DOI: 10.18372/2410-7840.25.17673
УДК 004.056.5

РОЗРОБКА КОНЦЕПЦІЇ МЕТОДУ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПОБУДОВИ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ

Василь Побережник, Іван Опірський

В сучасних реаліях, швидкий обмін інформацією становить важливий аспект діяльності людини. Відповідно, інформація, яка циркулює в системах обміну повідомленнями потребує захисту. Для реалізація цього існує низка способів, втім швидкий розвиток технологій може спонукати до пошуку альтернативних рішень. Одним з таких рішень може стати технологія блокчейн, яка ще не широко застосовується в даному контексті, втім набула популярності в сфері криптовалют та децентралізованих фінансових сервісів, зокрема через можливість забезпечення приватності користувачів. Основна ідея блокчейну полягає в тому, що це розподілена децентралізована мережа, яка дозволяє зберігати інформацію в незмінному виді та надавати доступ до неї всім користувачам мережі одночасно та запобігає існуванню користувачів із особливими правами, що дозволяє розглядати технологію блокчейн як основу для побудови якісної системи обміну повідомленнями забезпечуючи цілісність та доступність до інформації. В даній статті розглянуті особливості технології блокчейн та децентралізованих застосунків, проведено аналіз слабких та сильних сторін та можливостей, які вони можуть запропонувати такій системі, а також запропоновано концепцію методу використання технології блокчейн для побудови системи обміну повідомленнями. Окрім цього проаналізовано недоліки такої системи та запропоновано методи для їх подолання.

Ключові слова: *блокчейн, приватність, обмін повідомленнями, DPoS, децентралізація, захист інформації.*

ВСТУП

В наш час необхідність наявності способу для комунікації між людьми на відстані, не залежно від того чи ця комунікація потрібна для збереження роботи бізнесу, відпочинку, навчання чи спілкування є такою самою звичною, як використання персональних комп'ютерів чи мобільних телефонів. Одним із способів забезпечення цієї можливості обмін повідомленнями за допомогою різних сервісів, наприклад електронної пошти, месенджерів, соціальних мереж тощо. Втім їхнє використання також може нести в собі ряд загроз, наприклад спам чи фішинг [1]. Окрім цього загрози можуть становити самі лінії передачі інформації, оскільки вони можуть прослуховуватися, інформація перехоплюватися, а зловмисники можуть видавати себе за легітимних учасників [2].

Невід'ємною частиною життя стали месенджери, зокрема через свою простоту у використанні та можливість встановлення на різні типи пристроїв: мобільні телефони, персональні комп'ютери, ноутбуки чи веб-версії. Наприклад, месенджер WhatsApp завантажили 2 мільярди разів [3]. Однак, значна популярність даних сервісів, може свідчити й про наявність низки загроз для їхніх користувачів. Персональна інформація, яка збирається даними сервісами, містить широкий перелік даних. Наприклад, раніше згаданий месенджер WhatsApp збирає такі дані як номер телефону, електронну скриньку, інформацію про покупки, геолокацію, список контактів, фінансові дані, контактні дані, медіа-контент, ідентифікатори, діагностичні дані та дані про використання [4]. Інші месенджери можуть збирати ще більше даних. Збирання цих даних може спричинити до їхнього витоку, що відбулося у 2019 році, коли через вразливі у Messenger було викрадено персональні дані 533 мільйонів користувачів. Також, користувачі можуть не знати про те, що той чи інший сервіс збирає дані про них або можуть не цікавитися інформацією, що про них збирається, в той час як поєднання даних про них у соцмережах із даними застосунків можуть значно збільшити кількість зібраної інформації [5].

Одне з досліджень, проведених за допомогою Lumen Privacy Monitor [6] виявило трекери й витоки персональних даних із таких застосунків як Viber, Slack. Ayoba.

Також було виявлено атаки, що використовують такі програми як Zoom, як частину вектору

атаки спрямованої на отримання доступу до даних користувачів чи записів конференції [7].

Зважаючи на це, можна зробити висновок, що програми для обміну повідомленнями несуть не тільки позитивні аспекти їхнього використання, але й мають ряд загроз, які потребують пошуку підходів для їхнього вирішення.

В сфері кіберзахисту можна використовувати різні методи й засоби для захисту інформації. Одним з таким засобів є використання штучного інтелекту [8]. Іншим методом можна стати використання програмних приманок [9], що дозволять як захистити інформацію так і дослідити дії зловмисника. Втім, однією із технологій яка може допомогти захистити інформацію є використання методу, який за замовчування базується на принципі приватності користувачів [10] – технології блокчейн.

В даній роботі розглядаються властивості технології блокчейн та децентралізованих застосунків, які базуються на ній, для побудови системи обміну повідомленнями. Проводиться аналіз переваг та недоліків технології як самостійної технології та у контексті системи обміну повідомленнями. Розроблено концепцію методу побудови сервісу та проведено аналіз його недоліків.

Метою роботи є розробка концепції методу який би дозволив використовувати технології блокчейн та децентралізованих застосунків для побудови системи обміну повідомленнями.

Завданнями даної роботи є:

1. Провести огляд технологій блокчейн та децентралізованих застосунків;
2. Здійснити аналіз переваг та недоліків технологій;
3. Розробити концепції методу використання технології блокчейн, як основи для системи обміну повідомленнями;
4. Провести аналіз переваг та недоліків розробленої концепції;
5. Здійснити пошук шляхів нівелювання недоліків пропонованої концепції;
6. Сформувати висновок про придатність застосування технології блокчейн для побудови системи обміну повідомленнями.

ОСНОВНА ЧАСТИНА

Огляд технології блокчейн

Блокчейн – це список записів, також відомих як блоків, що криптографічно пов'язані між собою, кожен з яких містить хеш попереднього блоку, відмітку часу, дані транзакції, та утворюють своєрідний ланцюжок з блоків (рис. 1).

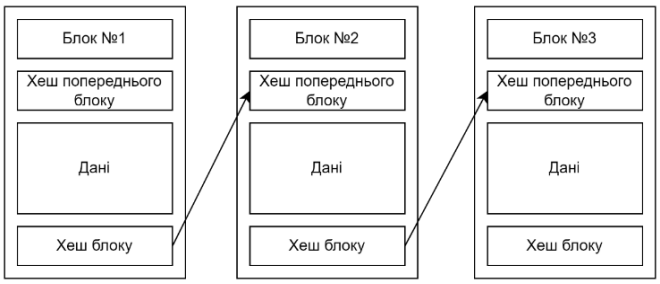

Рис. 1. Репрезентація структури блокчейну

Хеш блоку обчислюється із вмісту даних за допомогою Дерева Меркла [11], яке дозволяє узагальнити всі дані у блоці, зображено на рисунку 2, а позначка часу дозволяє ідентифікувати те, що дані в блоці були реальними у момент створення блоку. Саме наявність в блоці хешу попереднього блоку дозволяє пов'язати блок в один, раніше згаданий, ланцюжок із попередніми блоками.

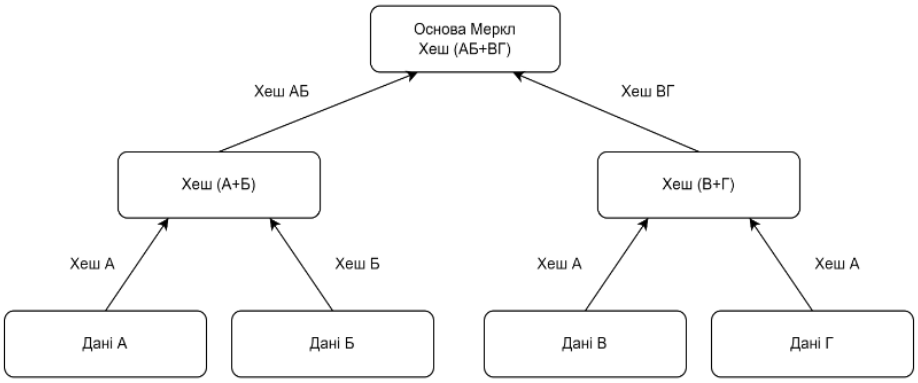

Рис. 2. Зображення дерева Меркла

Таке поєднання дозволяє відслідкувати будь-які зміни внесені в один з блоків у якісь конкретній версії блокчейну, оскільки ланцюжок із змінами буде відрізнятися від тих ланцюжків, які є у кожного вузла мережі. Отже, наявність в кожного вузла власної копії блокчейну дозволяє ідентифікувати несанкціоновані зміні в певному ланцюжку та відкинути їх.

Наявність цих копій в кожному вузлі забезпечується тим, що сама технологія блокчейну є, за своєю ж природою, децентралізованою. Властивість децентралізації буде надавати такі переваги:

- легке відстеження змін, через відносно високу швидкість їх розповсюдження між вузлами
- стійкість до відмов через децентралізацію;
- відсутність центральної точки вразливості;
- стійкість до збоїв;
- відсутність посередників;
- прозорість мережі;
- підтримка мережі та активів учасників самими учасниками;
- рівноправність вузлів;
- незмінність збереженої інформації.

Зважаючи на дані особливості технології блокчейн її можна розглядати, як своєрідну базу даних, з ключовою відмінністю в тому, що на відміну від класичних базах даних, таких як SQL-бази чи noSQL-бази, де існують користувачі із правами адміністратора, в даній системі таких користувачів не існує. Загроза існування цих користувачів полягає в тому, що з одного боку вони виконують функції адміністрування бази, а з іншого – можуть вносити зміни в базу даних без відома інших користувачів, а децентралізована природа вирішує цю проблему банальною відсутністю користувачів із особливими правами. Окрім цього, вона забезпечує відсутність центру управління блокчейном.

Ще однією ключовою властивістю, що дозволяє розглядати блокчейн в якості бази даних, є збереження всієї інформації і змін від моменту створення блокчейну. Тобто, в будь-який момент кожен вузол мережі може переглянути будь-який блок який існує в мережі, не залежно від часу його створення.

Останньою ключовою властивістю є незмінність, що дозволяє впевнитися в тому, що дані в блокчейні ж цілісними. Дана властивість випливає із того, що кожен блок містить власний хеш, принцип формування якого було розглянуто раніше. Відповідно будь-яка зміна в блоці змінить значення хешу блоку, що дозволить ідентифікувати зміни та позбутися їх.

Зважаючи на дані факти, блокчейн можна розглядати як якісну основу для побудови системи обміну повідомленнями, яка буде забезпечувати збереження інформації у надійному місці, забезпечуючи такі характеристики інформації як цілісність та доступність.

Зважаючи на те, що застосунки в децентралізованій мережі також мають бути децентралізовані, необхідно розглянути принципи їх побудови, що виконується в наступному розділі.

Огляд технології децентралізованих застосунків

DApp – це децентралізовані застосунки, які працюють в децентралізованих системах, таких як Ethereum, Solana, Tron, тощо. Їхньою особливістю є те, що як і у випадку з блокчейном, відсутні сервери, а всі обчислення проводяться вузлами мережі, в якій працює DApp. Окрім того, застосунок має забезпечувати виконання низки вимог [12]:

1. DApp має мати відкритий код, бути автономним і жоден користувач не має мати в своєму розпорядженні більшість токенів. Всі зміни в застосунку повинні впроваджуватися через консенсус між учасниками та засновуватися на їхніх пропозиціях.

2. Дані та результати операцій застосунку повинні зберігатися у криптографічно захищеному вигляді та зберігатися у публічному блокчейні.

3. Токени повинні використовуватися, щоб винагороджувати користувачів, які підтримують роботу мережі та надавати доступ до послуг користувачам.

4. Токени повинні генеруватися децентралізованим застосунком відповідно до стандартизованих криптографічних алгоритмів. Ці токени мають використовуватися як доказ цінності для вкладників. Наприклад винагорода майнерів в мережі Bitcoin.

До прикладу, дані застосунки використовуються для надання послуг різного спектру, наприклад розваги [13], децентралізовані фінансові послуги [14], медичні послуги [15], логістика [16], тощо. Ключовим механізмом роботи даних застосунків є консенсус мережі, який дозволяє переконатися в тому, що нещодавно доданий блок є легітимним та його можна додати в мережу. У таблиці 1 наведено переваги та недоліки використання децентралізованих додатків.

Таблиця 1

Переваги та недоліки централізованих та децентралізованих систем

Процес аналізу	Централізовані	Децентралізовані
Переваги	-повний контроль над програмою та її виконанням; -можуть обробляти більший об'єм трафіку; -легко оновлювати, оскільки оновлення автоматично надсилається на пристрій користувача.	-завдяки децентралізації дані користувачів не знаходяться під загрозою у разі витоку даних або спроби злому; -можливість робити при виході з ладу одного чи кількох вузлів; -стійкість до цензурування; -рішення щодо системи приймають колегіально; -вузли системи рівні у правах; -незмінність уже збережених даних.
Недоліки	-у разі виникнення системної помилки сервіс може припинити роботу, доки проблема не буде усунена; -додаткові витрати на захист серверів.	-складність оновлення та виправлення помилок через децентралізовану природу; -низька придатність для використання у системах, що потребують швидкодії; -великі затрати пам'яті на збереження копії блокчейну у кожному вузлі.

Механізм консенсусу

Даний механізм дозволяє визначити вузол, який буде публікувати новий блок і відповідно отримає за це нагороду. Дане завдання вирішується шляхом реалізації одного із можливих алгоритмів досягання консенсусу.

Коли вузол приєднується до мережі блокчейн, він повинен погодитися із початковим станом системи. Інформація про цей стан міститься у єдиному попередньо налаштованому блоці, який відомий як блок генезису (найперший блок у блокчейні). Кожна мережа блокчейну має опублікований блок генезису і кожен наступний блок має бути доданим до ланцюжка, основою якою є блок генезису за допомогою алгоритму консенсусу. Варто зазначити, що незалежно від алгоритму консенсусу кожен блок має бути валідним та має мати можливість незалежної перевірки будь-яким вузлом у мережі. Основуючись на цьому, кожен вузол в мережі поєднуючи перевірку блоку генезису та перевірку кожного вузла в мережі, вузол може узгодити для себе поточний стан мережі.

В ситуації, коли вузол отримує два ланцюги блоків, в більшості механізмів мережі блокчейн, легітимним ланцюжком буде вважатися, той ланцюг, чия довжина буде більшою, оскільки це означатиме, що над ним виконали більше роботи [17] (рис. 3).

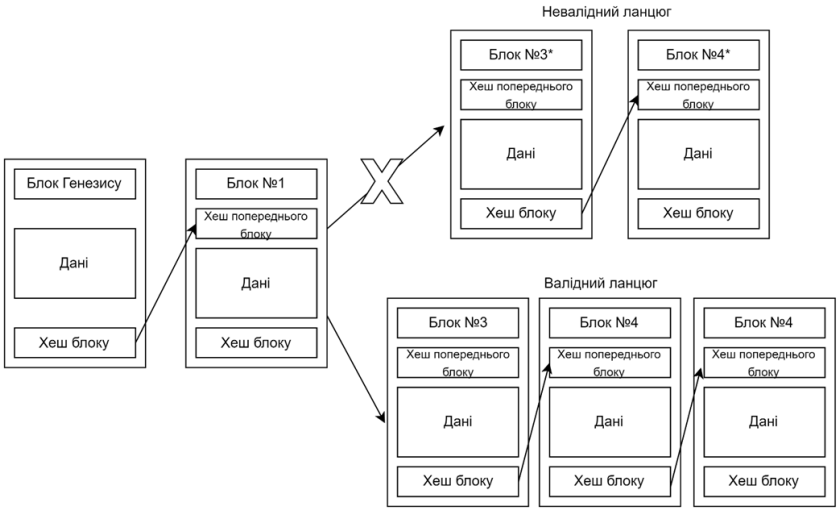

Рис. 3. Вибір довшого ланцюга як валідного

Першим алгоритмом був Proof of work [18], що використовується у Bitcoin, Litecoin, ідеєю якого було проводити складні математичні обрахунки для вирішення задачі, рішення якої надавало вузлу, що знайшов розв'язок, право на додавання блоку в мережу та отримання винагороди за свою роботу.

Ще одним із можливих варіантів є Proof of stake [19], який тепер використовується в Ethereum [20]. На відміну від PoW алгоритму, для додавання блоку в мережу вузлом використовується наявна кількість токенів у вузла. Тобто більша кількість токенів у вузла надає йому більше шансів бути обраним для валідації транзакцій та додавання нового блоку у мережу, а необхідність мати велику кількість токенів знижує вірогідність атаки на мережу, через економічну недоцільність для зловмисника.

Система обміну повідомленнями на основі методу блокчейну

Використання можливостей технології надає можливість для побудови системи обміну повідомленнями. Така система буде мати схему обміну інформацією схожу із системою проходження транзакцій в блокчейні. Втім, оскільки блоки фактично можуть містити будь-яку інформацію [21], а не тільки дані про транзакції, то цим можна скористатися для обміну інформацією між вузлами мережі. На рисунку 4 зображено алгоритм обміну повідомленнями.

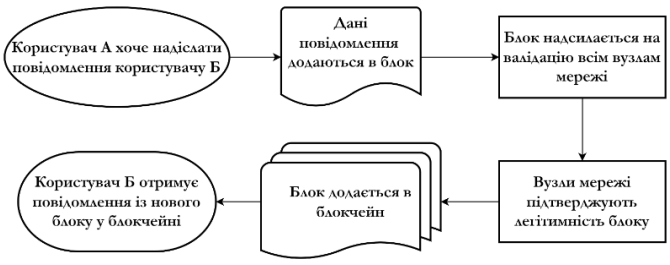

Рис. 4. Алгоритм обміну повідомленнями

Алгоритм обміну повідомленнями буде складатися із таких кроків:

1. Користувач А хоча надіслати повідомлення Користувачу Б;
2. Дані повідомлення додаються в блок;
3. Блок з повідомленням надсилається на валідацію всім вузлам мережі;
4. Вузли мережі підтверджують легітимність нового блоку;
5. Новий блок додається в блокчейн;
6. Користувач Б отримує повідомлення із нового блоку у блокчейні.

Використання даного способу матиме ряд переваг та недоліків, які випливають із властивостей самої технології, та відображаються в таблиці 2.

Таблиця 2

Порівняння переваг та недоліків методу блокчейну

Процес аналізу	Використання методу блокчейну
Переваги	-анонімність; -децентралізація; -незмінність; -рівноправність вузлів; -прозорість.
Недоліки	-необхідність додаткового криптографічного захисту повідомлень; -обмеження розміру повідомлення; -складність реалізації обміну медіа-файлами; -розмір блокчейну; -навантаження вузлів; -відсутність можливості організувати обмін повідомленнями у реальному часі.

Найвідчутнішим недоліком, з точки зору приватності, буде те, що через прозорість самої мережі, повідомлення які зберігатимуться у мережі будуть доступними усім вузлам мережі, а не тільки вузлам які приймають безпосередню участь в обміні.

Ще одним недоліком буде обмеження розмірів самого блоку в мережі, наприклад в мережі Bitcoin такий розмір становить 1 Мбайт [22], або ж в мережі Ehtereum фактичне обмеження встановлюється максимальною сумою за обробку – gas fee [23], що знову обмежуватиме розмір повідомлення. Дане обмеження також призводить до ще одного недоліку – складність у реалізації обміну медіа-файлами. Такий обмін буде недоцільним через сам блокчейн, оскільки розмір медіаданих, таких як голосові повідомлення, зображення чи відео є надто великими для обміну через блокчейн, а їхнє зберігання в блокчейні буде нести в собі

використання великих об'ємів пам'яті, що збільшуватиме розмір самого блокчейну.

Також, із ростом кількості користувачів та даних, якими вони обмінюються буде рости й розмір самого блокчейну, що підвищуватиме навантаження на самі вузли та займатиме велику кількість пам'яті. Даний фактор може призвести до неможливості використання мобільних пристроїв, для доступу до мережі через надто великий розмір блокчейну.

Ще одним вагомим недоліком такої системи є те, що реалізація миттєвого обміну повідомленнями фактично неможлива, оскільки блоки будуть потрапляти в мережу тільки після того, як новий блок буде знайдено, а потім й перевірено вузлами мережі й додано в блокчейн. Після чого адресат зможе завантажити новий блок та отримати повідомлення. На додачу до цього, передача повідомлення вимагатиме й певних витрат токенів, оскільки, як розглядалося раніше, однією з вимог до децентралізованих застосунків є те, що вузли мережі повинні отримати винагороду за знаходження нового блоку.

Дані недоліки спонукають до пошуку методів їхнього нівелювання. Наприклад проблемо із загальним доступом до вмісту повідомленням може бути вирішена шляхом криптографічного захисту вмісту даних. Втім даний спосіб буде нести додаткове навантаження через витрату ресурсів на криптографічні перетворення, а також потребуватиме розробки механізму обміну ключами між учасниками обміну.

Для забезпечення можливості обміну медіафайлами рішенням може стати використання IPFS-платформи [24], які дозволяють зберігати дані децентралізовано. Даний метод дозволить обмінюватися учасникам діалогу не самими медіафайлами, а їхніми хешами, для пошуку самих файлів у IPFS-платформі. Даний спосіб дозволяє скоротити об'єм використовуваних даних в блокчейні для обміну медіа, втім вводить додаткові сервіси в саму систему. Однак збереження медіа в блокчейні не завжди є недоліків, а може забезпечувати також переваги. Наприклад зберігання документів у блокчейні дозволить забезпечити їхню цілісність та доступність. Втім, такі документи однаково будуть мати обмеження в розмірі, задля протидії надмірного використання пам'яті в блокчейні чи можливості їхнього зберігання в блоці.

Методом боротьби із високим розміром блокчейну може стати "обнулення" даних. Принцип полягає в тому, щоб при досягненні певного критичного розміру блокчейну, з нього видалялися лані блоків, а зберігалися лише докази роботи та хеші блоків, для забезпечення неперервності ланцюжка блоків. Втім такий підхід буде порушувати принцип доступності, оскільки самі дані будуть втрачені разом з доступом до них. Даний фактор свідчить про необхідність створення додаткового сховища, яке б могло зберігати весь блокчейн, для збереження доступу до даних, які існували на момент обнулення.

Зважаючи на розглянуті фактори можна зробити висновок, що запропонований метод є можливим для реалізації, можливість його використання є обмеженою через його недоліки, що спонукає до пошуку інших підходів використання блокчейну в таких системах.

Метод побудови системи основаної на вузлах різного типу

Даний підхід ґрунтується на використанні вузлів різного типу у мережі, що дозволить залучити в мережу не лише потужні пристрої із великим обсягом пам'яті але й менш потужні пристрої на кшталт смартфонів. Структура запропонованої мережі зображена на рисунку 5.

Пропонована мережа буде використовувати три типи вузлів:

1. Полегшені вузли – вузли, які матимуть у собі лише блоки, що містять інформацію, яка стосується лише даного вузла;
2. Повні вузли – вузли, які зможуть виконувати весь функціонал;
3. Архівні вузли – вузли які міститимуть у собі копію всього блокчейну.

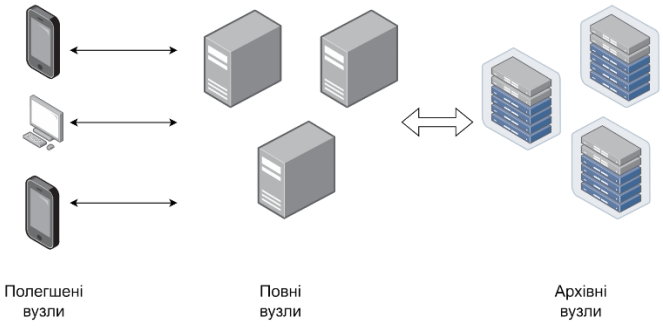

Рис. 5. Пропонована схема побудови мережі основаної на різних типах вузлів

Даний підхід дозволяє розглядати полегшені вузли як умовні клієнтські застосунки. Алгоритм обміну повідомленнями буде мати такий вид:

1. Користувач А хоче надіслати повідомлення користувачу Б;
2. Якщо користувач А повний вузол – він приймає участь у створенні нового блоку, якщо ні – делегує повному вузлу;
3. Новий блок валідується повними вузлами та додається в блокчейн;
4. Архівні вузли синхронізуються із новим станом блокчейну;
5. Полегшені блоки отримують новий блок з блокчейну, якщо в ньому міститься інформація, яка їх стосується.

В цьому підході основне навантаження лягає на повні вузли, оскільки полегшені вузли містять лише ті блоки, інформація в яких стосується вузла, а весь блокчейн відсутній, що виключає їхню можливість брати участь у створенні нових блоків та їхній валідації. Також полегшені вузли зможуть взаємодіяти лише із повними, для отримання доступу до оновлень в блокчейні, але не матимуть можливості взаємодіяти між собою.

Тобто, дані блоки будуть мати лише шматки блокчейну, які містять інформацію, щодо кожного конкретного вузла, а не про всю мережу, схематичне зображення цього наведено на рисунку 6.

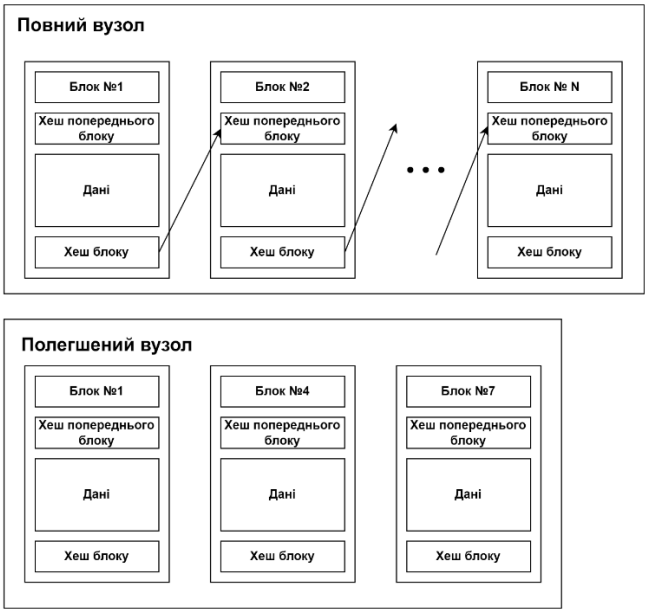

Рис. 6. Відмінність між копіями блокчейну у повних та полегшених вузлах

Оскільки дана мережа буде мати вузли, які не мають можливості приймати участь у валідації, то доцільно для даної мережі буде обрати метод консенсусу відомий як Delegated proof of stake [25] (DPoS). Даний алгоритм має певну схожість із Proof of Stake, оскільки він передбачає механізм накопичення токенів задля отримання можливості валідації блоку, втім основна відмінність полягає в тому, що в даному алгоритмі учасники мережі «голосують» токенами, обираючи вузол, який стане валідатором. Відповідно, даний алгоритм спонукає обрані вузли-валідатори бути чесними, оскільки вони зацікавлені в тому, щоб їх продовжували обирати на цю роль. Також, вузли-валідатори, можуть самі обирати відсоток винагороди за знайдений блок, який буде потім розподілений поміж учасниками мережі, які за нього голосували. Відповідно цей відсоток зможе ввести конкуренцію поміж вузлами-валідаторами та спонукати користувачів мережі обирати на цю роль вузли які пропонують вигідніші пропозиції та мають хорошу репутацію. Отже це дозволить опосередковано залучити неповні вузли до процесу валідації.

ВИСНОВКИ

В статті розглянуто можливості технології блокчейн в контексті побудови сервісів для обміну повідомленнями між учасниками мережі. Було виявлено, що використання підходу із використанням самого блокчейну є можливим, втім через ряд особливостей технології, його самостійне застосування є недоцільним, зокрема через можливі розміри блокчейну, обмеження розміру повідомлення максимально дозволеним розміром блоку в мережі та ріст навантаження через ріст самого блокчейну.

Для вирішення проблем було запропоновано варіант розробки мережі на основі вузлів різного типу із застосуванням обнулення блокчейну. Перевагами даного підходу буде зниження навантаження на вузли через їхній розподіл на різні типи та застосування обнулення блокчейну при досягненні критичного розміру. Наявність в мережі архівних вузлів позбавляє необхідності створення додаткових вузлів для збереження копії всього блокчейну.

Недоліком даного підходу є зниження рівня децентралізації разом із додаванням додаткових точок вразливості через наявність нових типів

вузлів та фізичний вивід полегшених вузлів із процесу валідації блоків.

Також даний методи матиме певні труднощі в реалізації, наприклад потреба розробки методу захисту архівних вузлів через те, що вони міститимуть всю історію блокчейну, яка вважається легітимною і їхня компрометація призведе до компрометації всієї мережі.

Наведені факти свідчать про те, що розробка методу для обміну повідомленнями на основі технології блокчейн потребує компромісних рішень, оскільки використання лише самого блокчейну із однотипними вузлами є не надто хорошим варіантом через свої особливості, а використання системи на основі вузлів різного призначення нестиме як переваги, так і недоліки. Також потрібно зважати на тип інформації, якою будуть обмінюватися. Наприклад обмін медіа даними через мережу блокчейн є недоцільним через різке збільшення самого блокчейну та обмеження розміру блоку, тому для обміну такими даними необхідно використовувати додаткові сервіси та інтегровувати їх в мережу.

ЛІТЕРАТУРА

[1] A review of spam email detection: analysis of spammer strategies and the dataset shift problem / F. Jáñez-Martino et al. Artificial Intelligence Review. 2022. URL: https: // doi.org/10.1007/s10462-022-10195-4.

[2] Cinar A. C., Kara T. B. The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications. 2023. URL: https: // doi.org/ 10.1007/s11042-023-14400-6.

[3] WhatsApp, wechat and meta messenger apps - global usage of messaging apps, penetration and statistics. MessengerPeople by Sinch. URL: https: //www. messengerpeople.com/global-messenger-usage-statistics.

[4] WhatsApp messenger. App Store. URL: https: // apps.apple.com/ua/app/whatsapp-messenger/id310 633997.

[5] Zhang L., Ji Q., Yu F. The Security Analysis of Popular Instant Messaging Applications. 2017 International Conference on Computer Systems, Electronics and Control (ICCSEC), Dalian, pp. 25-27 December 2017.URL:https://doi.org/10.1109/ iccsec.2017. 844 6863.

[6] Kalapodi A., Sklavos N. The Concerns of Personal Data Privacy, on Calling and Messaging, Networking Applications. Communications in Computer and Information Science. Singapore, 2021. pp. 275-289. URL: https: // doi. org / 10.1007 / 978-981-16-0422-5_20.

[7] Susukailo V., Opirskyy I., Vasylyshyn S. Analysis of the attack vectors used by threat actors during the pandemic. 2020 IEEE 15th international conference on computer sciences and information technologies (CSIT), Zbarazh, Ukraine, pp. 23-26 September 2020. URL: https: //doi.org/10.1109/csit49958. 2020. 932-1897.

[8] Detecting DDoS Attacks Using Adversarial Neural Network / A. Mustapha et al. Computers & Security. 2023, p. 103117. URL: https: // doi.org/10.1016/j. cose.2023.103117.

[9] Vasylyshyn, S., Opirskyy, I., Susukailo, V. Analysis of the use of software baits as a means of ensuring information security // 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020. Proceedings, 2020, 2, pp. 242-245, 9321925.

[10] Chentouf F. z., Bouchkaren S. Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering (IJECE). 2023. Vol. 13, no. 2, p. 1848. URL: https://doi.org/10.11591/ijece.v13i2.pp 1848-1857.

[11] CoinDesk. How Bitcoin Mining Works. 2018. URL: https: //www.coindesk.com/ information / how-bitcoin-mining-works.

[12] Bashir I. Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained. Packt Publishing, 2017, ISBN 9781787125445.

[13] Smith M. S. The Spectacular Collapse of Cryptokitties. IEEE Spectrum. 2022. Vol. 59, no. 9, pp. 42-47. URL: https://doi.org/10.1109/mspec.2022.9881234.

[14] Metelski D., Sobieraj J. Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations. International Journal of Financial Studies. 2022. Vol. 10, no. 4, p. 108. URL: https://doi.org/10.3390/ijfs10040108.

[15] BLOCKCHAIN IN LOGISTICS Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. DHL. URL: https: //www.dhl.com / content / dam / dhl /global/core/ documents / pdf / glo-core-blockchain-trend-report. pdf.

[16] MedRec: Using Blockchain for Medical Data Access and Permission Management / A. Azaria et al. 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 22-24 August 2016. 2016. URL: https://doi.org/10.1109/obd.2016.11.

[17] Mahmood M. S., Al Dabagh N. B. Blockchain technology and internet of things: review, challenge and security concern. International Journal of Electrical and Computer Engineering (IJECE). 2023. Vol. 13, no. 1. P. 718. URL: https://doi.org/10.11591/ijece.v13i1.pp718-735.
[18] Soria J., Moya J., Mohazab A. Optimal mining in proof-of-work blockchain protocols. Finance Research Letters. 2022, p. 103610. URL: https: //doi.org/ 10.1016/j.frl.2022.103610.
[19] Василишин С., Опірський І. Розробка безпеки систем електронного урядування на основі блокчейну. Ukrainian Information Security Research Journal. 2022. Т. 24, № 2. С. 58-70. URL: https://doi.org/10.18372/2410-7840.24.16931.
[20] Енергоспоживання Ethereum / ethereum.org. ethereum.org. URL: https: // ethereum.org / uk / energy-consumption/.
[21] Опірський І., Василишин С. Перспективи військового застосування технології блокчейну. Ukrainian Scientific Journal of Information Security. 2022. Т. 28, № 2. С. 57-66. URL: https://doi.org/10.18372/2225-5036.28.16950.
[22] What is block size? Bitstamp Learn Center / Learn Center. Learn Center. URL: https://www.bitstamp.net/learn/crypto-101/what-is-block-size/.
[23] Gas and fees / ethereum.org. URL: https: // ethereum. org/en/developers/docs/gas/.
[24] What is IPFS? / IPFS Docs. IPFS Documentation / IPFS Docs. URL: https://docs.ipfs.tech/concepts/what-is-ipfs/#defining-ipfs.
[25] What is Delegated Proof of Stake (DPoS)? / Analytics Steps. Analytics Steps. A leading source of Technical & Financial content. URL: https: // analyticssteps.com/blogs/what-delegated-proof-stake-dpos.

DEVELOPMENT OF THE CONCEPT OF THE METHOD OF USING BLOCKCHAIN TECHNOLOGY FOR BUILDING A MESSAGE EXCHANGE SYSTEM

In modern realities, fast information exchange is an important aspect of human life. That is why information, that circulates in message exchange systems, requires to be secured. There are several possible ways to implement this, but the fast development of technologies forces us to search for alternate ways. One of the possible ways may become blockchain technology, which is not widely used in such a context, but found its popularity in the sphere of cryptocurrency and decentralized finances for its user privacy-preserving possibilities. The main idea of blockchain consists of that this is the decentralized distributed network that allows storing of information in an immutable way and provides access to it for all users of the network alongside prohibitions of the existence of users with exceptional privileges, which allows considering the blockchain technology as the base of a quality system for message exchange system which will provide integrity and availability of information. This article examines the features of blockchain technology and decentralized applications, analyzes the weaknesses and strengths and opportunities they can offer to such a system, and proposes a concept of the method of using blockchain technology to build a messaging system. In addition, the shortcomings of such a system are analyzed and methods to overcome them are proposed.
Keywords: blockchain, privacy, messaging, DPoS, decentralization, information security.

Побережник Василь Олегович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Vasyl Poberezhnyk, Postgraduate Student of the Department of Information Protection of the National University "Lviv Polytechnic".
E-mail: vasyl.poberezhnyk@gmail.com.
Orcid ID: 0000-0002-7523-2557.

Опірський Іван Романович, д.т.н., проф., професор кафедри захисту інформації Національного університету «Львівська політехніка».
Ivan Opirskyy, Doctor of Technical Sciences, Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.25.17674
УДК 004.681.3

КІЛЬКІСНА ОЦІНКА КІБЕРЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Володимир Хорошко, Юлія Хохлачова, Наталія Вишневська

Створення, впровадження та експлуатація комп'ютерних систем привело до виникнення нових проблем в сфері безпеки інформації. Кіберзахист інформаційних технологій повинен за своїми характеристиками бути відповідним масштабам загроз і ризиків. Відхилення від цього правила приведе до значних збитків. Для кожної комп'ютерної системи (КС) має бути свій оптимальний рівень кіберзахищеності, який необхідно постійно підтримувати. Нажаль до цього часу не існує адекватної методики оцінки кількісного рівня