Форма № Н-9.02

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій та робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

бакалавр
(освітньо-кваліфікаційний рівень)

на тему **«Оптимізація характеристик блокчейн-технологій для підвищення безпеки та конфіденційності у телекомунікаційних мережах»**

Виконав: студент 4 курсу, групи 401-ТТ
спеціальності 172 «Телекомунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)

Будім В.П.
(прізвище та ініціали)
Керівник Шефер О.В.
(прізвище та ініціали)
Рецензент Дрючко О.Г.
(прізвище та ініціали)

Полтава 2024

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри автоматики, електроніки та телекомунікацій

_____О.В. Шефер
«01» квітня 2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРУ
СТУДЕНТУ

Будіму Віктору Петровичу

1. Тема роботи «**Оптимізація характеристик блокчейн-технологій для підвищення безпеки та конфіденційності у телекомунікаційних мережах**»
керівник роботи Шефер Олександр Віталійович, д.т.н., професор
затверджена наказом вищого навчального закладу від 08.12.2023 року № 1481/1-фа

2. Строк подання студентом проекту (роботи) 10.06.2024 р.
3. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ, особливості блокчейн технологій, алгоритм блокчейн технологій, галузі застосування, блокчейн технології в галузі телекомунікацій, переваги та недоліки блокчейну, вплив блокчейну на суспільство, українські компанії, які використовують блокчейн, побудова блокчейн мережі, алгоритм роботи консенсусу, налаштування мережі, тестування та впровадження, види захисту інформації, криптографія, алгоритми роботи криптографії, алгоритми шифрування інформації, сфери застосування алгоритмів шифрування, масштабованість, приватність та ефективність, інфраструктура, висновки, додатки.

Дата видачі завдання: «01» квітня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

По р. №	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів роботи			Примітка (плакати)
1	Вступ: Актуальність та мета дослідження блокчейн-технологій	25.04.24		5%	Пл.1
2	Розділ 1. Особливості блокчейн технологій, алгоритм блокчейн технологій, галузі застосування, блокчейн технології в галузі телекомунікацій, переваги та недоліки блокчейну, вплив блокчейну на суспільство, українські компанії, які використовують блокчейн	25.04.24	I	15%	Пл.3,4,5
3	Розділ 2. Побудова блокчейн мережі, Алгоритм роботи консенсусу, налаштування мережі, тестування та впровадження	23.05.24		40%	Пл.6,7,8
4	Розділ 3. Види захисту інформації, криптографія, алгоритми роботи криптографії, алгоритми шифрування інформації, сфери застосування алгоритмів шифрування	23.05.24	II	60 %	Пл.9,10
5	Розділ 4. Масштабованість, приватність та ефективність, інфраструктура	10.06.24		90%	Пл.11,12 ,13
6	Висновки. Оформлення кваліфакаційної роботи, оформлення додатків	10.06.24	III	100%	Пл.14

Студент _____ Будім В.П.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Шефер О.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Кваліфікаційна робота бакалавра: 68 с., 7 рисунків, 2 додатків, 18 джерел.

Об’єкт дослідження: Блокчейн технології в телекомунікаційних мережах

Мета роботи: Оптимізація характеристик блокчейн-технологій для підви щення безпеки та конфіденційності у телекомунікаційних мережах

Ключові слова: Блокчейн, хеш, вузол, блок, транзакція, децентралізація, розумні контракти

ABSTRACT

Bachelor's qualification work: 68 pages, 7 drawings, 2 appendixes, 18 sources.

Object of research: Blockchain technologies in Telecommunication networks

Purpose: Optimizing security and privacy characteristics in telecommunication networks.

Keywords: Blockchain, hash, node, block, transaction, decentralization, smart contracts, sha256, md5, https

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕННЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

Блокчейн (від англ. Blockchain) – Розподілена база даних, яка складається з блоків, пов'язаних один з одним за допомогою криптографічних хешів.

Хеш (від англ. Hash) – Алгоритм, який перетворює довільний набір даних у фіксований розмір.

Вузол (від англ. Node) – це комп'ютер, який зберігає копію блокчейну та бере участь у його роботі

Блок (від англ. Блок) – запис у блокчейні, який містить дані транзакцій, мітку часу та хеш попереднього блоку.

Транзакція (від англ. Transaction) – запис у блокчейні, який описує передачу цінності між двома або кількома адресами.

Децентралізація (від англ. Decentralization) – Відсутність центрального органу влади, який контролює блокчейн.

Розумний контракт (від англ. Smart Contract) – це комп'ютерна програма, яка автоматично виконує умови угоди між двома або кількома сторонами.

SHA256, Безпечний Хеш Алгоритм (від англ. Secure Hash Algorithm) – це криптографічна хеш-функція, яка використовується для перетворення довільного повідомлення у фіксований розмір вихідних даних (хеш).

MD5 (Message-Digest Algorithm 5) – це старша криптографічна хеш-функція, яка також використовувалася для перетворення повідомлень у фіксовані розміри хешів.

HTTPS (Hypertext Transfer Protocol Secure) – це захищений протокол передачі гіпертекс

ЗМІСТ

ВСТУП

Мета роботи: Дослідити параметри блокчейн технологій в галузі телекомунікацій з метою поліпшення умов безпеки.

Основні задачі: Актуальність теми полягає в тому, що блокчейн технології стрімко розвиваються та набувають все більшої актуальності у різних сферах життя. Їх унікальні властивості, такі як децентралізація, безпека, прозорість та ефективність, роблять привабливими для вирішення багатьох проблем сучасного світу. Ось декілька ключових факторів, що підкреслюють актуальність блокчейну:

Перший фактор це потреба в децентралізації, бо користувачі та організації все більше прагнуть до того, щоб їх особиста інформація не потрапляла до рук централізованих посередників. Блокчейн, з його децентралізованою природою, має відповідь на це питання.

Наступнип аспектом є зростання кіберзагроз, які можуть нанести шкоду нашій особистій інформації. Блокчейн, з його стійкістю до злому та незмінністю даних, може допомогти у захисті інформації від несанкціонованого доступу.

Третім аспектом є потреба у прозорості. Цей фактор є дуже важливим у всіх галузях. Говорячи про галузь телекомунікацій, цей аспект є надважливим, оскільки саме прозорість може забезпечити безпеку та конфіденційність для ваших особистих даних, а також це суттєво зменшує ризик потрапити на шахраїх, оскільки ви зможете знайти їх дані без великих зусиль та повідомити про них правоохоронним органам. Блокчейн, з його відкритими та прозорими транзакціями, може допомогти у вирішенні цієї проблеми.

Також важливим фактором є зниження витрат та підвищення ефективності надання телекомунікаційних послуг.

Блокчейн може допомогти автоматизувати багато процесів, що може призвести до зниження витрат та підвищення ефективності, а зекономлені кошти можна витратити на додаткове обладнання для розширення можливостей самої мережі.

Сфера блокчейну постійно розвивається і це має позитивний вплив на галузь телекомунікацій, оскільки розробляються нові блокчейн-протоколи, які є більш масштабованими, енергоефективними та безпечними. З'являються нові блокчейн-платформи, які пропонують різні функції та послуги для розробників та користувачів. Розширення сфер застосування дозволяє блокчейн технологіям впроваджуватися в нових сферах. Також важливо враховувати те, що у блокчейн-технології інвестують мільярди доларів, що свідчить про значний інтерес до їх потенціалу і не потрібно навіть сумніватися в тому, чи будуть ці зміни позитивними чи ні.

Очікується, що розвиток блокчейну триватиме й надалі, роблячи цю технологію все більш потужним інструментом для вирішення проблем сучасного світу.

1 АНАЛІТИЧНИЙ ОГЛЯД БЛОКЧЕЙН ТЕХНОЛОГІЙ

1.1 Особливості блокчейн технологій

Блокчейн - це інноваційна технологія, яка дозволяє надійно зберігати всі дані за допомогою комп'ютерної мережі. Ця база даних використовується для зберігання інформації для багатьох інших цілей [1].

Цифровий запис даних мережі блокчейн складається з ланцюгів, що містять інформацію про всі виконувані транзакції. Історія транзакцій створює блок, де всі дані розташовані в певному порядку. Зберігання цієї інформації підтримується великою кількістю комп'ютерів по всьому світові. Завдяки організованим блокам, мережа блокчейнів захищена від зовнішніх перешкод. Все це досягається тому, що для цього потрібна згода всіх учасників. Таким чином, з інформаційних блоків формується система, що працює з обміну віртуальної валюти без посередників.

Перша блокчейн-мережа була створена вченими Стюартом Хабером і Скоттом Сторнеттою на початку 90-х років. Вчені працювали над покращенням захисту цифрових документів від підробок. Це призвело до того, що інші вчені надихнулися ідеєю блокчейну та створили Біткойн, перший криптоактив, заснований на технології блокчейн. Ця цифрова технологія також використовується для запису інших видів інформації, не пов'язаних з криптовалютами.

У мережі блокчейнів немає центрального регулятора. Всі користувачі мережі мають дозволи на управління виконуваними операціями. Відсутність контролю з боку уряду, бізнесу чи окремої особи називається децентралізацією. Тому люди, наприклад, в такій банківській системі, яка знайома багатьма людьми, торгують тільки між собою, без посередників [1].

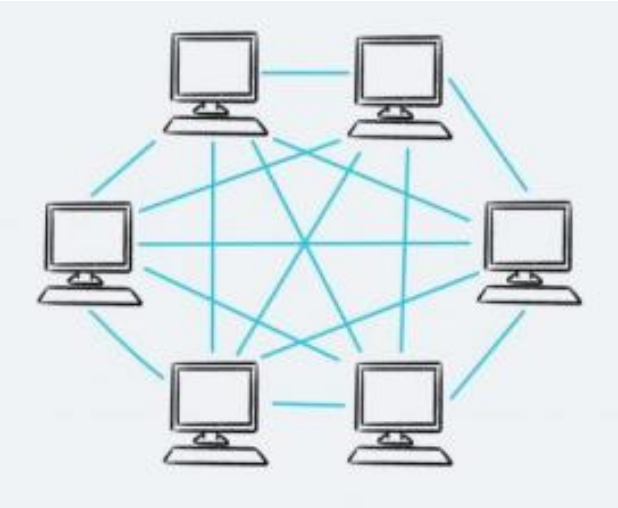


Рисунок 1.1 - Блокчейн структура

Рисунок 1.2 - Серверна структура

1.2 Алгоритм блокчейн технологій

Блокчейн - це цифровий реєстр, який надійно записує транзакції між двома сторонами, захищеними від несанкціонованого доступу. Ці транзакційні дані записуються мережею спеціалізованих комп'ютерів, розподілених по всьому світу, які називаються вузлами або **нодами**.

Коли користувач ініціює транзакцію, транзакція транслюється в мережу. Кожен нод перевіряє справжність транзакції, перевіряючи її цифровий підпис

та інші дані транзакції. Коли транзакція перевіряється, вона додається до блоку разом з іншими транзакціями, які були перевірені раніше [2].

Блоки об'єднуються в ланцюжок з використанням методів шифрування для створення ланцюжка блоків або так званого **чейну** (англ. chain). Процес перевірки транзакції та додавання її до блокчейну здійснюється за допомогою механізмів консенсусу. Це набір правил, які визначають, як вузли в мережі домовляються про стан блокчейну та дійсність транзакції.

Шифрування є основою для ведення безпечного, прозорого і захищеного від несанкціонованого доступу журналу транзакцій. Наприклад, хешування є найважливішим методом шифрування, який використовується в блокчейні. Це процес шифрування, який перетворює вхідні дані будь-якого розміру в рядок фіксованого розміру. Хеш-функції, що використовуються в блокчейнах, як правило, стійкі до зіткнень, а це означає, що шанси знайти двоє одинакових даних, які дають однаковий результат, майже рівні нулю. Інша особливість називається лавинним ефектом, що означає явище, при якому невеликі зміни вхідних даних призводять до різних результатів [2].

Давайте проілюструємо це за допомогою SHA256 – функції, яка широко використовується в багатьох мережах. Хеш-функції є також односторонніми функціями, тому що з обчислювальної точки зору неможливо отримати вхідні дані шляхом зворотного проєктування хешу результату.

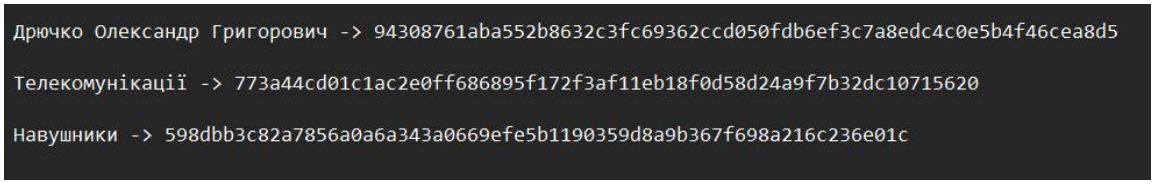


Рисунок 1.3 - Кодування текст через алгоритм SHA256

1.3 Галузі застосування блокчейн технологій

Технологія блокчейн вже використовується в багатьох галузях, хоча вона все ще знаходиться на ранніх стадіях виробництва і потребує зусиль для

свого розвитку. Зазвичай процес переказу коштів з країни в країну займає доволі багато часу, вимагає значних коштів, і цей процес є централізованим, оскільки процес здійснюється за допомогою централізованого органу, в даному випадкові - банку. Блокчейн гарантує децентралізацію, тобто тільки ви і друга сторона будуть знати про всі деталі транзакції [3].

Друга галузь застосування блокчейн технологій це **захист авторського права**. На сьогоднішній день ця проблема є найпоширенішою, оскільки є дуже багато осіб, які можуть використовувати творчість тих чи інших людей з ціллю отримати з цього певну вигоду, а саме, зароботи гроші руками іншим людей. В даному випадку блокчейн технології будуть дуже корисними для артистів, музикантів, художників, тощо. Вони можуть підтвердити право власності за допомогою унікальних цифрових підписів та сертифікатів.

Наступна галузь - **розумні контракти**. Такі контракти доступні у вигляді алгоритмів, які дозволяють вам укладати контракти з самообслуговуванням на блокчейні. Цей тип контракту був би особливо корисним інструментом для початківців, оскільки смарт-контракти для використання в ділових операціях не вимагають участі посередників і виконуються автоматично, оскільки вони гарантують переказ коштів та інші транзакції, як тільки сторони виконають всі зобов'язання, зазначені в контракті [3].

Такий підхід значно зменшує ризик потрапити в пастку до шахраїв, а навіть якшо таке трапиться, то шахраям просто заблокують рахунок, а ваші кошти повернуться на ваш рахунок.

Четвертою галузею є **безпека ідентифікації**. Взагалі, безпека це надважливий аспект незвачаючи на місце використання, будь то фінанси, охорона здоров’я чи телекомунікації. До появи блокчейн технологій мільйони людей по всьому світові страждали через шахрайство та викрадення особистих даних. Шахрайство таких масштабів може відбуватися від чого завгодно, починаючи підробкою документів і закінчуючи викраденням особистих файлів з вашого ПК, використовуючи віруси та інше шкідливе ПО [3].

У цьому випадку технологія блокчейн покращила ситуацію, а кількість випадків шахрайства та крадіжки особистих даних значно скоротилася. Все це сталося завдяки багаторівневій системі ідентифікації, в якій ви повинні спочатку надати електронну копію свого документа, яка може підтвердити вашу особу, надавши паспорт громадянина країни, закордонний паспорт, посвідчення водія, тощо.

Здавалося б, нічого незвичайного, документи можна підробити чи вкрасти, але не все так просто. Потім потрібно доказати те, що ви є тією самою людиною, за яку себе видаєте. Потрібно пройти ідентифікаю по обличчу, де потрібно буде зробити певні дії. Наприклад, посміхнутися, покрутити головою в різні сторони, тощо [3].

Також в поєднанні з такою системою ідентифікації використовується класичний метод автентифікації, використовуючи ваш номер телефону, електронну пошту та пароль.

1.4 Блокчейн технології в галузі телекомунікацій

Незважаючи на те, що технологія блокчейна знаходиться на ранніх стадіях розробки, багато телекомунікаційних компаній намагаються інтегрувати блокчейн в телекомунікаційну галузь і створювати мережі [1].

Першим важливим аспектом інтеграції блокчейна в телекомунікаційну галузь є **захист персональних даних користувачів**. Це важливо, тому що для кожного користувача потрібно переконатися, що його особисті дані в безпеці і вам не потрібно про це турбуватися.

Блокчейн можна використовувати для **безпечного зберігання особистих даних** користувачів, таких як номери телефонів, адреси електронної пошти та інформація про використання сервісу. Це допоможе захистити ваші дані від крадіжки та витоку [1].

Наступним фактором є **ідентифікатор користувача**. Цей аспект також важливий, оскільки користувачі повинні підтвердити свою особу. Таким

чином, ризик потрапити в пастку шахраїв практично дорівнює нулю, оскільки ні один зловмисник не зацікавлений в тому, щоб ви знали його особу.

Третім напрямком, де може використовуватися технологія блокчейн це **роумінг**. Інтеграція блокчейну в телекомунікаційну галузь є дуже хорошим рішенням для телекомунікаційних компаній, оскільки вона зменшує кількість використовуваного обладнання і відповідно економить значні суми грошей. Така зміна буде позитивною і для звичайних користувачів, оскільки вартість дзвінків та послуг буде значно нижчою [1].

Наступним фактором є **управління власними даними**. Для багатьох користувачів це також є важливим фактором, оскільки всі люди різні, тому поняття особистої інформації також відрізняється. Одні не хочуть, щоб хтось бачив його фотографії на своїй сторінці, а інші не хочуть, щоб хтось дізнався його номер телефону або адресу електронної пошти. Таким чином, дане рішення є дуже ефективним, оскільки користувач сам вибирає інформацію, яку потрібно приховати, що робить використання блокчейн гнучким у використанні [2].

Останнім аспектом є **боротьба з шахрайством**. Враховуючи всі аспекти, описані вище, можна зрозуміти, що всі вони спрямовані на те, щоб поліпшити якість викорстання телекомунікаційних послуг та вивести рівень безпеки та конфіденційності користувачів на новий рівень. Завдяки прозорості, децентралізації та багаторівненій ідентифікації, блокчейн значно ускладнює процес викрадання та використання ваших особостих даних, що робить рішення інтеграції блокчейну дуже привабливим для таких, як ми з вами, користувачів.

1.5 Переваги та недоліки блокчейну

На сьогоднішній день блокчейн технології стрімко розвиваються, дуже багато різних компаній по всьому світові інтегрують блокчейн в свої сфери користування через такі переваги, як:

Децентралізація. Блокчейн не залежить від централізованих органів, що підвищує рівень вашої безпеки та конфіденційності. Це свідчить про те, що ваші дані будуть відомі тільки вам і при використанні таких послуг, як дзвінки чи переказ коштів, деталі використання вами даних послуг будуть відомі тільки вам і нікому іншому [2].

Безпека. Криптографія забезпечує високий рівень захисту даних від несанкціонованого доступу та модифікацій. Існує багато різних методів шифрування, але найпоширенішими з них є MD5 та SHA256, оскільки вони гарантують високий рівень захисту інформації.

Прозорість. Всі транзакції в блокчейні відкриті для перегляду, забезпечуючи довіру і підзвітність і значно знижуючи ризик потрапляння в пастку шахраїв, оскільки ви зможете або самі взнати їх особисті дані, або завдяки оператору та звернутися до відповідних органів для правового регулювання [2].

Ефективність. Насправді, інтеграція блокчейн в галузь телекомунікацій є дуже ефективним рішенням, оскільки це допомагає зменшити кількість затрат на обладнання, зменшити вартість послуг для звичайних користувачів та значно покращити якість роботи.

Незважаючи на такий великий потенціал блокчейну, потрібно оставатися реалістом та дивитися на речі широким поглядом, оскільки серед виділених переваг можна виділити і наступні недоліки:

Першим з них є **масштабованість**. Існуючі блокчейн-мережі можуть бути повільними та дорожчими в обслуговуванні в порівнянні зі звичайними базами даних, оскільки блокчейн знаходиться на ранній стадії виробництва,

але компанії активно працюють на тим, що поліпшити швидкість роботи та зробити блокчейн-мережі доступними для звичайних користувачів [2].

Регулювання. Правове регулювання блокчейну тільки починає розвиватися, що створює певну невизначеність для підприємств.

Енергоспоживання. Деякі блокчейн-мережі, наприклад Bitcoin, споживають доволі велику кількість енергії, що може бути дуже ресурно-затратно та неприваблимим рішенням для багатьох компаній, враховуючи те, що не у кожної компанії є достатньо великий капітал для інвестицій та підтримки робото-здібності мережі [2].

Технологія блокчейн відкриває новітні можливості для телекомунікаційної галузі. Децентралізація, безпека, прозорість та ефективність блокчейна можуть вирішити багато проблем і поліпшити обслуговування користувачів. Технологія все ще знаходиться на ранній стадії розробки, але інвестиції телекомунікаційних компаній в блокчейн-рішення демонструють її високий потенціал. Очікується, що використання блокчейна в комунікаціях буде рости в найближчі роки і сприятиме створенню більш безпечної, надійної та ефективної інфраструктури зв'язку.

1.6 Перспективи використання блокчейну

Розвиток блокчейну відбувається стрімко. Очікується, що найближчим часом відбудуться наступні зміни:

Перша і одна з основниж змін це **зростання потужностей**. Розробляються нові рішення для блокчейну, які є більш масштабованими та енергоефективними, що дозволить їм суттєво збільшими обсяг транзакцій та знизити витрати на обладнання. Таке рішення суттєво збільшить кількість компаній та приведе до збільшення кільості робочих місць, що позитивно вплине на ринок праці [3].

Наступним, та не менш важливим, є **сприятливе регулювання**. Оскільки питання правового регулювання знаходиться на ранній стадії

виробництва, це ускладнює процес інтеграції блокчейну для багатьох компаній, але уряди багатьох країн світу працюють над створенням чіткого та сприятливого регуляторного середовища для блокчейну, що сприятиме його більш широкому впровадженню.

Наступна зміна це **взаємне інвестування**. Телекомунікаційні компанії об'єднуються в так звані “консорціуми” для розробки стандартів блокчейну для галузі. Спільні зусилля допоможуть подолати технічні бар'єри, прискорити інновації, зменшити витрати на них та дати можливість іншим компаніям використовувати їх стандарти [3].

Четверта зміна має значний вплив на сферу фінансів, оскільки вона призводить до розвитку **децентралізованих фінансів**. Блокчейн стане основою для розвитку децентралізованих фінансових сервісів, які пропонують альтернативу традиційним фінансовим установам. Децентралізовані фінанси стають все популярнішими, оскільки вони пропонують кращий рівень захисту ваших даних, гнучкість та більшу зручність в користуванні.

Остання змінна є однією з найважливіжих, оскільки вона стосується **безпеки ідентифікації**. Незважаючи на всі ті методи багаторівневої ідентифікації користувача, які є у блокчейні, компанії придумують ще більше методів ідентифікації для того, щоб захистити дані своїх користувачів та унеможливити для зловмисників викрасти ці дані [3].

1.7 Вплив блокчейну на суспільство

Оскільки блокчейн гарантує цілісніть даних та високий рівень безпеки, не потрібно бути психологом, що зрозуміти, що він буде широко розповсюджений, оскільки цілісніть даних для звичайного користувача стоїть на першому місці. Звичайно, це приведе до наступних наслідків у суспільстві:

Першим наслідком є **підвищення довіри**, оскільки прозорість, децентралізація та складна ідентифікація користувача дають впевненість в

цілісності ваших даних, а майбутнє правове регулювання лише посилить довіру звичайних користувачів та унеможливить для зловмисників можливість нанести шкоду чи викрасти ваші дані [3].

Другий наслідок є надважливим, оскільки це **демократизація інформації**. Варто зазначити, що ми живемо у тяжкий для всіх час, коли пропаганда робить усе, щоб заставити людей вірити в брехню та приховати правду. Наразі, як ніколи раніше, правдива інформація є на вагу ковтка чистого повітря і дуже багато людей не мають змоги висловлювати цю інформацію, через сумніви в безпеці своїх даних та конфіденційності. Кожна людина має невід'ємне право на свободу слова, тому завдяки блокчейну люди зможуть не боячись висловлювати власну думку, що є однією з найкращих змін для суспільства.

Також зміни торкнуться і **бізнесу**, оскільки це приведе до створення нових бізнес моделей, які будуть в рази ефективнішими, ніж попередні. Таке рішення буде мати дуже позитивний вплив на бізнес, оскільки питання безпеки даних для бізнесу також стоїть на першому місці [3].

Останніми є **зміни в управлінні**. Це напряму стосується демократизації інформації, оскільки через низький рівень конфіденційності не можен працівник може поскаржитися на ті чи інші дії свого керівника, який знаючи того, хто залишив такий відгук, може вчинити неправомірні дії стосовно свого працівника. Наприклад, звільнити його без причини, понизити рівень заробітньої плати або взагалі знущатися.

Напревеликий жаль, такі явища є дуже розповсюдженими по всьому світі, тому свобода слова, права людини, конфіденційність та безпека даних повинні бути на першому місці [3].

1.8 Українські компанії, які використовують блокчейн

У галузі телекомунікацій існує багато різних компаній, які вже використовують блокчейн технології для поліпшення параметрів безпеки,

конфіденційності та взагалі якості роботи їх сервісів. Виділимо наші вітчизняні компанії, яке теж використовують новітні технології.

ESKA. Дана компанія займається створенням програмного забезпечення та інтеграцією блокчейну для IT інфраструктури та IT безпеки. Компанія активно використовує новітні технології в моніторингові інфраструктури та роботоздатності програмного забезпечення з метою своєчасного виявлення шкідливого ПО, поліпшення якості користування та параметрів безпеки. Також компанія активно працює над мережевою безпекою та безпекою хмарних сервісів, шоб користувачі були впевнені в безпеці своїх особистих даних [4].

FLIIST. Ця компанія буде дуже корисную для тих, хто хоче створити власну компанію, використовуючи блокчейн технології, але не знає як протестувати блокчейн рішення. Основою метою даної компанії є допомога більшій кількості клієнтів та партнерів інтегрувати блокчейн рішення в їх бізнес справи та повсякденне життя, оскільки творці компанії вірять, що в майбутньому, блокчейн повністю змінить наш світ в кращу сторону [4].

INNOHUB. Вже з 2015 року, компанія активно створює цифрову продукцію та надає консалтингові послуги своїм клієнтам, використовуючи окрім блокчейну, ще й штучний інтелект. Компанія спеціалізується на поліпшенні якості кібер-безпеки, швидкодії власної продукції, штучного інтелекту та машинного навчання. Інтеграція таких технологій, в особливості штучного інтелекту є дуже сприятливим фактором для зросту компанії, оскільки здібності блокчейну та штучного інтелекту розширюються в геометричній прогресії [4].

Lifecell. Одна з найвідоміших компаній, яка надає телекомунікаційні послуги, теж почала активну інтеграцію блокчейну в сферу свого користування. На даний момент, компанія тільки почала процес інтеграції, але в майбутньому це приведе до великих змін в зручності користування і безпеці взагалом. Наприклад, при поповненні рахунку більше не потрібно

буде платити додаткову комісії, в розмірі декількох відсотків від суми поповнення [4].

Наразі набирає популярності сервіс e-sim. Це та ж сама сім-карта, але в електронному виді. Це рішення є дуже зручним, оскільки тепер не потрібно йти в магазин, шоб купити номер телефону для користування, а інтеграція блокчейну може зробити це майже безкоштовним та зробити зв’язок доступним для кожного [4].

2 КОНСТРУКТОРСЬКА ЧАСТИНА

Для того, щоб виконувати завдання у сфері блокчейн технологій, критично важливо розуміти принцип побудови таких мереж, оптимальність того чи іншого вибору при створенні мережі. Тож розглянемо принцип побудови блокчейн мережі та всі аспекти, пов’язані з цим.

2.1 Побудова блокчейн мережі

Взагалі, блокчейн мережа працює доволі просто, хоча сам по собі, процес складний і складає він з наступних кроків:

Першим кроком є **створення блоку**. Транзакція створюється та надсилається до розподіленої мережі вузлів. Кожен вузол у мережі повинен перевірити транзакцію, використовуючи один із типів консенсусу. Після перевірки транзакції вузлом надана інформація зберігається в блоці [5].

Другим кроком є **з’єдання блоків**. Кожен блок може містити лише певну кількість інформації і як тільки блок повністю заповнюється, створюється новий блок, і виконується той самий процес запису інформації з перевіркою вузла. Щоб зв'язати блок, новий блок використовує унікальний код, який називається хешем. Якщо деталі транзакції змінюються хоча б незначно, хеш повністю змінюється, що полегшує розпізнавання перешкод. Такі посилання утворюють цілий ланцюжок, який показує, як створюється конкретний об'єкт.

Останнім крокод є **додання блоку до самого блокчейну**. Всі транзакції блокуються разом повністю фіксованим чином, утворюючи ланцюжок блоків. Кожного разу, коли додається блок, мережа використовує той самий тип консенсусу для перевірки валідності інформації попереднього. Такий підхід забезпечує дуже високий рівень інформаційної безпеки, що дозволяє користувачам повністю довіряти безпеці своїх даних [5].

2.2 Алгоритм роботи консенсусу

Алгоритми консенсусу - це набір механізмів, які дозволяють користувачам або пристроям координувати свою діяльність у розподіленому середовищі. Навіть якщо деякі сторони зазнають невдачі, вам потрібно переконатися, що всі сторони в системі можуть домовитись про одне джерело точності. Це означає, що система повинна бути відмовостійкою [6].

У технології блокчейн інформація зберігається в базі даних, тобто в блокчейні. Дуже важливо, щоб усі (точніше кожен вузол) зберігали ідентичну копію бази даних. В іншому випадку ви отримаєте суперечливу інформацію, яка підриває всю мету мережі блокчейн. Шифрування з відкритим ключем не дозволяє користувачам використовувати активи один одного. Але навіть тоді учасники мережі повинні мати лише одне джерело фактів, на яке вони можуть покластися, щоб мати можливість визначити, чи були вже витрачені кошти чи ні.

По-перше, потрібно, щоб користувачі, які хочуть додати блоки, надали заставу. Застава – це певна кількість активу, яку повинен надати валідатор, що відбиває у нього бажання діяти зловмисно. Якщо валідатор буде діяти зловмисно то відповідно, він втратить свої активи. Наприклад, певну обчислювальну потужність, гроші або навіть репутацію [6].

Навіщо їм ризикувати власними ресурсами? Але існує також винагорода. В більшій кількості випадків, це актив протоколу, який утворюється з комісій, що сплачуються іншими користувачами.

Остання потреба це прозорість. Звичайні користувачі повинні мати можливість визначати спроби шахрайства. В ідеалі, виробництво блоків має бути дорогим для шахраїв, але дешевим для будь-кого, хто їх перевірятиме. Це гарантує, що валідатори перебувають під контролем звичайних користувачів [6].

Тож давайте тепер розглянемо типи алгоритмів консенсусу та чим вони відрізняються:

Першим алгоритмом є **Proof of Work (PoW) - Доказ роботи**. У цьому алгоритмі так звані майнери розв'язують певні математичні задачі, які вимагають значної обчислювальної потужності. Перший майнер, який успішно вирішує завдання, може створити новий блок і отримати за це винагороду у вигляді певного активу або обчислювальної потужності [6].

Серед переваг такого алгоритму можна виділити його високу **безпеку**, оскільки здійснити атаку на мережу через велику обчислювальну потужність є важким завданням. Також дуже важливим аспектом є і **децентралізація**, так як більшість рішень у мережі приймаються відповідно до внеску майнерів.

Серед недоліків можна виділити **великі енергетичні витрати**, оскільки потужна обчислювальна техніка потребує багато енергії. В список недоліків також можна додати і **періодичність** тому, що між створеннями блоків повинен пройти певний проміжок часу [6].

Наступним алгоритмом є **Proof of Stake (PoS) - Доказ власності**. В даному алгоритмові вибір нового блоку залежить від власності активів, тобто чим більшу кількість активів користувач має, тим вища ймовірность вибору його блоку для створення [6].

Дивлячись на переваги, можна виділити його енергоефективність, оскільки даний алгоритм споживає не велику кількість електроенергії. Енергоефективність досягається за рахурнок того, що процес вибору блоку залежить від власності активу. Вагомим аспектом є зменшення централізації, так як вибір блоку залежить від кількості власних активів, що може допомогти зменшити владу в руках великих майнерів але присутність хоч і малої централізації є недоліком тому, що такі майнери мають більшу вагу при прийнятті рішень.

Останнім алгоритмом консенсусу є **Practical Byzantine Fault Tolerance (PBFT) - Практична візантійська стійкість**. Алгоритм використовується в тих випадках, коли учасники мережі можуть вчинити злочинні дії. Він виявляє і вносить корективи в таких випадках, щоб запобігти потраплянню

до рук зловмисників. В порівнянні з попередніми алгоритмами, даний алгоритм пропонує високу швидкість транзакцій та підвищену ефективність, незважаючи на те, що деякі вузли мережі можуть бути несправними або на них здійснюються кібер-атаки [6].

Нажаль, як в попередньому алгоритмові, тут присутня централізація. Алгортм потребує довіри до певного набору вузлів, що може викликати проблеми з безпекою та централізацією. Також доволі складного інтегрувати його у мережі широкого доступу, оскільки кількість повідомлень зростає квадратично відносно кількості вузлів.

На сьогоднішній день алгоритми консенсусу є основою блокчейнів та дозволяють розробникам запускати свій код в розподіленій мережі. Вони важливі для довгострокової життєздатності різних мереж. З усіх наявних алгоритмів, алгоритм доказу роботи (Proof of Work) є найкращим вибором, оскільки він є самим надійним та безальтернативним в своєму колі [6].

2.3 Налаштування мережі

Для якісного налаштування мережі потрібно розуміти з чим ми взагалі працюємо і що нам потрібно, оскільки побудування мережі може залежати від багатьох аспектів, наприклад, масштабованість мережі чи мета її використання. Тож оглянемо загальні складові мережі:

Основна складова в контексті мереж це **вузол (англ. node)**. Це будь-який мережевий пристрій, який здатний обмінюватися інформацією з іншими пристроями. Вузли можуть бути різними за типами та функціональністю, але всі вони відіграють важливу роль у підтримці роботи мережі. Ось деякі з найпоширеніших типів вузлів [2].

Вузлами можуть бути кінцеві пристрої, тобто такі пристрої, які використовуються кінцевими користувачами, такі як комп'ютери, смартфони, планшети, тощо. Вони підключаються до мережі, щоб отримувати доступ до ресурсів, таких як Інтернет, веб-сайти, електронна пошта, файли тощо.

Вузлом може бути **маршрутизатор**, пристрій, який направляє трафік між різними сегментами мережі. Він аналізує адреси призначення пакетів даних та визначає самий оптимальний маршрут для їх транспортування [2].

Не варто забувати і про **комутатори**, які з'єднують декілька пристроїв в одному сегменті мережі. Вони дозволяють пристроям, які знаходяться в одному і тому самому сегменті взаємодіяти один з одним.

Але в більшості випадквів в якості вузлів виступають **сервери**. Простішими словами, це потужні комп'ютери, які надають ресурси та послуги користувачам, які знаходяться в даній серверній мережі. Вони можуть хостити веб-сайти, зберігати файли, надавати доступ до певної інформації, тощо [7].

Отже, розглянувши, які пристрої можуть виступати в ролі вузолу, тепер розглянемо які є параметри у вузла:

Першим з них є це **пропускна здатність**. Це швидкість, з якою вузол може передавати дані до інших вузлів.

Другим параметром є **час затримки**. Це час, який потрібен пакету даних для переміщення з одного вузла до іншого.

Наступним параметров є **надійність**. Визначення цього параметра точно таке саме, як і в математиці. Це ймовірність того, що вузол буде працювати без збоїв [7].

Останнім і самим основним параметром є **безпека**. Даний параметр характеризує здатність вузла до захисту даних від несанкціонованого доступу, що дає впевненість користувачеві в користуванні мережею.

Вузли взаємодіють один з одним, забезпечуючи роботу мережі. Маршрутизатори направляють трафік між різними сегментами мережі, комутатори з'єднують пристрої в одному сегменті мережі, сервери забезпечують користувачів ресурсами та послугами в мережі, а шлюзи з'єднують різні мережі між собою [2].

Вузли є основою будь-якої мережі тому, що забезпечують зв'язок між пристроями. Вони надають необхідні компоненти для роботи мережі. Від їх працездатності залежить загальна продуктивність та надійність мережі.

2.4 Тестування та впровадження

Перед тим, як запустити мережу для всіх користувачів, потрібно провести багато часу тестування для виявлення помилок з метою їх усунення. Для цього потрібно створити тестову мережу. Як це зробити:

В першу чергу необхіодно запустити декілька вузлів мережі у тестовому режимі використовуючи віртуальні машини або спеціалізовані сервіси, які призначені для тестування мереж [7].

Наступним чином потрібно налагодити мережі відповідно до її параметрів тестування, таких як алгоритм консенсусу, приватність та масштабування, а після перших тестів потрібно перевірити результати тестування та зробити висновки, чи відповідають результати вашим вимогам чи ні.

В третю чергу, коли тестування вже проведено, мережа налаштована і працює відносно стабільно, потрібно перевірити, чи працюють її основні функції. Наприклад, чи створюються блоки, як проходить процес підписання та передачі транзакцій, перевірка балансу, налаштування параметрів користування, тощо [7].

Також дуже важливо визначити наскільки продуктивною є мережа. Потрібно лише виміряти швидкість, з якою відбуваються транзакції, час створення нового блоку та час затримки при виконанні тих чи інших операцій. Краще всього, після вимірів зрівняти свої результати з результатами якоїсь відомої мережі, щоб зрозуміти, до чого приблизно потрібно намагатися йти.

Незважаючи на фіксовані масштаби мережі, варто протестувати її збільшивши її масштаби, додавши багато різних вузлів. Такий крок суттєво поліпшить якість користування та швидкодію мережі [7].

Четвертим і одним із самих основних пунктів є тестування параметрів безпеки. В даному випадку вам потрібно побути в ролі зловмисника і намагатися усіма можливостями нанести шкоду вашій мережі, роблячи кібер-атаки на неї, щоб перевірити, наскільки вона стійка до різних видів атак та внести відповідні корективи.

П’ятим пунктом є проведення тестування роботи мережі після збоїв. Потрібно змоделювати різні сценарії збою, наприклад, втрата з'єднання, низька швидкість інтернету, втрата даних, чи кібер атака. Все це потрібно для того, щоб визначити, який час потрібен мережі, щоб продовжити нормальне функціонування, цілісність даних, тощо [7].

Останнім пунктом налаштування мережі буде проведення аналізу роботи мережі. Своєчасно виявлені проблеми та помилки потрібно усунути і провести тестування ще раз для виявленних других “підводних каменів”.

Після завершення тестування, ви можете впевнено випускати мережу у світ, але не зважаючи на впевненість в її ефективності, завжди потрібно ретельно наглядати за тим, як працює мережа, щоб у разі збоїв чи помилок ви могли швидко усунути їх та не створювати перешкоди звичайним користувачам.

3 ЗАХИСТ ІНФОРМАЦІЇ

На сьогоднішній день, інформація є найціннішим ресурсом у житті кожної людини. Сучасні технології дозволяють отримувати інформацію практично миттєво. Світові події, наукові відкриття, музика – все, що тільки душа забажає. Тому використання новітніх технологій для захисту інформаційних ресурсів стає все більш актуальним. Основна мета створення системи інформаційної безпеки полягає у забезпеченні надійного зберігання та ефективного використання інформації у будь-якій сфері діяльності [8].

Передусім, на сучасному етапі кібербезпека стикається з постійно зростаючими загрозами. Кібер атаки, віруси, шпигунське програмне забезпечення та інші кіберзлочини стали буденною реальністю. Інформаційні системи, бази даних, особисті пристрої – всі вони піддаються ризику. Тому фахівці з інформаційної безпеки стають незамінними у боротьбі з цими загрозами.

Іншим важливим аспектом є розвиток законодавства, яке стосується захисту персональних даних. У багатьох країнах приймаються нові закони, що регулюють збір, зберігання та обробку інформації. Це створює потребу в кваліфікованих спеціалістах, які допоможуть підприємствам виконувати ці вимоги та захищати дані [8].

Третій аспект це швидкий розвиток технологій. Зі збільшенням використання штучного інтелекту, блокчейну та інших інноваційних технологій виникають нові потенційні вразливості.

Захист інформації не лише актуальний, але й невід'ємний елемент сучасного світу. Від ефективності заходів захисту залежить не тільки безпека даних, але й стабільність функціонування телекомунікаційних мереж, індивідуальна приватність та навіть національна безпека [8].

Тому розвиток кваліфікованих фахівців у цій галузі є критично важливим для нашого суспільства.

3.1 Види захисту інформації

Існують різноманітні засоби захисту інформації, які активно використовуються для забезпечення конфіденційності, цілісності та доступності даних. Ось декілька основних засобів захисту інформації:

Спершу варто виділити **морально-етичні** засоби. До цієї категорії належать норми поведінки, які традиційно сформувалися або формуються з поширенням комп'ютерних систем, мереж тощо. Ці норми не є обов'язковими і не затверджені законодавчо, але їх невиконання часто призводить до втрати авторитету особи, групи людей, організації або навіть країни. Морально-етичні норми можуть бути як неписаними, так і оформленими в певні статути. Найбільш яскравим прикладом є Кодекс професійної поведінки членів Асоціації користувачів комп'ютерних систем США [9].

Наступними в цьому переліку є **правові засоби захисту**. До них належать закони, укази та інші нормативні акти, що регламентують правила використання інформації та відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ. Перехід до інформаційного суспільства вимагає вдосконалення карного та цивільного законодавства, а також судочинства.

На сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно оновлюються. Порівняти їх між собою практично неможливо, оскільки кожен закон потрібно розглядати у контексті всього законодавства [9].

Загальною тенденцією, яку можна простежити, є підвищення суворості кримінальних законів щодо комп'ютерних злочинців. Наприклад, у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу ІТ-системи або веб-сайту, є 10 років позбавлення волі.

Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти

неоподатковуваних мінімумів доходів громадян, виправними роботами на строк до двох років або обмеженням волі на той самий строк.

3.2 Криптографія

Криптографія — це наука, що займається захистом інформації через її перетворення у вигляд, який може бути оброблений і прочитаний тільки одержувачами, яким відомий спосіб шифрування. Її перше відоме використання відбулося приблизно в **XIX** столітті до нашої ери у вигляді символів, знайдених у єгипетській гробниці. Одним із найперших і найвідоміших прикладів криптографії є шифр Цезаря, створений Юлієм Цезарем близько 40 року до нашої ери. Цей метод шифрування використовує секретний ключ, який визначає, як зашифрувати і розшифрувати повідомлення. Шифр Цезаря є прикладом шифру заміни, де кожна літера алфавіту замінюється на літеру, що знаходиться на певній фіксованій відстані далі по алфавіту. Наприклад, алфавіт може бути зміщений на п’ять позицій вправо, тобто буква «A» стає «F», «B» — «G» і так далі. Це дозволяло Цезарю передавати повідомлення, не боячись їх перехоплення, оскільки тільки його офіцери знали, як їх розшифрувати [10].

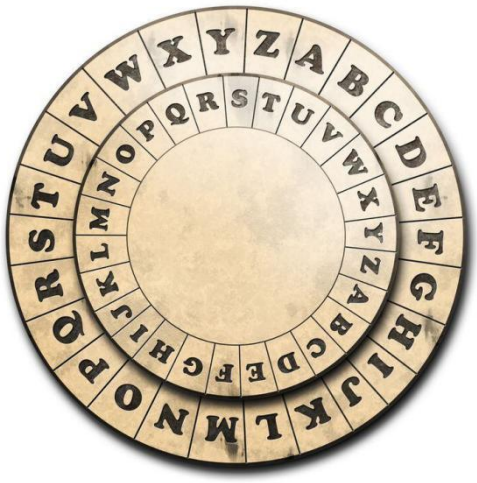


Рисунок 3.1 - Колесо шифру Цезаря

3.3 Алгоритм роботи криптографії

Існує багато способів шифрування інформації, і рівень складності залежить від ступеня захисту даних, який може вимагатися. Але ми зазвичай бачимо три типи криптографічних алгоритмів [10].

Першим з них є **симетричне шифрування**. Симетричне шифрування, також відоме як шифрування з секретним ключем, базується на використанні одного ключа. Це означає, що і відправник, і одержувач даних застосовують один і той самий ключ для шифрування та розшифровування інформації. Секретний ключ повинен бути узгоджений заздалегідь. Хоча симетричне шифрування є ефективним способом захисту даних, наявність лише одного ключа створює певний ризик, особливо при передачі його через незахищені з'єднання [11].

Наступним способом шифрування є **асиметричне шифрування**. Відмінністю цього методу від симетричного є використання пари ключів. Цей додатковий рівень безпеки значно підвищує захист даних. В асиметричному шифруванні кожен ключ має свою унікальну функцію. Існує відкритий ключ, який можна передати будь-кому в будь-якій мережі. Він використовується для шифрування даних і доступний для всіх. Однак є також закритий ключ, який залишається конфіденційним і використовується для розшифровування повідомлень. Обидва ключі створюються за допомогою алгоритму, що використовує великі прості числа, щоб згенерувати дві унікальні математично пов'язані ключі [11].

Іншим засобом захисту інформації є **хеш-функції**. Цей метод не використовує ключі, а покладається на алгоритми, які перетворюють будь-які вхідні дані в рядок символів фіксованої довжини. Хеш-функції відрізняються від інших видів шифрування тим, що працюють лише в один бік, тобто неможливо відновити вихідні дані з хешу. Хеші відіграють важливу роль в управлінні блокчейном, оскільки можуть шифрувати великі обсяги інформації, не змінюючи вихідні дані.

Організований спосіб структурування даних не тільки підвищує ефективність, але й дозволяє хешам виступати як цифрові відбитки пальців для зашифрованих даних. Це допомагає перевіряти інформацію та захищати її від неавторизованих змін під час передачі через мережі. Якщо вихідні дані змінюються, створюється новий хеш, який вже не збігається з оригінальним, і тому не може бути перевірений у блокчейні [11].

Останнім засобом захисту інформації є **цифрові підписи**, які відіграють важливу роль у забезпеченні безпеки, автентичності та цілісності даних у повідомленнях, програмному забезпеченні чи цифрових документах. Як випливає з їхньої назви, вони діють аналогічно фізичним підписам і є унікальним способом прив'язати вашу особу до даних, виступаючи як метод верифікації інформації. Проте, на відміну від фізичних підписів, які мають унікальний символ для представлення особи, цифрові підписи ґрунтуються на криптографії з використанням відкритого ключа [11].

Цифровий підпис представляє собою код, який додається до даних за допомогою двох взаємно автентифікованих ключів. Відправник створює цифровий підпис, використовуючи свій закритий ключ для шифрування даних, пов'язаних з підписом, тоді як одержувач отримує відкритий ключ від відправника для розшифрування даних.

Даний код служить доказом того, що повідомлення було створено відправником і не було змінено під час передачі. Він забезпечує, що відправник не може заперечити факт відправлення повідомлення. Якщо одержувач не може розшифрувати та прочитати підписаний документ за допомогою наданого відкритого ключа, це свідчить про певні проблеми, що робить його неможливим до автентифікації [11].

3.4 Алгоритми шифрування інформації

Оглянувши детально, що з себе представляють різні засоби захисту інформації, можна глибше зануритися в дану тему та дізнатися про

алгоритми різних засобів захисті інформації, виявити їх перспективи, взвісивши їх всі переваги та недоліки.

Давайте розпочнемо з симетричних алгоритмів шифрування AES (Advanced Encryption Standard) та DES (Data Encryption Standard). Ці алгоритми використовуються для перетворення даних у формат, що не може бути прочитаний без відповідного дешифрування, яке може проводити лише уповноважений користувач. Ось рисунок, що порівнює AES та DES (рисунок 3.2) [12]:

Характеристика	AES	DES
Розмір блоку	128 біт	64 біт
Розмір ключа	128, 192 або 256 біт	56 біт
Стійкість до злому	Висока	Низька
Швидкість	Швидший	Повільніший
Складність	Складніший	Простіший

Рисунок 3.2 - Порівняння AES та DES

Поговоривши про AES, варто відзначити декілька його переваг. По-перше, це **висока стійкість до злому**, оскільки алгоритм вважається стійким до сучасних методів криптоаналізу. Крім того, AES відзначається **гнучкістю**, оскільки підтримує різні розміри ключів (128, 192, 256 біт), що дозволяє налаштувати рівень безпеки відповідно до потреб. Не останню роль грає і **швидкість** цього алгоритму, що робить його відмінним вибором для шифрування великих обсягів інформації. Однак серед його недоліків можна відзначити **складність**, що може призвести до додаткового навантаження на технічне обладнання [12].

Порівнюючи DES з AES, слід відзначити наступні переваги. По-перше, DES відрізняється **простотою** у порівнянні з AES, що робить його легким для розуміння та реалізації. Крім того, цей алгоритм **має широке поширення** і був прийнятий як стандарт ще багато років тому, тому він широко застосовується в різних системах [12].

З даних плюсів також випливають свої мінуси. Через свою простоту DES стає вразливим до атак. Навіть якщо цей алгоритм вважається стійким до атак грубою силою, він залишається вразливим до більш складних методів криптоаналізу. Крім того, він використовує малий розмір ключа - всього 56 біт, що у сучасному світі вважається недостатньо безпечним. По своїй структурі, DES є повільнішим алгоритмом, ніж AES, що може створювати проблеми при шифруванні великих обсягів даних.

У порівнянні з DES, AES є більш безпечним, гнучким та швидшим алгоритмом шифрування. Тому для більшості випадків, де потрібне шифрування даних, рекомендується використовувати AES. DES може застосовуватися лише для неконфіденційних даних або в системах, де за якихось причин AES не може бути реалізований [12].

Продовжимо з асиметричними алгоритмами шифрування **RSA та Elliptic Curve Cryptography**, які використовуються для безпечного обміну даними та цифрових підписів. Ось рисунок, що порівнює RSA та ECC (рисунок 3.3):

Характеристика	RSA	ECC
Математична основа	Множення великих чисел	Еліптичні криві
Розмір ключа	1024, 2048, 4096 біт або більше	256, 384, 521 біт або більше
Швидкість	Повільніший	Швидший
Стійкість до злому	Вважається стійким, але існують теоретичні атаки	Вважається стійким
Складність	Складніший	Простіший

Рисунок 3.3 - Порівняння RSA та ECC

Почнемо з переліку переваг та недоліків RSA. Цей алгоритм має широке поширення і був прийнятий як стандарт ще багато років тому. Крім того, RSA підтримує багато мов програмування, що полегшує процес його інтеграції [17].

Проте, RSA є повільним методом захисту і не підходить для роботи з великими обсягами інформації. Він також використовує великий розмір

ключа (1024, 2048, 4096 біт і більше), що може створити проблеми зі зберіганням та обчисленням.

Тепер розглянемо ECC (Elliptic Curve Cryptography), який може похвалитися більшою швидкістю роботи порівняно з RSA, а також має менший розмір ключа (256, 384, 521 біт і більше), що робить його зручним для зберігання та обчислення. Варто відзначити його стійкість до атак квантових комп'ютерів, що робить його перспективним алгоритмом на майбутнє [17].

Серед недоліків ECC можна виділити його складність порівняно з RSA та меншу популярність, через що можливо буде складніше реалізувати його в деяких системах. ECC є швидшим, безпечнішим та економічнішим алгоритмом, ніж RSA. Тому ECC рекомендується для більшості випадків, де потрібне асиметричне шифрування. RSA може бути використаний лише для систем, де впровадження ECC неможливе.

Ну і на останок, проведемо детальний огляд двох алгоритмів хешування **SHA256 та MD5** які використовуються для перетворення даних у фіксований розмір хеш-значення. Хеш-значення використовуються для перевірки цілісності даних, аутентифікації та цифрових підписів. Ось рисунок, що порівнює параметри SHA256 та MD5 (рисунок 3.4) [18]:

Характеристика	SHA256	MD5
Розмір хешу	256 біт	128 біт
Стійкість до злому	Вважається стійким	Вразливий до атак
Швидкість	Швидший	Повільніший
Складність	Складніший	Простіший

Рисунок. 3.4 - Порівняння SHA256 та MD5

SHA256 володіє значною стійкістю до злому, що робить його надійним перед сучасними методами криптоаналізу. Даний алгоритм також відрізняється більшим розміром хешу (256 біт), що забезпечує вищу стійкість до колізій, порівняно з 128-бітовим MD5.

Однак основними недоліками SHA256 є його складність, яка може призвести до збільшення навантаження на процесор та повільніша швидкість роботи, порівняно з таким самим MD5. Це може виникнути труднощі при хешуванні великого обсягу даних [18].

У контексті MD5, слід зауважити, що він має простоту в користуванні та розумінні, проте він менш стійкий до зломів, ніж SHA256. Хоча MD5 все ще використовується в окремих системах, його використання рекомендується лише для неконфіденційних даних або в системах, де не можна реалізувати SHA256.

Важливо підкреслити, що криптографія - це постійно розвиваючася область, і з часом з'являються нові алгоритми хешування. Саме тому важливо слідкувати за останніми досягненнями у цій сфері та використовувати найсучасніші методи хешування для захисту ваших даних. Хеш-функції використовуються в різних сферах, таких як:

Цифрові підписи. Хеш-функції використовуються для створення цифрових підписів, які забезпечують гарантії автентичності та цілісності повідомлення. Це важливий засіб для підвищення рівня безпеки та збереження цілісності даних [18].

Контроль цілісності даних. Хеш-функції використовуються для перевірки цілісності даних, щоб гарантувати, що дані не були змінені під час конвертації або зберігання.

Аутентифікація паролів. Хеш-функції використовуються для збереження паролів у безпечному форматі. Замість зберігання паролів у відкритому вигляді, система перетворює їх на хеш-коди. Коли користувач вводить свій пароль для входу в систему, система генерує хеш введеного пароля та порівнює його зі збереженим хешем. Якщо вони співпадають, система допускає користувача [18].

Захист від підробки файлів. Хеш-функції застосовуються для перевірки цілісності завантажених файлів. Перед завантаженням файлу автор може надати його хеш-значення. Після завантаження користувач може

обчислити хеш-код завантаженого файлу та порівняти його з опублікованим значенням. Якщо вони співпадають, це означає, що файл не був змінений під час завантаження.

Блокчейн. Хеш-функції грають ключову роль у блокчейні. Кожен блок має своє хеш-значення, яке базується на хеші попереднього блоку, утворюючи послідовний ланцюжок блоків. Це забезпечує надійну стійкість до будь-яких спроб змінити дані: якщо хтось намагається змінити блок, це призведе до зміни його хеш-значення та всіх наступних блоків у ланцюжку [18].

Такий підхід робить будь-які зміни легко виявимими. Вибір між SHA256 та MD5 залежить від конкретних обставин. Якщо вам потрібна надійна стійкість до вторгнень, варто обрати SHA256. У випадку, коли критичним є швидкість обробки, MD5 може бути розглянутий, але тільки для некритичних даних.

3.5 Сфери застосування алгоритмів шифрування

Алгоритми шифрування грають вирішальну роль у забезпеченні безпеки даних, захищаючи їх від несанкціонованого доступу, модифікації або видалення. Вони використовуються у різних ситуаціях, щоб забезпечити конфіденційність, цілісність та автентичність даних [10].

Наприклад, вони використовуються для захисту фізичних пристроїв, таких як комп'ютери, ноутбуки та мобільні пристрої, шифруючи їхні жорсткі диски та SSD-накопичувачі. Це дозволяє зберігати конфіденційну інформацію безпечно, навіть у разі втрати або крадіжки пристрою.

Крім того, за допомогою шифрування створюються захищені резервні копії, що забезпечують захист даних навіть у випадку витоку резервних копій. Шифрування також використовується для захисту окремих файлів або папок з чутливою інформацією, такою як фінансові документи або медичні записи. У мережах шифрування застосовується для захисту трафіку між пристроями і

серверами, а також між браузерами та веб-сайтами, щоб забезпечити безпечне з'єднання [10].

Також важливо забезпечити шифрування електронних листів, оскільки це один із найпоширеніших способів комунікації, і забезпечення безпеки та конфіденційності цих даних є вельми важливим.

В кінці кінців, хоча ми вже знаємо про широке використання шифрування в нашому житті, криптографія охоплює значно більше сфер, ніж ми можемо собі уявити, і її роль постійно зростає разом із збільшенням обсягу зберігання, передавання та обробки інформації [10].

4 ОПТИМІЗАЦІЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Детально розглянувши інформацію про блокчейн технології, методи захисту інформації, їх переваги та недоліки, ми можемо перейти до питання оптимізації характеристик блокчейн-технологій для підвищення безпеки та конфіденційності у телекомунікаційних мережах.

Блокчейн може стати ключовим інструментом для підвищення безпеки та конфіденційності в телекомунікаційних мережах, завдяки своїй децентралізованій природі, стійкості до змін та прозорості. Для оптимізації використання блокчейну у телекомунікаційних мережах рекомендується врахувати наступні підходи:

4.1 Масштабованість

Насправді, масштабованість завжди була надважливою темою у світі блокчейну. Більшість мереж блокчейнів просувають високу швидкість обробки транзакцій на секунду як свою головну перевагу, але це не завжди відображає їхню справжню продуктивність. Оцінка продуктивності мереж стає складною через різноманітність транзакцій. Треба мати на увазі, що не всі транзакції є однаковими [13].

Для компенсації виконавцям транзакцій, блокчейни стягують плату, яка залежить від обчислювального навантаження, необхідного для виконання транзакцій. Оскільки транзакції можуть мати різний рівень складності і, відповідно, різний розмір комісії, які вони використовують, порівнювати кількість транзакцій на секунду у різних блокчейнах має обмежене значення. Замість цього, більш цілісною є порівняльна оцінка їх обчислювальної потужності або пропускної здатності.

Наступним чином, варто розуміти, які є обмеження масштабованості, оскільки блокчейн-мережа прагне бути максимально децентралізованою та інклюзивною [13].

Для досягнення цього, слід спрямовувати зусилля на **контроль апаратних вимог**, оскільки рівень децентралізації мережі залежить від потужності найслабшого вузла, який перевіряє блокчейн та зберігає його стан. Тому важливо знизити витрати на запуск вузла (зокрема, витрати на апаратне забезпечення, пропускну здатність і зберігання даних), щоб залучити якнайбільше учасників до мережі.

Далі, важливо враховувати **зростання стану мережі**, що визначається швидкістю розвитку. Чим більшу пропускну здатність блокчейн може забезпечити за одиницю часу, тим швидше він розвивається. Повні вузли мережі зберігають її історію і повинні бути здатні перевіряти її стан [13].

Також варто звернути увагу на **час синхронізації** повного вузла. При першому запуску він повинен синхронізуватися з усіма існуючими вузлами, завантажити і перевірити стан мережі від генезисного блоку до вершини ланцюжка. Цей процес повинен бути максимально швидким і ефективним, щоб будь-хто міг стати учасником протоколу без додаткового дозволу.

Щодо визначення масштабованості мережі, слід враховувати, що це поняття часто неправильно тлумачиться в блокчейн-галузі. Хоча збільшення пропускної здатності є бажаним аспектом, воно лише один з багатьох факторів, що складають поняття масштабованості. Насправді, масштабованість це здатність збільшувати кількість транзакій не використовуючи додаткового обладнання [13]. З цієї причини масштабованість можна розділити на дві категорії.

Перша категорія це **масштабованість секвенсора**. Процес секвенування означає упорядкування та обробку транзакцій у мережі. Хоча можна легко збільшити пропускну здатність будь-якого блокчейну, змінивши розмір блоку та час його обробки, це не завжди приводить до бажаних результатів,

оскільки може негативно вплинути на децентралізацію мережі. Тому важливо враховувати інші аспекти, такі як масштабованість верифікації [13].

Масштабованість верифікації описує підходи, які збільшують пропускну здатність без збільшення апаратних витрат на вузли. Один із таких підходів - це використання криптографічних інновацій, наприклад, доказів валідності. Такі інновації дозволяють створювати так звані "роллапи", які ефективно масштабують блокчейн.

Валідація у роллапі переміщує обчислення та зберігання стану за межі ланцюжка, залишаючи невелику кількість даних у ланцюжку. Під час роллапу, стиснуті транзакції та поточний стан надсилаються позаланцюговому верифікатору, який генерує докази валідності результатів. Після цього він перевіряється в ланцюжку, що дозволяє оновлювати стан роллапу. Важливо розуміти, що багато підходів до масштабування блокчейну фокусуються лише на збільшенні пропускної здатності, ігноруючи вплив на вузли та децентралізацію мережі [13].

З появою криптографії з перевіркою достовірності блокчейн може досягти справжньої масштабованості, яка не навантажує вузли постійно зростаючими витратами і забезпечує високий рівень децентралізації. Тепер можлива більша кількість транзакцій з потужними і більш складними обчисленнями на тому ж обладнанні.

4.2 Приватність та ефективність

У нашому сучасному світі, де роль технологій блокчейн зростає, забезпечення конфіденційності та ефективності залишається однією з найважливіших задач. Aleo - відома платформа першого рівня в цій області використовує докази з нульовим знанням, щоб забезпечити максимальний рівень конфіденційності. Особливою технологією є **zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)**, яка забезпечує високий рівень конфіденційності без втрати ефективності [14].

Впровадження адаптивних протоколів zk-SNARK на платформі Aleo відзначається як значний крок уперед у розвитку блокчейн-технологій, оскільки вона вирішує ключові проблеми та встановлює нові стандарти в цій області. Для розуміння інновацій адаптивних zk-SNARK важливо ознайомитися з основами цієї технології.

zk-SNARK - це криптографічний метод, який дозволяє одній стороні підтверджувати правильність певного твердження перед іншою стороною, не розкриваючи при цьому деталей цього твердження. Традиційні методи zk-SNARK вже були важливими для забезпечення конфіденційності, але вони мали свої обмеження, такі як складність обчислень та великий розмір, що ускладнювало їхнє використання в масштабних системах. Адаптивні zk-SNARK пропонують рішення цих проблем, дозволяючи гнучко налаштовувати процеси створення та перевірки доказів, що значно полегшує масштабування та підвищує ефективність мережі [14].

Технічне занурення в адаптивний протокол zk-SNARK в мережі Aleo базується на передових криптографічних дослідженнях, які стежать за динамікою транзакцій. Ось кілька деталей цих технічних аспектів:

Першим з них є **стиснення доказів без втрати цілісності даних**, де алгоритми стиснення гарантують, що докази залишаються компактними, але повними, використовуючи складні математичні моделі.

Другим з них є **паралельна обробка**, оскільки її використання дозволяє генерувати та перевіряти кілька доказів одночасно, що значно зменшує час, необхідний для цих операцій. Наступним аспектом є алгоритмічна оптимізаці, оскільки алгоритми в даній технології повністю оптимізовані для продуктивності, мінімізуючи обчислювальне навантаження та кількість кроків, необхідних для генерації та перевірки доказів [14].

Впровадження адаптивних алгоритмів приносить такі переваги як, **покращена конфіденційність**, оскільки зберігаючи цілісність доказів з нульовим знанням, мережа гарантує конфіденційність та захищеність транзакцій користувачів.

Завдяки можливості обробляти велику кількість транзакцій і зменшити час та ресурси, збільшується масштабованість мережі, що дозволяє приймати більше користувачів та транзакцій [14].

Ну а якщо ми можемо масштабувати мережу без додаткого обладнання та затрат, то звідси можна виявити таку перевагу, як **зменшення вартості**, оскільки оптимізовані процеси генерації та перевірки доказів зменшують витрати, пов'язані з обробкою транзакцій, роблячи мережу економічно вигідною для користувачів.

У підсумок важливо відзначити, що впровадження адаптивних протоколів є вагомим кроком у розвитку блокчейн-технологій, зокрема, Aleo визначає себе як лідера у конфіденційних блокчейн-транзакціях, преодолавши обмеження традиційних протоколів. Динамічна та ефективна природа адаптивних алгоритмів дозволяє мережам масштабуватися та працювати оптимально, відповідаючи потребам сучасних децентралізованих додатків [14].

З розвитком екосистеми блокчейнів, інновації стають важливими для майбутнього конфіденційності та ефективності. Aleo активно працює над розширенням цих технологій, створюючи безпечну, масштабовану та зручну блокчейн-мережу. Чи то у фінансовому секторі, охороні здоров'я або управлінні ланцюгами постачання, переваги адаптивних zk-SNARK очевидні, відкриваючи шлях до більш приватного та ефективного цифрового світу.

4.3 Інфраструктура

З появою стрімкого розвитку технології блокчейн виявилася потреба в подальшому поліпшенні можливостей та характеристик. Це призвело до виникнення різних рівнів блокчейну, які включають Рівень 0, Рівень 1, Рівень 2 і Рівень 3 [15].

Кожен з цих рівнів вносить свої корективи, які поліпшують технологію та роблять її більш практичною для використання у різних галузях. Кожен з цих рівнів також має свої переваги та недоліки, які важливо враховувати розробникам блокчейну при виборі найбільш оптимального рівня для своїх проектів.

Блокчейн рівня 0. “Нульовий” рівень блокчейну є основним рівнем технології, який є фундаментом для всіх інших рівнів. Даний рівень включає в собі загальні принципи роботи блокчейну, наприклад алгоритми консенсусу, методи забезпечення безпеки та механізми обробки транзакцій. Структура всієї системи визначається завдяки цьому рівню [16]. Взагалі блокчейн даного рівня вважається подібним до операційної системи, на якій працює ваш ПК. Подібно до операційної системи, він виконує основні функії.

Так для чого взагалі потрібен блокчейн рівня 0? Взагалі, це інновація в галузі блокчейну. Багато старих мереж вбудували протоколи рівня 0 у свої початкові структури. Однак є деякі переваги для того, щоб ці протоколи були вбудовані окремо [16].

Перша вагома перевага полягає у **взаємодії**. У світі сучасних блокчейн-систем переважно спостерігається велика закритих мереж. Такі мережі функціонують самі по собі, без можливості простої та швидкої передачі даних між собою. Проте, ключова перевага рівня 0 полягає в тому, що будь-які мережі, які побудовані на його основі, є взаємними. Оскільки будь-який блокчейн, зведений на рівні 0, має однакову базову структуру, різні мережі можуть легко взаємодіяти одна з одною.

Інфраструктура рівня 0 відкриває можливості для різних ланцюгів, дозволяючи їм самостійно запускати однакові типи смарт-контрактів та обмінюватися даними в обидва напрямки [16].

Це значно спрощує процес розробки застосунків для розробників, бо вони можуть використовувати одні й ті ж інструменти та ресурси для створення різноманітних блокчейн-додатків. Такий підхід сприяє створенню більш зручного та дружнього середовища для всіх учасників екосистеми блокчейну.

Ще однією вагомою перевагою є рішення проблеми **масштабованості**. Багато провідних мереж намагаються впоратися з великою кількістю користувачів, що часто породжує проблеми з масштабованістю. Коли велика кількість осіб здійснює транзакції, час обробки може сповільнитися, а комісії зростати [16].

На щастя, сумісність мереж на даному рівні також призводить до унікальних рішень для масштабованості, які використовуються розробниками для створення схожих мереж, що функціонують паралельно разом з мережею. Це дозволяє їм керувати більшою кількістю трансакцій без значного навантаження на апаратне забезпечення. Можливість використання таких рішень у системах поліпшує ефективність та сприяє зниженню комісій.

Останньою перевагою цього рівня є його гнучкість у створенні, що сприяє вирішенню проблем з розвитком. Створення блокчейн-мереж часто є складним завданням, і багато розробників шукають систему, яка б могла надати інструменти для розробки програмного забезпечення. Завдяки мережам цього рівня, розробка блокчейн-мереж стала набагато зручнішою.

Розробники блокчейну отримують корисну структуру і вони не обмежені абсолютно нічим. Вони можуть легко створювати власний блокчейн-рівень, який задовольнить потреби їх власних проєктів [16].

Тепер поговоримо про те, як працює блокчейн рівня 0. Взагалі, кожен блокчейн цього рівня трішки відрізняється тому, що деякі з них можуть використовувати різні смарт-контракти або різні алгоритми консенсусу для обробки даних, але незважаючи на всі ці відмінності, більшість мереж все одно базуються на одній і тій самій концепції блокчейну.

У типовому блокчейні рівня 0 використовується поєднання всіх цих механізмів. Серед ланцюгів блокчейну можна виділити два типи ланцюгів [16].

Першим з них є **головний ланцюг (англ. mainchain)**, який поєднує у собі всі інші компоненти. У свій журнал він облікує всі транзакції, які регулярно

оновлюються інформацією, яка знаходиться на інших блокчейнах мережі. Блокчейн базового рівня дуже схожий на традиційну базу даних.

Далі йдуть **сторонні або бічні ланцюги (англ. sidechains)**. Це можна назвати системами з власними параметрами. Кожен з них функціонує на основі загальної структури основного рівня, але також має можливість включати унікальні програмні рішення, відповідні власним конкретним потребам [16].

За допомогою **кросчейн платформ**, передається інформація між ланцюгами. Вони надійно з'єднуються як з бічним, так і з основним ланцюгом. Крім того, вони можуть передавати як токени, так і дані, щоб усі типи необхідних цифрових активів могли проходити назад і вперед між різними частинами блокчейну рівня 0.

Після детального огляду даної технології варто перерахувати всі переваги та недоліки для впевненості свого вибору під час створення власної мережі.

Серед переваг можна виділити **безпеку**, оскільки вибір правильних та надійних протоколів забезпечать користувачеві повну безпеку [16].

Технологія може похизувати **відсутністю централізованого органу**, що робить ваші дані ще конфіденційнішими.

Ну і на останок можна виділити **сумісність**. Всі протоколи блокчейну в цьому рівні дозволяють декільком мережам легко взаємодіяти один з одним [16].

Говорячи про недоліки, першим з них можна виділити **складність**, оскільки використання більше, ніж однієї мережі, робить будь-який проєкт складнішим в створенні та використанні.

Наступним недоліком є **велике споживання електроенергії**, що може призвести до великих затрат на апаратне забезпечення. Звідси можна зрозуміти те, що і комісії транзакцій в мережі будуть значно більшими, що робить мережу менше привабливою для користувачів [16].

На останок, можна сказати те, що надаючи фундаментальну інфраструктуру іншим мережам, вона забезпечує додаткову масштабованість

блокчейну та сумісність з іншими мережами. Не зважаючи на те, що розробка проєктів в даній галузі потребує часу та значних зусиль, цей рівень блокчейну може значно спростити роботу розробникам втілити свої ідеї в реальність [16].

Блокчейн рівня 1. Виходячи з розповіді про блокчейн рівня 0, можна зрозуміти що він є базовим рівнем, на якому будуються всі інші рівні. По принципу побудови і своїм характеристикам, всі рівні схожі між собою, але кожен рівень кращий від свого попередника.

Блокчейн даного рівня є наступним рівнем і включає протоколи та системи, які притаманні для конкретної платформи. Цей рівень встановлює правила роботи з коштами та транзакціями. Він значно розширює можливості свого попередника, надаючи гнучкіші інструменти для роботи з даними [15].

Блокчейн рівня 2. Блокчейн даного рівня додає новітні протоколи та механізми, які поповнюють функціонал та підвищують масштабованість блокчейну. Цей рівень вирішує проблеми масштабування, швидкості та розміру комісії, які можуть виникати під час використання базових блокчейнів [15].

Блокчейн рівня 3. Третій рівень додає ще один рівень абстракції та функціональності, пов'язаний з додатковими сервісами та застосунками, що працюють поверх Другого рівня. Цей рівень включає децентралізовані застосунки, фінансові протоколи, послуги управління ідентифікацією та багато іншого. Цей рівень ідеально підходить для тих, хто хоче поєднати творчість з блокчейном. Наприклад, розробка ігор, тощо [15].

Кожен рівень блокчейну вносить свій внесок у розвиток технології. Від базової інфраструктури до розширених функцій - кожен рівень надає нові можливості та глибину. Ця взаємодія створює потужну екосистему, яка постійно розвивається та відкриває нові перспективи для інновацій.

ВИСНОВКИ

В дипломній роботі було детально розглянуто всі аспекти відносно блокчейну та яким чином він може буде інтегрований в галузі телекомунікацій. Теоретичний матеріал дає чітко зрозуміти те, що ми знаходимося на самому початку розвитку блокчейн технологій і за цим стоїть наше майбутнє.

Було проведено аналіз всіх наявних способів захисту в блокчейн сфері, порівняно їх ефективність, підраховано їх переваги та недоліки. Такий аналіз дає змогу звичайному користувачеві або розробнику зрозуміти, що саме йому потрібно.

Також було розглянуто предмет захисту інформації, оскільки це є невід’ємною частиною оптимізації безпеки та конфіденційості у сфері блокчейну. Було розглянуто багато аспектів, включаючи актуальність предмету, засоби захисту інформації, алгоритми шифрування, їх переваги та недоліки, різниця між кожним з них та який краще використовувати.

При виконанні завдання дипломного проєкту було розглянуто засоби поліпшення безпеки та конфіденційності відносно таких параметрів як, масштабованість, конфіденційність, безпека та інфраструктура.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Все про блокчейн: як працює, хто користується, де застосовують. [Електронний ресурс] – Режим доступу: https://tsn.ua/groshi/vse-pro-blokcheyn-yak-pracyuye-hto-koristuyetsya-de-zastosovuyut-2378878.html

2. Що таке блочейн і як він працює. [Електронний ресурс] – Режим доступу: https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work

3. В яких сферах застосовують блокчейн-технології. [Електронний ресурс] – Режим доступу: https://nachasi.com/crypto/2021/12/23/v-yakyh-sferah-zastosovuyut-blokchejn-tehnologiyi/

4. Українські блокчейн компанії. [Електронний ресурс] – Режим доступу: https://recruitika.com/tag/blockchain/

5. The Developer’s Guide to Blockchain Development. [Електронний ресурс] – Режим доступу: https://www.xilinx.com/products/design-tools/resources/the-developers-guide-to-blockchain-development.html

6. Що таке алгоритм консенсусу на блокчейні. [Електронний ресурс] – Режим доступу: https://academy.binance.com/uk/articles/what-is-a-blockchain-consensus-algorithm

7. Що таке розумний контракт. [Електронний ресурс] – Режим доступу: https://www.binance.com/uk-UA/square/post/43229

8. Актуальні аспекти захисту інформаційних ресурсів. [Електронний ресурс] – Режим доступу: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/46-10.pdf

9. Технології захисту інформації. [Електронний ресурс] – Режим доступу: https://shorturl.at/W48FF

10. Що таке криптографія. [Електронний ресурс] – Режим доступу: https://www.coindesk.com/uk/learn/what-is-cryptography/

11. Шифрування: типи і алгоритми. [Електронний ресурс] – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/

12. Difference between AES and DES ciphers. [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/

13. Переосмислення масштабованості. [Електронний ресурс] – Режим доступу: https://shorturl.at/mu2xD

14. Збільшення приватності та оптимізація продуктивності у мережі Aleo. zkSNARK. [Електронний ресурс] – Режим доступу: https://shorturl.at/1SMdm

15. Різниця між Layer 0, Layer 1, Layer 2, Layer 3 блокчейнами. [Електронний ресурс] – Режим доступу: https://teletype.in/@mexcukraine/Blockchain_layers

16. Блокчейн рівня 0. Інфраструктура за масштабованими мережами. [Електронний ресурс] – Режим доступу: https://learn.bybit.com/uk/blockchain/what-is-layer-0-blockchain/

17. What Are the Differences Between RSA, DSA, and ECC Encryption Algorithms. [Електронний ресурс] – Режим доступу: https://www.sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption

18. A comparative study of Message Digest 5(MD5) and SHA256 algorithm. [Електронний ресурс] – Режим доступу: https://iopscience.iop.org/article/10.1088/1742-6596/978/1/012116/pdf

ДОДАТКИ

Додаток А. Optimizing safety and privacy in telecommunication networks

After in-depth review on blockchain-technologies, data protection methods, their pros and cons, we can finally come up to the question of safety and privacy.

Blockchain is able to become a key instrument in safety and privacy improving because of it's decentralized nature, durability to changes and transparency. In order to improve the quality of blockchain-use, it's highly recommended using the ensuing approaches [13]:

The first one is **scaling**. Frankly speaking, scaling has always been the most important part of the blockchain. The vast majority of blockchains usually try to make common users pay attention to the number of transactions per second in order to promote their network, however, usually it does not provide a user the whole picture of the network productivity. And now it's quite a sophisticated task to evaluate a network productivity owing to various transation types.

In order to make a compensation for a transaction-maker, you'll have to pay fees, which size depends on computing load that is needed to perform all the transactions. As the transactions can have different levels of difficulty and respectively different amount of fees, comparing the number of transactions per second in various blockchain is not the best decision. Instead of it, it would be much more rational to use computing load and troughput capability as the methods of network evaluation [13].

Even though the network aspires to be as decentralized as even possible, we must not forget about scalability limitations. In order to reach this you should pay close attention to hardware requirements because the level of decentralization depends on power of the weakest node that checks up the blockchain and conserves it's condition. That's why you have to dwindle your spendings on a node launching process in order to involve as many users to your network as even possible.

In the next step it's of vital importance to take the g**rowth of the network state** into consideration. It is defined by the speed of development. The bigger throughput cabality it has, the faster it does grow up. Full nodes of the network save up it's history and must be capable to check up it's condition [13].

Moreover, it's worth to pay your attention to a full node s**ynchronization time**. When launched for the first time, it should get synced with all the existing nodes. It should download and check up the condition of the network starting from a fundamental block and finishing with top of the chain. The process must be as quick and effective as possible in order to involve more and more users to your network without any additional permission.

Usually, scalability is erroneously considered as a bigger amount of tools and hardware used up in the network, whereas it's actually a capability of network to increase the number of transaction withoun using any additional software of hardware. According to it, scalability can be broken up into two categories [13].

The first one is scalability of sequencer. Sequencing is the process of ordering and performing transactions in a network. Although you can easily increase throughput capability of any blockchain by changing size of a block and time of it's processing. However, it's highly likely it won't live up to your expectations and moreover it will definitely have a bad impact on decentralization of a network. So it's important to to take into consideration other aspects such as scalability of verification.

Scalability of verification describes approaches that increase throughput capability without increasing hardware amount. One of them involves cryptography innovations. For instance - validity proofs. Such an approach let's you develop "roll-ups" which can have a great impact on the network's scalability [13].

Validation in a roll-up transfers computation and state storage off-chain leaving only a little bit of data in a chain. During the roll-up process, compressed transactions and the network's current state are being sent to a off-chain verificator

who generates validity proofs. Afterward, verificator is checked up in the chain and it let's update the roll-up's state.

You need to know that a lot of approaches are focused only on increasing the network's thoughput capability ignoring an impact on nodes and decentralization of the network [13].

After validity check emergence the blockchain can reach it's real scalability that doesn't involve huge spendings on the network and provides decentralization. Now it's possible to make a lot of transactions with powerful and much more complicated computation on the same hardware. The much more it's used, the lower fees are.

Privacy and efficiency

Nowadays, blockchain technologies are being involved in lots of various spheres so it's of vital importance to ensure privacy and efficiency [14].

Aleo - a well know layer-1 platform that uses zero knowledge validity proofs in order to ensure the best level of privacy. There is a great technology - zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) that ensures a high level on privacy withoug losing it's efficiency.

The implementation of adaptive zk-SNARK protocols on the Aleo platform is marked as a significant step forward in the development of blockchain technology, as it solves key problems and sets new standards in this area. To understand the innovations of adaptive zk-SNARKs, it is important to familiarize yourself with the basics of this technology.

zk-SNARK is a cryptographic method that allows one party to confirm the correctness of a certain statement to another party without disclosing the details of that statement. Traditional zk-SNARK techniques were already important for privacy, but they had their limitations, such as computational complexity and large size, which made them difficult to use in large-scale systems. Adaptive zk-SNARKs offer a solution to these problems by allowing flexible customization of

the proof generation and verification processes, which greatly facilitates scaling and increases network efficiency [14].

Technical immersion in the adaptive zk-SNARK protocol on the Aleo network is based on advanced cryptographic research that monitors transaction dynamics. Here are some details of these technical aspects:

The first is evidence **compression without loss of data integrity**, where compression algorithms ensure that evidence remains compact but complete by using complex mathematical models [14].

The second of them is **parallel processing**, since its use allows the generation and verification of several pieces of evidence at the same time, which significantly reduces the time required for these operations. The next aspect is algorithmic optimization, since the algorithms in this technology are fully optimized for performance, minimizing the computational load and the number of steps required for proof generation and verification.

The implementation of adaptive algorithms brings such advantages as improved privacy, because by maintaining the integrity of proofs with zero knowledge, the network guarantees the privacy and security of user transactions.

Due to the ability to process a large number of transactions and reduce time and resources, the scalability of the network increases, allowing it to accept more users and transactions [14].

Well, if we can scale the network without additional hardware and costs, then from here we can find such an advantage as a **reduction in cost**, since the optimized processes of generation and verification of proofs reduce the costs associated with processing transactions, making the network economically profitable for users.

In conclusion, it is important to note that the introduction of adaptive protocols is an important step in the development of blockchain technologies, in particular, Aleo defines itself as a leader in confidential blockchain transactions, overcoming the limitations of traditional protocols.

The dynamic and efficient nature of adaptive algorithms allows networks to scale and work optimally, meeting the needs of modern decentralized applications [14].

As the blockchain ecosystem evolves, innovation becomes essential for the future of privacy and efficiency. Aleo is actively working to expand these technologies, creating a secure, scalable and user-friendly blockchain network. Whether in the financial sector, healthcare or supply chain management, the benefits of adaptive zk-SNARKs are clear, paving the way for a more private and efficient digital world.

Infrastructure

With the emergence of the rapid development of blockchain technology, there was a need for further improvement of capabilities and characteristics. This led to the emergence of different layers of the blockchain, which include Layer 0, Layer 1, Layer 2 and Layer 3 [15].

Each of these levels makes adjustments that improve the technology and make it more practical for use in various industries. Each of these levels also has its advantages and disadvantages, which are important for blockchain developers to consider when choosing the most optimal level for their projects.

Layer 0. Layer 0 blockchain is the fundamental level of technology that is the basis for all other layers. This level includes the fundamental principles of the blockchain, such as consensus algorithms (such as Proof of Work or Proof of Stake), security methods, and transaction processing mechanisms. The structure of the entire system is determined thanks to this level [16].

In general, blockchain at this level is considered similar to the operating system that runs on your PC. Like an operating system, it performs basic functions. So why do you even need a level 0 blockchain? In general, this is an innovation in the blockchain industry. Many legacy networks built layer 0 protocols into their

original architectures. However, there are some advantages to having these protocols embedded separately [16].

The first significant advantage is **interaction**. In the world of modern blockchain systems, there is mostly a large closed network. Such networks function by themselves, without the possibility of simple and fast data transfer between them. However, the key advantage of layer 0 is that **any networks that are built on top of it are mutual**. Since any blockchain at level 0 has the same basic structure, different networks can easily interact with each other.
Layer 0 infrastructure opens up possibilities for different chains, allowing them to independently run the same types of smart contracts and exchange data in both directions [16].

This greatly simplifies the application development process for developers, as they can use the same tools and resources to create a variety of blockchain applications. This approach contributes to the creation of a more convenient and friendly environment for all participants of the blockchain ecosystem.

Another significant advantage is the s**olution to the problem of scalability**. Many leading networks struggle to cope with large numbers of users, which often creates scalability issues. When a large number of people transact, processing times may slow and fees may increase [16].

Fortunately, network interoperability at this level also leads to unique scalability solutions that developers use to create similar networks that function in parallel with the network. This allows them to manage a larger number of transactions without a significant load on the hardware. The possibility of using such solutions in systems improves efficiency and helps reduce commissions.

A final advantage of this layer is its **flexibility** in creation, which helps to solve development problems. Building blockchain networks is often a challenging task, and many developers are looking for a framework that can provide tools for software development. Thanks to networks of this level, the development of blockchain networks has become much more convenient [16]. Blockchain developers get a useful structure and they are not limited by absolutely anything.

They can easily create their own blockchain layer that will meet the needs of their own projects.

Now let's talk about how a blockchain at level 0 works. In general, each blockchain at this level is slightly different because some of them may use different smart contracts or different consensus algorithms to process data, but despite all these differences, most networks still are based on the same blockchain concept.

A typical layer 0 blockchain uses a combination of all these mechanisms. Among blockchain chains, two types of chains can be distinguished [16]. The first of them is the **mainchain** , which combines all other components. It records all transactions in its log, which is regularly updated with information that is on other blockchains in the network. A basic-level blockchain is very similar to a traditional database.

Then there are **sidechains**. These can be called systems with their own parameters. Each of them operates on the basis of a common base-level structure, but also has the ability to include unique software solutions to suit its own specific needs [16].

With the help of **cross-chain platforms**, information is transferred between chains. They securely connect to both the side chain and the main chain. Additionally, they can transfer both tokens and data so that all types of digital assets required can pass back and forth between different parts of the Layer 0 blockchain.

After a detailed review of this technology, you need to list all the advantages and disadvantages to be sure of your choice when creating your own network.
Security can be highlighted among the advantages, since the choice of correct and reliable protocols will provide the user with complete security [16].
The technology can boast the absence of a centralized authority, which makes your valuable data even more confidential.

And finally, you can highlight compatibility. All blockchain protocols at this level allow multiple networks to easily interact with each other. Speaking about the

disadvantages, the first of them is **complexity**, since the use of more than one network makes any project more difficult to create and use [16].

The next drawback is **high power consumption**, which can lead to high hardware costs. From this it can be understood that transaction commissions in the network will be much higher, which makes the network less attractive for users .

In conclusion, we can say that the level 0 blockchain is an innovation in the blockchain industry. By providing the fundamental infrastructure to other networks, it provides additional blockchain scalability and interoperability with other networks. Despite the fact that the development of projects in this field requires time and considerable effort, this level of blockchain can significantly simplify the work of developers to turn their ideas into reality [16].

Layer 1. Based on the story about blockchain level 0, it can be understood that it is the basic level on which all other levels are built. According to the principle of construction and their characteristics, all levels are similar to each other, but each level is better than its predecessor.

A blockchain of this level is the next level and includes protocols and systems that are specific to a particular platform. This level sets the rules for working with funds and transactions. It significantly expands the capabilities of its predecessor, providing more flexible tools for working with data [15].

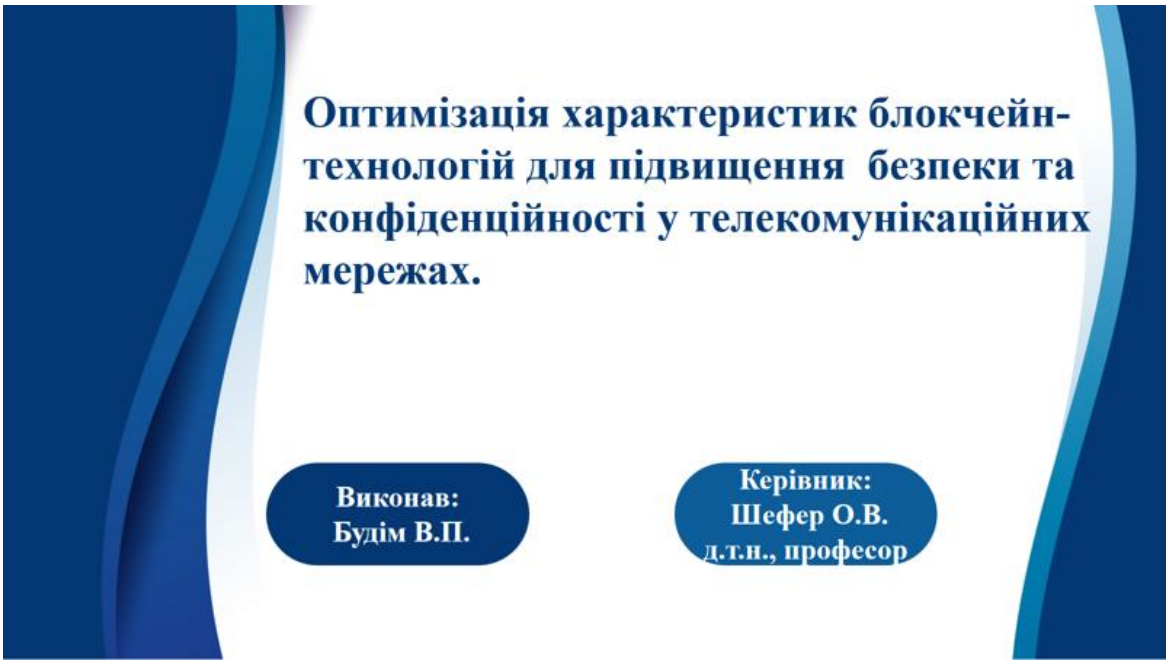
Layer 2. The blockchain of this level adds the latest protocols and mechanisms that supplement the functionality and increase the scalability of the blockchain. This layer addresses scalability, speed, and fee size issues that may arise when using underlying blockchains [15].

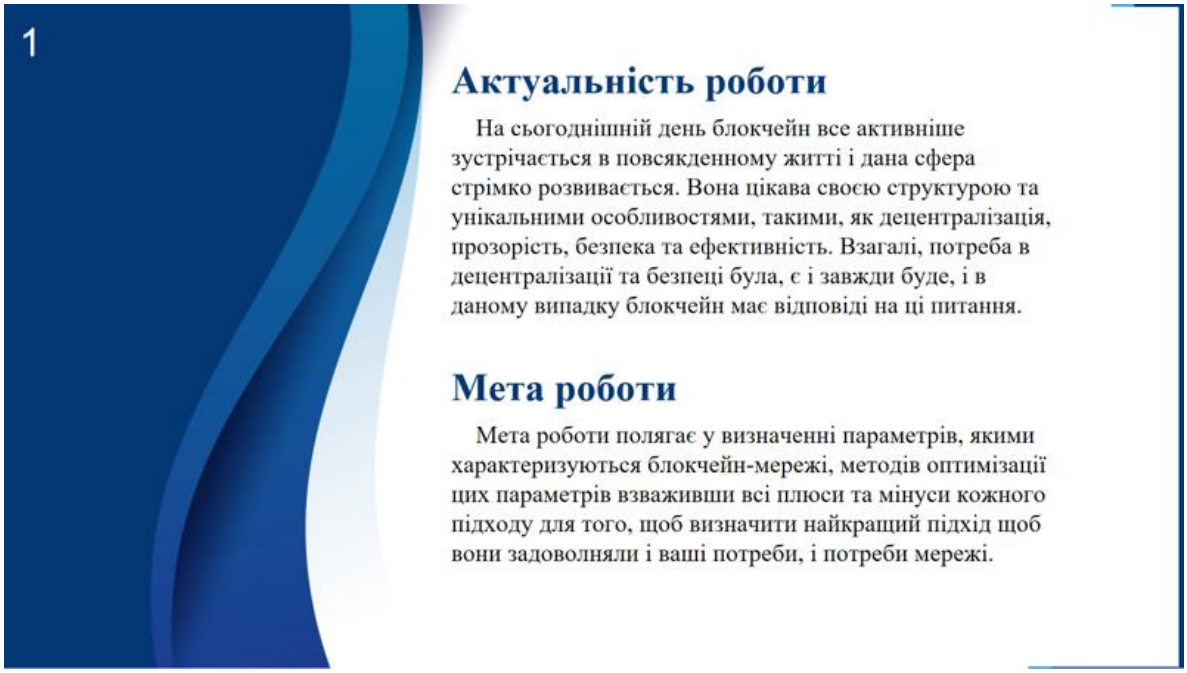
Layer 3. Layer Three adds another layer of abstraction and functionality related to additional services and applications running on top of Layer Two. This layer includes decentralized applications, financial protocols, identity management services, and more. This level is ideal for those who want to combine creativity with blockchain [15].

In conclusion, each layer of the blockchain contributes to the development of the technology. From basic infrastructure to advanced features, each level provides

new capabilities and depth. This interaction creates a powerful ecosystem that is constantly evolving and opening new perspectives for innovation.

Додаток Б. Плакати





2

Етапи у виконанні кваліфікаційної роботи

Аналітичний огляд блокчейн технологій, а саме їх особливості, алгоритми, галузі застосування врахуванння їх переваг та недоліків та огляд перспектив блокчейну.

Конструкторська частина. Побудова та налаштування блокчейн мережі, алгоритми консенсусу, тестування мережі.

Захист інформації. Види захисту інформації, криптографія та її алгоритми, алгоирми шифрування інформацію та сфери їх застосування.

Оптимізація безпеки та конфіденційності у телекомунікаційних мережах. Масштабованість, приватність та інфраструктура.

3

Огляд блокчейну

Блокчейн - це технологія, яка дозволяє зберігати дані за допомогою комп'ютерної мережі. Запис даних у мережі складається з ланцюгів, які містять всю інформацію про транзакції. Історія всіх транзакцій створює блок, де вся інформація розташована в конкретному порядкові і за зберігання цієї інформації відповідають багато комп'ютерів по всьому світові.

Блокчейн-мережі є найпоширенішими через свою ключову властивість, а саме - децентралізованість. Це означає, що процеси, які відбуваються всередині мережі, не контролюються третіми сторонами. Даний аспект відіграє ключову роль в забезпеченні цілісності даних, оскільки тільки ви можете володіти власними даними та процесами в мережі.

зображення децентралізації

4

Блокчейн та серверна структура

Серверна структура має центральний комп'ютер, до якого під'єднані всі інші пристрої та обмінюються інформацією один з одним завдяки цьому центральному пристрою.

В блокчейні немає цього центрального комп'ютера. Всі користувачі можуть взаємодіяти один з одним. Відсутність централізованого посередника називається децентралізацією.

Блокчейн мережа

Серверна мережа

5

Сфери застосування блокчейну

Блокчейн успішно використовується для захисту персональних даних користувачів. Забезпечується це завдяки прозорості, децентралізації та новітніх алгоритмів шифрування.

Також блокчейн використовують для ідентифікації користувачів. Здавалось би, це схоже на централізацію, де ваші дані відомі ще комусь, але ні, все зовсім не так. Це потрібно лише для того, щоб, наприклад, при проведенні угоди, забезпечити високий рівень безпеки та зменшити ризик натрапити на зловмисників.

Блокчейн використовується і для роумінгу. Наявні заходи забезпечення безпеки та конфіденційності ваших даних можуть значно скоротити кількість використовуваного обладнання, що може значно розширити спектр функціонування мережі.

6

Побудова блокчейну

Найпершим кроком є створення блоку. Транзакція створюється та надсилається до мережі вузлів, де кожен вузол повинен перевірити інформацію і після цього зберегти її в блоці.

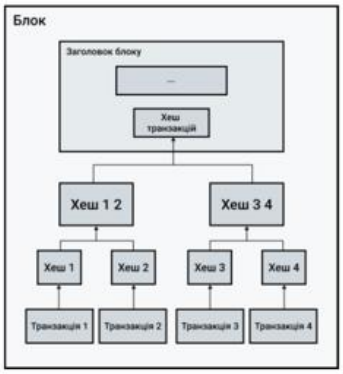
Наступним кроком є з'єднання блоків. Блок має обмежений розмір тому, як тільки він заповнюється, зразу ж створюється новий, який проходить той самий процес перевірки інформації. Щоб пов'язати блоки, новий блок використовує хеш і якщо інформація в попередньому блоці була змінена хоча би трішки, то хеш код зміниться повністю, що буде свідчити про певні перешкоди.

Останнім кроком є поєднання блоків, що і створює блокчейн. Всі транзакції блокуються разом конкретним чином та використовують один і той самий алгоритм консенсусу для підтвердження валідності інформації попереднього блоку.

7

Генерація блоку

А ось графічне представлення того, як будується блок. Мережа хешує дані транзакцій та у разі цілісності інформації записує її до блоку.



Процес утворення блоку

8

Алгоритми консенсусу

Алгоритм консенсусу це метод підтвердження валідності інформації. Першим з них Proof of Work (доказ роботи) - де використовується обчислювальна потужність вашого пристрою для вирішення певних математичних завданнь. Перший пристрій, який успішно вирішує завдання, може створити новий блок і отримати за це винагороду у вигляді певного активу або обчислювальної потужності

Другим з них є Proof of Stake (доказ власності), де вибір нового блоку залежить від кількості активу, тобто чим більшу кількість активів користувач має, тим вища ймовірность вибору його блоку для створення

Останнім з них є Practical Byzantine Fault Tolerance (практична візантійська стійкість). Даний алгоритм застосовується в тих випадках, коли користувачі можуть вчинити зловмисні дії. В таких випадках, алгоритм швидко це виявляє та вносить корективи, щоб запобігти потраплянню до зловмисників.

9

Алгоритми шифрування інформації

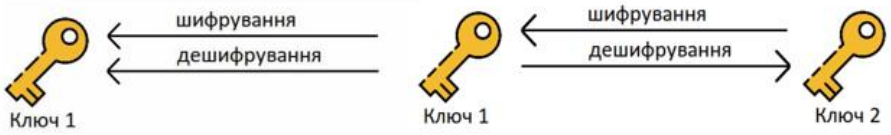
Симетричне шифрування - відоме, як шифрування з одним ключем. Логіка такого шифрування полягає в тому, що тільки ви і та особа, якій ви надсилаєте певні дані, будуть мати ключ до цих даних. Секретний ключ повинен бути узгоджений заранiше.

Асиметричне шифрування. На відміну від симетричного, тут вже використовується пара ключів. Це значно підвищує рівень безпеки даних. Існує відкритий ключ, який можна передати будь-кому в будь-якій мережі. Він використовується для шифрування даних і доступний для всіх, однак є також закритий ключ, який залишається конфіденційним і використовується для розшифровування повідомлень.

10

Різниця між симетричним та асиметричним алгоритмами шифрування

Фундаментальна відмінність між цими двома методами шифрування полягає в тому, що в симетричному шифруванні використовується тільки один ключ, а в асиметричному два різних ключі, що значно підвищує рівень безпеки.



Симетричне шифрування

Асиметричне шифрування

11

Масштабованість блокчейн-мережі

Масштабованість означає більшу кількість транзакцій без використання додаткового обладнання. Щоб дійти до цього, потрібно контролювати апаратні вимоги, оскільки децентралізація в мережі забезпечується завдяки можливості найслабшого вузла.

Також потрібно враховувати зростаючий стан мережі, оскільки чим більшу пропускну здатність блокчейн може забезпечити за одиницю часу, тим швидше він розвивається.

Час синхронізації повного вузла також має місце, оскільки при запускові мережі він повинен синхронізуватися з іншими вузлами і даний процес повинен відбуватися максимально швидко та ефективно.

12

Приватність та ефективність

Кожного дня створюються все кращі і кращі технології забезпечення безпеки та конфіденційності і однією з них є zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) - це криптографічний метод, який дозволяє одній стороні підтверджувати правильність певного твердження перед іншою стороною, не розкриваючи при цьому деталей цього твердження.

Приватність та ефективність забезпечується завдяки стисненню доказів без втрати цілісності даних, алгоритмічній оптимізації, та паралельній обробці. Все це разом значно підвищує продуктивність та параметри безпеки мережі.

13

Інфраструктура. Рівні блокчейну

Блокчейн рівня 1 встановлює правила роботи з коштами та транзакціями. Він значно розширює можливості свого попередника, надаючи гнучкіші інструменти для роботи з даними.

Блокчейн рівня 2 додає новітні протоколи та механізми, які поповнюють функціонал та підвищують масштабованість блокчейну. Цей рівень вирішує проблеми масштабування, швидкості та розміру комісії, які можуть виникати під час використання базових блокчейнів

Третій рівень додає ще один рівень абстракції та функціональності, пов'язаний з додатковими сервісами та застосунками, що працюють поверх Другого рівня. Цей рівень включає децентралізовані застосунки, фінансові протоколи, послуги управління ідентифікацією та багато іншого.

14

Висновки

Незважаючи на те, що блокчейн технології знаходяться на ранній стадії розвитку, можна зрозуміти, що за ними стоїть наше з вами майбутнє, оскільки блокчейн буде ще більше інтегрований в наше життя, забезпечуючи безпеку та конфіденційність наших даних новітніми технологіями.

Інтеграція блокчейну матиме дуже впливовий ефект на суспільство загалом, оскільки прозорість та децентралізація підвищать довіру суспільства та забезпечить демократизацію інформації, без чого в наші дні - нікуди.

Говорячи про телекомунікації, це значно допоможе зменшити витрати на обладнання, зменшить споживану енергію та забезпечить безпеку та доступність у використанні телекомунікаційних послуг.

ДЯКУЮ ЗА УВАГУ!