Issue 17, 2025

https://doi.org/10.23939/sisn2025.17.001

УДК 004.415

СТВОРЕННЯ СИСТЕМИ ВИЗНАЧЕННЯ АВТЕНТИЧНОСТІ ТОВАРУ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

Владислав Лях[1], Тарас Басюк[2]

1, 2 Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж, Львів, Україна
[1]E-mail: vladyslav.liakh.mnitm.2023@lpnu.ua, ORCID 0009-0002-7870-721X
[2] E-mail:Taras.M.Basyuk@lpnu.ua, ORCID 0000-0003-0813-0785

© Лях В., Басюк Т.,2025

У статті розглянуто вирішення проблеми виявлення контрафактних товарів за допомогою використання технології Blockchain. Проведено аналіз існуючих методів та засобів для боротьби з підробками і обґрунтовано вибір блокчейну, як ефективного способу забезпечення прозорості трансакцій та захисту даних. Авторами статті проаналізовано проектування інформаційної системи з використанням структурного підходу, що дозволило систематизувати завдання та визначити ключові аспекти функціонування. Для моделювання системи застосовано методологію відому як Data Flow Diagrams (DFD), що дало змогу створити контекстну діаграму та діаграми декомпозиції. Розроблено архітектуру системи на базі Hyperledger Fabric, яка включає кілька вузлів і сертифікаційних центрів, що забезпечують надійність та достовірність перевірок. Наведено функціональне призначення системи, яка дозволяє користувачам перевіряти автентичність товарів. Проведено верифікацію роботи системи, продемонстровано її ефективність та надано опис основних етапів функціонування.

Ключові слова – блокчейн, автентичність товару, децентралізована мережа, Hyperledger Fabric, Docker.

Постановка проблеми

Сучасні методи боротьби з контрафактною продукцією, такі як використання QR-кодів, RFID-міток, серійних номерів та голографічних етикеток, мають свої обмеження, оскільки вони часто піддаються підробці та не гарантують повної автентичності товарів. В умовах глобального зростання обсягів контрафактного ринку, який досяг 600 мільярдів доларів у 2023 році, необхідно впроваджувати новітні технологічні рішення (David, 2024). Одним із найперспективніших підходів є використання блокчейн-технології, що забезпечує високий рівень безпеки, прозорість транзакцій та ефективність завдяки децентралізованій структурі мережі.

Застосування технології блокчейн у боротьбі з контрафактною продукцією дозволяє значно підвищити ефективність існуючих методів захисту товарів. Використання децентралізованої мережі забезпечує незмінність даних про походження продукції, мінімізуючи ризики шахрайства та підробки. Це сприяє економії коштів, які витрачаються на традиційні способи боротьби з фальсифікацією та забезпечує прозорість усіх процесів. Дослідження у цій сфері сприятимуть впровадженню сучасних рішень для автоматизації перевірки автентичності товарів, інтеграції зазначених підходів у глобальну економіку, а також підвищуватимуть довіру людей до якості та безпеки придбаних ними продуктів (Beaver, 2021).

Сучасні методи боротьби з контрафактною продукцією демонструють обмежену ефективність у протидії підробкам, які постійно вдосконалюються. Використання блокчейн-технології є перспективним рішенням, яке забезпечує децентралізований механізм реєстрації та зберігання інформації

про походження продукції. Такий підхід дозволяє вирішити проблему незмінності даних, мінімізуючи ризики шахрайства (Vardhan, 2023). З огляду на це, важливим науково-практичним завданням є визначення шляхів інтеграції блокчейн у процеси перевірки товарів, що сприятиме вдосконаленню механізмів боротьби та відстеження підробок (Gudadhe, 2023).

Перспективність дослідження полягає у аналізі можливостей блокчейн-технології для створення інформаційних систем перевірки автентичності товару, що надасть засоби для ефективного зберігання, передавання та перевірки інформації про товари. Розв'язання цього завдання сприятиме розробці науково-методологічної бази для впровадження рішень у виробничі процеси. Зокрема, це дозволить зменшити витрати на традиційні методи боротьби з фальсифікацією, підвищити ефективність ланцюгів постачання та забезпечити довіру споживачів до якості товарів.

Аналіз останніх досліджень та публікацій

Контрафактна продукція завдає значних збитків як економіці, так і суспільству. Щорічно виробники втрачають мільярди доларів, а споживачі стикаються з ризиками, що загрожують їх здоров'ю та життю. У 2023 році обсяг ринку підробок, переважно зосередженого в Китаї, досяг 600 мільярдів доларів, що становило 2,1 % світової торгівлі. Попри заходи, спрямовані на захист інтелектуальної власності, прогнози вказують на подальше зростання цього ринку, який у найближчі роки може перевищити три трильйони доларів. Згідно зі статистикою, найбільшими постачальниками контрафактної продукції у світі є такі країни (David, 2024): Китай ~ 661 млд.; Гонконг ~ 429 млд; Туреччина ~ 31 млд.; В'єтнам ~ 26 млд; інші країни ~ 88 млд. доларів.

Водночас найбільше від цього страждають розвинені країни, на ринку яких домінують товари, що найчастіше підробляються. Додатково проаналізувавши дані щодо галузей, які найбільше потерпають від підробок (рис.1), можна зауважити, що ситуація є вкрай складною, і з кожним роком стає все гіршою (OECD, 2019).

Рис. 1. Список галузей, що найбільше страждають від підробок (Richter, 2019)

Стосовно наукових праць, то дослідженнями у сфері "перевірки автентичності товарів" займались ряд дослідників, серед яких можна виділити праці Gao (2022), предметом дослідження яких стала інтеграція технології блокчейн із засобами відстеження для створення системи автентифікації товарів у сфері електронної торгівлі. Під керівництвом Li (2022) розробляється система відстеження продукції на основі Hyperledger Fabric і EPICS, особливістю якої є поєднання on-chain та off-chain управління з автентифікацією IoT-пристроїв. У дослідженнях Wasnik (2022) аналізується розробка системи на основі блокчейн-технології для боротьби з контрафактною продукцією, яка забезпечує прозорість, ідентифікацію та відстеження товарів, усуваючи недоліки традиційних методів, таких як QR-коди.

Зазвичай для перевірки автентичності товарів використовують традиційні методи: QR-коди, RFID-мітки. Проте ці підходи мають суттєві недоліки. QR-коди можуть бути скопійовані для маркування підробок, а RFID-мітки піддаються клонуванню. Окрім цього, побудова інформаційної системи на основі централізованого підходу передбачає обмежену прозорість, єдину точку відмови та недостатню довіру між учасниками торгівельної операції (Kamble, 2023). При цьому, використання децентралізованих рішень в управлінні ланцюгами постачання, дозволяє покращити прозорість, довіру та відстежуваність товарів в боротьбі з контрафактною продукцією. Це підтверджується, зокрема, проектами таких компаній, як Walmart та Provenance, які успішно застосовують блокчейн для відстеження продуктів та перевірки їх автентичності (Wang, 2018). Технологія блокчейн також демонструє значний потенціал для покращення стійкості та зменшення ризиків у ланцюгах постачання, завдяки можливості надання прозорих, захищених даних, що дозволяє швидко реагувати на зміни, тим самим зменшуючи витрати (Henry, 2023).

Технологія блокчейн (Harbert, 2019) дозволяє автоматизувати верифікацію через смарт-контракти, що значно скорочує час та зусилля, необхідні для підтвердження автентичності товарів на основі унікальних кодів. При цьому, важливим етапом є власне вибір блокчейну, який зазвичай залежить від специфіки задачі, яку потрібно вирішити. Основними критеріями при цьому є тип блокчейну, цілі проєкту та підтримка смарт контрактів.

Перед тим, як здійснити вибір того чи іншого блокчейну важливо зрозуміти, як він працює. У центрі роботи технології лежать відмінні математичні аспекти для забезпечення безпеки, прозорості дій та функціональності. Безпека технології реалізується з використанням криптографічних хеш-функцій. Хеш-функції забезпечують цілісність даних і запобігають їх підміні. Якщо змінюється частина блоку, його хеш змінюється повністю, сповіщаючи про це мережу. Дана особливість має вирішальне значення для підтримки незмінності блокчейну. Наприклад, одна з найпоширеніших хеш функцій SHA-256, яка створює 256-бітне (32-байт) хеш-значення фіксованого розміру з вхідних даних будь-якого розміру. SHA-256 використовує шість логічних функцій, де кожна функція оперує 32-бітними словами, які представлені у вигляді x, y і z. Результатом кожної функції є нове 32-бітне слово. Розглянемо детальніше кожну із заданих функцій алгоритму хешування SHA-256 з метою вивчення особливостей незмінності технології блокчейн та можливості її застосування для вирішення даної задачі.

$$Ch(x, y, z) = (x \wedge y) \oplus (x \wedge z), \quad (1)$$

де $Ch(x, y, z)$ – функція " вибору", яка обирає біти з двох входів на основі бітів першого входу. Якщо біт x дорівнює 1, вона обирає відповідний біт з y, в іншому випадку із z. Дана функція використовується в алгоритмі для прийняття рішень на основі значень двох вхідних слів,

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z), \quad (2)$$

де $Maj(x, y, z)$ – функція "більшості", яка повертає найбільше значення з трьох вхідних бітів. Якщо два або більше бітів серед x, y та z дорівнюють 1, то результат рівний 1, в іншому випадку - 0. Дана функція використовується для об'єднання інформації з декількох вхідних потоків гарантуючи, що вихід базується на найпоширеніших бітах.

Наступні побітові функції зміщення, об'єднують обернені та зсунуті версії 32-бітового слова x для забезпечення рівномірного розподілу змін у вихідних даних. Ці функції використовуються для обчислення проміжних значень хешу. У функції (3), біти x змішуються шляхом кругових зсувів вправо на 2, 13 і 22 позиції, а потім об'єднуються за допомогою побітової операції($\oplus$).

$$\sum_{\{0\}}^{\{256\}}(x) = ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x), \quad (3)$$

де $ROTR^{n}(x)$ – операція кругового зсуву вправо;

n – ціле число $x \leq n \leq w$;

x – слово певної довжини (біт - w).

Функція (4) здійснює таку ж операцію, що й (3), але із обертанням вправо на 6, 11 і 25 позицій.

$$\sum_{\{1\}}^{\{256\}}(x) = ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x), \quad (4)$$

Подальші функції побітового змішування, працюють аналогічно, але використовують менші зсуви, а також включають зсуви вправо ***(SHR – right shift)***, які замінюють нулями біти, що зсуваються. Функція (5) поєднує повороти вправо на 7 і 18 з логічним зсувом вправо на 3 позиції.

$$\sigma_0^{256}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x). \quad (5)$$

Функція (6) поєднує повороти вправо на 17 і 19 з логічним зсувом вправо на 10.

$$\sigma_1^{256}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x). \quad (6)$$

Дані операції забезпечують необхідну нелінійність і дифузію та дозволяють протидіяти атакам на зіткнення (зловмиснику потрібно знайти два різних повідомлення з однаковим хешем) та атакам на попереднє зображення (зловмисник намагається відновити вхідне повідомлення, знаючи хеш).

Іншим важливим елементом технології є публічні та приватні ключі, що є основою блокчейн та процесу автентифікації транзакцій й включають в себе еліптичні криві, які описуються рівнянням (7) (Dhor, 2022):

$$y^2 = x^3 + ax + b, \quad (7)$$

де a та b – константи, що визначають форму кривої;

p – просте число (визначає скінченне число $\mathbb{F}_p$);

x та y – координати точок на кривій.

У криптографії з еліптичною кривою (ECC) система працює таким чином:

- еліптична крива задається над скінченим полем $\mathbb{F}_p$;
- G – фіксована твірна точка (базова точка на кривій),
- k – приватний ключ, представлений як випадкове ціле число,
- P – публічний ключ, обчислюється як $P = k * G$, де операція множення представляє скалярне множення на кривій.

Для виконання криптографічних операцій використовуються ефективні з точки зору обчислень методи множення, до яких належить алгоритм “подвоїти і додати (Double-and-Add)”, що оптимізує процес обчислення результату множення точки на велике ціле число. Зокрема, обчислення відкритого ключа як $P = k * G$ включає відносно невелику кількість кроків, навіть для великих k. Еліптична крива, що графічно інтерпретує описані математичні залежності представлена на рис. 2.

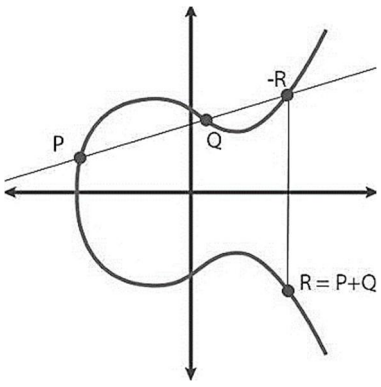

Рис. 2. Еліптична крива (ECC)

Безпека ECC ґрунтується на складності розв’язання задачі дискретного логарифмування еліптичних кривих (ECDLP). Це означає, що відносно легко обчислити відкритий ключ з закритого ключа, а зворотний процес є обчислювально-нездійсненним. Криптографія еліптичних кривих широко використовується в блокчейні, оскільки вона забезпечує надійний захист при набагато менших розмірах ключів у порівнянні з іншими криптографічними алгоритмами, такими як RSA. Що стосується технології блокчейн, то ECC лежить в основі алгоритму еліптичної кривої цифрового підпису ECDSA, що надає засоби підписання та верифікації транзакцій у системі. Підписування повідомлень реалізується такою послідовністю дій:

Повідомлення msg хешується для створення h. Хешування забезпечує стиснення повідомлення до значення фіксованого розміру.

Генерація випадкового числа k, що буде виступати в ролі приватного ключа PrivKey. Число k вибирається випадковим чином в межах певного діапазону $[1, n]$. Ця випадковість гарантує, що навіть якщо одне і те ж повідомлення буде підписано декілька разів, підпис буде відрізнятися.

Обчислення значення R реалізується шляхом множення k на відому точку еліптичної кривої G.

Знаходження частини підпису S здійснюється на основі формули (8):

$$s = k^{-1} * (h + r * PrivKey)\ (mod\ n). \tag{8}$$

Після об'єднання r та s отримується повний підпис, який можна перевірити на валідність. Отож, для перевірки підпису одержувач використовує повідомлення msg, підпис $\{r, s\}$ та публічний ключ відправника $PubKey$. Даний процес визначається такими кроками:

1. Обчислення хешу отриманого повідомлення $h = hash(msg)$.
2. Обчислення R':

$$\mathrm{R'} = (\mathrm{h} * \mathrm{s1}) * \mathrm{G} + (\mathrm{r} * \mathrm{s1}) * \mathrm{PubKey}, \tag{9}$$

де $\mathrm{s_1} = \mathrm{s} - 1\ (\mathrm{mod\ n})$.

На основі цієї залежності здійснюється представлення точки на еліптичній кривій *y*.

3. Визначення r', по отриманій координаті x на основі R'.
4. Перевірка рівності $r' = r$. Якщо вони однакові, то підпис дійсний.

Поєднуючи криптографію еліптичних кривих і хешування, ECDSA гарантує безпечний і ефективний спосіб автентифікації транзакцій і даних в системах блокчейн.

Важливим елементом технології є ключ до незмінності блокчейну, механізм консенсусу. Він полягає у знаходженні унікального випадкового числа, яке гарантує, що хеш блоку починається з певної кількості нулів. У деяких криптовалютах це означає, що хеш повинен починатися з 19 нулів. Якщо блок змінюється, хеші всіх наступних блоків повинні бути перераховані, що вимагає величезних обчислювальних потужностей, а відтак робить підробку практично неможливою. По мірі розростання технології блокчейн її безпека посилюється завдяки застосуванню ланцюгу блоків, які схематично продемонстровані на рис. 3.

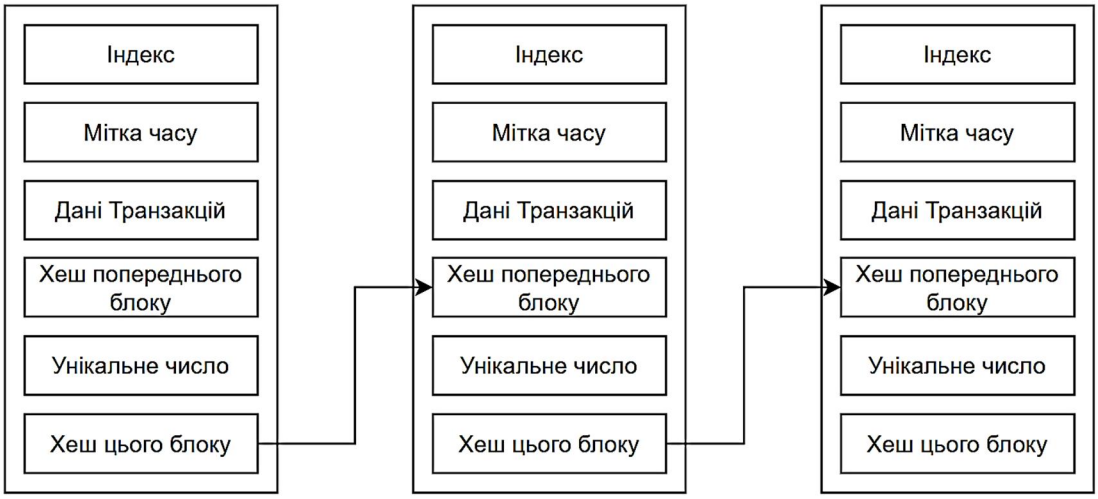

Рис. 3. Приклад ланцюжку блоків у блокчейн

З огляду на те, застосування технології блокчейн у сфері боротьби з контрафактною продукцією стає все більш очевидною, а розробка системи на її основі актуальною задачею.

Формулювання цілі статті

Метою дослідження є аналіз та використання методів та засобів забезпечення автентичності товарів на основі технології Blockchain, для створення інформаційної системи визначення автентичності товару. Для досягнення поставленої мети необхідно вирішити такі основні задачі: здійснити аналіз ринку та проблем пов'язаних з автентичністю товарів; здійснити порівняльний аналіз функціональних можливостей поширених варіацій технології блокчейн; виконати системний аналіз об'єкта дослідження; здійснити проектування інформаційної системи з використанням структурного підходу; розробити блокчейн мережу для функціонування системи та здійснити конструювання та верифікацію роботи системи для перевірки автентичності товарів.

Результати виконаної роботи сприяють вирішенню актуальної проблеми з визначення контрафактних товарів, на основі аналізу стану справ у світі та технологій для вирішення проблеми, а також розроблення програмної системи з використанням технології блокчейн.

Виклад основного матеріалу

Застосування технології блокчейн для розв'язання поставленої задачі потребує вибору відповідного блокчейну, як такого, що впливає на безпеку, масштабованість та функціональність системи загалом. З огляду на проведений аналіз вибір був здійснений між Hyperledger Fabric, Hyperledger Besu (Dawson, 2019) та Corda (Malchenko, 2021). Hyperledger Fabric вирізняється своєю модульною архітектурою на основі P2P-мережі, що дозволяє легко налаштовувати, додавати чи видаляти компоненти системи залежно від потреб користувача. Завдяки приватному характеру мережі даний блокчейн забезпечує високий рівень конфіденційності за допомогою каналів, які дозволяють здійснювати транзакції між учасниками з обмеженим доступом. Hyperledger Fabric використовує протоколи Gossip (Gadgilwar, 2019) та gRPC (Gęsior, 2020) для забезпечення комунікації між учасниками та підтримує різноманітні способи розгортання (Docker та Kubernetes), та має детальну документацію, що спрощує інтеграцію в бізнес-процеси. У порівнянні з Hyperledger Besu та Corda, Hyperledger Fabric надає стабільне та готове рішення для використання у великих і малих проєктах завдяки широкій спільноті користувачів і розробників, а також великій кількості наявних інструментів та підтримки. Результати порівняння блокчейнів наведені в табл. 1.

З огляду на визначені критерії як тип блокчейну було обрано приватний блокчейн Hyperledger Fabric. Hyperledger Fabric має очевидні переваги в таких аспектах, як масштабованість, конфіденційність, модульність, безпека і інтеграція з бізнес-процесами. Ці фактори роблять його особливо привабливим для великих підприємств і бізнесів, які потребують високої гнучкості та можливості налаштування системи під особливі вимоги. У той же час, Corda і Besu можуть бути корисними фінансовій сфері, зокрема для фінансових транзакцій (Corda) або для розробки децентралізованих додатків, орієнтованих на Ethereum (Besu).

Таблиця 1.

Таблиця порівнянь технологій блокчейн

Параметри порівняння	Hyperledger Fabric	Hyperledger Besu	Corda
1	2	3	4
Масштабованість	Підтримує масштабовані мережі з окремими каналами	Підтримує публічні та приватні мережі, при незначній гнучкості	Підтримує масштабовані мережі, орієнтований на обмежені області
Механізм консенсусу	Raft, Kafka, PBFT	PoW (Proof of Work), PoA (Proof of Authority), IBFT 2.0	Raft, Notary (BFT)

Продовження табл. 1

1	2	3	4
Підтримка смарт-контрактів	Chaincode на Go, Java, JavaScript - високий рівень кастомізації	Смарт-контракти на основі Solidity, орієнтовані на Ethereum	Смарт-контракти, які реалізуються як “CorDapps” на Kotlin або Java
Мови програмування	Go, Java, JavaScript	Java	Kotlin, Java
Конфіденційність	Канали з ізоляцією транзакцій, висока конфіденційність	Обмежена конфіденційність в публічних мережах	Висока конфіденційність завдяки застосуванню Notary
Модульність	Висока модульність, можна налаштовувати під різні бізнес-процеси	Модульний, але обмежений для створення великих бізнес рішень	Модульний, гнучкий для різних галузей (фінанси, логістика, тощо)
Продуктивність	Оптимізований для високих навантажень і великих обсягів даних	Оптимізований для Ethereum і DApps, обмежені навантаження	Оптимізований для транзакцій у фінансових системах, але менш ефективний для загальних бізнес-процесів
Інтеграція з бізнес-процесами	Легко інтегрується з ERP, CRM та іншими корпоративними системами	Обмежена інтеграція з корпоративними системами	Легко інтегрується з фінансовими системами
Безпека	Висока безпека завдяки багаторівневій автентифікації та управлінню доступом	Висока безпека для публічних та приватних мереж	Висока безпека для транзакцій у фінансах та суміжних галузях

Важливо зазначити, що незмінність і завершеність транзакцій в системі блокчейн досягається шляхом розбиття транзакцій на впорядковані в часі блоки й обчислення криптографічного хешу кожного з цих блоків (рис.4).

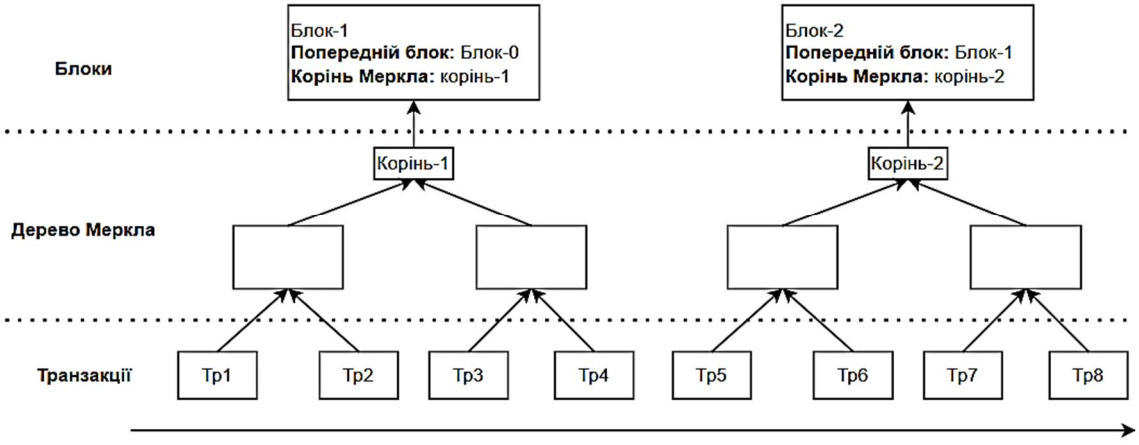

Рис. 4. Структура блокчейну, де кожен з двох відображених блоків містить 4 транзакції

Обчислення хешу для перевірки автентичності товару здійснюється з використанням дерева Merkle (2020), яке складається з декількох хеш транзакцій розташованих у деревоподібній структурі.

Хеш-функції використовуються в блокчейні для простого і послідовного представлення деталей транзакцій. В загальному випадку блокчейн складається з блоків пов'язних між собою, де кожен блок здатен зберігати тисячі записів про транзакції. Виділяють три типи вузлів у хеш-дереві:

- *Кінцевий вузол (Leaf node)* – в якому кожна окрема транзакція в блоці має своє хеш-значення, яке зберігається у кінцевій вершині.
- *Некінцевий вузол (Non-leaf node)* - даний вузол складається з хеш-значень різних кінцевих вузлів, він є проміжною ланкою між кінцевим і кореневим вузлами.
- *Кореневий вузол (Root node)* - містить єдиний хеш, що представляє всі транзакції в блоці, який зберігається в заголовку блоку.

Дерево Merkle розбиває великі масиви даних на менші одиниці, які можна легко опрацьовувати. Воно об'єднує всі транзакційні дані в блок, щоб створити єдиний цифровий відбиток. Таким чином, перевірка транзакцій стає простішою і швидшою.

Особливості застосування дерева Merkle, для даної задачі продемонструємо на прикладі блоків з восьми різними транзакціями: *Tp1, Tp2, Tp3, Tp4, Tp5, Tp6, Tp7 і Tp8*. Кожна транзакція хешується для отримання *X1, X2, X3, X4, X5, X6, X7 і X8*. Далі хеші об'єднуються в пари і знову хешуються, щоб отримати *X(12), X(34), X(56) і (X78)*. Результат знову розбивається на пари і хешується, щоб отримати *X(1234)* і *X(5678)*. На наступному кроці отримується *X(12345678)*, корінь дерева Merkle. Результат зазначеного процесу наведено на рис. 5.

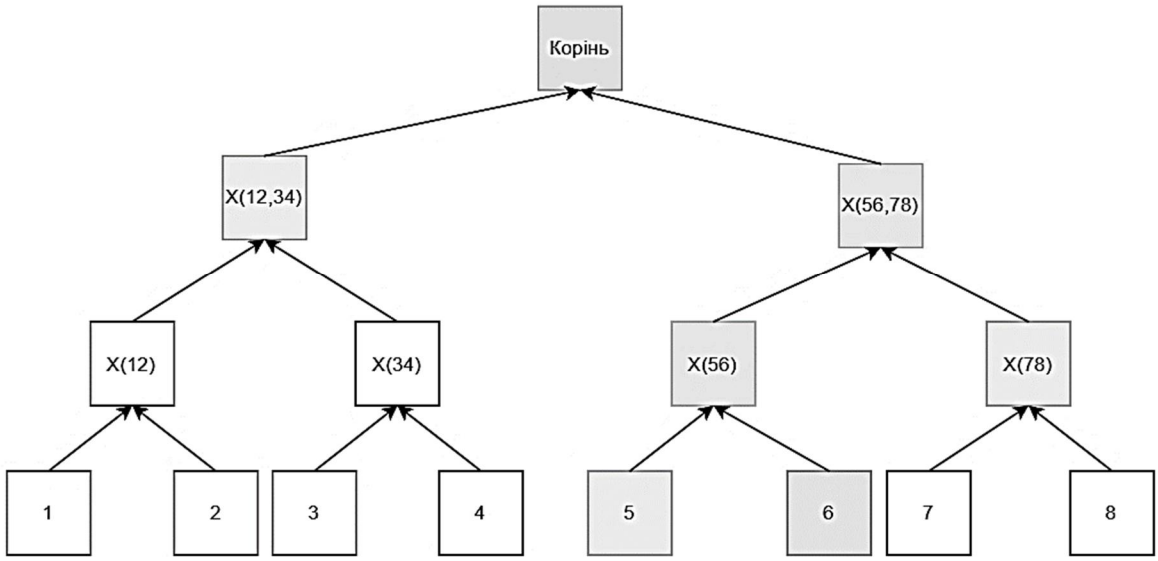

Рис. 5. Приклад дерева Merkle з восьми транзакцій

Наступним етапом дослідження став вибір алгоритму консенсусу для здійснення координації між декількома вузлами. Вибір був між такими алгоритмами: Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault-Tolerant (PBFT) та Raft. Алгоритми Proof of Work (PoW) і Proof of Stake (PoS) мають хорошу підтримку безпеки, відмовостійкості та масштабованості для загальнодоступних блокчейнів. Вони підходять для використання в децентралізованих мережах, де немає довірчих відносин між вузлами, але мають обмежену швидкість підтвердження транзакцій. Для приватних блокчейн-мереж, більш ефективні алгоритми, такі як PBFT і Raft, які обираються через жорсткі договірні зобов'язання та контрольоване середовище передавання даних. Алгоритм Raft забезпечує простоту впровадження, безпечність та можливість роботи навіть за умови виходу з ладу до 50 % вузлів (Howard, 2014). В даному алгоритмі, кожен вузол може знаходиться в одному з трьох станів: лідер, послідовник або кандидат (рис.6).

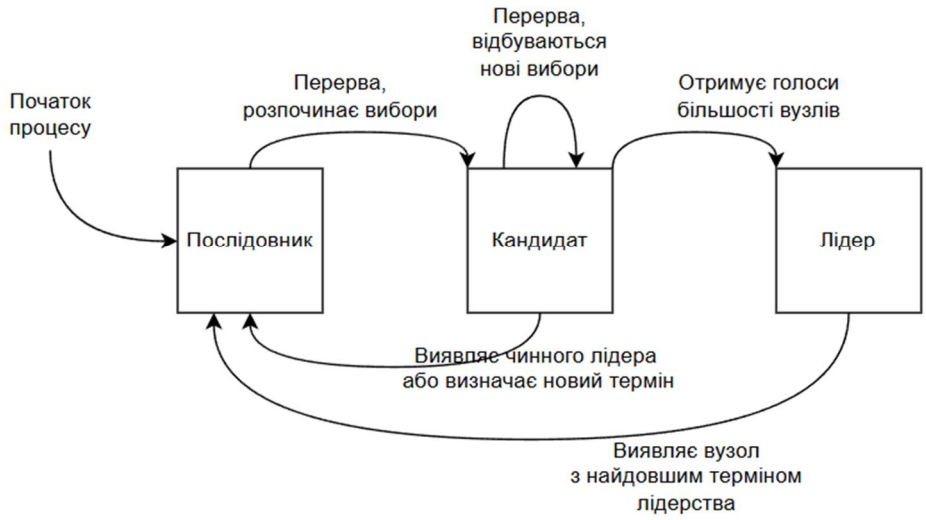

Рис. 6. Стан вузлів протягом виборів

Серед всіх процесів, що відбуваються всередині даного алгоритму важливими, для вирішення даної задачі, є етапи: обчислення термінів проведення виборів лідера, вимоги до кворуму, властивість зіставлення регістрів, перевірка узгодженості доданих записів. Обчислення термінів проведення виборів лідера здійснюється за наступною формулою:

$$\mathrm{E}[T_s] = N_1 + \frac{N_2 - N_1}{s+1}, \tag{10}$$

де N_1- мінімальний виборчий час;

N_2- максимальна тривалість виборів;

s – кількість серверів, що беруть участь у виборах.

Сукупна функція розподілу часу для мінімізації колізій під час виборів :

$$f_s(t) = \begin{cases} \frac{s(N_2 - t)^{s-1}}{(N_2 - N_1)^s}, \\ 0, \end{cases} \tag{11}$$

де t - момент часу, для якого обчислюється ймовірність;

N_1, N_2- мінімальне та максимальне значення часу виборів;

s – кількість серверів.

При використанні алгоритму Raft обмеженням є вимоги до кворуму. А саме, наявна умова n > 2f, де n – загальна кількість вузлів у кластері, f - максимальна кількість допустимих відмов вузлів, яка вказує на мінімальну кількість вузлів для забезпечення відмовостійкості. Ця умова забезпечує здатність системи витримувати f відмов вузлів для забезпечення узгодженості.

Забезпечення узгодженості журналів звітності між вузлами реалізується умовою (12):

$$if\ Log[i] = Log'[i], then\ Log[j] = Log'[j], \forall j < I, \tag{12}$$

де, $Log[i]$- запис у журнал звітності за індексом i у журналі одного вузла;

$Log'[i]$- запис у журнал звітності за індексом j у журналі іншого вузла;

$\forall j < i$ – якщо два журнали, що мають однаковий запис за індексом i, то всі записи на попередніх індексах також повинні збігатися.

Перевірка узгодженості доданих записів визначається двома умовами. *Перша* здійснює перевірку чи індекс попереднього запису в журналі більший за індекс останнього запису в журналі. Якщо це так, то спроба додати новий запис у журнал є недійсною:

$$PrevLogIndex > LastLogIndex. \tag{13}$$

Друга умова перевіряє чи збігається термін попереднього запису в журналі із зазначенням певного індексу з очікуваним терміном, і якщо не збігається, то необхідно здійснювати синхронізацію:

$$Log[PrevLogIndex].Term \neq PrevLogTerm\ , \qquad (14)$$

де ***PrevLogIndex*** - індекс попереднього запису в журналі;

LastLogIndex - індекс останнього запису в журналі на послідовнику;

PrevLogTerm - термін запису в журнал ***PrevLogIndex***.

Визначення погоджених записів у системі відбувається згідно із залежністю:

$$CommitIndex = max\{Index: Log[Index.Term]\ received\ by\ majority\}\ , \qquad (15)$$

де ***Index*** – це індекс звіту у журналі;

$Log[Index.Term]$ - номер терміну використовується для ідентифікації та порівняння валідності записів журналу між різними вузлами в кластері Raft.

Після аналізу та вибору технологій розроблення було здійснено проєктування з використанням структурного підходу. В якості методології проектування було обрано IDEF0, яка призначена для формалізації і опису бізнес-процесів (Spec In, 2024). На контекстній діаграмі (рис.7) зображено основний процес “Забезпечення автентичності товару”.

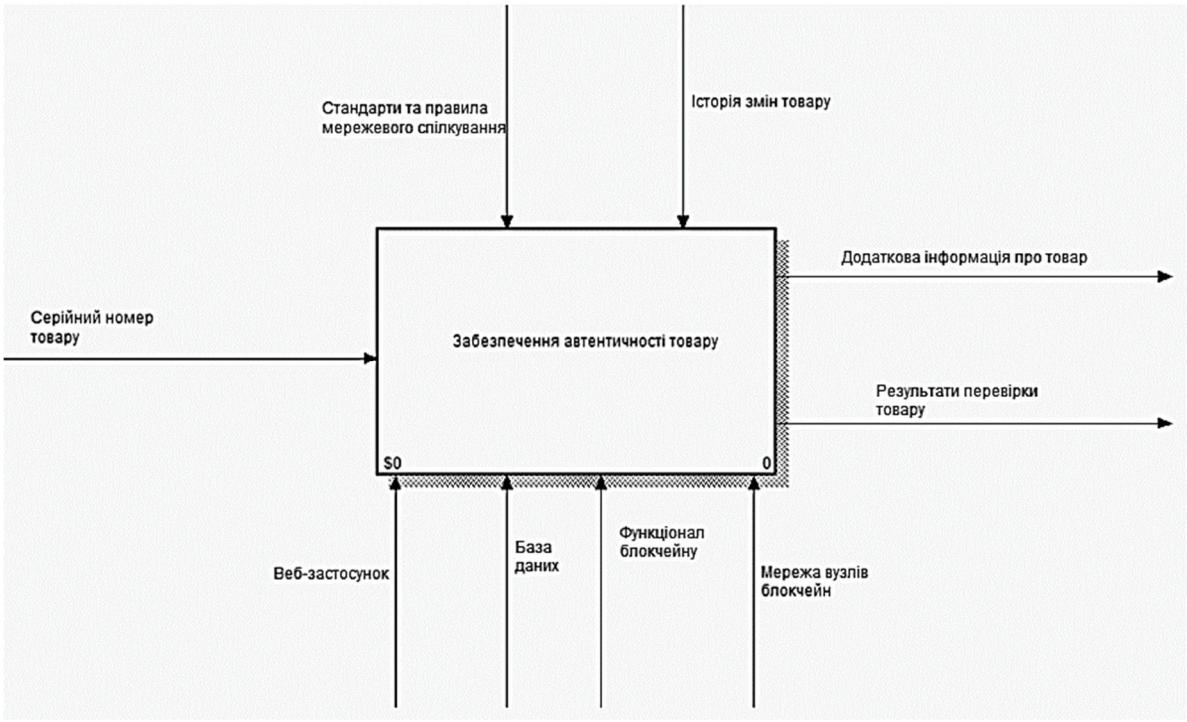

Рис. 7. Контекстна діаграма

Як вхідний інформаційний потік використовується інформація про серійний номер товару, який ідентифікує продукт. Вихідними потоками є результати перевірки товару, а також додаткова інформація про товар у разі успіху; у випадку невдачі результатом є повідомлення про схиблену перевірку. Інформаційна система використовує ресурси, зокрема веб-застосунок для комунікації та отримання серійного номера, базу даних у блокчейні для зберігання інформації про товари, функціонал блокчейн-технології для забезпечення передачі та перевірки даних, а також мережу вузлів блокчейн P2P (Helmy, 2024) для обміну даними. Фактори впливу включають стандарти мережевої комунікації, які регулюють взаємодію вузлів та історію змін товару, що впливає на процеси перевірки автентичності. Для перевірки товару планується використання стандартизованого серійного номера, що вноситься у блокчейн.

Після побудови контекстної діаграми відбувається декомпозиція її головного процесу – “Забезпечення автентичності товару”. Порівняно з першою діаграмою, декомпозиція дозволяє детальніше описати роботу системи, розділивши її на чотири нові процеси, забезпечуючи глибший аналіз роботи системи. У результаті декомпозиції основного процесу, отримуємо такі процеси (рис.8) як отримання серійного номера товару, надсилання серійного номера у блокчейн, перевірка товару на автентичність, оновлення статусу блокчейн.

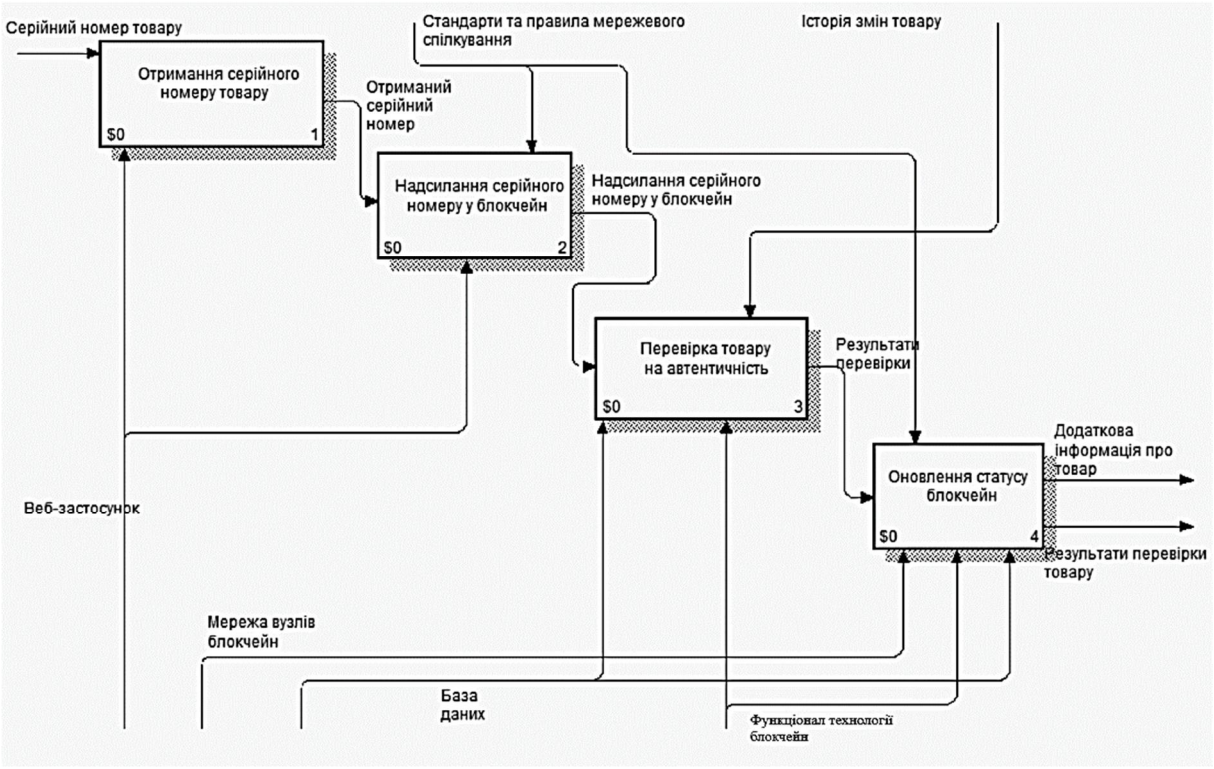

Рис. 8. Деталізована (декомпозиція 1 рівня) діаграма IDEF0

На початковому етапі споживач вводить серійний номер товару через веб-застосунок, після чого ці дані передаються на сервер для подальшого опрацювання. Серійний номер готується до перевірки та надсилається у блокчейн, при цьому дотримуються стандарти мережевої взаємодії, які регулюють правила передачі даних між вузлами системи. Далі відбувається встановлення з’єднання між сервером і вузлом блокчейну. Система знаходить доступний вузол за IP-адресою та портом відповідно до конфігураційного файлу. Процес передбачає автентифікацію користувача з необхідним рівнем доступу, оскільки саме він ініціює створення транзакції для перевірки автентичності товару. Після підтвердження з’єднання серійний номер передається у вигляді транзакції, а точність її виконання забезпечується дотриманням комунікаційних стандартів.

Перевірка автентичності здійснюється шляхом аналізу отриманих із блокчейну даних. Інформаційна система порівнює введений серійний номер із записами в базі даних та визначає його відповідність. Якщо перевірка успішна, споживач отримує підтвердження автентичності товару та додаткову інформацію. У разі невідповідності інформаційна система сповіщає про можливу підробку. Завершальним етапом є оновлення статусу блокчейну, що дозволяє поширювати актуальну інформацію серед усіх вузлів мережі. Після підтвердження даних механізмом консенсусу блок остаточно додається в блокчейн, забезпечуючи цілісність і синхронізацію інформації між усіма учасниками системи.

Наступним етапом дослідження було проведення аналізу доступних програмних рішень для конструювання інформаційної системи. В результаті, для розробки клієнтської частини веб-застосунку було обрано мову програмування JavaScript. На платформі Node.js з використанням

фреймворків Express.js та Fabric-Network розроблена серверна частина застосунку. Для проектування архітектури серверної частини застосунку обрано стиль REST, а написання смарт-контрактів здійснювалось на мові програмування Go. Зберігання даних про товари та смарт-контракти здійснюється у CouchDB. Розгортання системи виконалось за допомогою таких технологій, як VirtualBox, Vagrant, Docker, Docker-Compose та Bash для автоматизації процесів. Для розгортання клієнтської частини веб-застосунку було використано веб-сервер NGINX.

Робота інформаційної системи передбачає створення цифрового реєстру, у якому кожен товар має унікальний серійний номер, а всі транзакції перевірки зберігаються у розподіленій мережі. Процес перевірки автентичності товару починається з введення користувачем серійного номера у веб-застосунок, який передає запит на сервер. Система здійснює пошук відповідної інформації у базі даних блокчейну, порівнює її з наявними записами та визначає справжність товару (рис.9).

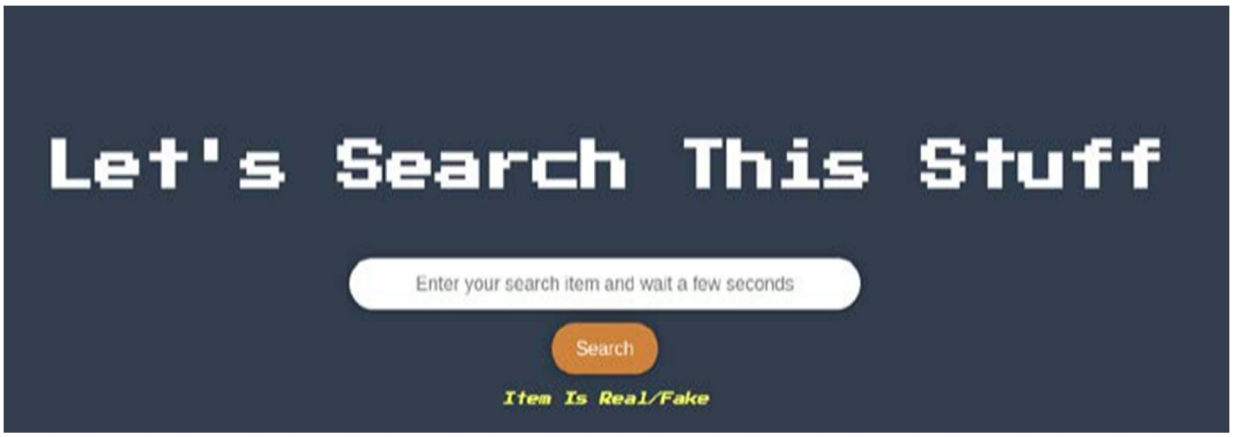

Рис. 9. Головна сторінка веб-застосунку

Після надсилання серійного номера, можливі ситуації підтвердження автентичності товару (рис. 10) або його підробки (рис. 11).

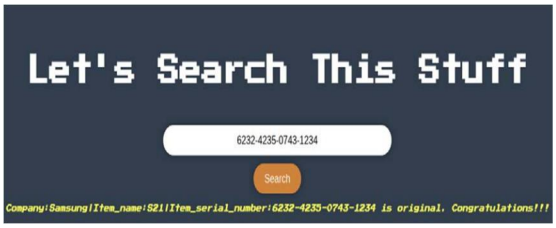

Рис. 10. Успішна перевірка товару

Рис. 11. Товар є підробкою

Функціонування системи передбачає використання ряду технологічних процесів. Першим етапом є встановлення з'єднання між веб-застосунком і мережею блокчейн через спеціалізовані вузли, які забезпечують обмін даними. Далі інформаційна система здійснює перевірку транзакції, проводячи аналіз отриманих даних, звіряє та проводить процес валідації за допомогою механізмів консенсусу. У разі підтвердження інформації вона записується в блокчейн, а всі вузли мережі синхронізують свої записи, що унеможливлює внесення змін заднім числом. Таким чином, інформаційна система забезпечує високий рівень захисту інформації та автоматично оновлює статус товарів у розподіленій мережі.

Перевірка автентичності товару базується на використанні таких основних ресурсів як веб-застосунок, що виступає інтерфейсом для взаємодії з користувачами; база даних, у якій зберігається інформація про всі товари, блокчейн-мережі, яка гарантує надійність та незмінність даних. Приклад зберігання одного з товарів (рис.12) та посилання на схвалений блок у блокчейні наведено на рис.13.

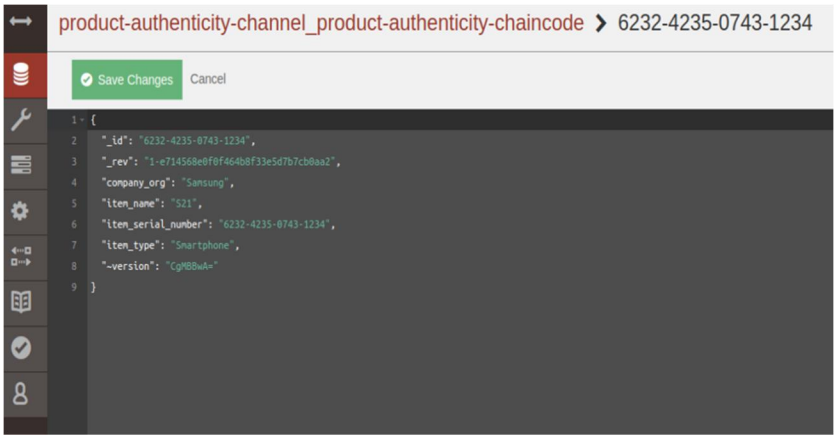

Рис. 12. Приклад зберігання товару у базі даних

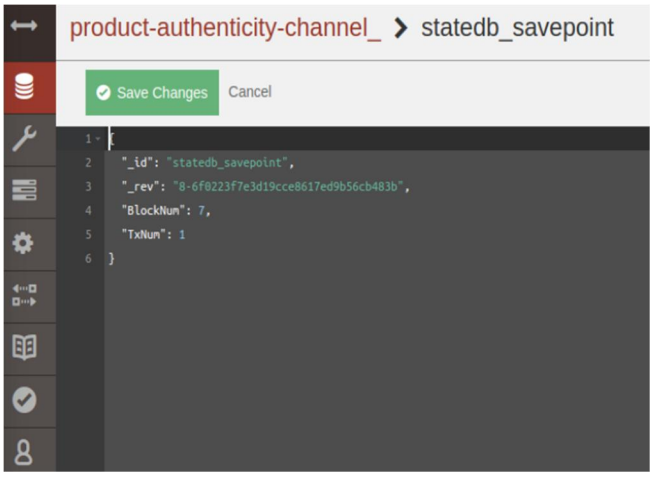

Рис. 13. Приклад зберігання посилання на схвалений блок у базі даних

На роботу системи впливають також зовнішні чинники. Зокрема, стандарти інформаційної взаємодії визначають правила обміну даними між вузлами блокчейну, а також забезпечують сумісність із різними інформаційними платформами. Ще одним важливим аспектом є історія змін товару. Якщо товар проходив певні транзакції, наприклад, зміну характеристик або перереєстрацію, це враховується під час перевірки автентичності.

Завершальним етапом дослідження став розрахунок продуктивності прототипу з використанням елементів теорії черг. Основними елементи системи черг є:

- *клієнти* – надсилають запити із серійними номерами;
- *черга* - запити, які очікують опрацювання;
- *сервер* - смартконтракт на Hyperledger Fabric, який взаємодіє з CouchDB для перевірки серійних номерів;
- *час прибуття (λ)* - середня кількість запитів на одиницю часу;
- *час обслуговування (μ)* - середня кількість запитів, які може опрацювати сервер за одиницю часу.

В якості імітації черги було обрано модель *M/M/1* (потік запитів має експоненційний розподіл, один сервер), де *M* (експоненційний розподіл часу між прибуттям запитів), *M* (експоненційний розподіл часу обслуговування), *1* (Один сервер (смартконтракт). Здійснимо розрахунок “потенційної продуктивності прототипу” на прикладі таких вхідних даних: $\lambda = 10$ (запитів/хв), $\mu = 15$(запитів/хв). Спершу буде розраховано *коефіцієнт навантаження:*

$$\rho = \frac{\lambda}{\mu} = \frac{10}{15} = 0.666. \quad (16)$$

Тобто система завантажена на 33,4 %, при згаданих параметрах. Далі обчислимо *середню кількість запитів у системі (L)*:

$$L = \frac{\rho}{1-\rho} = \frac{0.666}{1-0.666} = 2\ . \quad (17)$$

Отриманий результат свідчить, що в середньому, при зазначених вхідних даних два запити перебувають у системі (включаючи ті, що очікують і опрацьовуються). Обчисливши коефіцієнт навантаження та середню кількість запитів у системі, можна обчислити *середній час перебування запиту в системі (W):*

$$W = \frac{1}{\mu-\lambda} = \frac{1}{15-10} = 0.2\ хв. \quad (18)$$

Тобто, кожен запит перебуває в системі 12 секунд. Далі здійснимо обчислення *середнього часу очікування в черзі (W_q):*

$$Wq = W - \frac{1}{\mu} = 0.2 - \frac{1}{15} = 0.2 - 0.066 = 0.134\ хв. \quad (19)$$

Тобто, запит очікує в черзі близько 8 секунд. А *ймовірність відсутності черги (P_0)*:

$$P_0 = 1 - \rho = 1 - 0.666 = 0.334\ . \quad (20)$$

Здійснивши розрахунки можна зробити наступні висновки. Середній час опрацювання одного запиту (включаючи очікування в черзі) становить 12 секунд.

Висновки

В проведеному дослідженні здійснено аналіз та описано використання методів та засобів забезпечення автентичності товарів на основі технології Blockchain. Реалізовано програмний застосунок, що надає можливість здійснювати перевірку оригінальності придбаного товару. Проведено аналіз існуючих підходів боротьби з підробками і обґрунтовано вибір блокчейну Hyperledger Fabric, як ефективного способу забезпечення прозорості та захисту даних. Здійснено системний аналіз та проектування інформаційної системи з використанням методології функціонального моделювання (IDEF0), що дало змогу деталізувати процеси системи та здійснити опис бізнес-процесів. Описано особливості роботи із програмною системою, яка реалізована на поточний момент у вигляді прототипу. Результати виконаної роботи зосереджені на дослідженні методів і засобів забезпечення автентичності товарів для створення ефективної системи боротьби з контрафактною продукцією. Розроблений прототип системи відрізняється від існуючих аналогів можливістю дистанційно здійснювати перевірку із застосуванням децентралізованої блокчейн-мережі, що забезпечує високий рівень безпеки та прозорості й практично унеможливлює маніпуляцію з даними.

Незважаючи на значний потенціал блокчейн-технології для забезпечення автентичності товарів, існує низка викликів, пов’язаних із її впровадженням. Основними обмеженнями є ризики фізичної підміни маркувань, складність інтеграції з існуючими системами, правові бар'єри, обмеження масштабованості та високі витрати на розгортання системи. Вирішенням цих проблем можуть бути додаткові заходи фізичної безпеки, адаптація нормативно-правової бази, розвиток технологій масштабування (наприклад, шарові рішення для блокчейну) та впровадження BaaS-моделей, які знижують вартість входу для малого та середнього бізнесу.

Подальші дослідження будуть зосереджені на оптимізації процесів інтеграції блокчейну в існуючі системи, а також пошуку рішень для підвищення масштабованості та зниження витрат на її впровадження. Успішна реалізація таких підходів сприятиме підвищенню ефективності та безпеки процесів перевірки автентичності товарів у глобальних ланцюгах постачання.

СПИСОК ЛІТЕРАТУРИ

1. Beaver, N.A., Solomon, G.B., Wang, E., & Wegrzyn, K.E. (2021). Get Real: Preventing Counterfeit Product with Blockchain. Retrieved from: https://www.foley.com/insights/publications/2021/10/preventing-counterfeit-product-with-blockchain/
2. David, M. (2024). The Yiwu market in China: where tradition meets innovation in global trade expansion. Daxue Consulting – Market Research and Consulting China. Retrieved from: https://daxueconsulting.com/yiwu-market-in-china/
3. Dawson, R., & Baxter, M. (2019). Announcing Hyperledger Besu. Retrieved from: https://www.lfdecentralizedtrust.org/blog/2019/08/29/announcing-hyperledger-besu
4. Dhor, P.S. (2022). The Mathematics behind Blockchain. Retrieved from: https://blockchain.ieee.org/images/files/pdf/techbriefs-2022-q3/the-mathematics-behind-blockchain.pdf
5. Gadgilwar, C. (2019). Role of Peers in Hyperledger Fabric Blockchain. Retrieved from: https://medium.com/@chetan.gadgilwar/role-of-peers-in-hyperledger-fabric-blockchain-fe383d8ee84c
6. Gao, X., Zhang, W., Zhao, B., Zhang, J., Wang, J., & Gao, Y. (2022). Product Authentication Technology Integrating Blockchain and Traceability Structure. Retrieved from: https://www.researchgate.net/publication/364405489_Product_Authentication_Technology_Integrating_Blockchain_and_Traceability_Structure
7. Gęsior, T. (2020). P2P in Hyperledger Fabric. Retrieved from: https://brightinventions.pl/blog/p2p-in-hyperledger-fabric/
8. Gudadhe, M., Alchewar, S., Shelke, R., Mohariya, K. , Moon, S., & Dhote, P. (2023). Unveiling Fakes: A Blockchain-Backed Approach for Product Authentication. Retrieved from: https://www.ijraset.com/research-paper/blockchain-backed-approach-for-product-authentication
9. Harbert, T. (2019). Blockchain for business starts in the supply chain. Retrieved from: https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-business-starts-supply-chain
10. Helmy, B.E., & Aibin, M. (2024). An Introduction to Peer-to-Peer Network Model. Retrieved from: https://www.baeldung.com/cs/peer-to-peer-network-model
11. Henry, W., Kathawate, R., Chen, E., & Coulter, J. (2023). Using blockchain to drive supply chain transparency. Retrieved from: https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html
12. Howard, H. (2014). ARC: Analysis of Raft Consensus. Retrieved from: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-857.pdf
13. Kamble, D., Singh, A., Chaudhari, V., Koli, R., & Menon, S. (2023). Integrating QR Code and Blockchain Technologies for Enhanced Authenticity and Traceability of Products. Retrieved from: https://stmcomputers.stmjournals.com/index.php/JoADMS/article/view/486
14. Li, L., Qu, H., Wang, H., Wang, J., Wang, B., Wangm, W., Xu, J., & Wang, Z. (2022). A Blockchain-Based Product Traceability System with Off-Chain EPCIS and IoT Device Authentication. Retrieved from: https://www.mdpi.com/1424-8220/22/22/8680
15. Malchenko, S. (2021). Why Choose Corda For Your Project? Retrieved from: https://4irelabs.com/articles/why-choose-corda-for-your-project
16. Merkle, R.C. (2020). A digital signature based on a conventional encryption function. In: Advances in Cryptology – CRYPTO 'S (Lecture Notes in Computer Science). Vol. 293. Conference paper. 2020. pp. 369–378
17. OECD. (2019). Trade in fake goods is now 3.3 % of world trade and rising. OECD. Retrieved from: https://web-archive.oecd.org/2019-03-19/511489-trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm
18. Richter, F. (2019). U.S. Companies Most Affected by Counterfeiting. Retrieved from: https://www.statista.com/chart/17407/countries-most-affected-by-counterfeit-and-pirated-goods/
19. Spec In. (2024). IDEF0 Diagram. Retrieved from: https://help.specinnovations.com/idef0-diagram
20. Vardhan, H.V., Rohan, L., Reddy, A.K., & Mourya, M. (2023). Mitigating Counterfeiting Using Blockchain Enabled Product Authentication. Retrieved from: https://www.ijraset.com/research-paper/mitigating-counterfeiting-using-blockchain-enabled-product-authentication
21. Wang, Y., Han, J., & Beynon-Davies, P. (2018). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Retrieved from: https://www.researchgate.net/publication/329813013_Understanding_blockchain_technology_for_future_supply_chains_a_systematic_literature_review_and_research_agenda
22. Wasnik, K., Sondawle, I., Wani, R., & Pulgam, N. (2022). Detection of Counterfeit Products using Blockchain. Retrieved from: https://www.researchgate.net/publication/ 360414345_Detection_of_Counterfeit_Products_using_Blockchain

DEVELOPMENT OF A PRODUCT AUTHENTICATION SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

Vladyslav Liakh[1], Taras Basyuk[2]

[1, 2] Lviv Polytechnic National University,
department of information systems and networks, Lviv, Ukraine
[1] E-mail: vladyslav.liakh.mnitm.2023@lpnu.ua, ORCID 0009-0002-7870-721X
[2] E-mail: Taras.M.Basyuk@lpnu.ua, ORCID 0000-0003-0813-0785

© Liakh V., Basyuk, T.,2025

The article addresses the problem of counterfeit goods using Blockchain technology. An analysis of existing methods and tools for combating counterfeiting has been conducted, justifying the choice of blockchain as an effective means of ensuring transparency and data protection. An analysis of existing anti-counterfeiting approaches has been conducted, justifying the choice of blockchain as an effective method for ensuring transparency and data protection. The authors designed the system using a structured approach, which allowed for task systematization and the identification of key operational aspects. For system modeling, the Data Flow Diagrams (DFD) methodology was applied, enabling the creation of a context diagram and decomposition diagrams. The system architecture was developed based on Hyperledger Fabric, incorporating multiple nodes and certification authorities to ensure reliability and verification integrity. The functional purpose of the system is presented, allowing users to verify product authenticity. System verification was conducted, demonstrating its effectiveness and providing a description of the key operational stages.

Keywords – blockchain, product authenticity, decentralized network, Hyperledger Fabric, Docker.