системі (КС) розуміють подію або дію, яка може викликати зміну функціонування цієї системи, пов'язану з порушенням захищеності інформації, що обробляється в ній. Вразливість інформації - це можливість виникнення на будь-якому етапі життєвого циклу КС такого її стану, при якому створюються умови для реалізації загроз безпеці інформації [5].

Атакою на комп’ютерну систему називають дію, що вживається порушником, яке полягає у пошуку та використанні тієї чи іншої вразливості. Інакше кажучи, атака на КС є реалізацією загрози безпеці інформації в ній.

Загрози інформаційної безпеки можуть бути поділені на загрози, що не залежать від діяльності людини (природні загрози фізичних впливів на інформацію стихійних природних явищ), і загрози, викликані людською діяльністю (штучні загрози), які є набагато більш небезпечними.

Штучні загрози виходячи з їх мотивів поділяються на ненавмисні (випадкові) і навмисні [7].

До ненавмисних загроз відносяться:

- помилки в проектуванні КС;
- помилки в розробці програмних засобів;
- енергопостачання;
- помилки користувачів системи;

- вплив на апаратні засоби фізичних полів інших електронних пристроїв (при недотриманні умов їх електромагнітної сумісності) та ін.

Умисними загрозами вважають:

- несанкціоновані дії обслуговуючого персоналу системи;
- несанкціонований доступ до ресурсів КС з боку користувачів КС та сторонніх осіб, шкода від якого визначається отриманими порушником повноваженнями.

Залежно від цілей навмисних загроз безпеці інформації загрози можуть бути поділені на три основні групи [7]:

- загроза порушення конфіденційності, тобто витікання інформації обмеженого доступу, що зберігається в системі або передається від однієї КС до іншої;
- загроза порушення цілісності, тобто навмисного впливу на інформацію, що зберігається в КС;
- загроза порушення доступу до інформації, тобто відмова в обслуговуванні, викликана навмисними діями порушника, при якій блокується доступ до деякого ресурсу з боку інших користувачів.

Опосередкованою загрозою безпеці інформації є загроза розкриття параметрів підсистеми захисту інформації. Реалізація цієї загрози дає можливість реалізації перерахованих раніше безпосередніх загроз безпеки інформації. Результатом реалізації загроз безпеки інформації в КС може бути витік (копіювання) інформації, її втрата (руйнування) або спотворення (підробка), блокування інформації.

Каналами витоку інформації є безпосередні канали, пов'язані з фізичним доступом до елементів системи. До безпосередніх каналів витоку, що не потребують зміни елементів КС, відносяться [7]:

- розкрадання носіїв інформації;

- видалених файлів, помилково збережених тимчасових файлів);
  · копіювання носіїв інформації;
- маскування під інших користувачів шляхом викрадення їх ідентифікуючої інформації (паролів, карт тощо) ;
- обхід засобів розмежування доступу до інформаційних ресурсів внаслідок недоліків у їх програмному забезпеченні
- зловмисна зміна програм для виконання несанкціонованого копіювання інформації при її обробці.

Крім витоку інформації можливо також її несанкціоноване знищення або спотворення (наприклад, зараження комп'ютерними вірусами), а також несанкціоноване використання інформації при санкціонованому доступі до неї (наприклад, порушення авторських прав власників або власників програмного забезпечення) для її несанкціонованого використання.

Оскільки найбільш небезпечні загрози інформаційної безпеки викликані навмисними діями порушника, звідси випливають висновки, що при вирішенні завдання захисту інформації необхідно застосовувати так званий системно-концептуальний підхід.

1.4 Аналіз методів та засобів захисту інформації

Для боротьби з існуючими загрозами інформаційної безпеки існує ряд методів захисту. До методів захисту інформації відносять спеціальні заходи, засоби та практики, які захищають інформаційний простір від загроз.

Класифікація методів та способів захисту виглядає наступним чином [6]:

- способи зміни виду та структури передачі інформації в мережі та її зберігання, наприклад, застосування криптографічних методів захисту;

- організаційні методи захисту даних, що ґрунтуються на управлінні інформаційними системами та регламентуванні правил безпеки;
- технічні та технологічні методи захисту інформації, що передбачають використання спеціальних програмних та апаратних засобів.

Окрім того, методи забезпечення безпеки поділяють на організаційно-адміністративні, правові, та інженерно технічні заходи захисту інформації.

Правове забезпечення інформаційної безпеки утворене сукупністю правових режимів, принципів, закріплених у законодавстві і джерелах міжнародного права, вимоги яких є обов'язковими до системи захисту інформації. У рамках цього напряму інформаційного права регулюються суспільні відносини щодо забезпечення безпеки, насамперед інформації та інформаційної інфраструктури, які використовуються людиною, суспільством та державою для задоволення законних інтересів, реалізації прав та виконання юридичних обов'язків. В Україні правові основи забезпечення безпеки інформації складають Конституція України, постанови Кабінету Міністрів України, Закони України, кодекси та інші нормативно-правові акти.

Організаційно-адміністративне захисту інформації – це врегулювання взаємовідносин виконавців та виробничої діяльності на нормативно-правовій основі таким чином, що розголошення, витік та несанкціонований доступ до конфіденційної інформації стає неможливим або суттєво утруднюється за рахунок проведення організаційних заходів. Практично неможливо уникнути впливу цих аспектів за допомогою технічних засобів, програмно-математичних методів та фізичних заходів. Для цього необхідна сукупність організаційно-правових та організаційно-технічних заходів, які б виключали (або принаймні зводили до мінімуму) можливість виникнення небезпеки для інформації [7].

Інженерно-технічні заходи являють собою сукупність спеціальних органів, технічних заходів та засобів, що спільно виконують завдання щодо захисту інформації. Технічний захист інформації є цілим комплексом робіт: від обладнання приміщень засобами обмеження доступу, шифрування даних, інформування колективу та виявлення передбачуваних каналів витоку до постійного оновлення засобів та способів підтримки безпеки.

Інженерно-технічні засоби захисту включають апаратні та програмні засоби захисту, які запобігають появі атаки, допомагають виявити факт її виникнення та позбутися наслідків, їх основними функціями являються [7]:

- ідентифікація та автентифікація користувачів;
- створення перешкод на можливих шляхах проникнення та доступу потенційних порушників до системи та інформації, що захищається;
- розмежування доступу до ресурсів;
- реєстрація подій;
- криптографічний захист інформації.

1.4.1 Методи захисту інформації від несанкціонованого доступу

Методами захисту від несанкціонованого доступу є програмні, технічні чи програмно-технічні засоби, призначені для запобігання несанкціонованого доступу до інформації, а саме [7]:

- реалізація дозвільної системи допуску користувачів до інформаційних ресурсів, інформаційних систем та пов'язаних з її використанням робіт, документів;
- обмеження доступу користувачів до приміщень, де розміщені технічні засоби, що дозволяють здійснювати обробку персональних даних, а також зберігаються носії інформації;

- розмежування доступу користувачів до інформаційних ресурсів, програмних засобів обробки (передачі) та захисту інформації;
- реєстрація дій користувачів та обслуговуючого персоналу; контроль несанкціонованого доступу та дій користувачів;
- облік та зберігання знімних носіїв інформації та їх звернень, що виключає розкрадання, заміну та знищення;
- резервування технічних засобів, дублювання масивів та носіїв інформації;
- використання засобів захисту інформації, які пройшли в установленому порядку процедуру оцінки відповідності;
- використання захищених каналів зв'язку;
- розміщення технічних засобів, що дозволяють здійснювати обробку персональних даних у межах території, що охороняється;
- організація фізичного захисту приміщень та технічних засобів, що дозволяють здійснювати обробку персональних даних;
- запобігання впровадженню в інформаційні системи шкідливих програм та програмних закладок.

1.5 Технологія Blockchain та забезпечення інформаційної безпеки

При виникненні загроз інформаційної безпеки у мережі потрібно зберігати послідовність та опис усіх подій, що призвели до появи такої загрози.

При такій постановці завдання блокчейн є ідеальним засобом збереження подій у мережному середовищі, оскільки блокчейн записує і вибудовує їх у строго хронологічному порядку. Блокчейн у даному випадку може розглядатися як односпрямована (без зворотного зв'язку) структура даних (ланцюг) з пов'язаним списком блоків, кожен із яких посилається на

попередній, використовуючи хеш-коди-покажчики, що зберігаються в заголовку блоку [8].

Децентралізація блокчейну знижує ймовірність фальсифікації баз даних. Хакери зазвичай отримують доступ до даних, за допомогою атаки точки, де кластеризовані всі дані. На щастя, блокчейн не дає шансів на шахрайство. Завдяки розподіленому зберіганню інформації по мережі блокчейн хакери не можуть пошкодити головний блок даних, натомість вони повинні завдати шкоди одним і тим же даними у всіх блоках. Така атака вимагає шалених зусиль, що миттєво зупиняє злочинців.

Вузли блокчейна здійснюють алгоритми консенсусу, якщо кілька вузлів знаходяться в автономному режимі, інші продовжують працювати, навіть якщо вони були переведені в автономний режим внаслідок хакерської атаки. Робота відновлюється, коли вузли відновлюють зв'язок між собою, повертаються в оперативний режим і проводять реплікацію (пересинхронізацію) станів вузлів, щоб забезпечити послідовність і цілісність всього ланцюжка блокчейн. Ця можливість існує завдяки унікальному набору закодованих алгоритмів у блокчейні.

1.5.1 Перспективи застосування технології Blockchain у забезпеченні інформаційної безпеки

Маючи великий потенціал, блокчейн може бути реалізований у багатьох сферах. Одним із найкращих варіантів використання є забезпечення цілісності для рішень кібезбезпеки. Нижче наведено деякі приклади використання блокчейну в майбутньому для посилення кібербезпеки [8]:

- Захист особистих повідомлень. Кількість платформ соціальних мереж постійно зростає. Під час користування соціальними мережами збирається безліч метаданих. Більшість користувачів платформ соціальних мереж захищають сервіси та дані за

допомогою ненадійних паролів. Компанії, що займаються обміном повідомленнями, можуть застосовувати блокчейн для захисту даних як більш досконалий варіант порівняно з наскрізним шифруванням, яке вони в даний час використовують. Блокчейн можна використовувати для створення стандартного протоколу безпеки. У недавньому минулому було здійснено численні атаки на соціальні платформи, такі як Twitter та Facebook. Ці атаки призвели до витоку даних, внаслідок чого зламали мільйони облікових записів, а інформація про користувачів потрапила в чужі руки. Технологія блокчейн, при правильній реалізації у системах обміну повідомленнями, може запобігти подібним кібератакам у майбутньому.

- Безпека Інтернету речей. Хакери все частіше використовують периферійні пристрої, такі як термостати та маршрутизатори для отримання доступу до систем в цілому. З розвитком систем штучного інтелекту, хакерам стало простіше отримати доступ до загальних систем, таких як домашня автоматизація через периферійні пристрої, такі як «розумні» перемикачі. У більшості випадків велика кількість цих пристроїв Інтернету речей має ненадійні функції забезпечення безпеки. У цьому випадку блокчейн можна використовувати для захисту таких систем або пристроїв у цілому шляхом децентралізації адміністрування. Такий підхід дасть можливість пристрою самостійно приймати рішення щодо безпеки. Незалежно від центрального адміністратора або органу, пристрої стають безпечнішими, виявляючи підозрілі команди з невідомих мереж та діючи відповідно до них. Зазвичай хакери проникають у центральне адміністрування пристрою та автоматично

отримують повний контроль над пристроями та системами. Шляхом децентралізації таких систем керування пристроями, блокчейн гарантує, що такі атаки практично неможливо буде виконати.

- Захист DNS та DDoS. Розподілена атака типу «відмова в обслуговуванні» (DDoS) відбувається, коли користувачам цільового ресурсу, наприклад мережного ресурсу, сервера чи веб-сайту, відмовлено у доступі чи обслуговуванні цільового ресурсу. Ці атаки відключають чи уповільнюють роботу ресурсних систем.З іншого боку, неушкоджена система доменних імен (DNS) дуже централізована, що робить її ідеальною метою для хакерів, які проникають у з'єднання між IP-адресою та ім'ям веб-сайту. Ця атака робить веб-сайт недоступним, і навіть перенаправляє користувача на інші шахрайські веб-сайти.На щастя, блокчейн можна використовувати для зменшення таких атак за рахунок децентралізації записів DNS. Застосовуючи децентралізовані рішення, блокчейн захистив би окремі вразливі точки, використовувані хакерами.
- Децентралізація сховища. Злом та крадіжка бізнес-даних стають основною очевидною причиною занепокоєння організацій. Більшість компаній, як і раніше, використовують централізовану форму носія даних. Щоб отримати доступ до всіх даних, що зберігаються в цих системах, хакер просто використовує одну вразливу точку. Внаслідок такої атаки важливі та конфіденційні дані, такі як фінансові звіти підприємств, цінні папери та документи, залишаються у володінні злочинця. За допомогою блокчейну конфіденційні дані можуть бути захищені шляхом забезпечення

децентралізованої форми зберігання даних. Цей метод зниження ризику ускладнить і навіть унеможливить проникнення хакерів у системи зберігання даних. Багато компаній, що надають послуги зберігання, оцінюють способи, якими блокчейн може захистити дані від хакерів. Apollo Currency Team – гарний приклад організації, яка вже впровадила технологію блокчейн у свої системи (Apollo Data Cloud).

- Комп'ютерне програмне забезпечення. Блокчейн можна використовувати для забезпечення цілісності програмного забезпечення та запобігати встановленню шкідливого програмного забезпечення. Так само, як використовуються хеші MD5, блокчейн може застосовуватися для перевірки дій, таких як оновлення прошивки та виправлення помилок у версіях, щоб запобігти проникненню шкідливого програмного забезпечення на комп'ютери. У сценарії MD5 новий ідентифікатор програмного забезпечення порівнюється з хешами, доступними на веб-сайтах постачальників. Цей метод не є повністю надійним, оскільки хеші доступні на платформі провайдера вже можуть бути скомпрометовані. Однак у разі використання технології блокчейн хеші постійно записуються у ланцюг, а інформація, записана у блоках, не підлягає зміні чи редагуванню програмного забезпечення.
- Перевірка кіберфізичних систем. Підробка даних, неправильна конфігурація систем разом із відмовою компонентів порушили цілісність інформації, що генерується кіберфізичними системами. Однак можливості технології блокчейн щодо цілісності та перевірки інформації можуть використовуватись для автентифікації статусу будь-якої кіберфізичної інфраструктури. Інформація, отримана про компоненти

інфраструктури за допомогою блокчейна, може бути надійнішою для всього ланцюжка поставок.

- Захист передачі даних. Блокчейн можна використовувати в майбутньому для запобігання несанкціонованому доступу до даних під час передачі. Використовуючи повну функцію шифрування, передача даних може бути захищена, щоб запобігти доступу до неї зловмисників, будь то приватна особа чи організація. Такий підхід призведе до загального підвищення надійності та цілісності даних, що передаються через блокчейн.

Таким чином, незалежно від того, як блокчейн використовується, ключовим компонентом є його здатність до децентралізації. Ця функція видаляє єдину цільову точку, яка може бути зламана. В результаті стає абсолютно неможливо проникнути в системи або сайти, контроль доступу, зберігання даних та мережевий трафік яких, більше не знаходяться в одному місці.

1.5.2 Складнощі впровадження технології Blockchain

Технологія блокчейн надала світові інноваційний прорив, який можна досліджувати в широкому спектрі галузей, однак ця технологія несе в собі унікальний набір проблем, які значною мірою впливають на її повільне та проблематичне впровадження [9].

Блокчейн покладається на шифрування для забезпечення своєї безпеки, а також досягнення консенсусу в розподіленій мережі. По суті це означає, що для «доказу» того, що користувач має дозвіл на запис у ланцюжок, повинні бути запущені складні алгоритми, що, у свою чергу, вимагають великих обчислювальних потужностей. Звісно, за це доводиться платити. Минулого року було заявлено, що обчислювальна потужність, необхідна для підтримки роботи мережі найбільш відомого ланцюга

блокчейну - Bitcoin, потребує стільки ж енергії, скільки було використано 159 країнами світу.

Відомо, що успадковані мережі обробки транзакцій обробляють тисячі транзакцій за секунду. І навпаки, мережі блокчейнів значно повільніші, коли справа доходить до транзакцій на секунду. Як показник найвідоміших публічних блокчейнів, блокчейн Біткойн може обробляти від трьох до семи транзакцій на секунду, а Ethereum може обробляти приблизно 20 транзакцій на секунду. Ця продуктивність, порівняно з їх централізованими аналогами, зробила технологію нежиттєздатною для великомасштабних програм та масового впровадження.

Більшість блокчейн-мереж працюють ізольовано та не взаємодіють з іншими одноранговими мережами. Немає стандартів, що дозволяють безперешкодно взаємодіяти між блокчейн-проектами. Згідно з звітом Deloitte, понад 6500 проектів використовують різні платформи блокчейнів з різними протоколами, мовами кодування та механізмами консенсусу. Така зміна значно скорочує обсяг співробітництва та транзакцій між блокчейнами. Крім того, існуючі блокчейни не можуть полегшити передачу даних між ланцюжками або інтегруватися з традиційними платформами [10].

Також кожен приклад новаторської технології потребує часу, щоб співтовариство розробників прийняло її на озброєння, а освітні установи – на запровадження відповідних курсів. Сфера блокчейн-мереж нині перебуває у початковому стані і тому страждає від гострої нестачі кваліфікованих розробників.

При великій різноманітності мереж, що існують сьогодні, не існує універсальних стандартів для додатків блокчейну. Стандартизація може допомогти знизити витрати, розробити ефективніші механізми консенсусу та забезпечити можливість взаємодії. Відсутність такої одноманітності в

протоколах ланцюжка блоків ще більше ускладнює проблему залучення нових розробників, а також знижує узгодженість основних процесів.

З 2009 року глобальні підприємства та медіа-компанії наголошували на відсутність ясності регулювання щодо криптовалют і, як наслідок, базової технології блокчейн, що є серйозною перешкодою для масового впровадження. Хоча підприємства, які використовують блокчейн, не вимагають довіри та децентралізовані, існують певні галузі, які потребують нормативної підтримки, зокрема смарт-контракти.

За минулі роки було досягнуто певного прогресу у сфері регулювання. Згідно з дослідженням Deloitte, законодавчі органи 17 штатів США ухвалили законопроекти про впровадження блокчейну. Крім того, кілька інших країн, включаючи Мальту, Естонію, Швейцарію, Сінгапур та Японію, формулюють законодавство, що регламентує блокчейн, щоб використати переваги цієї технології.

Технологія блокчейн має величезний потенціал і істотні переваги, однак інтегрувати блокчейн у великих масштабах не так просто через ряд технічних, соціальних, економічних, нормативно-регулюючих бар'єрів. Обмежена масштабованість, енерговитратність блокчейну, відсутність нормативно-правової бази, що регулює використання технології, та фахівців, які знаються на ній, – основні проблеми на шляху впровадження розподіленого реєстру.

Шляхами подолання бар'єрів є дослідження методів подолання існуючих перешкод, підготовка кадрів у сфері застосування технології та формування законів, що описують правила її експлуатації. На даний момент робляться активні та виважені кроки щодо усунення цих проблем та збереження траєкторії впровадження блокчейнів у висхідному напрямку.

ВИСНОВКИ ДО РОЗДІЛУ 1

Проаналізована основна мета забезпечення інформаційної безпеки, передачі даних в комп’ютерних мережах. Окрім того, досліджено основні загрози інформаційної безпеки, їх класифікація, канали витоку інформації, проблеми несанкціонованого доступу. Також, було досліджено існуючі методи захисту інформації, їх види та класифікацію.

Враховуючи недоліки існуючих методів захисту інформації та постійний розвиток нових загроз, зроблено висновок про те, що система захисту інформаційної безпеки потребує нових підходів та рішень. На основі даних про існуючих методів захисту інформації, доведена необхідність впровадження технології Blockchain, як методу захисту інформації, розглянуто можливі приклади та перспективи використання блокчейну в майбутньому для посилення кібербезпеки.

Показано, що на даний момент існує ряд проблем, які значною мірою впливають на повільне та проблематичне впровадження технології. Основними проблемами є: обмежена масштабованість, енерговитратність, відсутність нормативно-правової бази, що регулює використання технології, та відсутня достатня кількість фахівців. Проте, з кожним роком цих проблем стає дедалі менше, а тому уже зараз технологія Blockchain може слугувати відмінним засобом захисту інформації.

2. ДОСЛІЖЕННЯ ТЕХНОЛОГІЇ BLOCKCHAIN

2.1 Технологія Blockchain

Розробка криптовалюти Bitcoin програмістом Сатоші Накамото у 2009р. започаткувала розвиток блокчейн-технології. Це пов'язано з тим, що Bitcoin запропонував незалежність від будь-якого централізованого впливу, що досягається саме завдяки блокчейн-технології.

Блокчейн – це децентралізований журнал запису транзакцій, який є частиною ширшої обчислювальної інфраструктури, яка також повинна включати функції зберігання, комунікації, обслуговування файлів і архівування. Блокчейн є вибудуваним за певними правилам безперервним та послідовним ланцюжком блоків, що містять інформацію. На рис.1 наведено структурну схему блоків у блокчейн мережі.

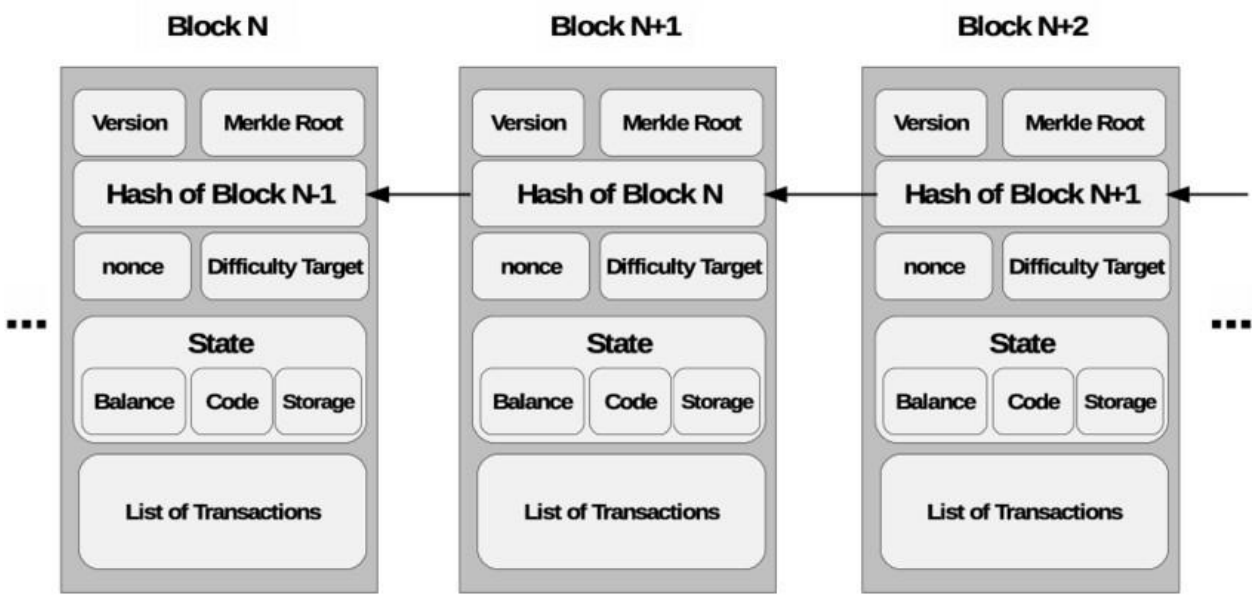

Рисунок 1 – Послідовність блоків у блокчейн мережі

Блок — це контейнерна структура даних, яка об’єднує транзакції для включення у ланцюг [10]. Блок складається із заголовка; містить метадані, а

потім довгий список транзакцій. Блок можна ідентифікувати двома способами: посилаючись на хеш блоку, або за допомогою посилання на висоту блоку. Слід зазначити, що також існує так званий блок генезис (genesis block). Генезисний блок унікальний, оскільки це єдиний блок у блокчейні, який не посилається на попередній блок [11].

Також кожен блок у блокчейн-мережі складається з двох головних частин – заголовка (head) та тіла (payload). Head містить інформацію, яка відповідає за стабільність, а також незмінність мережі. Payload – містить список усіхтранзакцій, які мають бути збережені в даному блоці та потрапити до блокчейн-мережі. На рис. 2 наведено структуру блока блокчейну.

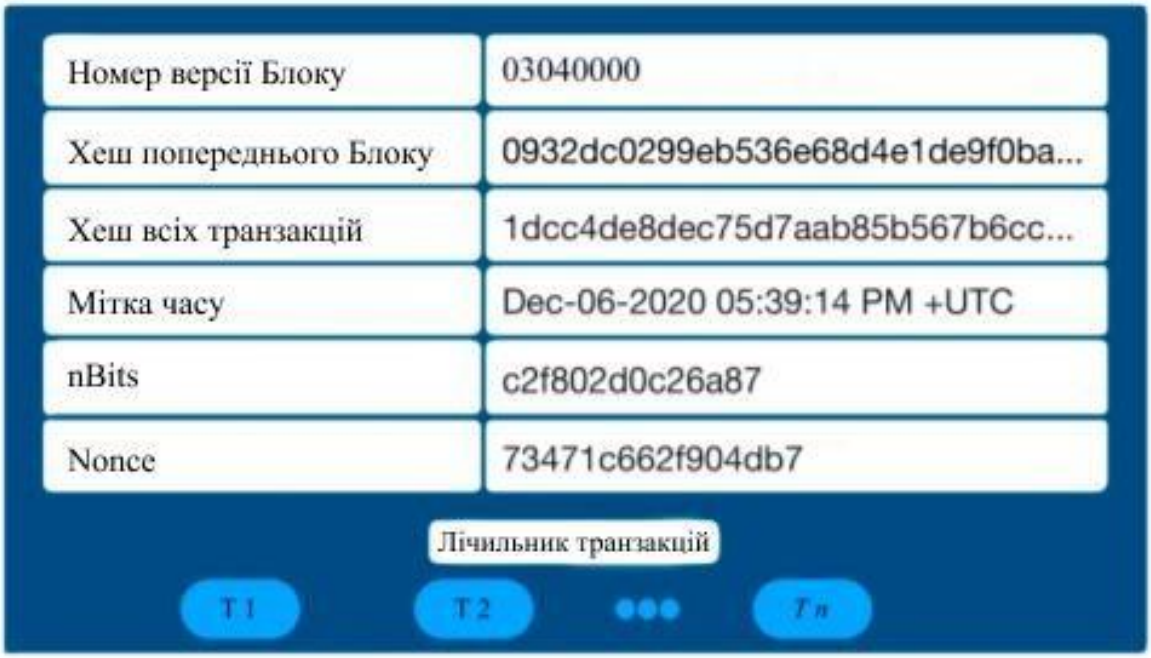

Рисунок 2 – Структура блоку

У класичній блокчейн мережі Head містить такі поля [12]:

- номер версії блоку (ver_block);
- хеш попереднього блоку (prev_block);
- хеш усіх транзакцій у поточному блоці (mrkl_root);
- тимчасову мітку, коли було створено блок (timestamp);

– «bits» і «nonce» параметри, що використовуються при майнінгу.

Як раніше згадувалося, payload складається з лічильника транзакцій та списку всіх транзакцій, що входять до поточного блоку. Також існує максимальна кількість транзакцій, що може містити блок. Це значення залежить від розміру транзакції. Для того, щоб перевірити справжність транзакції використовується механізм асиметричної криптографії.

Цифровий підпис – це криптографічний алгоритм, що застосовується користувачем до документа (повідомлення), який використовується для перевірки справжності та цілісності документа (повідомлення), а також для визначення авторства стосовно документа (повідомлення) [11]. Криптографія з відкритими ключами (public-key cryptography) та хеш-функції надають математичні засоби, що дозволяють ефективно використовувати цифровий підпис. Використання шифрування та цифрових підписів є необхідним для функціонування блокчейн мережі. Хешування дає можливість кожному з учасників мережі визначити поточний стан блокчейна, а цифрові підписи забезпечують доказ того, що всі транзакції здійснено тільки справжніми власниками.

Коли відбувається нова транзакція чи модифікація існуючої транзакції, більшість вузлів у мережі Blockchain здійснюють алгоритми для перевірки цього блоку. Якщо транзакція проходить перевірку, вона додається у вигляді нового окремого блоку у базу даних (рис. 3)

Для того, щоб додати новий блок, необхідно отримати відповідь на криптографічну хеш-функцію, після чого додається новий блок у ланцюг [12].

При завершенні транзакції, вона створює унікальний хеш-код з використанням криптографічної техніки хешування, яка зв’язує транзакцію з наступним блоком.

Якщо більшість блоків забороняють введення нової чи зміненої транзакції, вона не буде додана у базу даних.

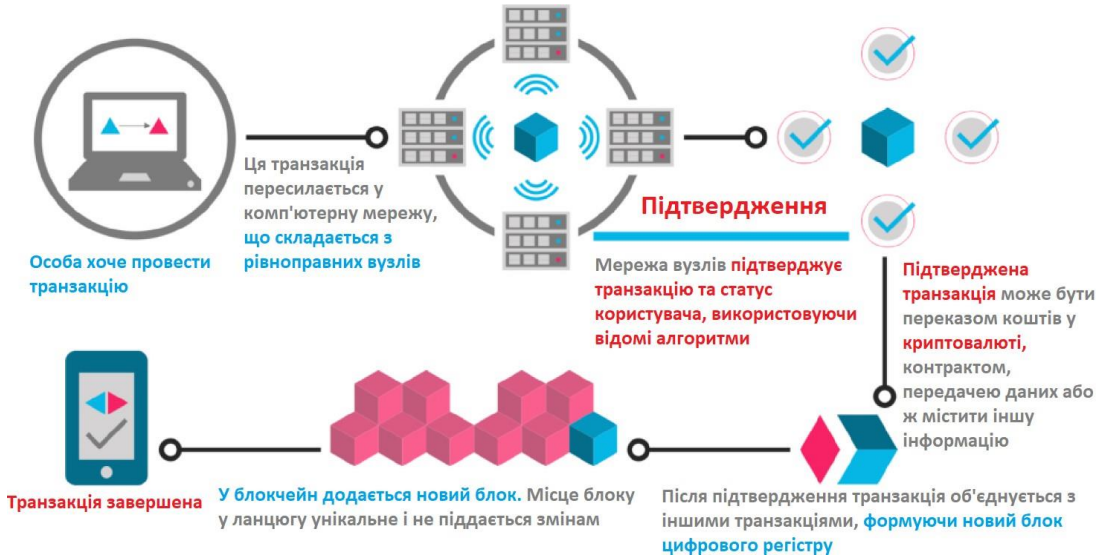

Рисунок 3 – Проведення транзакцій у мережі

2.1.1 Ключові характеристики блокчейн-технології

Блокчейн-технологія має низку переваг, зокрема, можна виділити кілька ключових характеристик, які вплинули на її розвиток [11].

Децентралізація. Якщо розглядати звичайні централізовані системи (керівні органи), то кожна транзакція має бути підтверджена центральною довіреною ланкою, наприклад, як така ланка може виступати центральний банк. У свою чергу, це призводить до неминучих витрат для забезпечення ІБ. Інакше кажучи, транзакція в блокчейн мережі може бути проведена між будь-якими двома рівними користувачами без перевірки автентичності з боку центрального сервера. Таким чином, застосування блокчейн-технології може значно знизити витрати на підтримку функціонування серверів (у тому числі витрати на розробку та експлуатаційні витрати) та вирішити певні завдання безпеки та забезпечення необхідної продуктивності.

Незмінність. Будь-яка транзакція в блокчейн мережі підтверджується іншими учасниками цієї мережі і фіксується у відповідному блоці. Кожен вузол мережі має у своєму розпорядженні дані всіх транзакцій, що відбулись

у мережі. Внести зміни в транзакції неможливо, оскільки блоки та транзакції перевіряються іншими вузлами. Якщо більшість вузлів (користувачів) вважатиме, що транзакція є дійсною, її записують до реєстру. Це сприяє забезпеченню прозорості та цілісності інформації. Таким чином, без згоди більшості вузлів ніхто не зможе додати блоки транзакцій до розподіленого реєстру.

Анонімність. Кожен користувач може взаємодіяти з блокчейн мережею за допомогою згенерованих адрес. Крім того, користувач може генерувати безліч адрес, щоб уникнути однозначної ідентифікації. Відсутня центральний сервер, що зберігає ідентифікаційні дані користувачів. Цей факт забезпечує певний ступінь конфіденційності щодо операцій, включених до блокчейну. Анонімність досягається тільки в публічних блокчейн мережах, докладніше описано в наступному розділі.

Прозорість. Так як кожна з транзакцій у мережі перевіряється та записується з міткою часу, користувачі можуть легко перевірити та відстежити попередні записи. Наприклад, у криптовалюті Bitcoin кожна транзакція може бути ітеративно простежена до попередніх транзакцій. Це покращує простежуваність та прозорість даних, що зберігаються у блокчейні.

2.2 Хешування у Blockchain

Хеш-функції – це одні із найбільш широко використовуваних криптографічних алгоритмів у технології блокчейн. Це криптографічні (але не шифрувальні) алгоритми, призначені для захисту цілісності даних. Будь-яка частина даних може бути хешована, незалежно від її розміру або типу [13]. У традиційному хешуванні, незалежно від розміру, типу або довжини даних, хеш, який генерують будь-які дані завжди має однакову довжину. Хеш призначений для використання як одностороння функція.

Хеш-функція приймає вхідний рядок (числа, алфавіти, мультимедійні файли) будь-якої довжини та перетворює її на новий рядок фіксованої довжини. Фіксована бітова довжина може змінюватись (наприклад, 32-бітна, 64-бітна, 128-бітна або 256-бітна) залежно від використовуваної хеш-функції. Рядок фіксованої довжини називається хешем. Цей хеш і є результатом хеш-алгоритму (рис.4).

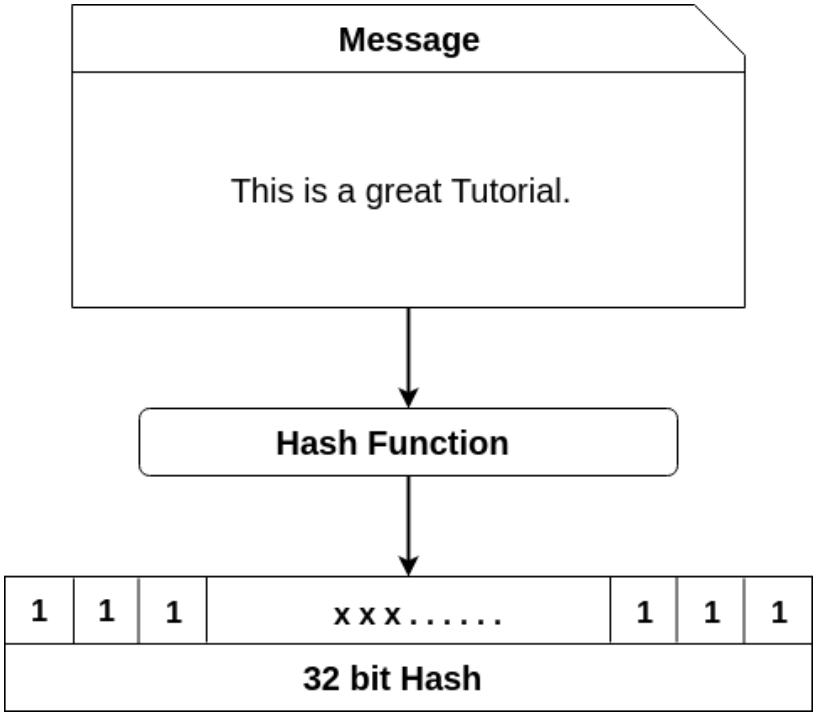

Рисунок 4 – Алгоритм хешування

Хеш-функції виникли через необхідність зробити контент одноманітним та для використання унікальних ідентифікаторів. Хеш-функція забезпечує криптовалюті високий рівень безпеки, і хоча теоретично ніщо не захищене від зламів повною мірою, такий підхід дає максимально високий із доступних нині рівнів складності. При використанні хеш-функції можна досягати високого рівня безпеки систем. У тому числі, з її допомогою можливе хешування паролів та шифрування інших даних. Щоб бути безпечною та використовуватися для криптовалют, хеш-функція повинна

бути стійкою до колізій, а це означає, що неможливо знайти два вхідних рядка, які дадуть однаковий результат.

Для ідеальної хеш-функції виконуються такі умови [13]:

— хеш-функція є детермінованою, тобто те саме повідомлення призводить до одного і того ж хеш-значення;

— значення хеш-функції швидко обчислюється для будь-якого повідомлення;

— неможливо знайти повідомлення, яке дає задане хеш-значення;

— неможливо знайти два різні повідомлення з однаковим хеш-значенням;

— невелика зміна в повідомленні змінює хеш настільки сильно, що нове та старе значення здаються некорелюючими.

Хеш-функції у блокчейні гарантують «незворотність» всього ланцюжка транзакцій. Кожен новий блок транзакцій посилається на хеш попереднього блоку в реєстрі. Хеш самого блоку залежить від усіх транзакцій у блоці, але замість того, щоб послідовно передавати транзакції хеш-функції, вони збираються в одне хеш-значення за допомогою двійкового дерева з хешами (дерево Меркла). Таким чином, хеші використовуються як заміна покажчикам у звичайних структурах даних: пов'язаних списках та двійкових деревах.

Найменша зміна будь-якої частини вхідних даних призводить до величезної зміни вихідних даних; в цьому полягає незаперечна безпека технології блокчейн. Зміна будь-якого запису, який раніше відбувся в блокчейні, змінить усі хеші, зробивши їх хибними та застарілими. Це стає неможливим, враховуючи децентралізовану структуру блокчейну.

Перший блок блокчейна, відомий як блок genesis, містить транзакції, які при об'єднанні та перевірці виробляють унікальний хеш. Цей хеш і всі нові транзакції, які обробляються, потім використовуються як вхідні дані для створення абсолютно нового хеша, який використовується в наступному

ланцюжковому блоці. Це означає, що кожен блок посилається на свій попередній блок через його хеш, утворюючи ланцюжок назад у блок genesis. Таким чином, транзакції можуть бути безпечно додані.

Алгоритм хешування вважається безпечним доти, доки йому не вдасться знайти колізію. Як тільки це сталося, алгоритм вважається офіційно недійсним, так як сталось із MD5 та SHA-1.

Для перетворення масиву інформації на хеш у криптовалютах використовується алгоритм хешування SHA-256 (Secure Hashing Algorithm) (рис.5).

Input	Output
Hello	185F8DB32271FE25F561A6FC938B2E264306EC304EDA518007D1764826381969
hello	2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824
BANKEX Proof-of-Asset protocol	6C3C86FD24B044BC19FD1764EEB5D04E7EC8833199A62C85150B92B39D2C8CF5

Рисунок 5 – Приклад хешування SHA-256

SHA-256 є односпрямованою функцією для створення цифрових рядків фіксованої довжини (256 біт, 32 байт) з вхідних даних розміром до 2,31 ексабайт (2^{64} біт) і є окремим випадком алгоритму з сімейства криптографічних алгоритмів SHA-2 (Secure Hash 2) опублікованим АНБ США у 2002 році [14]. Хеш-функції сімейства SHA-2 побудовані на основі структури Меркла-Дамгарда.

Основні характеристики алгоритму:

— індикатор розміру блоку: 64 байти;

— максимально допустима довжина повідомлення: 33 байти;

— характеристика розміру дайджесту повідомлення: 32 байти;

— стандартний розмір слова: 4 байти;

— параметр довжини внутрішньої позиції: 32 байти;

— кількість ітерацій в одному циклі: 64;

— швидкість, досягнута за протоколом: приблизно 140 Мб/с.

Вхідне повідомлення розбивається на блоки, кожен блок – на 16 слів. Алгоритм пропускає кожен блок повідомлення через цикл із 64 ітераціями. На кожній ітерації 2 слова перетворюються, функцію перетворення задають інші слова. Результати обробки кожного блоку складаються, сума є значенням хеш-функції. Оскільки ініціалізація внутрішнього стану виробляється результатом обробки попереднього блоку, немає можливості обробляти блоки паралельно. На рисунку 6 зображено графічне подання однієї ітерації обробки блоку даних.

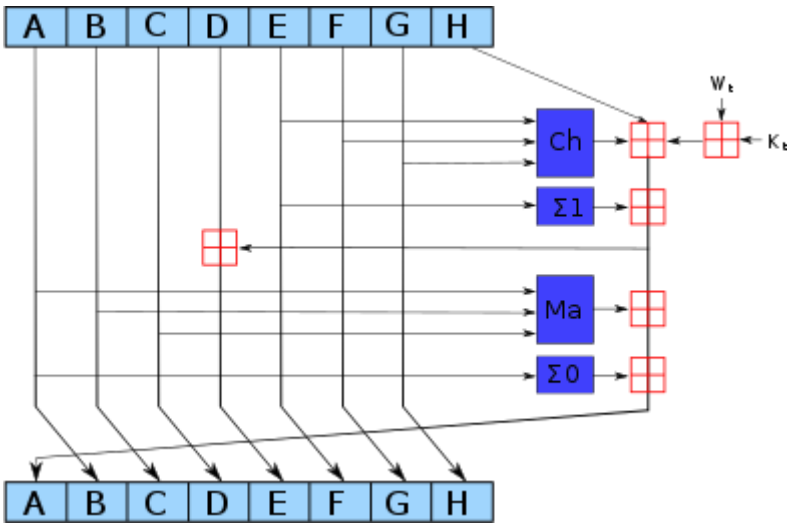

Рисунок 6 - Графічне подання однієї ітерації обробки блоку даних у алгоритмі SHA-256

2.2.1 Дерево Меркла

Кожен блок у блокчейні містить підсумок усіх транзакцій у блоці з використанням дерева Меркла. Дерева Меркла є фундаментальною

частиною технології блокчейну. Це структура даних на основі хешів, яка є узагальненням хеш-списку, та дозволяє ефективно та безпечно перевіряти контент у великому масиві даних. Дерево Меркла. Це деревоподібна структура, в якій кожен листовий вузол є хешем блоку даних, а кожен нелистовий вузол є хешем своїх дочірніх вузлів. Зазвичай дерева Меркла мають коефіцієнт розгалуження 2, що означає, що кожен вузол має до 2-х дочірніх елементів (рис. 7) [15].

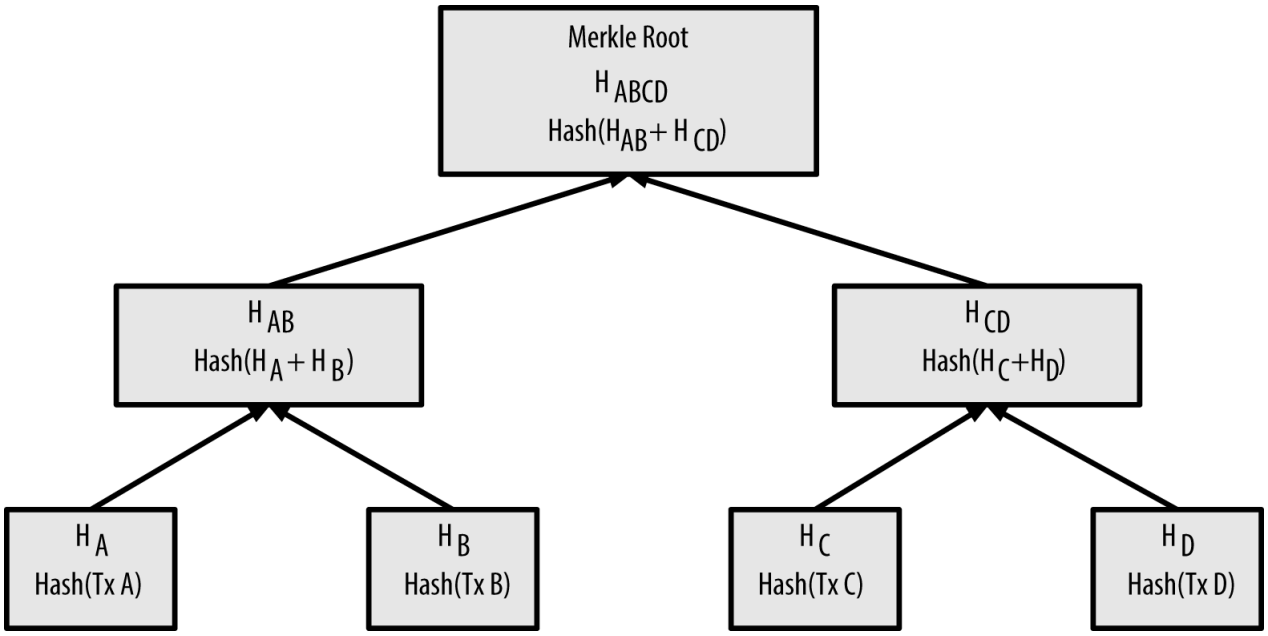

Рисунок 7 – Дерево Меркла

Дерева Меркла створюють загальний цифровий відбиток усього набору транзакцій. Дерево Меркла створюється шляхом рекурсивного хешування пар вузлів до тих пір, поки не залишиться лише один хеш, який називається коренем Меркла. Криптографічний хеш-алгоритм, який використовується в символічних деревах Меркла – це SHA256, застосовуваний двічі, також відомий як подвійний SHA256 [14].

Коли N елементів даних хешуються та підсумовуються в дереві Меркла, можна перевірити, чи певний елемент включений до дерева з кількістю обчислень не більше 2*log2(N), що забезпечує дуже ефективний спосіб перевірки, чи транзакція дійсно включена в блок. Дерево Меркла будується знизу вгору. На рисунку 8 побудова починається з чотирьох транзакцій, що позначаються як T_xA, T_xB, T_xC, T_xD. Ці транзакції не зберігаються в дереві Меркла, а лише їх дані хешуються, а отриманий хеш зберігається в кожному листовому вузлі – H_A, H_B, H_C і H_D.

Математичну функцію для отримання H_A можна розглядати як H_A = SHA256(SHA256(Транзакція A)), де транзакція A була криптографічно хешована двічі за допомогою SHA256.

Потім послідовні пари вузлів об’єднуються в батьківський вузол шляхом конкатенації двох хешів і хешування їх разом. Відповідно до прикладу, щоб побудувати батьківський вузол H_{AB}, два 32-байтових хеші дочірніх об’єднуються, щоб створити 64-байтовий рядок. Потім цей рядок подвійно хешується, щоб отримати хеш батьківського вузла: H_{AB} = SHA256(SHA256(H_A + H_B)) [15].

Дерево Меркла — це бінарне дерево. У випадку, якщо є непарна кількість транзакцій для підсумовування, хеш останньої транзакції буде продубльований.

Процес продовжується вгору, поки зверху не залишиться лише один вузол. Цей вузол відомий як корінь Меркла. 32-байтовий хеш зберігається в заголовку блоку і підсумовує всі дані у всіх чотирьох транзакціях. Використовуючи цей метод, дерево Меркла може підсумувати будь-яку кількість транзакцій у блоці до 32 байт.

Дерево Меркла дозволяє значно полегшити навантаження на мережу, так як при доказах правильності блоку потрібно пройти тільки по вітці з потрібним блоком. Немає необхідності перевіряти абсолютно всі блоки з підмножини. Спрощена перевірка економить енергозатрати і час. Це

вирішальне перевага хеш-дерев перед іншими схемами побудови хешей. Воно дозволяє наростити масштабування, пришвидшивши процеси перевірки.

Основні переваги дерев Меркла:

- Вони дають можливість довести цілісність та достовірність даних;
- Вони вимагають мало пам'яті або дискового простору, тому що докази в обчислювальному співвідношенні легкі та швидкі;
- Їхні докази та управління вимагають лише невеликої кількості інформації для передачі мережами.

Можливість довести, що ланцюг повний і узгоджений, необхідна для технології блокчейна і концепції розподіленої бази даних. Дерева Меркла допомагають перевірити, що пізніші версії журналу включають усі, починаючи з більш ранньої версії, і всі дані записуються і подаються у хронологічному порядку. Для підтвердження відповідності журналу потрібно показати, що попередні записи не були додані, змінені або підроблені, і що журнал ніколи не був розгалуженим або розгалуженим.

Дерева Меркла приносять користь майнерам та користувачам у блокчейні. Користувач може індивідуально перевірити частини блоків і може перевірити окремі транзакції, використовуючи хеші інших гілок дерева.

2.3 Алгоритми досягнення консенсусу

На відміну від традиційної бази даних, контрольованої адміністратором, публічний ланцюжок блоків є одноранговою децентралізованою мережею, в яку потенційно може зробити свій внесок будь-який учасник. Консенсус необхідний для функціонування такої розподіленої мережі з огляду на величезну кількість потенційних операторів вузлів: усі вони повинні узгодити стан мережі, щоб вона працювала належним чином.

У блокчейні, що є децентралізованою системою, яка не має єдиного управляючого органу, задля досягнення консенсусу розроблені різні алгоритми. У блокчейн-мережі немає значення, довіряють учасники системи одне одному чи ні. Вони мають домовитися про певні принципи роботи, які стосуватимуться всіх. І це пряма функція механізму консенсусу.

Алгоритмом консенсусу в блокчейні є набір певних математичних правил і функцій, які дозволяють досягти угоди між усіма учасниками та забезпечити працездатність мережі. Досягнення консенсусу стало основою математичної моделі побудови та розвитку блокчейн-технології [16].

У децентралізованій мережі можуть одночасно генеруватися кілька дійсних блоків. У результаті створюються розгалуження, які називають також форками. Форк – це зміна протоколу або відхилення від попередньої версії блокчейна [17]. Вибір однієї з гілок ланцюга блоків забезпечується алгоритмом консенсусу. На рисунку 8 продемонстровано сценарій розгалуження даних на різних вузлах мережі блокчейн.

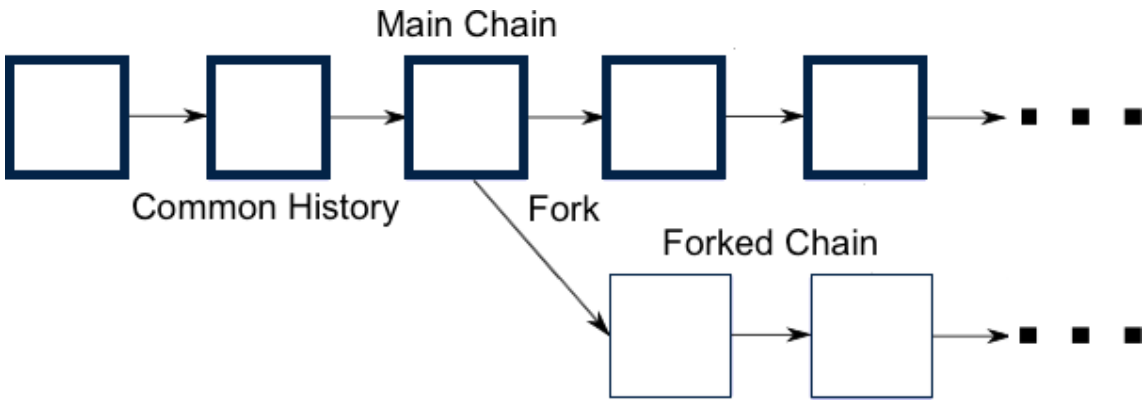

Рисунок 8 – Розгалуження у блокчейні

Існує два види розгалужень: м'які (soft forks) та жорсткі (hard forks).

Soft fork – це оновлення програмного забезпечення, яке має зворотну сумісність зі старими версіями [17]. Це означає, що учасники, які не

перейшли на нове програмне забезпечення (ПЗ), все одно можуть брати участь у процесах валідації та перевірки коректності транзакцій.

Реалізувати soft fork набагато простіше ніж hard fork, оскільки необхідно оновити лише клієнтське ПЗ. Всі учасники, незалежно від того, оновили вони ПЗ чи ні, продовжуватимуть розпізнавати нові блоки та підтримуватимуть сумісність із мережею.

Проте слід зазначити, що застаріла версія ПЗ впливає на функціональність. Учасники мережі із застарілим ПЗ, як і раніше, можуть бачити, що нові транзакції, що входять, дійсні, але проблема полягає в тому, що при додаванні нового блоку вони будуть відхилені блокчейн-мережею.

Hard fork – це оновлення програмного забезпечення, яке не має зворотної сумісності [17]. Всім учасникам необхідно перейти на нове програмне забезпечення, щоб продовжити брати участь у створенні нових блоків. Ті, хто не оновився, будуть відокремлені від мережі та надалі не зможуть перевіряти нові транзакції. Цей поділ призводить до постійного розходження блокчейн мереж. Доки в ланцюжку меншин є підтримка у вигляді учасників майнінгу, то два ланцюжки існуватимуть одночасно (наприклад: Bitcoin та Bitcoin Cash).

2.3.1 Алгоритм доказу виконаної роботи

Proof of Work (PoW, доказ виконання роботи). Протокол PoW пов'язаний з появою криптовалюти Bitcoin [18]. PoWє одним із ресурсномістких протоколів консенсусу. У цьому протоколі кожному вузлу необхідно обчислювати значення хеша змінного заголовоку блоку. У розподіленому середовищі всі вузли безперервно обчислюють значення хешу, використовуючи різні випадкові послідовності, які називаються "nonce". Загалом, рішенням є таким:

$$H(n \cup H(b)) < t,$$

де: H - це криптографічна хеш-функція (наприклад, SHA-256), n - значення "nonce", b - це поточний вміст блоку і t - час, що витрачається на знаходження нового блоку.

Наскільки швидко створюється блок залежить від того, наскільки складний ланцюг. Значення t не може бути дуже маленьким, так як це призводить до зайвих розгалужень у блокчейн мережі. Форки не тільки призводять до марнотратного витрачання ресурсів, але й мають негативні наслідки для безпеки, оскільки дозволяють реалізувати атаку подвійного витрачання.

Після отримання цільового значення хешу іншим учасникам необхідно взаємно підтвердити коректність хешу. Тоді транзакції, що зберігаються в новому блоці можуть бути перевірені у разі шахрайства. Таким чином з'являється новий блок у ланцюжку, який тісно пов'язаний із попереднім.

Вузли хеш-функцій, що обчислюють значення, називаються майнерами (miners), а сама процедура PoW називається майнінгом (mining). У цьому протоколі при виникненні розгалужень, коректним вважається той ланцюг, який довший.

Так як майнерам доводиться робити велику кількість комп'ютерних обчислень, які призводять до витрати ресурсів (електроенергії) розроблені більш ефективні протоколи, аніж PoW.

2.3.2 Алгоритми доказу володіння часткою

Proof of Stake (PoS) – доказ володіння часткою є більш ефективною альтернативою PoW. У протоколі PoS користувачам замість того, щоб обчислювати коректний "nonce" як у PoW необхідно довести право власності на кілька цифрових токенів. Вважається що користувачі з великою кількістю токенів менш схильні до атак на блокчейн мережу. У свою чергу

протокол PoS є несправедливим, оскільки один користувач з великою кількістю токенів обов'язково домінуватиме в мережі.

У зв'язку з цим розроблено нові модифікації відбору вузла мережі для створення наступного нового блоку. Зокрема, у Blackcoin використовується механізм рандомізації для прогнозування наступного вузла блоку [19]. Використовується формула, метою якої є знаходження найменшого значення хешу у комбінації з розміром частки. У роботі вузли з великою кількістю старих токенів мають велику ймовірність для створення нового блоку.

Багато блокчейн мереж спочатку використовували PoW для досягнення консенсусу, але поступово почали переходити на PoS. Наприклад, Ethereum планується перевести до нової реалізації Casper, яка в кінцевому підсумку перетворює Ethereum на блокчейн PoS (також відомий як Ethereum2.0) [18].

Також можна відзначити протокол Nxt – гібрид двох протоколів PoW та PoS [19]. Відмінною особливістю є те, що відбір вузла для генерації наступного блоку та право на підтвердження попереднього блоку обчислюється алгоритмом, який залежить від:

— хеша ідентифікатора попереднього блоку та відкритого ключа, який створив попередній блок;

— кількості токенів на рахунку користувача, підключеного до блокчейн мережі.

Ймовірність формування чергового блоку вище у користувача з більшим ефективним балансом на рахунку. Ефективним балансом вважається кількість токенів на рахунку користувача, що не змінювалося протягом останніх 1440 блоків.

Delegated Proof of Stake (DPoS) – делегований доказ володіння часткою є альтернативою консенсусам PoW і PoS. Протокол DPoS був

розроблений у 2014 р. у рамках проекту Graphene і вперше був задіяний у проекті Bitshares, пізніше у проекті Steemit [20].

Основний принцип роботи протоколу DPoS виглядає наступним чином: реалізовано поділ голосуючих та валідуючих вузлів, тобто учасники мережі, які мають право голосу в системі (утримувачі токенів) не є валідаторами транзакцій. Таким чином, одну підмножину учасників обирає інша підмножина, яке в свою чергу буде формувати блоки.

Умови, в яких працює даний алгоритм консенсусу, кардинально відрізняються від умов, у яких працюють протоколи PoW та PoS. А саме, валідаторам необхідно розкрити свої особи та заявити про готовності безперебійно підтримувати роботу повноцінного вузла мережі, своєчасно виконувати верифікацію транзакцій та формувати нові блоки.

2.3.3 BFT-орієнтовані протоколи

Досі були розглянуті протоколи консенсусу, які використовуються у відкритих БС, які працюють у відкритому середовищі та націлені на децентралізацію. Застосування вищерозглянутих протоколів у корпоративному секторі не є можливим так як вони мають низьку пропускну здатність.

Для збільшення продуктивності було розроблено новий клас протоколів консенсусу – Byzantine Fault Tolerance (PBFT), в яких анонімність не є важливим аспектом, тобто вузли знають інформацію про один одного (спочатку вузли автентифіковані). Завдяки цьому можна оптимізувати алгоритми консенсусу та досягти набагато більшої пропускної спроможності. Фактично швидкість може збільшитись у 10 разів, від сотень до тисяч транзакцій за секунду, що відмінно підходить для корпоративних реалій.

Practical Byzantine Fault Tolerance (PBFT) – є швидким і легко масштабованим протоколом консенсусу. Широко використовується в

проекті Hyperledger Fabric як протокол консенсусу, оскільки може обробляти до 1/3 нелегітимних транзакцій [19].

Принцип роботи протоколу виглядає так: на вхід валідатора надходить повідомлення, за яким йому потрібно прийняти рішення – вважати його істинним чи ні. Для цього валідатор виконує внутрішні перевірки, потім по черзі опитує інші вузли, чи дійсна транзакція. Якщо 2/3 учасників проголосують за цю транзакцію як коректну, валідатор приймає її та передає своє рішення в блокчейн мережу іншим валідаторам. Також необхідно зазначити, що у PBFT відсутня процедура хешування [19].

Delegated Byzantine Fault Tolerance (DBFT) – це делегований алгоритм консенсусу, стійкий до відмови з великим масштабуванням мережі. Цей алгоритм запропонувала команда розробників NEO на чолі з Еріком Чжаном, а у 2016 р. застосували його у проекті NEO [20]. Принцип роботи такий, що власники крипто-токенів обирають вузли погодження, які поділяються на спікерів та делегатів. Вузли-спікери відповідають за проведення транзакцій та формування блоків у мережі, а вузли-делегати відповідають за перевірку перших (вузлів-спікерів) для досягнення консенсусу. Тому алгоритм став вдалим рішенням, яке поєднує в собі безпеку та масштабування мережі. Але на тлі швидкості є можливість централізації. Це пов'язано з тим, що більша половина вузлів може бути зосереджена в одних руках [19].

Federated Byzantine Agreement (FBA) – протокол, який не вимагає дозволу чи заздалегідь відомого набору учасників, на відміну від PBFT та інших варіацій BFT. Транзакції у цьому протоколі перевіряються фіксованою кількістю учасників, які вибираються зі списку вузлів мережі, що перебувають у активному стані. Необхідно зазначити, що за правилами FBA існують шлюзи (gateways) та мейкери (market-makers), які забезпечують чесність та ліквідність мережі. Перші виступають у ролі традиційних банків, які володіють фінансовими коштами та створюють їх

еквівалент у цифрових токенах. Другі – ведуть облікові записи з численними шлюзами і у кількох валютах [20].

XRP Ledger Consensus Protocol (XRP Ledger) – це алгоритм консенсусу мережі XRP Ledger, який відповідає за згоду між серверами. Алгоритм здатний досягти консенсусу без повної згоди щодо того, які вузли є членами мережі. Розробником алгоритму стала компанія Ripple Labs Inc, яка запустила його в 2012 р. [21]. Принцип роботи такий, що реєстр XRP Ledger складається з серверів відстеження та валідаторів. Сервера відстеження розподіляють транзакції та відповідають на запити про стан реєстру, валідатори відповідають за обробку транзакцій. XRP Ledger використовує процес консенсусу для забезпечення того, що транзакції обробляються, а перевірені реєстри є узгодженими по розподіленій мережі.

2.3.4 Порівняльний аналіз протоколів досягнення консенсусу

Кожен протокол консенсусу має переваги і недоліки. Хороший протокол консенсусу має бути в ідеалі ефективним, безпечним та зручним у використанні. У поширених протоколах консенсусу досі дослідники існують вразливості, які можуть негативно вплинути на працездатність блокчейн мережі. Тому розробляються нові рішення, створені задля усунення знайдених недоліків.

У таблиці 1 наведено результати порівняльного аналізу розглянутих протоколів консенсусу.

Таблиця 1 – Порівняльний аналіз протоколів досягнення консенсусу

Протокол консенсусу	Тип блокчейн Мережі	Продуктивність	Розроблені рішення
PoW	Відкрита	низька	Bitcoin-NG, Byzcoin, Bitcoin
PoS	Відкрита	висока	Tendermint, Ethereum
DPoS	Відкрита	висока	EOS, BitShares
BFT	Закрита	висока	Hyperledger Fabric 1.0
PBFT	закрита з дозволами	висока	Hyperledger, Chain
PBFT - орієнтовані	Закрита	висока	Parallel BFT, Optimistic BFT
DBFT	Закрита	дуже висока	NEO, TON
FBA	Закрита	висока	Stellar
XRP	Закрита	висока	Ripple
Інші	Відкриті	-	Інші протоколи, засновані на PoW, що мають форму Proof of X, наприклад: Proof of Space, Proof of Activity, Proof of Authority та ін.

2.4 Класифікація блокчейн мереж

Блокчейн-проекти постійно видозмінюються і вдосконалюються, і навіть користуються розробками одне одного, оскільки більшість з них

засновані на відкритому вихідному коді. Майже будь-яка БС має свої особливості та ознаки, а також досить чітко окреслені рамки можливого застосування.

Найкоректнішим поділом блокчейн мереж прийнято вважати їх поділ за рівнем відкритості, таким чином їх можна розділити на публічні (відкриті), приватні та гібридні мережі [22]. Ступінь відкритості найчастіше залежить від кількох факторів. Одним із найбільш значущих факторів є доступність вихідного коду протоколу БС.

Наступним значущим фактором є можливість вільного підключення нового вузла до мережі без отримання будь-яких дозволів. Ця властивість є основною визначальною відмінністю відкритої блокчейн мережі від закритої. На сьогодні більшість БС є публічними та у більшості з них для досягнення консенсусу використовується протокол Proof of Work.

Для підключення нових користувачів у публічних блокчейн мережах достатньо лише завантажити сумісну з даною версією протоколу клієнтський додаток та встановити зв'язок з іншими вузлами мережі. Рівень участі користувача завжди визначається ним самим і залежить лише від його особистих (фінансових та апаратних) ресурсів. Необхідно також зазначити, що ніхто з користувачів публічної БС не може відключити інших користувачів від розподіленої мережі, оскільки всі учасники є рівноправними.

У закритих БС підключення та відключення користувачів регулюються певними вузлами або групою вузлів, що мають більш високий рівень повноважень порівняно з рештою учасників мережі.

2.4.1 Публічний блокчейн

Публічний блокчейн нерозривно пов'язаний з криптовалютами. Будучи базовим сценарієм, який сформував технологію в її поточному вигляді, криптовалюти та супутні фінансові інструменти продовжують

активно розвивати технологію та вирішувати архітектурні обмеження перших реалізацій. З іншого боку, капітал завжди привертає значну увагу зловмисників, і публічні блокчейн-мережі, що генерують та обслуговують цифрові активи, постійно зазнають різноманітних атак.

Найпоширеніші атаки безпосередньо не впливають на блокчейн-мережі. Вони мають на меті розкрадання активів, доступ до яких забезпечується за допомогою приватного ключа.

Кожна транзакція (наприклад, переклад криптовалюти з одного гаманця до іншого) всередині блоку підписується асиметричним електронним підписом. Цей додатковий криптографічний шар потрібен у публічній мережі, де учасники анонімні та не довіряють один одному.

Використання асиметричного механізму цифрового підпису відрізняється від традиційного асиметричного шифрування. Підпис здійснюється закритим або приватним ключем, а перевірка підпису — відкритим або публічним ключем (перевірити підпис транзакції може будь-який учасник). Значення відкритого ключа обчислюється на основі закритого ключа, а ось зворотне перетворення вимагає поки що практично неможливий обсяг обчислень.

Приватний ключ генерується користувачем, і забезпечує доступ до адреси в блокчейні, де може зберігатися цифровий актив. Знаючи значення приватного ключа, користувач фактично володіє і може розпоряджатися цифровим активом, закріпленим за ним. Публічний ключ використовується як адреса блоку або гаманця, а також як автентифікація підпису інформації в інших блоках іншими учасниками мережі. Можна сказати, що пара публічного та приватного ключа є блокчейн-гаманцем.

Вектор атаки, спрямований на отримання доступу до приватного ключа, безпосередньо не пов'язаний з блокчейн-мережею. Тим не менш, ступінь цього ризику намагаються знизити, зокрема, за допомогою архітектури блокчейн-мережі. Зокрема, набирають популярності

децентралізовані послуги, які принципово відрізняються від традиційних криптобірж. Вони не зберігають приватні ключі та персональні дані на своїх серверах і виступають у ролі посередників для зіставлення заявок на купівлю та продаж активів.

Додатковий захист цифрових активів реалізується також за допомогою технології мультипідпису. Фактично це вимога кількох підписів для підтвердження транзакції. Участь у процесі підтвердження транзакції кількох користувачів із приватними ключами, що зберігаються окремо, значно збільшує захист гаманця.

Архітектура, криптографічні функції та алгоритми консенсусу децентралізованої блокчейн-мережі також можуть бути потенційно проексплуатовані, тим самим наражаючи на загрозу базовий принцип блокчейна – незмінність даних. Нижче наведено основні види атак на інфраструктуру публічних блокчейн-мереж. Багато хто з них існують поки що в теорії та обговорюються як концептуальні.

Атака 51%. Концепція, при якій контроль над понад 50% ресурсами блокчейн-мережі, дозволяє створити свій форк, який замінить поточний реєстр блокчейну (блоки інших учасників тоді перестануть підтверджуватись) та стане актуальним. Окремим підвидом є атака дальньої дії (англ. Long-range attack), сенс якої полягає в тому, щоб почати збирати хибний форк задовго до актуального блоку. У деяких видах консенсусу це коштуватиме менше ресурсів. Залежно від алгоритму консенсусу, реалізація атаки відрізнятиметься. На даний момент виділяється дві основні групи алгоритмів: на основі доказу роботи (Proof-of-Work) та на основі підтвердження частки (Proof-of-Stake). У разі першого алгоритму (напр., Bitcoin та Ethereum) атакуючому потрібно заволодіти 51% обчислювальних ресурсів мережі. У випадку з Proof-of-Stake (напр., Tezos та Waves), для реалізації атаки 51% атакуючого потрібно заволодіти 51% основного активу мережі. Варто відзначити, що для розвинених і справді децентралізованих

мереж, таких як Bitcoin і Ethereum, подібна атака залишається дуже дорогою – для її успішної реалізації потрібна величезна обчислювальна потужність, порівнянна з сотнями суперкомп'ютерів. Однак у менш масштабних мережах такі атаки є цілком реальними. Зокрема, влітку 2020 року було проведено дві атаки 51% на блокчейн Ethereum Classic – форк оригінального Ethereum, який стався після зламування DAO у 2016 році.

Атака Сивілли. Вид атаки в однорангових мережах, коли зловмисник наповнює мережу підконтрольними йому вузлами, до яких підключаються вузли інших учасників. Атакуючий оточує вузол жертви так, щоб мати контроль над усіма вихідними та вхідними транзакціями. У великих децентралізованих мережах таку атаку реалізувати дуже складно, оскільки вузол учасника для підтвердження транзакції вибирає інший вузол мережі практично випадково. Хоча процес з'єднання практично рандомізований, можна зламати журнал довірених адрес жертв – він міститиме адреси вузлів зловмисника. Атака Сивілли дозволяє відключати інших користувачів від мережі, спостерігати за їх транзакціями або реалізовувати «подвійну витрату».

Злом підписів та хеш-функцій. У блокчейн-мережах використовуються різні криптографічні механізми, багато з них (наприклад, алгоритми SHA-256 та ECDSA) вважаються вкрай стійкими до злому поточним поколінням обчислювальних потужностей. Але поява квантових комп'ютерів дозволить долати нинішню стійкість, і в результаті зламувати механізми, що лежать в основі блокчейну, насамперед ЕП. До речі, вже починає розроблятися постквантова криптографія. Наприклад, команда Quantum Resistant Ledger створює блокчейн-систему, криптостійку до квантових атак.

Підсумовуючи види загроз для публічних блокчейн-мереж вразливими складовими блокчейн-стеку та рішеннями на його базі є:

- інтерфейсні компоненти, користувацькі програми (наприклад, гаманці) та централізовані рішення (наприклад, біржі). Зламування цих систем в більшості випадків призводить до захоплення приватного ключа;
- вузли мережі;
- ключі та криптографічні функції.

Багато з описаних вище загроз також можуть бути актуальними і для приватних блокчейнів, але корпоративні сценарії мають власні особливості забезпечення інформаційної безпеки.

2.4.2 Приватний блокчейн

Приватний блокчейн — це закритий блокчейн. Приватні блокчейни працюють на основі контролю доступу, який обмежує людей, які можуть брати участь у мережі. Є одна або кілька організацій, які контролюють мережу, і це призводить до того, що транзакції залежать від третіх сторін. У приватному блокчейні тільки суб’єкти, які беруть участь у транзакції, матимуть інформацію про неї, тоді як інші не зможуть отримати до неї доступ.Очевидно, що приватний блокчейн забезпечує кращий контроль над інфраструктурою з боку організації чи групи компаній. Це стосується як загальних IT-аспектів (наприклад, можливість швидко оновити функціональність), так і аспектів ІБ. Модель загроз для рішень, що працюють на приватному блокчейні, вже не включає ряд атак, актуальних для публічного блокчейну. Так, незважаючи на порівняно малий розмір розподіленої блокчейн-мережі, атака 51% або атака Сівіли стають важкими для виконання – всі вузли знаходяться під контролем у довірених зонах. Гіпотетично зловмисник може отримати доступ і до підконтрольного вузла, але в такому разі вартість атаки багаторазово зростає через необхідність подолання корпоративного периметра різних організацій та засобів ІБ, що використовуються.

Контроль доступу є базовою функцією приватної блокчейн-мережі, без дозволу оператора мережі не з'явиться новий учасник. Це забезпечує доступність інформації у класичному розумінні ІБ – доступ до інформації мають лише авторизовані учасники.

Іншою особливістю приватних мереж є можливість використання алгоритмів консенсусу для довіреної мережі. Оптимізуючи консенсус за допомогою полегшених протоколів взаємодії між автентифікованими учасниками мережі, можна досягти більшої пропускної спроможності та масштабованості. Пропускна здатність блокчейн-мереж та розподілених баз даних вимірюється транзакціями за секунду. Для порівняння, у публічних мережах на основі алгоритму консенсусу доказу роботи за секунду обробляються десятки транзакцій, тоді як у алгоритмах швидкого консенсусу це сотні та тисячі транзакцій. До них відносяться Byzantine/Crash Fault Tolerance, Raft, консенсус на основі підтвердження повноважень (Proof-of-Authority) та інші. Консенсуси, що застосовуються у приватних мережах, не підходять для складних економічних моделей, але забезпечують цілісність та доступність інформації за рахунок швидкої та надійної синхронізації у довіреній мережі.

Конфіденційність даних у приватних блокчейнах реалізується з контролем прав читання записів реєстру. Більш того, деякі приватні блокчейн-платформи дають змогу використовувати додаткові інструменти захисту даних. Можливий сценарій, у якому кілька учасників приватної блокчейн-мережі повинні зробити транзакції так, щоб інші учасники цієї мережі не могли їх бачити, навіть у зашифрованому вигляді.

2.4.3 Гібридний блокчейн

Гібридний блокчейн знаходиться на межі між публічними та приватними ланцюгами, поєднуючи елементи обох. Найбільш помітну відмінність від будь-якої системи можна спостерігати на рівні консенсусу.

Замість відкритої системи, в якій кожен може перевіряти блоки, або закритої, в якій тільки одна особа призначає валідатора, гібридний ланцюг розглядає відразу кілька рівнозначних сторін як валідаторів.

Гібридний блокчейн пропонує такі функції як цілісність, прозорість та безпека. Члени гібридного блокчейну приймають рішення щодо того, хто може брати участь у блокчейні та які транзакції будуть публічними.

Незважаючи на те, що транзакції в гібридному блокчейні не є публічними, за необхідності вони можуть перевірятись. Кожна транзакція, яка відбувається в гібридному блокчейні, може бути приватною і водночас відкритою для перевірки, якщо це необхідно. Але найголовнішу роль роботі блокчейна грає незмінність: кожна транзакція записується один раз і може бути змінена.

Гібридний блокчейн забезпечує кращу безпеку порівняно з публічним чи приватним блокчейном, тому що навіть група осіб, яка його контролює, не може змінити саму особливість блокчейну – незмінність, і тим самим не може підірвати безпеку транзакцій. Члени блокчейну можуть лише вирішувати, які транзакції є публічними, а які ні.

Як тільки користувач отримує доступ до гібридного блокчейну, він може повністю взяти участь у діяльності самого блокчейну. Однак особистість користувачів зберігається у секреті від інших учасників. Це робиться для захисту конфіденційності користувачів. Особи користувачів розкриваються тільки тоді, коли вони взаємодіють один з одним і тільки їм, сторонам, що взаємодіють.

Однак, незважаючи на те, що особа користувачів гібридних блокчейнів має обмежену анонімність у межах мережі (розкривається при взаємодії з іншими користувачами), за межами мережі зберігається повна анонімність користувачів гібридного блокчейну.

Гібридна блокчейн-мережа надає всі функції публічного блокчейну, такі як безпека, прозорість, незмінність та децентралізованість, проте водночас обмежує можливість безперешкодного доступу до транзакцій.

Враховуючи усі свої особливості, гібридна мережа блокчейну має ряд переваг:

- Робота в закритій екосистемі. Перевагою гібридного блокчейна є його здатність працювати у закритій екосистемі. Це означає, що компаніям чи організаціям не потрібно турбуватися про витік інформації.
- Захист від атаки 51%. Гібридний блокчейн несприйнятливий до атаки 51%, тому що хакери не можуть отримати доступ до мережі для проведення атаки.
- Захист конфіденційності та водночас взаємодія із зовнішнім світом. Незважаючи на те, що приватні блокчейни найкраще підходять для питань, пов'язаних із конфіденційністю, вони обмежені, коли справа доходить до взаємодії із зовнішнім світом. Тому багатьом компаніям, які працюють на приватному блокчейні, потрібно мати ще й блокчейн для зв'язку з усіма своїми акціонерами та громадськістю.
- Ще однією додатковою перевагою використання гібридного блокчейна є низька вартість транзакцій. Транзакції мають бути дешевими, оскільки для їх перевірки потрібно лише кілька нод. Перевіркою транзакцій у гібридній блокчейн-мережі займаються лише найвпливовіші ноди, у публічному блокчейні для цього можуть знадобитися тисячі нод.

2.5 Смарт-контракти

Смарт-контракт – інструмент, який формалізує і захищає комп'ютерні мережі шляхом об'єднання протоколів з інтерфейсом користувача [23].

Смарт-контракти дозволяють створювати протоколи, де обидві сторони можуть взяти на себе зобов'язання через блокчейн мережу, без знання чи довіри одна до одної. Учасники даного процесу можуть не турбуватися про правильність виконання зобов'язань, оскільки якщо умови не будуть задоволені, контракт анулюється. Зазвичай смарт-контракти створюються на базі Ethereum, так як це одна з найнадійніших криптоплатформ.

Смарт-контракти працюють, дотримуючись простих операторів, які записуються в код у ланцюжку блоків. Мережа комп'ютерів виконує дії, коли певні умови виконані та перевірені. Ці дії можуть включати виділення коштів відповідним сторонам, реєстрацію транспортного засобу, надсилання повідомлення, видачу квитка та багато іншого. Після завершення транзакції блокчейн оновлюється. Це означає, що транзакцію не можна змінити, і лише сторони, яким було надано дозвіл, можуть бачити результати.

У смарт-контракті може бути стільки умов, скільки необхідно, щоб учасники переконалися, що завдання буде виконане задовільно. Щоб встановити умови, учасники повинні визначити, як транзакції та їх дані представлені у ланцюжку блоків, узгодити правила, які регулюють ці транзакції, вивчити всі можливі винятки та визначити структуру для вирішення суперечок.

Потім смарт-контракт може бути запрограмований розробником – хоча все частіше організації, які використовують блокчейн для бізнесу, надають шаблони, веб-інтерфейси та інші онлайн-інструменти для спрощення структурування смарт-контрактів.

Переваги смарт-контрактів [23]:

- Швидкість, ефективність та точність. Як тільки умову виконано, контракт негайно виконується. Оскільки смарт-контракти є цифровими та автоматизованими, немає необхідності обробляти

документи та не витрачати час на узгодження помилок, які часто виникають через ручне заповнення документів.

- Довіра та прозорість. Оскільки третя сторона не задіяна, а зашифровані записи транзакцій спільно використовуються учасниками, немає необхідності сумніватися в тому, чи було змінено інформацію для особистої вигоди.
- Безпека. Записи транзакцій блокчейна зашифровані, що ускладнює їх злам. Більше того, оскільки кожен запис пов'язаний з попереднім і наступним записами в розподіленому реєстрі, хакерам доведеться змінити весь ланцюжок, щоб змінити один запис.
- Економія. Смарт-контракти усувають необхідність у посередниках для обробки транзакцій та, як наслідок, пов'язаних з ними тимчасових затримок та комісій.

Проте, смарт-контракти також мають ряд вразливостей. Вразливості дозволяють маніпулювати кодом та викрасти максимально можливі суми за короткий час.

Однією із вразливостей є можливість цілочисельного переповнення (integer underflow). З її допомогою зловмисник без коштів на рахунку може відправити один токен і отримати у відповідь мільярди токенів. Друга вразливість цілого переповнення полягає в тому, що коли баланс досягає максимального значення і атакуючий отримує один токен, все починається заново.

Третя вразливість – незахищене зняття коштів. Через неналежний механізм контролю доступу будь-хто може зняти кошти з контракту.

Четверта вразливість – незахищене самознищення, що дозволяє сторонньому атакуючому «вбити» контракт та надіслати кошти на будь-яку адресу.

Вразливості, безумовно, можуть заподіяти шкоду багатьом користувачам, залежно від того, чи вони тримають криптовалюту на основі Ethereum або токени на онлайн-платформі, що зберігає гроші. Якщо зловмисник створить шкідливий смарт-контракт і атакує платформи, які містять смарт-контракт, користувачі ризикують втратити гроші.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі роботи розглянута та проаналізована технологія Blockchain, її архітектура та особливості. На основі отриманих результатів зроблено висновок про ряд переваг технології блокчейн, а саме: незмінність, децентралізація, прозорість та конфіденційність.

Проведено порівняльний аналіз 3-х типів протоколів досягнення консенсусу, а також публічних, приватних та гібридних блокчейн-мереж. Окрім цього, визначено основні переваги, проблеми та недоліки видів блокчейну. Досліджено, що найдоцільнішим видом для захисту інформації являється гібридний blockchain, у якому ланцюги блоків поєднують переваги обох видів технології, намагаючись при цьому обмежити недоліки, та завдяки чому забезпечують усі аспекти інформаційної безпеки. Враховуючи вище наведено інформацію, гібридний blockchain є безпечним та надійним способом для захисту інформаційної безпеки.

Розглянуто смарт-контракти, що написані на основі публічної блокчейн-мережі та мають ряд недоліків у сфері забезпечення інформаційної безпеки. Тому, зроблено висновок про те, що смарт-контракти на основі гібридної блокчейн-мережі зможуть забезпечити відсутність цих недоліків та стануть відмінним методом для безпечної передачі інформації.

3. РОЗРОБКА ТА ТЕСТУВАННЯ ПРОГРАМНОГО ПРОДУКТУ

3.1 Solidity для розробки смарт-контракту

Solidity – це мова програмування високого рівня створена для реалізації смарт-контрактів. Смарт-контракти представляють собою програмне забезпечення, що працює в мережі Ethereum та дозволяють автоматизувати процес виконання угод та забезпечують контроль над їх виконанням [24]. На Solidity сильно повливали C++, Python і JavaScript, мова була розроблена для Ethereum Virtual Machine (EVM). EVM описується як віртуальний комп'ютер у ланцюжку блоків, який перетворює ідеї людей на код, що запускає програми у блокчейн мережі [25].

Мова була розроблена так, щоб програмісти, які вже знайомі з однією або декількома сучасними мовами програмування, могли з легкістю опанувати дану мову.

По суті, це мова з компілятором, який бере високорівневий код, що легкий для розуміння людині, і розбиває його на прості інструкції, які складають основу будь-якої програми мікропроцесора, що виконується. Solidity схожий на одну з найпоширеніших мов програмування – JavaScript. Як мова високого рівня, Solidity позбавляє необхідності вводити код у вигляді одиниць та нулів. Людям стає набагато простіше писати програми так, як їм простіше зрозуміти, використовуючи комбінацію літер та цифр.

Solidity має статичну типізацію з підтримкою успадкування, бібліотек та складних для користувача типів. Оскільки Solidity є статичним типом, користувач може вказати кожну змінну. Типи даних дозволяють компілятор перевіряти правильність використання змінних. Типи даних Solidity зазвичай поділяються на типи значень чи типи посилань.

Основна відмінність між типами значень і типами посилань полягає в тому, як вони присвоюються змінною і зберігаються в EVM (віртуальній машині Ethereum). Хоча зміна значення в одній змінній типу значення не

впливає на значення в іншій змінній, будь-хто, хто посилається на змінені значення в змінних типу посилання, може отримати оновлені значення.

Смарт-контракти, створені з використанням Solidity, можна розглядати як спосіб автоматизації ділових та не пов'язаних із бізнесом процесів між різними людьми. Це гарантує, що людям, які здійснюють транзакції в блокчейні, не доведеться турбуватися про такі ризики, як шахрайство або неможливість використати ту саму валюту.

Саме мова програмування Solidity обрана для написання смарт-контракту у даній роботі. Використовуватиметься найновіша версія мови 0.8.10, оскільки, остання версія містить в собі виправлення безпеки, у ній запровадженні критичні зміни та додано нові зручні функції.

3.2 Створення блокчейн мережі

Існують різні реалізації блокчейнів, серед яких найпопулярнішими зараз є Bitcoin та Ethereum. У той час як Bitcoin — це реалізація криптовалюти на базі blockchain, метою Ethereum є створення платформи, що дозволяє вирішувати найрізноманітніші завдання за допомогою розумних контрактів. Крім цього, мережа Ethereum може використовуватися для тестування та експериментів із блокчейном.

Як і всі блокчейн-платформи, платформа Ethereum функціонує завдяки вузлам мережі, які використовують розроблене під дану платформу програмне забезпечення. У випадку з платформою Ethereum, таким програмним забезпеченням є Ethereum Virtual Machine.

EVM можна назвати середовищем виконання контрактів Ethereum, оскільки їх код виконується саме нею. Віртуальна машина Ethereum повністю ізольована від глобальної мережі, що не тільки робить значний внесок у безпеку, але й дозволяє створювати та тестувати смарт-контракти локально.

Основне завдання EVM – виконання коду смарт-контракту. Однак EVM працює не з кодом, написаним мовою високого рівня, а з так званим EVM байт-кодом, який попередньо компілюється вихідний код контракту. Саме байт-код EVM зберігається у реєстрі. Цей байт-код є 16-терічним рядком, який є представленням кодів операцій та операндів.

Кожній операції відповідає вартість її виконання, так званий gas. Ця особливість EVM, вимога плати за кожну операцію, гарантує захист від DoS атак, що є найбільш популярним способом атаки в даний час. Кожен вузол у мережі Ethereum виконує одні й ті ж обчислення і зберігає одні й самі значення. Така надмірність якраз і дозволяє досягти консенсусу всередині мережі. Однак ця надмірність також є причиною, через яку виконання цих обчислень стає сильно ресурсомістким. Для того щоб мотивувати вузли, виконувати такі обчислення в мережі Ethereum, існує поняття плати за обчислення: кожна операція, що виконується має свою конкретну вартість, що виражається у так званій кількості gas'a.

Щоб запустити блокчейн, комп'ютер повинен стати вузлом у мережі Ethereum, тобто потрібно завантажити весь блокчейн мережі та синхронізувати його з основним ланцюжком Ethereum. Для цього можна використовувати різні інструменти (клієнти). За допомогою цих інструментів можна отримати доступ до консолі (терміналу) – середовища JavaScript, що містить всі основні функції, які нам знадобляться пізніше. Доступ до консолі – основне, що потрібно для запуску блокчейну Ethereum. У даній роботі обрано клієнт Go Ethereum.

Go Ethereum (або geth) це одна з трьох початкових реалізацій протоколу Ethereum (поряд з C++ та Python). Вона написана на Go, повністю відкрита та ліцензована під GNU LGPL v3. Go Ethereum можна завантажити або як окремий клієнт, що працює практично в будь-якій ОС, або як бібліотеку для вбудовування у проекти Go, Android чи iOS. З Geth можна здійснювати транзакції, створювати смарт-контракти, децентралізовані

програми, створювати приватні блокчейни та досліджувати історію блоків, а також багато іншого [26].

Розробка відбувається на комп’ютері з Ubuntu Linux – операційною системою для персональних комп'ютерів. На комп’ютер встановлюється Go Ethereum за допомогою команд зображених на рисунку 9.

```
$ sudo apt-get install software-properties-common
$ sudo apt-get install build-essential
$ sudo add-apt-repository -y ppa:ethereum/ethereum
$ sudo apt-get update
$ sudo apt-get install ethereum
```

Рисунок 9 – Установка Go Ethereum

Після написання вищеперерахованих команд було установлено Geth 1.10.13 та Go 1.17.14. (рис. 10).

```
inna@inna-PC ~ $ geth version
Geth
Version: 1.10.13 - stable
Git Commit: 6d74d1e5f762e06a6a739a42261886510f842778
Architecture: amd64
Protocol Versions: [65 64 63]
Go Version: go1.17.14
Operating System: linux
GOPATH=
GOROOT=/build/ethereum-TMvmgM/.go
```

Рисунок 10 – Версії установлених утиліт

Для реалізації смарт-контракту необхідно мати приватний блокчейн, який використовується для генерації хеша транзакцій та який пізніше перевірятиметься за допомогою загальнодоступного блокчейну.

Після встановлення та синхронізації Geth з Ethereum, можна запустити приватну тестову мережу. Це найкращий спосіб для вивчення технологій блокчейну, тому що в рамках приватної мережі Ethereum можна створювати, розгортати та тестувати смарт-контракти та децентралізовані програми, не витративши жодної монети реального ефіру.

Враховуючи отриману в попередніх розділах інформацію, відомо про те, що кількість блоків необмежена, але завжди є один окремий блок, який дає початок всьому ланцюжку – це генезис-блок.

Щоб створити приватний блокчейн, спочатку необхідно згенерувати цей блок. Для цього потрібно створити файл Genesis, прописати до нього потрібні команди (атрибути) та використовувати його за допомогою Geth (рис.11).

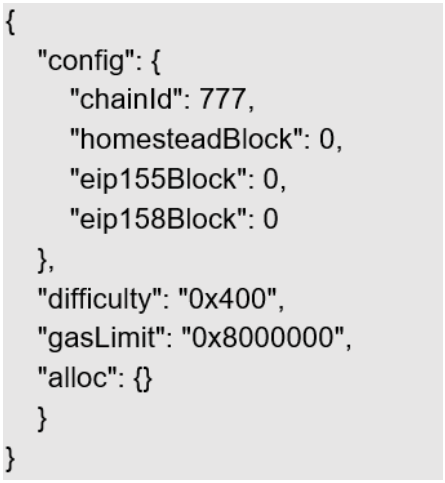

Рисунок 11 – Початкові установки для створення генезисного блоку

Прописані конфігурації означають наступне:

- config. Визначає конфігурацію блокчейна. Не налаштовує нічого конкретного для самого блоку генезису, але визначає те, як працюватиме мережа.
- chainId. Ідентифікатор використовуваного блокчейна (щось на зразок адреси). Можна вказати випадкове число за умови, що воно не збігається з номерами кількох важливих блокчейнів, наприклад номер основного ланцюжка Ethereum (1). В інструкції вказано випадковий тризначний ідентифікатор (777).
- HomesteadBlock. Homestead – перша офіційна стабільна версія протоколу Ethereum, яка замінила попередню версію під назвою Frontier. Для того щоб використати цей реліз, атрибут має бути

заданий як "0". Можна підключити й інші протоколи, наприклад, Byzantium, eip155B і eip158.

- difficulty. Визначає складність створення блоків. Чим вище складність, тим більше буде потрібно ресурсів для майнінгу. Щоб уникнути очікування під час тестів та написання даного ланцюга було встановлено відносно невисоке значення складності.
- gasLimit. Вказує поточний мережевий ліміт витрат газу блок. Газ – це «паливо», яке використовується для оплати трансакційних комісій у мережі Ethereum. Чим більше газу користувач готовий витратити, тим вищий пріоритет його транзакції у черзі.
- alloc. Дозволяє створити криптовалютний гаманець для створеного приватного блокчейну та наповнити його ефіром.

Створити genesis-файл з потрібними атрибутами можна за допомогою будь-якого текстового редактора, наприклад Notepad. Назва генезисного може бути будь-якою, головне — вказати розширення «json».

Після створення genesis-файлу у Geth вводиться наступна команда: “geth–identity–init/folder/genesis.jsondatadir/data_directory/ACPrivateChain”. Атрибут "folder" – це папка, в якій збережено genesis-файл. Тоді як атрибут data_directory вказує на папку, в якій будуть зберігатися дані приватного ланцюжка. Ця команда інструктує Geth використовувати раніше створений файл genesis.json для створення першого блоку приватного блокчейна Ethereum.

Після запуску даної команди Geth підключається до genesis-файлу і підтверджує успішне завершення дії (рис. 12).

Рисунок 12 – Успішне підключення генезис блоку

Створивши генезис-блок, можна запустити приватну мережу, щоб інші вузли могли додавати нові блоки. Для цього в консолі Geth потрібно ініціювати команду: “geth –datadir/data_directory/ACPrivateChain –networkid 7755”. Ця команда інструктує Geth на запуск приватного блокчейну. У команді також є ідентифікатор «7755». Це довільне число, яке не дорівнює ідентифікатору вже створених мереж, наприклад ідентифікатору основної мережі Ethereum («networkid=1»).

Існує список ідентифікаторів існуючих мереж блокчейна Ethereum, які не можна використовувати при створенні власної мережі(рис. 13).

- **0**: Olympic, Ethereum public pre-release PoW testnet
- **1**: Frontier, Homestead, Metropolis, the Ethereum public PoW main network
- **1**: Classic, the (un)forked public Ethereum Classic PoW main network, chain ID 61
- **1**: Expanse, an alternative Ethereum implementation, chain ID 2
- **2**: Morden Classic, the public Ethereum Classic PoW testnet
- **3**: Ropsten, the public cross-client Ethereum PoW testnet
- **4**: Rinkeby, the public Geth-only PoA testnet
- **5**: Goerli, the public cross-client PoA testnet
- **6**: Kotti Classic, the public cross-client PoA testnet for Classic
- **8**: Ubiq, the public Gubiq main network with flux difficulty chain ID 8
- **42**: Kovan, the public Parity-only PoA testnet
- **60**: GoChain, the GoChain networks mainnet
- **77**: Sokol, the public POA Network testnet
- **99**: Core, the public POA Network main network
- **100**: xDai, the public MakerDAO/POA Network main network
- **31337**: GoChain testnet, the GoChain networks public testnet
- **401697**: Tobalaba, the public Energy Web Foundation testnet
- **7762959**: Musicoin, the music blockchain
- **61717561**: Aquachain, ASIC resistant chain
- [**Other**]: Could indicate that your connected to a local development test network.

Рисунок 13 - Ідентифікаторів існуючих мереж Ethereum

При ініціалізації команди з ідентифікатором, запускається мережу приватного блокчейна. Ось що покаже термінал Geth після успішного виконання команди (рис.14):

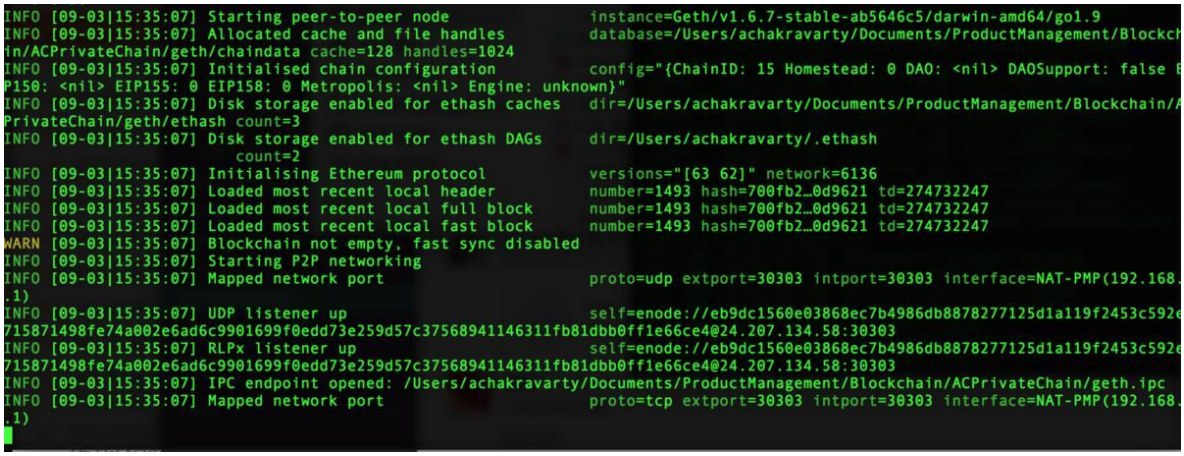

Рисунок 14 – Успішний запуск блокчейн мережі

Важливим є те, що Geth не запам'ятовує параметри приватної мережі блокчейна, тому щоразу для отримання доступу до приватного ланцюжка, потрібно буде запускати команди в консолі, що ініціюють підключення до genesis-файлу та запуск приватної мережі.

3.3 Реалізація смарт-контракту

Смарт-контракт, написаний мовою високої рівня, нагадує собою оголошення класу в парадигмі об'єктно-орієнтованого програмування. Нижче розроблено смарт-контракт, мовою Solidity, що є простим гаманцем. Смарт-контракт складається з набору змінних, що описують його стан, і набору функцій, кожна з яких містить ту чи іншу логіку, закладену в неї розробником контракту. Взагалі, значення змінних стану смарт-контракту зберігаються у його постійному сховищі. У наведеному смарт-контракті змінними стану є owner типу address, яка зберігає власника гаманця, і outflow типу відображення з безлічі address в uint, яка зберігає відтік коштів на кожну адресу у вигляді асоціативного масиву. Також договір неявно містить змінну баланс, значення якої відповідає сумі переведених на договір грошових одиниць. Змінні можуть бути позначені як публічні або приватні, оскільки стан смарт-контракту зберігається у гібридній мережі.

Функції смарт-контракту визначають «вхідні точки», якими можна ініціювати виконання конкретного коду. Крім звичайних функцій зі звичною сигнатурою, договір також містить функцію-конструктор, що викликається під час створення договору, і так звану fallback функцію з порожньою сигнатурою, що викликається у кількох особливих випадках:

- при переведенні на контракт тільки грошових одиниць;
- якщо функція, що викликається, не знайдена.

Для початку опису смарт-контракту необхідно установити початкові параметри (рис.15).

```
pragma solidity ^0.8.10;

contract Ownable {
    address public owner;

    mapping (address => uint) public outflow;

    constructor() public {
        owner = msg.sender;
    }


}
```

Рисунок 15 – Початкові установки смарт-контракту

Рядок pragma solidity 0.8.10 означає, що мінімальний необхідний компілятор для цього контракту – 0.8.10, це найактуальніша версія мови Solidity, оскільки саме ця версія містить виправлення помилок та ряд нових функцій.

Ім'я контракту задається після ключового слова contract. У тілі договору описуються всі дані, що зберігаються У тілі контракту описуються всі дані, що зберігаються. Маніпуляції з даними здійснюються через сеттери та гетери. Якщо дані не змінюються, то не потрібно платити за газ. Тому гетери виконуються моментально та безкоштовно. Сеттери вимагають

оплати і виконуються не миттєво (тільки внаслідок включення транзакції до чергового блоку блокчейну).

Оскільки даний контракт призначений саме для надійної і захищеної передачі даних, він повинен виключати вразливості існуючих смарт-контрактів. Саме тому, у даному смарт-контракті не використовуються функції низького рівня виклику. Для відправки засобів використовуються функції send і trance, так як вони не можуть повторно викликатись та забезпечують надійну передачу.

Для захисту від DDos – атак, у смарт-контракті все=і завідомо великі цикли діляться на кілька більш дрібних, щоб кожен із цих циклів виконувався в різних транзакціях.

Усі функції в Solidity відносяться до одного з чотирьох специфікаторів видимості: публічні, приватні, зовнішні та внутрішні. Функція без оголошення специфікатора автоматично відноситься до public, тобто її можна викликати з будь-якого місця. Тому, для обмежень доступу до публічних функцій необхідно обов’язково вказувати специфікатор видимості.

3.3.1 Опис методів та полів смарт-контракту

У Ethereum існує стандарт токена або монети. Якщо контракт відповідає стандарту, його можна назвати, і саме в такому випадку гаманці і біржи зможуть працювати з цим контрактом.

Контракт повинен містити три поля, зображених на рисунку 16.

```
string public constant name = "Coin Token";//повна назва монети
string public constant symbol = "CT";//скорочена назва монети
uint32 public constant decimals = 18;//кількість знаків після коми
uint public totalSupply = 0;//початковий баланс
```

Рисунок 16 – обов’язкові поля смарт-контракту

Поля вказують на назву монети, кількість знаків після коми, найпоширенішим значенням є 18, а також початковий баланс у гаманці. Обов'язкових вимог небагато, вони є доволі простими.

Також необхідно додати поле mapping. Mapping в Solidity діє як хеш-таблиця та використовується для зберігання даних у вигляді пар ключ-значення, ключ може бути будь-яким із вбудованих типів даних, але посилання на типи не дозволені, тоді як значення може бути будь-якого типу. Відображення в основному використовуються для зв'язування унікальної адреси Ethereum з відповідним типом значення. Перший ключ – адреса на зняття з якої надається дозвіл. У даному випадку mapping забезпечує доступ до гаманця (рис.17).

```
mapping (address => mapping (address => uint)) allowed;//поле дозволу
```

Рисунок 17 – Поле mapping

Смарт-контракт містить ряд основних функцій, зображених на рисунку 18.

```
function totalSupply() constant returns (uint256 totalSupply)
function balanceOf(address _owner) constant returns (uint256 balance)
function transfer(address _to, uint256 _value) returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) returns (bool success)
function approve(address _spender, uint256 _value) returns (bool success)
function allowance(address _owner, address _spender) constant returns (uint256 remaining)
function totalSupply() constant returns (uint256 totalSupply)
function balanceOf(address _owner) constant returns (uint256 balance)
function transfer(address _to, uint256 _value) returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) returns (bool success)
function approve(address _spender, uint256 _value) returns (bool success)
function allowance(address _owner, address _spender) constant returns (uint256 remaining)
```

Рисунок 18 – Основі функції смарт-контракту

Функція totalSupply – повертає сумарну кількість випущених монет. Цю функцію може викликати будь-хто.

Функція balanceOf – повертає кількість монет, що належать _owner. Може викликати будь-хто. Гаманці для відображення монети викликають саме цю функцію.

Функція transfer – передає _value монет на адресу _to. Коли користувач переміщатиме свої монети на іншу адресу, викликатиметься саме ця функція. Відповідно, монети повинні братися з балансу користувача, який викликав цю функцію. Метод повинен створювати подію Transfer у разі успішного переміщення монет.

Функція transferFrom – передає _ value монет від _from до _to. Користувач повинен мати дозвіл на переміщення монет між адресами, щоб будь-хто не зміг керувати чужими гаманцями. Фактично ця функція дозволяє довіреній особі розпоряджатися певним обсягом монеток на рахунку. Дати дозвіл на керування засобами можна наступною функцією. Метод повинен створювати подію Transfer у разі успішного переміщення монет.

Функція approve – дозволяє користувачеві _spender знімати з рахунку (з рахунку, що викликав функцію користувача) кошти не більше ніж _value. На основі цього дозволу має працювати функція transferFrom. Метод повинен створювати подію Approval (описано далі).

Функція allowance – повертає кількість монет, що дозволив знімати _owner користувачу _spender.

Окрім функцій, оголошено два типа подій. Події є успадкованими членами договорів, які змушують аргументи зберігатися у журналі транзакції – блокчейні. Ці журнали пов'язані з адресом контракту, включаються в ланцюжок блоків і залишаються там, поки блок доступний.

Події використовуються для інформування зовнішніх користувачів про те, що сталося в ланцюжку блоків. Самі собою смарт-контракти не можуть прослуховувати будь-які події.

Solidity визначає події за допомогою ключового слова event. Після виклику подій їх аргументи розміщуються в ланцюжок блоків. Щоб спочатку використати події, їх потрібно спочатку оголосити. У даному контракті оголошено два типи подій (рис. 19).

```
event Transfer(address indexed _from, address indexed _to, uint _value);//подія для функцій  transfer, transferFrom

event Approval(address indexed _owner, address indexed _spender, uint _value);//подія для функції approve
```

Рисунок 19 – Оголошення подій

3.3.2 Тестування та публікація смарт-контракту

Тестування смарт-контракту проводилось у середовищі Remix. Remix IDE - це програма для локальних та веб-додатків з відкритим вихідним кодом. Вона сприяє швидкому циклу розробки та має багатий набір плагінів з інтуїтивно зрозумілим графічним інтерфейсом. Remix використовується протягом усього шляху розробки контрактів. Remix IDE є частиною Remix Project, який є платформою для інструментів розробки, що використовують архітектуру плагінів.

Remix IDE – це потужний інструмент із відкритим вихідним кодом, який допомагає писати контракти Solidity прямо з браузера. У Remix IDE є модулі для тестування, налагодження та розгортання смарт-контрактів та багато іншого.

Після перенесення смарт-контракту у Remix, його можна скомпілювати та провести тестування функцій (рис.20, 21).

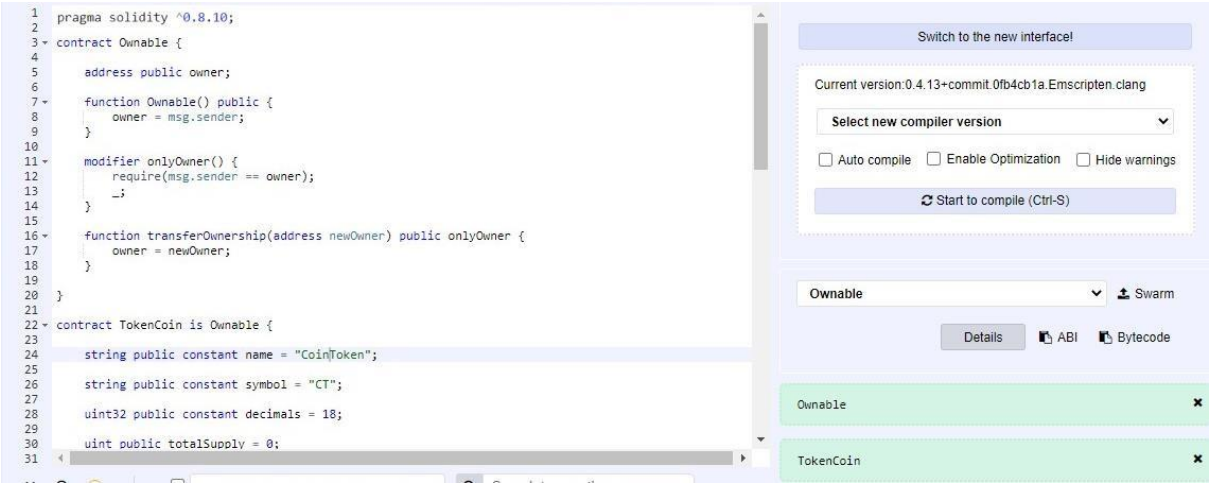

Рисунок 20 – Смарт-контракт у середовищі Remix

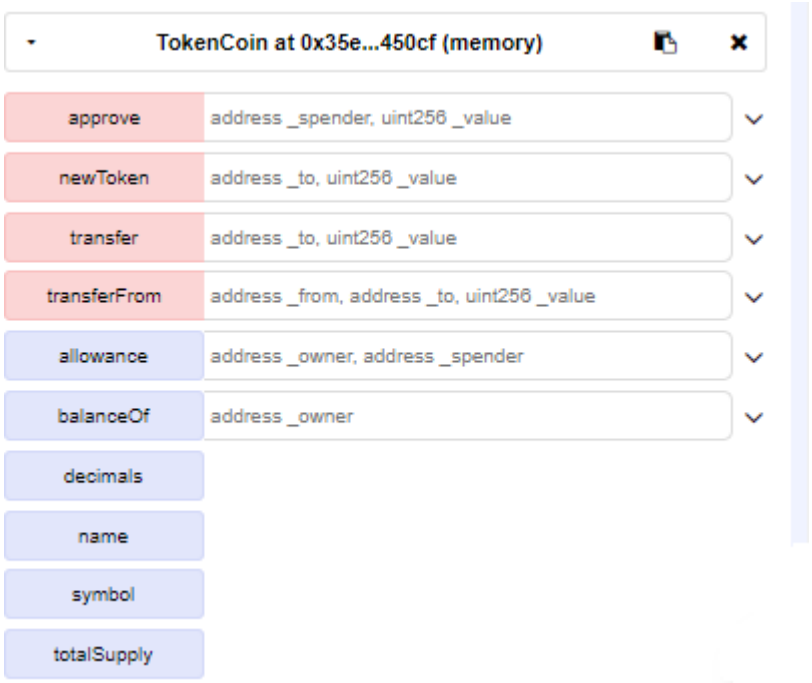

Рисунок 21 – Взаємодія з смарт-контрактом та наявними функціями

За допомогою інтерфейсу взаємодії з функціями можна протестувати їх, та переказати кошти з одного гаманця на інший (рис.22).

Рисунок 25 – Тестування функції переказу коштів

Функція пройшла не успішно, оскільки на рахунку немає коштів, тому створюються монети та додаються на рахунок, після чого можна перевірити загальний баланс гаманця (рис.26).

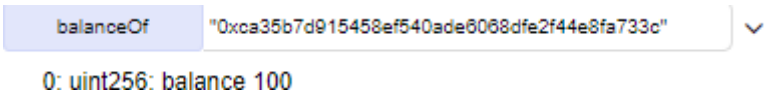

Рисунок 25 – Баланс гаманця

Отримавши монети на рахунку, можна перевірити функції переказу коштів на інший рахунок, для цього викликається функція transfer (рис. 26).

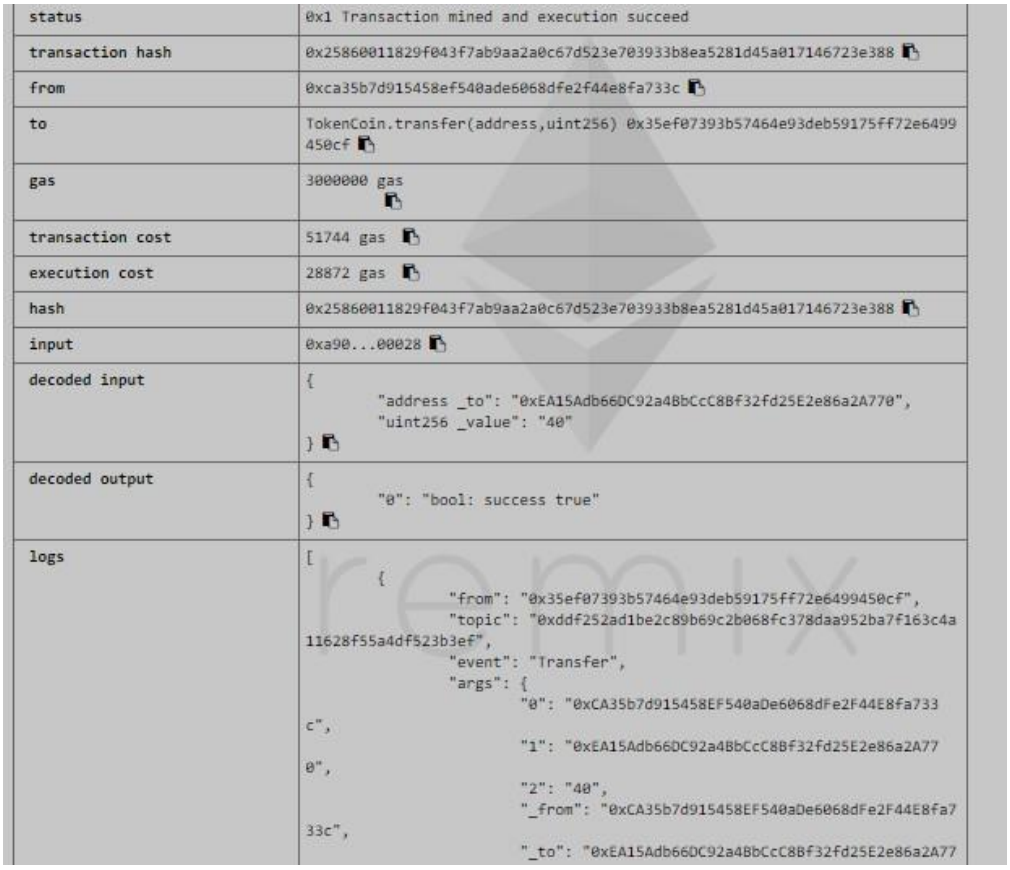

Рисунок 26 – Успішне виконання функції transfer

Після проведення тестування наявних функцій смарт-контракту його можна додати у створену блокчейн мережу та користуватися всіма функціями для реальних переказів.

Функції можуть бути викликані як звичайні користувачами, так і іншими контрактами через Application Binary Interface (ABI) або Application Programming Interface (API). ABI це набір угод, необхідних для доступу до низькорівневих сервісів.

У випадку з EVM визначення функції та параметрів, з якими її треба викликати, відбувається так:

1. Отримати хеш-сигнатури функції за допомогою алгоритму Keccak256.

2. Перші 4 байти отриманого хеша будуть початком цільового рядка та будуть вказувати на функцію, яку потрібно викликати.

3. Значення кожного параметра кодуєтьсяу 16-терічний рядок за правилами, визначеними для кожного типу і додаються в цільовий рядок.

4. Рядок, що вийшов, дозволяє EVM визначити, яку функцію, з якими значеннями параметрів викликати.

Для прямого звернення до функцій контракту необхідно попередньо оголосити його інтерфейс. Після цього виклик функцій стає можливим.

ABI є масивом JSON, який визначає інтерфейс договору, та створюється автоматично при компіляції смарт-контракту у середовищі Remix у блоці WEB3DEPLOY (рис.27).

```
WEB3DEPLOY

var tokencoinContract = web3.eth.contract([{"constant":true,"inputs":[],"name":"name","outpu
var tokencoin = tokencoinContract.new(
   {
     from: web3.eth.accounts[0],
     data: '0x6060604052600080553415610013576000 80fd5b5b610a2880610023600039600 0f30060606046
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' +
    }
 })
```

Рисунок 27 – ABI смарт-контракту

Отримавши даний код, за його допомогою можна опублікувати смарт контракт. Для цього використовується консоль Web3 у створеному блокчейні. Даний код додається та компілюється, після чого повідомляє про публікацію даного смарт-контракту (рис. 28).

```
Contract mined! address:
0x1c766c3cd0114771c0e9e45e54f4924b3f81f0d8
transactionHash:
0xcf6af22b774045e7730cd8862d9bef36b1d05dac46c57a491eea
2a386377e97e
```

Рисунок 28 – Публікація смарт-контракту у блокчейні

Опублікувавши смарт-контракт, можна провести транзакцію та перевірити працездатність функцій (рис. 29).

```
transaction fullhash=0x429eb0bbbc50
cca55c8446adca8bdd5ed4c7df6fdc32930f7e14ce7ccb51ea51
recipient=0x1C766C3CD0114771C0e9E45e54F4924B3F81f0d8
```

Рисунок 29 – Проведення транзакції у мережі

Смарт-контракт також опубліковано у публічній мережі, та проведено тестування.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі роботи розглянута мова програмування Solidity та зроблено висновок про те, що вона являється найкращою для написання смарт-контрактів.

На основі мови Solidity створено смарт-контракт. Як і будь-які програми, смарт-контракти можуть містити помилки, що дозволяють викрасти кошти, тому проведено аналіз, та передбачено функції, які забезпечують надійну та захищену передачу токенів. Смарт-контракт протестовано інтерфейсом Remix та розміщено у створеній блокчейн мережі.

Створивши даний смарт-контракт, його також опублікувано у приватній блокчейн мережі. Після публікації контракту проведено ряд тестувань, які показують значну відмінність між контрактом опублікованим у приватній мережі та контрактом опублікованим у гібридній мережі. Смарт-контракт що працює у гібридній мережі проводить транзакції значно швидше, середня комісія за проведення є нижчою, разом з тим нижчим є час проведення угоди, а сама робота ланцюга потребує менших енергоресурсів для своєї дієздатності.

ВИСНОВКИ

У даній магістерські роботі було проаналізовано основну мета забезпечення інформаційної безпеки, способи захисту інформації від несанкціонованого доступу, а також уже реалізовані системи забезпечення інформаційної безпеки на основі технології блокчейн. На основі отриманих результатів було запропоновано метод підвищення інформаційної безпеки, за рахунок розробки модифікованого смарт-контракту на основі гібридної блокчейн-мережі.

У першому розділі було досліджено основні загрози інформаційної безпеки, їх класифікація, канали витоку інформації, проблеми несанкціонованого доступу. Також, було досліджено існуючі методи захисту інформації, їх види та класифікацію. Враховуючи недоліки існуючих методів захисту інформації та постійний розвиток нових загроз, зроблено висновок про те, що система захисту інформаційної безпеки потребує нових підходів та рішень. Основою для розробки нового методу захисту інформаційної безпеки було обрано технологію Blockchain.

У другому розділі роботи детально досліджено та проаналізовано технологію Blockchain. На основі отриманих результатів зроблено висновок про ряд переваг технології – незмінність, децентралізацію, прозорість та конфіденційність.

Проведено порівняльний аналіз видів блокчейн-мереж, визначено їхні основні переваги, проблеми та недоліки. Досліджено, що найдоцільнішим видом для забезпечення інформаційної безпеки є гібридний blockchain, у якому ланцюги блоків поєднують переваги обох видів технології, намагаючись при цьому обмежити недоліки, та завдяки чому забезпечують усі аспекти інформаційної безпеки. Розглянуто смарт-контракти, що працюють на різних блокчейн-мережах. Зроблено висновок про те, що смарт-контракти на основі гібридної блокчейн-мережі зможуть забезпечити

відсутність цих недоліків та є відмінним методом для безпечної передачі інформації.

Аналізуючи інформацію отриману у першому та другому розділах роботи, у практичній частині розроблено смарт-контракт мовою Solidy на основі гібридної блокчейн-мережі. Після публікації контракту проведено ряд тестувань, які показують те, що смарт-контракт у гібридній блокчейн-мережі проводить транзакції значно швидше та надійніше, є енергоефективним. Він передбачає надійну передачу інформації, а будь-які спроби несанкціонованого доступу до інформації відразу ж стають помітними всім учасникам. Даний контракт може бути розширеним, та використовуватися компаніями для забезпечення надійної передачі інформації. Організації можуть використовувати характерні переваги блокчейну, використовуючи даний смарт-контракт, його високу продуктивність та повну контрольованість, одночасно підтверджуючи транзакції у ланцюгу блоків для підвищення прозорості та перевірки даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баранова Е.К. Информационная безопасность и защита информации Е.К. Баранова, А.В. Бабаш. – 3-е изд., перераб. и доп. – М.: ИНФРА-М, РИОР, 2016.
2. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
3. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. — К.: КНТ, 2007.
4. Chris Dannen. Introducing Ethereum and Solidity. — Brooklyn, New York, USA: Apress, 2017. — 197 с.
5. Information Security Problems and Solutions. — [Електронний ресурс]. – Режим доступу: https://www.delta-net.com/compliance/information-security/faqs/information-security-problems-and-solutions-deltanet.
6. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд «Мир», 2003. – 640 с.
7. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — 98 с.
8. Технология блокчейн с точки зрения информационной безопасности. — [Електронний ресурс]. – Режим доступу: https://cryptor.net/bitkoin-dlya-chaynikov/osnovnye-problemy-povsednevnogo-vnedreniya-blokcheyn-tehnologii.
9. Основные проблемы повседневного внедрения блокчейн технологии — [Електронний ресурс]. – Режим доступу: https://cryptor.net/bitkoin-dlya-chaynikov/osnovnye-problemy-povsednevnogo-vnedreniya-blokcheyn-tehnologii.

10. Blockchain Guide Documentation — [Електронний ресурс]. – Режим доступу: https://readthedocs.org/projects/blockchain-guide/downloads/pdf/latest/.
11. Лоран Лелу. Блокчейн от А до Я. Все о технологии десятилетия. — М Эксмо, 2018. — 256 с.
12. What Is a Block in the Blockchain? — [Електронний ресурс]. – Режим доступу: https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373.
13. Лекториум, Криптографические Хэш-функции [Електронний ресурс] – Режим доступу: https://www.lektorium.tv/course/22746.
14. Лапонина О.Р. Криптографические основы безопасности. — М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2004. — С. 320.
15. What Is a Merkle Tree? — [Електронний ресурс]. – Режим доступу: https://www.investopedia.com/terms/m/merkle-tree.asp.
16. Consensus Algorithm — [Електронний ресурс]. – Режим доступу: https://whatis.techtarget.com/definition/consensus-algorithm.
17. Puddu I., Dmitrienko A., Capkun S. How to forget without hard forks. IACR Cryptology, 2017. — [Електронний ресурс]. – Режим доступу: https://eprint.iacr.org/2017/106.pdf.
18. Описание работы Delegated Proof-of-stake — [Електронний ресурс]. – Режим доступу: https://distributedlab.com/blog/ru/description-of-delegated-proof-of-stake
19. Kwon J. Tendermint: Consensus without mining. — [Електронний ресурс]. – Режим доступу: https://github.com/tendermint/tendermint/wiki.

20. Chase B., Macbrough E. Analysis of the XRP ledger consensus protocol. Cornell University, 2018 — [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/1802.07242.
21. Классификация блокчейнов — [Електронний ресурс]. – Режим доступу: https://www.bitbon.space/ru/knowledge-base/distributed-ledger-technologies-blockchain/technological-aspects-of-blockchain/classification-of-blockchains
22. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", IEEE Consumer Electronics Magazine, Volume 7, Issue 4, July 2018, pp. 06–14.
23. The Idea of Smart Contracts — [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20060615044959/http://szabo.best.vwh.net/smart_contracts_idea.htm/.
24. Solidity — [Електронний ресурс]. – Режим доступу: https://docs.soliditylang.org/en/v0.8.10/.
25. Ethereum virtual machine — [Електронний ресурс]. – Режим доступу: https://ethereum.org/en/developers/docs/evm/
26. Geth Documentation — [Електронний ресурс]. – Режим доступу: https://geth.ethereum.org/