ISSN2224-087X. Електроніка та інформаційні технології. 2024. Випуск 27. С. 43–58
Electronics and information technologies. 2024. Issue 27. P. 43–58

УДК 004.9 DOI: https://doi.org/10.30970/eli.27.4

ІНФОРМАЦІЙНА ПІДТРИМКА ПРОЦЕСІВ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ДАНИХ НА ОСНОВІ BLOCKCHAIN

М. Назаркевич[1], О. Прокіпчук[2], В. Висоцька[2], Р. Голощук[2], Р. Федчук[2]

[1]Львівський національний університет імені Івана Франка,
вул. Тарнавського 107, 79017 Львів, Україна
[2]Національний університет «Львівська політехніка»,
вул. Степана Бандери 12, 79013 Львів, Україна
mariia.nazarkevych@lnu.edu.ua

Щорічно доля контрафактних товарів на ринку лише зростає, як і шкода, що вона завдає. При чому це не лише матеріальні збитки, але й шкода довкіллю та здоров'ю людей. У найгірших випадках така необачність може привести до смерті людей. Саме тому великі компанії сьогодні починають винаходити різноманітні рішення боротьби з контрафактом, в тому числі реалізаційя інформаційної підтримки процесів перевірки автентичності даних на основі blockchain технології. система, що зможе зменшити загрозу підроблених товарів в сучасних умовах є актуальною. Метою створення даної системи є забезпечення покупців товарів можливістю перевірки їхньої автентичності. Перевірка повинна бути можливою як до, так і після покупки з здатністю повернути товар у випадку виявлення підробки. Система повинна об'єднувати виробників в єдину мережу, досягаючи уникання прив'язаності до конкретного виробника. Таким чином кожен покупець може переглянути будь-яку частину потрібних даних. За умови такої прозорості даних розроблена система повинна забезпечувати надійний захист цієї інформації. Також система повинна забезпечувати додатковий функціонал відмінний від основного, що дозволить розширити сферу застосування та збільшити переваги використання системи користувачами. Наостанок вибраний спосіб перевірки повинен складатися з багаторазової частини, що може використовувати будь-хто та одноразової частини призначеної для конкретного покупця. Об'єкт дослідження: перевірка автентичності товарів з використанням blockchain технології. Предмет дослідження: засоби створення об'єднаної децентралізованої системи блокчейну, що забезпечує можливість перевірки товару на автентичність для усіх виробників-учасників цієї мережі.

Ключові слова: мережевий зв'язок, інформаційна система, контрафактний товар, технологія блокчейн, життєвий цикл продукту, інтелектуальна система пошуку інформації, ключ продукту.

Вступ

Швидке поширення підробок на ринку стало дуже актуальною проблемою XXI століття [1]. При сьогоднішній поширеності компаній-гігантів на ринку товарів багато виробників бояться вступати в конкуренцію та застосовують більш підступні методи заробітку – контрафакт [2-3]. На сьогоднішній день виробництвом підроблених товарів

займаються тисячі виробників з усього світу [4]. Підроблені товари завдають не тільки матеріальних збитків виробникам оригінальних товарів, а й становлять серйозну загрозу здоров'ю покупців таких товарів. Проте такі товари завдають значної шкоди людству. У результаті багато компаній уже намагаються боротися з цим явищем різними способами. Саме для цього розробляються методи боротьби з контрафактом та методи виявлення оригінальних товарів. Одним з таких методів є інформаційна система перевірки автентичності товарів на основі технології блокчейну. Дана система надає покупцю можливість перевіряти товари на автентичність після або перед покупкою, а також об'єднує виробників в єдину мережу з метою підвищення надійності та прозорості такого підходу. Використаний метод майже не має аналогів в своєму полі дії, а методи що працюють на різних рівнях лише доповнюють одне одного. Система є дешевшою у впровадженні та надійнішою при масовому використанні ніж аналоги. Саме тому, система, що зможе зменшити загрозу підроблених товарів в сучасних умовах є актуальною. Метою створення даної системи є забезпечення покупців товарів можливістю перевірки їхньої автентичності. Перевірка повинна бути можливою як до, так і після покупки з здатністю повернути товар у випадку виявлення підробки. Система повинна об'єднувати виробників в єдину мережу, досягаючи уникання прив'язаності до конкретного виробника. Таким чином кожен покупець може переглянути будь-яку частину потрібних даних. За умови такої прозорості даних розроблена система повинна забезпечувати надійний захист цієї інформації. Також система повинна забезпечувати додатковий функціонал відмінний від основного, що дозволить розширити сферу застосування та збільшити переваги використання системи користувачами. Наостанок вибраний спосіб перевірки повинен складатися з багаторазової частини, що може використовувати будь-хто та одноразової частини призначеної для конкретного покупця. Для реалізації мети необхідно реалізувати такі задачі:

- Опрацювати проблематику області для того, щоб скласти базу існуючих способів підробки товарів та методів боротьби з ними. Виокремити переваги та недоліки знайдених підходів та дослідити погляд покупця на привабливість таких методів.
- Спроектувати взаємозв'язки елементів системи для створення гнучкої та стабільного комплексу. Потрібно побудувати дерево цілей та обрати тип інформаційної системи на основі отриманих критеріїв, а також провести системний аналіз за допомогою побудови процесних діаграм та ієрархії задач.
- Визначити потрібні технологічні та програмні засоби для реалізації такої системи. При необхідності здійснити порівняння аналогів та встановити пріоритетні рішення.
- Розробити загальну структуру системи та зібрати статистичні дані, що дозволять оптимізувати роботу із системою в майбутньому.

Аналіз останніх досліджень та публікацій

Кожен принаймні раз помічав товари неналежної якості на полицях ринків або супермаркетів або ж при отриманні доставки з інтернет магазину. Покупець розчаровується в магазині або у виробнику товару, відповідно зменшує прибутки наступних. Притому ніхто не може уникнути зони ризику контрафактних товарів оскільки ця мережа проникла майже у всі сфери вироблення товарів, тож потрібно ретельно оглядати та перевіряти товар при покупці. На рис. 1 зображена світова статистика по галузях, що зазнають збитків від контрафактних товарів згідно OECD [5].

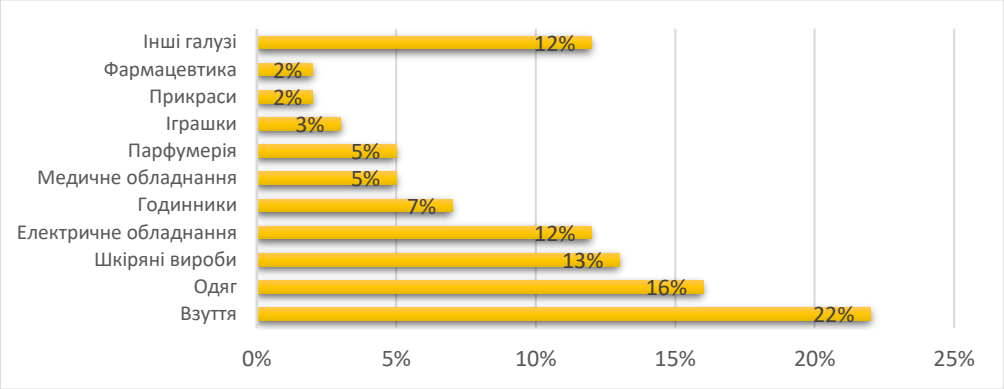

Рис. 1. Індустрії, що найбільше страждають від контрафакту [5]
Fig. 1. Industries most affected by counterfeiting [5]

До цього згадувалась лише матеріальна шкода для покупців, магазинів чи власників авторського права, але контрафактні товари наносять більш вагомі збитки, ставлячи під загрозу безпеку та здоров'я покупця. Причому часто ці загрози бувають неочевидними і це розкривається тоді, коли уже складно щось виправити. Оригінальні продукти розробляються за відповідними стандартами безпеки і якості та за відповідних вимог, визначених законодавством. При покупці оригінального товару, плата йде не тільки за сам товар, але і за те, що товар зроблений з дотриманням усіх вимог, тобто суттєво зменшує усі потенційні ризики для здоров'я. Чого не можна сказати про підробки, й про це потрібно пам'ятати, коли в наступний раз виникне бажання придбати дешевшу версію оригінального продукту. Навіть такі, з першого погляду безпечні, товари, як одяг, може завдати шкоди організму людини. Тканина, що вироблена з неякісних матеріалів в умовах антисанітарії може бути токсичною для людини, а також спричиняти різноманітні подразнення шкіри. Найбільш яскравий приклад токсичності матеріалів демонструє нам відділ косметики. Дослідники з "Homeland Security" тестують різні шкірні засоби й строго застерігають від покупки підроблених варіантів. Крім того, що такі продукти часто бувають токсичними, дослідники також повідомляють про те, що знаходять в них ціанід, свинець, урину людей та тварин, кал, миш'як та інші небезпечні речовини. При тому це стосується не тільки макіяжу, але й очищувачів шкіри, кремів для засмаги та інших [6]. Ще одним неочевидним прикладом загрози здоров'ю є неякісні сонцезахисні окуляри. Згідно опитуванню, проведеному Бразильською Асоціацією Оптичної Індустрії, з 24 мільйонів пар окулярів, вироблених країною, 7 мільйонів є нелегальними. Це є неймовірно великою кількістю й може нашкодити очам мільйонів покупців.

На відміну від оригінальних товарів, що містять всі необхідні сонцезахисні шари, контрафактні товари мають лише затемнене скло, що лише створює видимість захисту від сонця. Як наслідок – від затемненого скла зіниця ока розширяється, але кількість ультрафіолетового випромінювання залишається такою ж і око отримує більше шкоди, аніж узагалі без окуляр [7]. При носінні неякісного взуття нерідкісними є випадки деформації стопи носія, що також призводить до подальших захворювань опорно-рухової системи організму людини [7]. Вже більш очевидну загрозу становлять підроблені

електричні товари. Шкода від них часто буває миттєвою й фатальною. Йдеться про удари власника струмом або створення коротких замикань та пожеж.

Для прикладу візьмем зарядки для смартфонів. Більше половини людей на Землі користуються смартфонами. Їх необхідно час від часу заряджати. Деколи зарядні пристрої виходять з ладу й тоді, при покупці заміни, власники смартфонів часто обирають дешевші варіанти. Так з допомогою компанії Apple, організація Electrical Safety First протестувала велику кількість підроблених зарядних пристроїв для Iphone, куплених в Amazon, Ebay та інших магазинах. Результати дослідження показали, що 98% куплених пристроїв мають потенційний ризик завдати летальний удар струмом або спричинити пожежу [8].

Найбільш очевидною та небезпечною є загроза підроблених медичних приладів та фармацевтики (рис. 2). Несправне обладнання може запросто обірвати людське життя. За такими галузями потрібен найбільший контроль. При покупці подібних товарів варто слідкувати за найменшими відхиленнями, адже шкода спричинена ними може стати дуже великою.

В розвинутих країнах підроблена фармацевтика не набула особливого поширення й боротьба з нею проходить відносно успішно, але ситуація значно погіршується, якщо розглядати бідні країни. World Health Organization (WHO) стверджує, що 10% усіх медикаментів у бідних країнах є підробками. Якщо розглядати це число з точки зору потенційної загрози, то це дуже багато. Найменше відхилення в матеріалах чи умовах виготовлення фармацевтики може привести до великих втрат. З 2013 р. WHO отримала більше 1500 скарг про контрафактні товари із бідних країн. Ліки при малярії та антибіотики виявились найпопулярнішими серед виробників підробок. Найбільше скарг про контрафактні товари надходить з Африки і становить аж 42% [9].

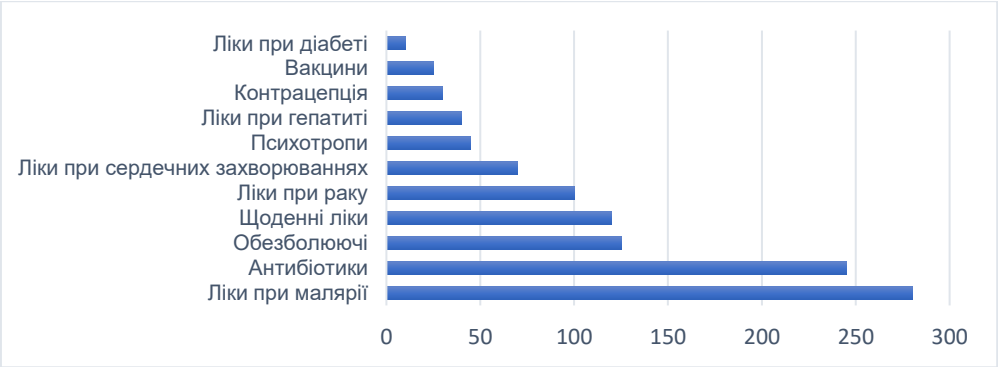

Рис. 2. Найбільш розповсюджені підроблені ліки [9]
Fig. 2. The most widespread fake medicines [9]

Методи інформаційної підтримки процесів перевірки автентичності даних

Зрозуміло, що поширення контрафактної продукції становить як матеріальну, так і шкоду здоров'ю. Для того, щоб залишатись на плаву та мінімізувати збитки компанії повинні розробляти методи виявлення справжньої продукції для того, щоб дати можливість покупцю, а також різним контролюючим службам відрізнити оригінал від підробки. Є декілька основних методів виявлення товару, від традиційних, до технологічних.

Законодавчий. Даний метод засновується на довірі покупця до дій держави по забороні та вилученню контрафактних товарів. Простіше кажучи, якщо товар продається в загальному доступі й досі не заборонений, то це оригінал. Багато сучасних країн серйозно ставляться до питання контрафакту та строго карають за розповсюдження такої продукції. Метод в основному залежить на тому, що той, хто придбає підроблений товар, поскаржиться на це й в залежності від результату джерело розповсюдження буде заблоковане. В Європі та Америці працює підхід "Save Harbor". Він накладає певні обмеження на інтернет магазини і працює наступним чином. Посередник між продавцем та покупцем звільнений від відповідальності за порушення авторських прав, якщо він дотримується двох вимог: є можливість подати скаргу про порушення; посередник реагує на скарги(видаляє чи блокує контент, що порушує права). З таким підходом можна виявляти довіру до тих продавців, що тривалий час знаходяться на ринку [10]. Зазвичай штрафи за поширення контрафактної продукції є великими. Так в Китаї штраф за порушення цих правил становить 7200$ - 72 000$, при тому, якщо контрафактна продукція загрожує здоров'ю покупця, то штраф може досягати 288$ тис. [11]. Плюси підходу: регулюється законом та не потребує великих матеріальних вкладень для впровадження. Мінуси підходу: базується на довірі, точність невелика та неможливо встановити автентичність для непровірених часом магазинів.

Розробка інструкцій для знаходження різниці між оригіналом та підробкою. Для кожного свого товару виробник створює інструкцію для того, щоб при покупці товару покупець міг відрізнити оригінал за певними прикметами. Метод базується на фізичному та візуальному огляді. Щоправда такий метод уже зазнавав поразки. В 2018 компанія Baby Foot створив на своєму офіційному сайті інструкцію з усіма необхідними пунктами, щоб визначити оригінал. Цією інструкцією скористались виробники контрафакту, щоб заплутати покупця [12]. Плюси підходу: не потребує великих матеріальних вкладень для впровадження. Мінуси підходу: базується на обізнаності покупця, точність низька та інструкції працюють як для покупців, так і для виробників підробок.

Моніторинг та блокування підозрілих ресурсів. Підхід полягає в тому, що компанія виробник здійснює моніторинг інтернет ресурсів на предмет товарів, що порушують авторське право, та їхнє подальше блокування. Моніторинг таких ресурсів в автоматичному або напівавтоматичному режимах вимагає розробки спеціалізованого програмного забезпечення, відповідно і ресурсів на цю розробку. Виявлення оригіналу базується на довірі покупця до того, що всі контрафактні ресурси заблоковані. Виробник товару може як сам здійснювати моніторинг, так і довірити цей процес іншій компанії. Для прикладу компанія Group-IB вже тривалий час надає подібні послуги та володіє широким функціоналом. Компанія здійснює моніторинг в наступних областях: доменні імена, агрегатори, дошки оголошень, пошукові системи, глибинний веб, соціальні мережі, магазини мобільних додатків, месенджери, контекстна реклама. При знаходженні контрафакту компанія здійснює усі необхідні досудові заходи по блокуванню ресурсів, а також надає повну юридичну підтримку [13]. Плюси підходу: надійність вище середньої, можна доручити іншій компанії та дозволяє ефективно заблокувати багато контрафактних ресурсів. Мінуси підходу: потребує немалих матеріальних вкладень, базується на довірі покупця та працює тільки для інтернет покупок.

Застосування штучного інтелекту для виявлення контрафакту. Аспекти машинного навчання сильно укорінились в наше буденне життя. Це дуже потужна технологія, що може автоматизувати працю багатьох людей. Ці технології застосовують зазвичай в розпізнаванні чогось і виявлення підроблених товарів не виняток. Різні

компанії уже почали використовувати штучний інтелект в подібних цілях і різними способами. Alibaba group застосовує новітні розробки в області машинного навчання для того, щоб виявити оголошення контрафактної продукції. Розроблена система дозволяє виявляти підробки за наступними ознаками:

- Ціна: система виявляє нереалістичні зміни від очікуваної ціни, а також враховує можливі сезонні знижки, конвертацію валюти і той факт, що товар є вживаним.
- Зображення: система може виявляти найменші відхилення у зображеннях оголошень потенційних підробок. При досягненні критичної кількості відхилень, програма сповіщає про підозрілість продукту.
- Опис: система аналізує опис алгоритму для пошуку підозрілих фраз, оригінальним товарам не потрібно нав'язувати покупцю свою справжність чи новизну, відповідно алгоритм враховує подібні деталі.

Оскільки система базується на навчанні, а не на визначеному алгоритмі, точність не може становити 100%. Можливі потенційні огріхи, й чим більше товарів аналізується, тим більше легальних товарів можна розпізнати як фальшивку. Саме тому така система може працювати лише в напівавтоматичному режимі, адже через заборону легальних товарів можуть виникнути проблеми з законом [14]. Згідно звіту за 2018 рік, Alibaba конфіскувала контрафактні товари сторонніх продавців на суму 536 мільйонів доларів [11]. Ще один спосіб застосування штучного інтелекту для виявлення контрафакту продемонструвала компанія IBM у своєму продукті Crypto Anchor Verifier. Ця новітня технологія являє собою мікро сканер, що може вбудовуватись в камери мобільних телефонів та здійснювати детальний аналіз матеріалу товару й на основі цього робити висновок про його автентичність. Система містить дані про оригінальний товар, та на їхній основі штучний інтелект помічає відмінності з підробленим товаром та робить висновок згідно з результатами порівнянь. Спочатку система розроблялась на розпізнавання автентичності алмазів й, після успішного використання, компанія швидко зрозуміла, який потенціал має подібна технологія [15]. Після розвитку та доопрацювання алгоритмів навчання система змогла успішно аналізувати матеріали таких товарів, як вино, одяг, ліки, коштовне каміння і т.д. Система може відрізняти дороге вино від дешевого, розпізнавати генно модифіковані продукти, аналізувати якість води і навіть знаходити бактерії по типу кишкової палочки [16]. Загалом технологія є дуже перспективною й в недалекому майбутньому можна очікувати плодів її широкого застосування. Плюси підходу: надійність висока, дешевий при застосуванні, працює в напівавтоматичному режимі та популярність технології машинного навчання дозволяє легше отримати довіру покупця. Мінуси підходу: технологія залишається неточною, розвиток таких систем може зайняти багато часу та потребує додаткових зусиль із впровадження.

Використання спеціальних маркувань для ускладнення підробки. Ще одним способом для захисту товарів є нанесення на упаковку або на сам товар спеціальних ідентифікуючих знаків. Дане рішення дозволяє користувачам ідентифікувати оригінальний товар в розрахунку на те, що виробники контрафактних товарів не зможуть скопіювати технологію. Застосування даної технології містить підводний камінь, що полягає у постійних перегонах між виробником товарів та зловмисниками у створенні вище згаданих знаків. Місією виробника є розробка та використання маркування з якомога вищою складністю її підробки, а місія зловмисника – це якнайбільш точне копіювання маркувань для ускладнення знаходження різниці покупцем [17]. За свою історію виробники використовували різноманітні маркування, як тактильні, так і

візуальні. На сьогоднішній день найбільш популярним способом є використання голограм [18]. Даний спосіб є хорошим варіантом для захисту товарів середньої та низької цінової категорії. При досягненні балансу між складністю та ціною можна передавати у масове використання без серйозних втрат у собівартості кінцевого продукту. Плюси: недорогий при розумному використанні та середня надійність. Мінуси: маркування можна скопіювати та маркування може спотворитись при перевезенні

Використання серіалізації задля ідентифікації товарів. Технологія передбачає серіалізацію кожної одиниці товару ще при виробництві та присвоєння унікального ідентифікатора, за допомогою якого покупець може визначити автентичність даної одиниці. Впровадження підходу поділяється на 2 етапи: занесення кожної одиниці товару у базу даних та винесення посилання на об’єкт бази даних у спеціальний ідентифікатор. База даних повинна вміщати дуже велику кількість товарів, використовувати індексацію задля швидкого пошуку необхідного товару та мати захист від небажаних спроб отримання даних зловмисниками. Алгоритм генерації унікального ідентифікатора повинен уникати будь-яких можливих кореляцій. Сама ж ідентифікаційна мітка повинна передбачувати її машинне зчитування. У реальних застосунках можуть використовуватись такі типи міток, як QR-Code, Data Matrix або NFC-мітка [19]. Одною із реалізацій даного підходу є спільна розробка Louis Vuitton SE та компанії Microsoft. Розробка називається Aura Ledger та працює на основі технології блокчейн. Продукт використовує NFC-мітки для ідентифікації товарів та блокчейн як базу даних. У блокчейні зберігаються дані про весь життєвий цикл продукту, починаючи матеріалами та виробництвом і закінчуючи кінцевим покупцем. Щоправда зберігання такого об’єму інформації часто виявляється надлишковим [20-21]. Використання блокчейну має багато плюсів для даного підходу. Технологія характеризується високою безпекою, надійністю та прозорістю. Плюси: висока надійність, можливість відслідковування кожної одиниці продукту та викликає довіру в клієнтів. Мінуси підходу: зовнішню мітку можливо скопіювати та необхідні витрати вище середніх.

Найбільш перспективною виявилась реалізація серіалізації товарів з допомогою технології блокчейну в проекті Aura Ledger від Microsoft та LVMH (табл. 1). Потенціал цього підходу пояснюється високою точністю та безпекою реалізації, а також проявлена висока довіра покупців. Окрім зазначених вище плюсів, технологія має простір до покращення та виправлення існуючих недоліків, основними з яких є використання недешевих NFC-міток до кожного продукту та можливість багаторазового використання міток виробниками контракту. Предметом розробки даної роботи є вдосконалення системи серіалізації з допомогою технології блокчейну, використанням більш дешевих QR-кодів та впровадження 2-степеневої ідентифікації товару, що передбачає мітки ззовні та всередині упаковки задля запобігання можливості повторного використання міток. Зовнішня мітка служить ідентифікацією товару, а внутрішня – містить приватні дані кожного продукту та слугує інвалідатором міток.

Таблиця 1. Порівняння підходів
Table 1. Comparison of approaches

Підхід	Плюси	Мінуси
Законодавчий	– Регулюється законом – Не потребує великих матеріальних вкладень для впровадження	– Базується на довірі – Точність невелика – Неможливо встановити автентичність для непровірених магазинів
Розробка інструкцій для знаходження різниці між оригіналом та підробкою	Не потребує великих матеріальних вкладень для впровадження	– Базується на обізнаності покупця – Точність низька – Виробники підробок також користуються інструкціями
Моніторинг та блокування підозрілих ресурсів	– Надійність вище середньої – Можна доручити іншій компанії – Дозволяє ефективно блокувати контрафактні ресурси	– Потребує немалих матеріальних вкладень – Базується на довірі покупця – Працює тільки для інтернет покупок
Застосування штучного інтелекту для виявлення контрафакту	– Надійність висока – Дешевий у застосуванні – Працює в напівавтоматичному режимі – Популярність технології машинного викликає довіру покупця	– Технологія залишається неточною – Розвиток таких систем може зайняти багато часу – Потребує додаткових зусиль із впровадження
Використання спеціальних маркувань для ускладнення підробки	– Недорогий при розумному використанні – Середня надійність	– Маркування можна скопіювати – Маркування може спотворитись при перевезенні
Використання серіалізації задля ідентифікації товарів	– Висока надійність – Можливість відслідковування кожної одиниці продукту – Викликає довіру в клієнтів	– Зовнішню мітку можливо скопіювати – Необхідні витрати вище середніх

Виклад основного матеріалу

Загальні відомості про програму. Інформаційна система перевірки автентичності товарів на основі технології блокчейну складається з двох програм: ProductChain і ProductChainServer. Головною програмою є ProductChain, що запускається за допомогою виконуваного файлу «ProductChain.jar». Програма виконує основну логіку системи та складається з трьох модулів:

- Blockchain: модуль є технологічним коренем усієї системи. Відповідає за всі операції пов’язані із логікою блокчейну.
- GUI: модуль містить користувацький інтерфейс типового робочого простору виробника. Даний модуль розроблений лише в цілях демонстрації роботи системи, при передачі продукту, кожен виробник реалізує цей модуль на свій розсуд.
- Webserver: модуль містить логіку, що відповідає за взаємодію клієнтського інтерфейсу із застосунком. Даний модуль розроблений лише в цілях демонстрації роботи системи, при передачі продукту, кожен виробник реалізує цей модуль на свій розсуд.

Допоміжною програмою для роботи головної програми є сервер, що об’єднує різні процеси основного застосунку. Запускається за допомогою виконуваного файлу «ProductChainServer.jar». Мова інтерфейсу програм: Англійська. Розмір виконуваного файлу «ProductChain.jar»: 33 640 КБайт. Розмір виконуваного файлу «ProductChainServer.jar»: 254 КБайт.

Функціональне призначення. Реалізація системи є дуже обширною та складається з різних модулів. У зв'язку з тим наводимо найбільш важливі функції програми. Модулі Blockchain, GUI та Webserver організовані за допомогою спеціальних компонент – менеджерів, кожен з яких відповідає за свою область функціональності. Таким чином можна зручно розділити робочі об'єкти та їхню поведінку. При бажанні цю поведінку можна змінювати без додаткових редагувань робочих об'єктів.

- TransactionManager: *initiateTransaction*, *processTransaction*, *signTransaction* та *commitTransaction* (методи відповідають за життєвий цикл транзакції та виконують такі операції, як створення транзакції, наповнення даними, застосування ЕЦП та використання транзакції; *validateTransaction* (перевіряє транзакцію на правильність. Передбачає перевірку балансу та цифрового підпису транзакції).
- TransactionOutputManager: *updateUnspentOutputs* та *removeUnspentOutputs* (методи відповідають за додавання та видалення вибраних виходів); *getUnspentOutputsByPublicKey* (дозволяє отримати виходи за отримувачем виходу.
- BlockManager: *createBlock* (відповідає за створення та майнінг блоку за наданим списком транзакцій).
- WalletManager: *createWallet* (метод створює гаманець за парою ключів); *sendFunds*: (використовуючи наданий гаманець, надсилає його кошти на інший гаманець).
- *getBalance*: обраховує баланс гаманця за підрахуванням невикористаних виходів.
- BlockChainManager: *init* (відповідає за процес ініціалізації програми. Виконує усі стартові дії такі, як створення базового блоку, базової транзакції, базового гаманця і т.д.); *requestFromCoinBase* (здійснює запит по кошти до базового гаманця) *addTransaction* (додає транзакцію в пул транзакцій); *flush* (використовує доступні транзакції з пулу для формування блоку та додавання його у блокчейн).
- ProductManager: *createProductType* і *createProductUnit* (методи створюють типи продуктів та одиниці продуктів); *applyProductUnit* (додає одиницю товару до блокчейну шляхом надсилання їй 1 балансу); *consumeProductUnit* (споживає одиницю товару шляхом повертання 1 балансу назад до типу продукту); *isProductUnitConsumed* (перевіряє чи одиниця товару спожита за наступним алгоритмом. Якщо баланс одиниці товару = 0, тоді одиниця спожита).
- Miner: *mineBlock* (здійснює майнінг блоку згідно заданої складності); *checkBlock* (перевіряє чи для блоку був здійснений майнінг коректно).
- ChainValidator: *isChainValid* (перебудовує блокчейн з нуля та здійснює перевірку кожного блоку на предмет неузгодженостей).
- Sha256HashGenerator: *doDataHashing* (хешує стрічку за алгоритмом SHA256).
- MerkleTreeCreator: *createMerkleTree* (будує хеш дерево за списком хешів транзакцій).
- RSAKeyGenerator: *generateKeys* (генерує випадкові ключі за допомого криптографічного алгоритму RSA та алгоритму генерації випадкових чисел SecureRandom); *restoreKeys* (відновлює ключі з отриманих байтових масивів).
- RSASignatureManager: *applySignature* (створює ЕЦП на основі отриманих даних та приватного ключа); *verifySignature* (перевіряє чи ЕЦП був створений власником отриманого публічного ключа).

- RSAEncryptionManager: *encrypt* (шифрує дані використовуючи публічний ключ); *decrypt*: розшифровує дані використовуючи приватний ключ); *Util* (клас містить методи перетворення та порівняння ключів).
- BlockChainToFXTreeConverter: *convert* (перетворює блокчейн у вигляді JSON об'єкту у деревовидний інтерфейс).
- JavaFXBlockChainInteractionController: даний клас містить методи, що є слухачами подій блокчейну. Клас слугує мостом між мережевою частиною та інтерфейсом.
- PeerClient: *sendMethodRequest* (надсилає запит за допомогою сокет-з'єднання); *loadBlockChain* (завантажує найбільший блокчейн з P2P мережі); *sendBlock* (надсилає блок усім вузлам P2P мережі); *registerPeer* (реєструє вузол на P2P сервері); *loadPeerList* (отримує список вузлів в P2P серверу);
- PeerServer – клас що відповідає за сервер P2P вузла. Сервер працює у фоновому режимі та приймає усі запити інших вузлів.
- PeerWorkerThread – клас P2P серверу, відповідає за прийом запиту від інших вузлів.
- Методи що реалізують поведінку конкретного методу серверу P2P вузла реалізують інтерфейс PeerServerMethodHandler та абстрактний клас AbstractPeerServerMethodHandler: *GetBlockChainMethodHandler* (клас надсилає блокчейн на запит); *GetBlockChainSizeMethodHandler* (клас надає розмір актуальної версії блокчейну на запит); *SendBlockMethodHandler* (клас відправляє новий блок після його успішного майнінгу).
- MainController: *showProduct* (метод HTTP серверу віддає HTML сторінку публічної інформації про товар); *consumeProduct* (метод HTTP серверу віддає HTML сторінку приватної інформації про товар та споживає товар у блокчейні).

За конфігурацію усіх процесів та методів відповідає файл application.properties. Даний файл містить параметри різних модулів, що дозволяє швидко змінювати поведінку програми.

Опис логічної структури системи. В цілях демонстрації роботи блокчейну дані програмні застосунки виконуються у ручному режимі. Програма ProductChain сервер організована у вигляді застосунку, що керується у режимі діалогу з користувацьким інтерфейсом. При запуску програми відображається вікно завантаження, що відповідає ініціалізації програми у P2P мережі. Після успішного завантаження блокчейну користувач потрапляє у головне меню програми. Дане меню складається з 4 опцій: Продукти, Транзакції, Блокчейн, Вихід. Перші три кнопки ведуть до запуску відповідних варіантів використання:

- Продукти: відкриває сцену перегляду та створення типів продукту. Дана сцена організована у вигляді таблиці. Під таблицею є можливі опції сцени: повернутись назад, створити тип товару, відкрити одиниці товару. Створити тип товару відкриває модальне вікно, що містить поля для заповнення нового типу товару. Відкрити одиниці товару веде до відкриття схожої табличної сцени, проте для одиниць товару.
- Транзакції: відкриває сцену перегляду транзакції. Сцена організована у вигляді таблиці. Під таблицею наведені опції сцени: повернутись назад, оновити транзакції, створити та здійснити майнінг блоку. Опція створення блоку відкриває модальне вікно, що вимагає підтвердження початку операції. На час

виконання майнінгу вікно відображає екран виконування операції. Після успішного або неуспішного додавання блоку вікно показує статус виконання операції та клавішу закриття вікна.

- Блокчейн: відкриває сцену перегляду блокчейну. Сцена організована у вигляді деревовидного списку, що можна розгортати та згортати. По замовчуванню даний список є згорнутий, а блоки в ньому відсортовані у порядку спадання.

Клавіша «Повернутись назад» в усіх сценах відтворює попередню сцену з історії відкриття сцен. Клавіша «Вихід» відповідає за закриття програми. Серверна частина застосунку на HTTP запити повертає HTML сторінки, що не мають можливості взаємодії. Дані сторінки відкриваються браузером та поділяються на 2 основні блоки: заголовок та інформаційна частина. ProductChainServer є програмою, що працює в режимі діалогу з командним рядком.

Використовувані технічні засоби. Програма розроблена для виконання на пристроях типу персональний комп'ютер. Програма керується в режимі діалогу з оператором. Для керування використовуються пристрої: монітор, клавіатура, маніпулятор типу «Миша». Програма зберігається на жорсткому диску. В робочому стані дані зберігаються в оперативній пам'яті. Для комунікацій використовується мережевий адаптер. Клієнтські запити виконуються як на стаціонарних пристроях (ПК), так і на мобільних пристроях. Вимоги до ПК: операційна система Windows; встановлене програмне забезпечення Java версії 11 і вище; вільне місце на жорсткому диску 64 МБ; вільне місце оперативної пам'яті 4 ГБ; доступ до інтернету з пропускною здатністю 10 Мбіт/с. Вимоги до мобільного пристрою: встановлений інтернет-браузер Chrome/Opera/Firefox/Safari або інший браузер, що підтримує HTTP комунікацію та стандарт ECMAScript6; доступ до інтернету з пропускною здатністю 1 Мбіт/с.

Виклик та завантаження. Обидві програми ProductChain та ProductChainServer поставляють у вигляді запакованого архіву. Після розпаковування програми запускаються за допомогою командного рядку та необхідних параметрів. Програма ProductChain викликається за допомогою наступної команди: *java [параметри командного рядка у вигляді **назва_параметру=значення параметру**] -jar (відносний шлях до виконуваного файлу)/ProductChain.jar*. Програма ProductChainServer викликається за допомогою наступної команди: *java -cp (відносний шлях до виконуваного файлу)/ProductChain.jar com.oprokipchuk.ProductChainServer.Main (параметри командного рядка у вигляді **назва_параметру=значення параметру**)*. Відкриття браузерної сторінки здійснюється в результаті переходу по відповідних посиланнях.

Вхідними даними для розроблених програмних застосунків є вхідні параметри командного рядка. Параметри запуску програми ProductChain наведені у таблиці 2.

Розглянемо призначення кожного з параметрів детальніше:

- WEB_SERVER_PORT. Параметр відповідає за порт, на якому розгортається HTTP сервер застосунку. Вказаний порт повинен бути вільний, тобто не зайнятий іншою програмою. Для запуску декількох процесів програми на одному пристрої потрібно використовувати різні значення цього параметру.
- SERVER_IP. Параметр повинен вказувати дійсну IP адресу P2P серверу.
- SERVER_PORT. Параметр повинен вказувати дійсний порт P2P серверу.
- CLIENT_IP. Параметр відповідає за IP, на якому розгортається P2P вузол. Вказана IP адреса використовується при реєстрації вузла на P2P сервері.
- CLIENT_PORT. Параметр відповідає за порт, на якому розгортається P2P вузол.

Порт повинен бути вільний. Для запуску декількох процесів вказуються різні значення.

ProductChainServer містить один параметр під назвою port (стандартне значення 8001), що відповідає за порт на якому розгортається P2P сервер. Для коректної роботи системи параметри port та SERVER_PORT повинні співпадати. При реальному застосуванні стандартні значення IP параметрів потрібно змінити, адже вони вказують на локальну адресу пристрою (localhost).

Таблиця 2. Параметри командного рядка програми ProductChain
Table 2. Command line parameters of the ProductChain program

Параметр	Тип	Стандартне значення
-DWEB_SERVER_PORT	Число у межах [0, 65535]	8080
-DSERVER_IP	Рядок формату x.x.x.x	127.0.0.1
-DSERVER_PORT	Число у межах [0, 65535]	8001
-DCLIENT_IP	Рядок формату x.x.x.x	127.0.0.1
-DCLIENT_PORT	Число у межах [0, 65535]	8101

Вихідні дані розроблених програм виконані у вигляді візуального відображення у відповідних інтерфейсах. Для програми ProductChain результатами роботи є актуальний стан блокчейну, що можна переглянути в сцені блокчейну користувацького інтерфейсу, а також інформація про товар і стан товару, що надсилаються в якості відповіді на HTTP запит. Для програми ProductChainServer результатом роботи є історія запитів, що відображається у командному рядку.

Для демонстрації роботи комплексної системи перевірки автентичності товарів на основі технології блокчейну наводимо контрольний приклад використання. Даний приклад складається з двох частин: дій, що виконує виробник при створенні та додаванні товару у блокчейн, а також з дій, що виконує покупець для перевірки товару на автентичність. Для початку необхідно запустити P2P сервер (рис. 3-6). Запускаємо сервер в командному рядку наступною командою: *java -cp ProductChainServer.jar com.oprokipchuk.ProductChainServer.Main port=8001*. Напис «Waiting for next connection» сигналізує про готовність серверу до початку роботи. Після цього можна запускати клієнтський застосунок виробника. Для першого процесу це було виконано наступною командою: *java -DSERVER_PORT=8001 -DCLIENT_PORT=8101 -DWEB_SERVER_PORT=8081 -jar ProductChain.jar*. При запуску додатку з'являється екран завантаження, що може тривати досить довго в залежності від швидкості інтернету та потужностей пристрою.

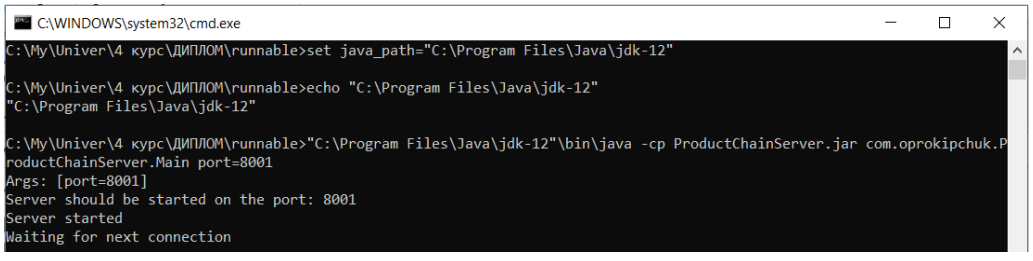

Рис. 3. Запущений P2P сервер
Fig. 3. Launched P2P server

Рис. 4. Головне меню
Fig. 4. Main menu

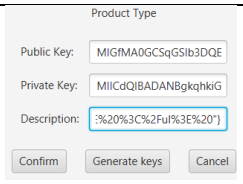

Рис. 5. Вікно створення типів продукту
Fig. 5. Product types creation window

Рис. 6. Сцена типів продуктів
Fig. 6. Scene of product types

Першим кроком у використанні програми є перехід в меню продуктів «Products». Після переходу можна спостерігати пусту таблицю типів продуктів та можливі опції (рис. 6). Для створення нового типу товару необхідно натиснути клавішу «Units». Після натискання відкривається модальне вікно з можливістю введення даних нового товару. Особливістю даного вікна є можливість як ручного запису ключів типу товару, так і автоматичної генерації за допомогою клавіші «Generate Keys» (рис.5).

Висновки

Перевага розроблюваного продукту в тому, що він об’єднує багатьох виробників у єдину мережу для забезпечення більшої надійності та прозорості даних, а також використання двох-ступеневої ідентифікації, що дає більшу точність. Основними споживачами є виробники товарів, що зазнають матеріальних збитків від виробників контрафакту. Такі виробники бажають мінімізувати вплив контрафактної продукції на їхній прибуток, а також зберегти репутацію та довіру їхніх покупців. Конкурентами є інші постачальники програмного забезпечення для захисту від підробок на тому ж рівні захисту. Рівні захисту на окремому виробництві можуть комбінуватись. Згідно уже існуючих прикладів держави позитивно ставляться до методів боротьби з контрафактом та готові співпрацювати. Враховуючи загальний стан боротьби з контрафактом, а також низьку поширеність таких методів в Україні можна зробити висновок про те, що доцільно розробити метод боротьби з контрафактом для українського ринку, що є вдосконаленням схожого програмного продукту (Microsoft Aura Ledger), який уже набув певної популярності закордоном. Споживачами продукту стануть виробники товарів, що при покупці отримають набір необхідного програмного забезпечення, а також доступ до спільної мережі блокчейну. В результаті виконання роботи розроблена інформаційна система перевірки автентичності товарів на основі технології блокчейну. Були розроблені усі необхідні модулі для повної демонстрації роботи системи, зокрема модулі блокчейну, користувацький інтерфейс виробника та web-server. Також реалізовано P2P сервер, що дозволяє взаємодіяти розробленим програмним застосункам.

Подяка

Дана стаття підготована завдяки грантової підтримки Національного Фонду Досліджень України, реєстраційний номер проєкту 2023.04/0012 «Розроблення інформаційної системи автоматичного виявлення джерел дезінформації та неавтентичної поведінки користувачів чатів» за конкурсом ««Наука для зміцнення обороноздатності України».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] *Li X., Wang C.* The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision support systems, 2017, 95: 49-60. https://doi.org/10.1016/j.dss.2016.12.001.

[2] *Чубенко А.Г., Лошицький М.В., Павлов Д.М., Бичкова С.С., Юнін О.С.* Термінологічний словник з питань запобігання та протидії легалізації доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції, К.: Ваіте, 2018. – 826 с.

[3] Allison. Behind the industry of counterfeit products in China and lawsuit success cases, 2021. URL: https://daxueconsulting.com/counterfeit-products-in-china/.

[4] *Butticè, V., Caviggioli, F., Franzoni, C., Scellato, G., Stryszowski, P., & Thumm, N.* Counterfeiting in digital technologies: An empirical analysis of the economic performance and innovative activities of affected companies. Research Policy, 49(5) (2020) 103959. https://doi.org/10.1016/j.respol.2020.103959

[5] *Richter F.* The Industries Most Affected by Counterfeit Products, 2019. URL: https://www.statista.com/chart/17410/counterfeit-and-pirated-products-by-category/

[6] *Prokipchuk, O., Chyrun, L., Bublyk, M., Panasyuk, V., Yakimtsov, V., & Kovalchuk, R.* (2021). Intelligent System for Checking the Authenticity of Goods Based on Blockchain Technology. In MoMLeT+ D, pp. 618-665. https://ceur-ws.org/Vol-2917/paper40.pdf

[7] *Kumar R., Tripathi R.* Traceability of counterfeit medicine supply chain through Blockchain. In: 11th international conference on communication systems & networks (COMSNETS). IEEE, 2019. p. 568-570. DOI: 10.1109/COMSNETS.2019.8711418

[8] *Alipour S.* Ninety Eight Per Cent Of Fake Or Lookalike IPhone Chargers Put Consumers At Risk Of Lethal Electric Shock And Fire, 2017. URL:https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2017/12/ninety-eight-per-cent-of-fake-or-lookalike-iphone-chargers-put-consumers-at-risk-of-lethal-electric-shock-and-fire/ .

[9] *Casassus B.* Health agency reveals scourge of fake drugs in developing world, 2017. URL: https://www.nature.com/news/health-agency-reveals-scourge-of-fake-drugs-in-developing-world-1.23051.

[10] *Hamelin N., Nwankwo S., El Hadouchi R.* Faking brands': consumer responses to counterfeiting. Journal of Consumer Behaviour, 12(3), (2013) 159-170. DOI: 10.1002/cb.1406

[11] Zhang L. Platformizing family production: The contradictions of rural digital labor in China. The Economic and Labour Relations Review, 32(3), (2021). 341-359. DOI: https://doi.org/10.1177/10353046211037093

[12] *Nermain A. I., Thanasi-Boçe M., Ali O.* Boosting Luxury Sustainability Through Blockchain Technology. Blockchain Technologies in the Textile and Fashion Industry, 17 (2022). DOI: 10.1007/978-981-19-6569-2_2

[13] *Doszhan R., Alimbekova G., Kalymbekova Z., Talasbek M.* Risk management in the financing of ICO projects: Prospects for the use of modern technologies in Kazakhstan.

In E3S Web of Conferences 159 (2020) 04017. EDP Sciences. DOI: 10.1051/e3sconf/202015904017

[14] *Asadizanjani N., Tehranipoor M., Forte D*. Counterfeit electronics detection using image processing and machine learning. In Journal of physics: conference serie, 787 (2017) 012023. DOI: 10.1088/1742-6596/787/1/012023

[15] *Lee H., Yeon C.* Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions. Sustainability, 13(19) (2021) 11057. DOI: 10.3390/su131911057

[16] *Pal K.* Internet of things and blockchain technology in apparel manufacturing supply chain data management. Procedia Computer Science, 170 (2020) 450-457. DOI: 10.1016/j.procs.2020.03.088

[17] *Mlalila N., Kadam D. M., Swai H., Hilonga A*. Transformation of food packaging from passive to innovative via nanotechnology: concepts and critiques. Journal of food science and technology, 53 (2016) 3395-3407. 10.1007/s13197-016-2325-6

[18] How holograms can stop counterfeiting, 2014. URL: https://www.packagingdigest.com/smart-packaging/how-holograms-can-stop-counterfeiting.

[19] *Saxena N., Thomas I., Gope P., Burnap P., Kumar N.* Pharmacrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs. Computer, 53(7) (2020) 29-44. DOI: 10.1109/MC.2020.2989238

[20] *Bulchand-Gidumal J., Melián-González S.* Fighting fake reviews with blockchain-enabled consumer-generated reviews. Current Issues in Tourism, (2023) 1-15. DOI: 10.1080/13683500.2023.2173054

[21] *Lytvyn V., Vysotska V., Kuchkovskiy V., Bobyk I., Malanchuk O., Ryshkovets Y., Pelekh I., Brodyak O., Bobrivetc V., Panasyuk V.* Development of the system to integrate and generate content considering the cryptocurrent needs of users, Eastern-European Journal of Enterprise Technologies 1(2-97), pp. 18-39 (2019). Doi http://nbuv.gov.ua/UJRN/Vejpte_2019_1%282%29__3

INFORMATION SUPPORT OF DATA VERIFICATION PROCESSES BASED ON BLOCKCHAIN

M. Nazarkevych[1], O. Prokipchuk[2], V. Vysotska[2], R. Holoshchuk[2], R. Fedchuk[2]

[1]Lviv Ivan Franko National University,
St. Tarnavskogo 107, 79017 Lviv, Ukraine

[2]Lviv Polytechnic National University,
12 Bandery St., UA-79013, Lviv, Ukraine

mariia.nazarkevych@lnu.edu.ua

Every year, the share of counterfeit goods on the market only increases, as does the damage it causes. Moreover, this is not only material damage, but also damage to the environment and people's health. In the worst cases, such recklessness can lead to the death of people. That is why large companies today are starting to invent various solutions to combat counterfeiting, including

the implementation of information support for data authentication processes based on blockchain technology. a system that can reduce the threat of counterfeit goods in modern conditions is relevant. The purpose of creating this system is to provide buyers of goods with the opportunity to check their authenticity. Verification should be possible both before and after purchase with the ability to return the product in case of detection of counterfeit. The system should unite manufacturers into a single network, achieving avoidance of attachment to a specific manufacturer. In this way, each buyer can view any part of the required data. Under the condition of such data transparency, the developed system should provide reliable protection of this information. Also, the system should provide additional functionality different from the main one, which will allow to expand the scope of application and increase the benefits of using the system by users. Finally, the selected verification method should consist of a reusable part that can be used by anyone and a one-time part intended for a specific buyer. The object of the study: checking the authenticity of goods using blockchain technology. The subject of research: means of creating a unified decentralized blockchain system, which provides the possibility of checking the authenticity of goods for all manufacturers participating in this network.

Keywords: network communication, information system, counterfeit good, blockchain technology, product life cycle, intelligent information retrieval system, manufacturer environment.

Стаття надійшла до редакції 22.08.2024.
Прийнята до друку 05.09.2024.