УДК 004.056.53:004.738.1 **DOI:** 10.31673/2412-9070.2024.012025

І. О. ШАХМАТОВ, асистент,
Державний університет інформаційно-комунікаційних технологій, Київ

ТЕХНОЛОГІЯ BLOCKCHAIN ЯК ІНСТРУМЕНТ ПРОТИДІЇ НЕПРАВОМІРНОМУ ВИКОРИСТАННЮ ДОСТУПУ ДО ВЕБСАЙТІВ

Запропоновано новий підхід до кібербезпеки, який об'єднує блокчейн та економічний аналіз. Досліджено сучасні виклики безпеки вебсайтів, зокрема несанкціонований доступ і витік даних, а також розглянуто наявні методи захисту та їх недоліки. Розкрито, як унікальні властивості блокчейну, включно з незмінністю, розподіленим зберіганням даних та криптографічним шифруванням, можуть підвищити безпеку вебсайтів. Для аналізу розподілу доступу до вебресурсів використано коефіцієнт Джині та криву Лоренца, що допомогло виявити потенційні слабкі місця та надати математичне обґрунтування для оцінювання ефективності системи безпеки. Було створено детальний алгоритм, який інтегрує блокчейн і економічні аналітичні методи, і проведено його тестування за допомогою реальних даних. Результати демонструють, що така інтеграція може значно підвищити здатність вебсайтів протистояти кіберзагрозам, пропонуючи рекомендації для практичного впровадження цієї моделі для підвищення безпеки вебресурсів. Це дослідження має вагоме практичне значення, висуваючи новий підхід до захисту вебсайтів, який може бути застосований у широкому спектрі вебзастосунків, разом із корпоративними порталами та електронною комерцією. Також зроблено важливий внесок у наукове співтовариство, об'єднавши кібербезпеку, блокчейн-технологію та економічний аналіз, відкриваючи нові напрямки для подальших досліджень.

Ключові слова: блокчейн; кібербезпека; коефіцієнт Джині; розподілене зберігання даних; несанкціонований доступ; цифрова безпека; доступ до вебресурсів; UML-діаграма; Python.

ВСТУП

З розвитком інтернету та збільшенням кількості вебсайтів та сервісів, що надають важливі дані, значно зростає потреба в ефективних механізмах захисту цих ресурсів. Проблеми безпеки та конфіденційності стають особливо актуальними, адже традиційні методи захисту часто є неефективними проти сучасних кіберзагроз, зокрема несанкціонованого доступу та витоку даних. Це створює ризики не лише для особистої інформації користувачів, а й для ділової таємниці компаній.

Швидкий розвиток технології блокчейн відкриває нові можливості у сфері цифрової безпеки. Блокчейн забезпечує надійний механізм реєстрації та зберігання даних з унеможливленням їх зміни чи видалення без дозволу всіх учасників мережі. Ця характеристика робить блокчейн важливим інструментом у захисті від несанкціонованого доступу та маніпуляцій із даними.

Унікальні властивості блокчейну, як-от розподілене зберігання даних та неможливість їх підроблення, формують нові перспективи для забезпечення цифрової безпеки. Використання цієї технології може значно покращити здатність систем виявляти та протидіяти спробам несанкціонованого доступу, забезпечуючи вищий рівень захисту даних.

До того ж інтеграція блокчейну з економічними методами аналізу, такими як коефіцієнт Джині та крива Лоренца, здатна надати додаткове розуміння розподілу доступу до вебресурсів. Це дасть змогу не тільки виявляти слабкі місця в захисті, а й відстежувати динаміку ризиків та адаптувати захисні стратегії відповідно до змінюваних умов.

Також важливо звернути увагу на роль блокчейну в підвищенні прозорості та підзвітності в керуванні даними. Забезпечуючи незмінність історії доступу до ресурсів, блокчейн може стати інструментом для аудиту та виявлення неналежного використання даних.

Зважаючи на ці переваги, блокчейн може стати ключовим елементом у розробленні нових та більш ефективних підходів до цифрової безпеки. Його застосування може зробити значний внесок у створення міцніших, більш надійних та адаптивних систем захисту вебсайтів, що є критично важливим у сучасному цифровому світі.

ОСНОВНА ЧАСТИНА

Дедалі більша кількість цифрових загроз та зростання обсягів даних в інтернеті сьогодні робить захист вебресурсів критично важливою частиною в їх розробленні та керуванні, з особливим акцентом на конфіденційність користувацької інформації. З розвитком кіберзагроз, які стають все складнішими, традиційні системи безпеки часто виявляються неефективними. Це ставить під загрозу не тільки приватність користувачів, а й фінансову та репутаційну безпеку організацій. У зв'язку з цим розвиток нових технологій, особливо використання блокчейну, відіграє ключову роль у підвищенні безпеки та

прозорості керування даними. Інтеграція блокчейну із сучасними методами кібербезпеки, а також застосування економічних аналізів є важливими для виявлення слабких місць у системах безпеки та потребують комплексного підходу, який об'єднує технологічні інновації та стратегії керування даними.

Аналіз літературних даних. Блокчейн може покращити безпеку вебсайтів, роблячи системи контролю доступу більш ефективними і безпечними [1]. Ця технологія пропонує децентралізацію, стійкість до змін, надійність, а також підвищення довіри, що може розв'язати проблеми з безпекою та конфіденційністю. Застосування смарт-контрактів через блокчейн забезпечує більшу безпеку, гнучкість, цілісність даних та конфіденційність порівняно з традиційними системами.

Блокчейн значно підвищує безпеку в Інтернеті речей (IoT), пропонуючи децентралізований підхід для ефективного керування доступом, що вирішує недоліки традиційних централізованих систем [2]. Модель безпеки ZAIB, застосовуючи принципи нульового довір'я та атрибутивного контролю доступу (ABAC) з використанням блокчейну та IPFS, гарантує цілісність та конфіденційність даних в IoT-середовищах [3]. Алгоритми, зокрема TCPDA, забезпечують доступ лише авторизованим користувачам, підвищуючи безпеку в системах контролю доступу IoT [5]. Водночас блокчейн застосовується для захисту мереж, віртуалізації, криптографії в IoT, із перспективою інтеграції зі штучним інтелектом та безпекою бічних ланцюжків [8], а децентралізована схема контролю доступу на базі блокчейну зі списком контролю доступу (ACL) мінімізує ризики від зловмисних пристроїв [10].

Блокчейн використовується для підвищення безпеки даних та надійності вебзастосунків, особливо на платформах онлайн-курсів, де безпека даних є важливою [4]. Часто ці сайти стикаються із шахрайством і крадіжкою даних. Блокчейн може захистити від атак, зокрема націлених на авторизацію користувачів і передавання даних. У тексті розкриваються основні елементи блокчейну, такі як хеш-функції, і подається спеціальна модель блока транзакцій для вебкурсів. Обговорюються різні кіберзагрози для вебсайтів та можливості поліпшення їх безпеки за допомогою блокчейну.

Традиційні методи захисту даних часто виявляються неефективними. Проте блокчейн пропонує рішення для розв'язання цих проблем, забезпечуючи криптографічний захист і цілісність даних без централізованих посередників [6]. Ця технологія, уже використовувана у фінансовому секторі, включно з цифровими валютами, має потенціал підвищити інформаційну безпеку в різних галузях.

Аналіз у сфері кібербезпеки зосереджується на викликах, пов'язаних із блокчейном. Виокремлено 30 типів викликів [7], згрупованих у шість класів, які впливають на бізнес-процеси та операції. Виявлено нестачу конкретних стратегій для мінімізації цих викликів, особливо в конкретних промислових секторах. Ризики кібербезпеки блокчейну потребують більш фокусованих досліджень для розроблення ефективних стратегій пом'якшення.

Використання блокчейну в різних секторах сприяє зниженню розриву в знаннях серед різних організацій [9], забезпечуючи безпечне зберігання даних і смарт-контракти для транзакцій. Водночас існують такі виклики, як кібербезпека та різні правові стандарти, що вимагають прозорості та відповідальності, особливо в процесі інтеграції з Big Data та машинним навчанням.

Використання технології блокчейну в програмно-визначених мережах (SDN) допомагає покращити обмін інформацією про кіберзагрози та захист від кібератак, особливо від DDoS-атак, забезпечуючи надійне зберігання даних і автоматизований обмін через смарт-контракти, що підвищує загальну кібербезпеку в мережах.

Метою запропонованого дослідження є розроблення та аналіз моделі, яка інтегрує технологію блокчейн із методами аналітики доступу до вебресурсів для забезпечення підвищеної безпеки та прозорості в контексті вебсайтів. Це дослідження прагне виявити, як використання блокчейну може поліпшити механізми контролю доступу до вебсайтів, знижуючи ризик несанкціонованого використання та витоку даних. Також планується дослідити вплив економічних показників, зокрема коефіцієнта Джині та кривої Лоренца, на аналіз розподілу доступу до вебресурсів, щоб підвищити ефективність виявлення та протидії потенційним загрозам безпеки.

Модель та методологія дослідження

Запропонована модель базується на використанні блокчейну для контролю доступу до вебсайтів, інтегрованого з економічними аналітичними інструментами. В основі моделі лежить структура блокчейну, де кожен блок у ланцюжку містить набір даних про транзакції, які в нашому разі є запитами на доступ до вебресурсів.

Кожен блок у блокчейні має у своєму складі унікальний індекс, часову позначку, хеш попереднього блока та список транзакцій, які він містить. Хеш кожного блока генерується за формулою

$$H = hash(index + timestamp + previousHash + transactions), \quad (1)$$

де *hash* є хеш-функцією; *index* — індекс блока; *timestamp* — часова позначка створення блока; *previousHash* — хеш попереднього блока; *transactions* — список транзакцій у блоці. Цей хеш забезпечує цілісність та безпеку кожного блока та усього ланцюжка загалом.

Також модель охоплює аналіз розподілу доступу до ресурсів за допомогою коефіцієнта Джині та кривої Лоренца. Коефіцієнт Джині G використовується для вимірювання нерівності доступу серед користувачів і обчислюється як відношення площі між лінією рівності та кривою Лоренца до загальної площі під лінією рівності за формулою

$$G = A/(A + B), \quad (2)$$

де A — площа між лінією рівності та кривою Лоренца; B — площа під кривою Лоренца.

Крива Лоренца (рис. 1) графічно відображає розподіл доступу до ресурсів, інформуючи, який відсоток загального доступу припадає на певний відсоток користувачів. Цей аналіз дає змогу ідентифікувати нерівності в доступі та адаптувати заходи безпеки відповідно до виявлених тенденцій. Така модель поєднує надійність та прозорість блокчейну з глибоким аналізом розподілу доступу, що дає можливість ефективно встановлювати та реагувати на потенційні загрози безпеці вебресурсів.

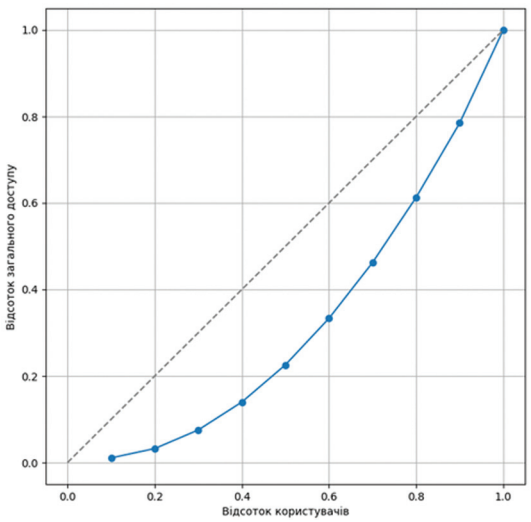

Рис. 1. Крива Лоренца для аналізу доступу до вебресурсів

Для застосування в системі контролю доступу до вебсайтів на основі технології блокчейн запропоновано блок-схему, яка базується на інтеграції кількох головних компонентів (рис. 2). Цей алгоритм починається з моменту, коли користувач відправляє запит на доступ до вебресурсу. Система фіксує цей запит як транзакцію, яка містить усі потрібні деталі, зокрема ідентифікатор користувача, час запиту та цільовий ресурс.

Ця транзакція додається до поточного блока блокчейну. Блоки заповнюються транзакціями до досягнення встановленої межі, що може бути визначена кількістю транзакцій або часовим обмеженням. Після закриття блока він додається до ланцюжка блоків, створюючи незмінну послідовність записів. Для кожного блока розраховується унікальний хеш на основі його вмісту, включно з хешем попереднього блока, що забезпечує безпеку та взаємозв'язок усього ланцюжка блоків.

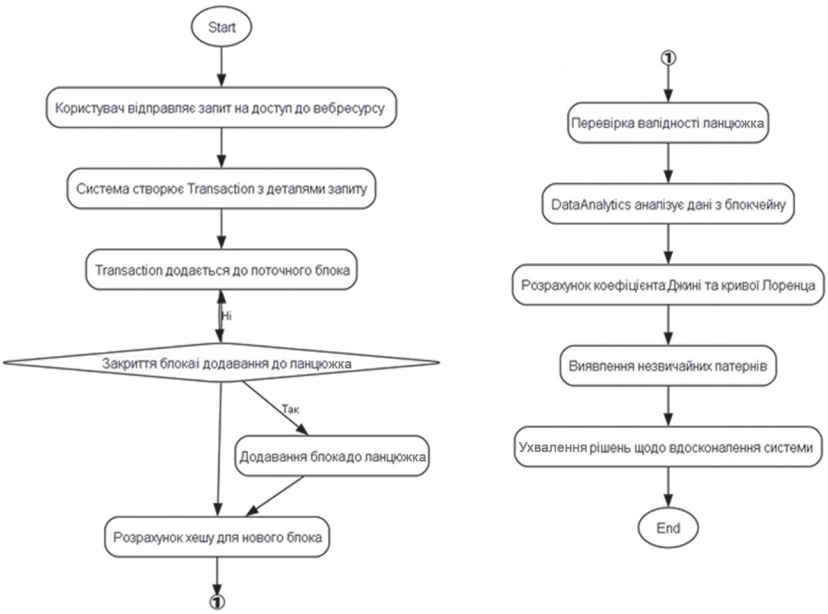

Рис. 2. Алгоритм роботи системи вдосконалення протидії неправомірному доступу

Далі алгоритм (див. рис. 2) включає аналітичний компонент, де клас *DataAnalytics* аналізує дані з ланцюжка блоків. Застосовуючи коефіцієнт Джині та криву Лоренца, алгоритм вивчає розподіл доступу до вебресурсів серед користувачів. Це дає змогу ідентифікувати нерівності або аномалії в поведінці користувачів, які можуть вказувати на потенційні ризики або вразливі місця в системі безпеки.

На основі цього аналізу система може виявляти незвичайні патерни доступу та ухвалювати рішення про вдосконалення механізмів контролю доступу. Це може охоплювати зміну правил доступу, адаптацію до нових видів загроз, а також підвищення загальної ефективності системи захисту вебресурсів.

Отже, використання блокчейну в поєднанні з економічними аналітичними методами дає змогу створити більш надійну й адаптивну систему контролю доступу до вебресурсів, здатну протистояти різноманітним кіберзагрозам.

UML-схема (рис. 3) відображає структуру класів, розроблених для системи на основі блокчейну, що використовується для контролю доступу та аналізу даних вебсайтів.

Кожен клас має чітко визначені атрибути та методи, що забезпечують його функціональність. Взаємодія між класами створює ефективну систему, яка дає змогу зберігати, відслідковувати та аналізувати транзакції доступу до вебсайтів. Схема забезпечує зрозуміле візуальне подання архітектури системи, що є важливим для розуміння її роботи та подальшого розвитку.

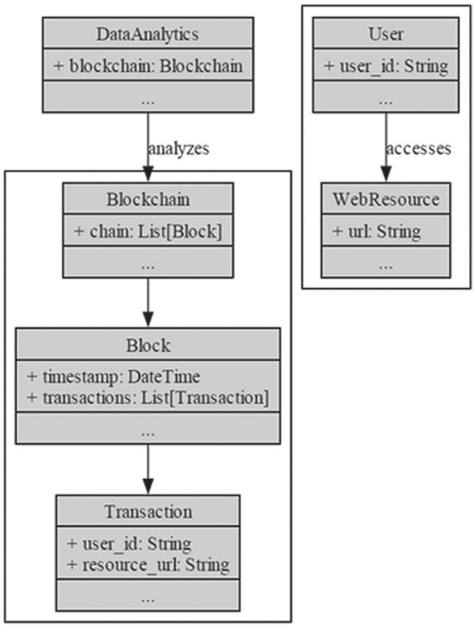

Рис. 3. UML-діаграма класів моделі на основі структури класів

У процесі дослідження було здійснено тестування запропонованого алгоритму на Python (рис. 4), яке інтегрувало блокчейн для контролю доступу до вебресурсів. Тестування показало позитивні результати щодо функціональності та надійності програми. Використання ООП дає можливість розширювати функціонал та застосовувати його в різних вебсистемах. Використані класи відповідають за різні аспекти блокчейну та аналітики даних. Блоки блокчейн містять транзакції, а саме інформацію про запити користувачів на доступ до вебресурсів.

Після додавання блоків програма застосовує аналітичні інструменти для аналізу цих транзакцій.

```
blockchain.add_block(Block([transaction1], blockchain.get_last_block().hash))
blockchain.add_block(Block([transaction2], blockchain.get_last_block().hash))
blockchain.add_block(Block([transaction3], blockchain.get_last_block().hash))

analytics = DataAnalytics(blockchain)
user_requests = analytics.analyze_transactions()

print("User Requests Analysis:", user_requests)
print("Blockchain valid:", blockchain.is_chain_valid())

for block in blockchain.chain:
    print("Block Hash:", block.hash)
```

Рис. 4. Програмний код програми на Python

Під час виконання програми (рис. 5) відстежуються та реєструються кілька запитів на доступ до вебсайтів. Ці дані згодом використовуються для аналізу розподілу доступу та перевірки валідності ланцюжка блоків. Результати виконання програми підтверджують її здатність ефективно реєструвати й аналізувати дані доступу, що є ключовим для забезпечення безпеки вебресурсів.

```
User Requests Analysis: Counter({'user1': 2, 'user2': 1})
Blockchain valid: True
Block Hash: 417e8843a698054d52fd2b5eb7a22fc2cd60f5627dab38c943dec07c4f5f0cc0
Block Hash: fa49cfeaeed02272156f076c79496107ab229fed0ad49ecf9def5d29a5326816
Block Hash: 23af557aa5851e46cd2cd5bfd9ac3e757fad6a4ed5be70b7b51471eb2e5fe8cd
Block Hash: 0d7dec4db32f59759d1a70d3f223429c3f2b8b5643f7f68c5a0acb776a61cd52
```

Рис. 5. Результат тестового виконання програми на Python

ВИСНОВКИ

Аналіз проведеного дослідження та розробленої на Python програми, яка інтегрує технологію блокчейн для контролю доступу до вебресурсів, дав можливість досягти цінних висновків. Виявилось, що блокчейн ефективно забезпечує безпеку та цілісність записів доступу до вебсайтів, завдяки хешуванню та ланцюжковій структурі блоків, які надійно протистоять несанкціонованому втручанню.

Водночас інтеграція аналітичних інструментів, таких як коефіцієнт Джині та крива Лоренца, дала змогу ефективно аналізувати поведінку користувачів та виявляти нерівності в доступі до ресурсів, що сприяє виявленню потенційних уразливих місць та підвищенню рівня безпеки системи. У контексті доступу до вебресурсів, коефіцієнт Джині допомагає визначити, наскільки рівномірно розподілений доступ між користувачами. Наприклад, дуже високий коефіцієнт Джині може означати, що невелика кількість користувачів має велику частку доступу до ресурсів, тоді як більшість має дуже обмежений доступ.

Запропонована методологія є адаптивною та масштабованою, має здатність адаптуватися до різних сценаріїв використання та обробляти дедалі більший обсяг транзакцій, що є ключовим для її реального застосування. Практичність використання блокчейну в системах контролю доступу підкреслюється його потенціалом слугувати основою для подальшого розроблення та вдосконалення систем безпеки.

Новаторське поєднання блокчейну з аналітичними методами в контексті контролю доступу відкриває нові перспективи в галузі кібербезпеки, пропонуючи інноваційні рішення для традиційних викликів безпеки.

У цілому, дослідження та розроблена програма демонструють великий потенціал блокчейну й аналітичних методів у сфері кібербезпеки, відкриваючи нові можливості для підвищення безпеки та ефективності систем контролю доступу і пропонуючи напрямки для подальших досліджень та розвитку.

Список використаної літератури

*1. **Hu V. C.** Blockchain for Access Control Systems // Computer Security Division Information Technology Laboratory. December 2021 [Електронний ресурс]. URL:*
https://doi.org/10.6028/NIST.IR.8403-draft.

*2. **Namane S., Ben Dhaou I.** Blockchain-Based Access Control Techniques for IoT Applications // Security and Privacy in Blockchain/IoT. 15 June 2022 [Електронний ресурс]. URL:*
https://doi.org/10.3390/electronics11142225.

*3. **A Blockchain-Inspired** Attribute-Based Zero-Trust Access Control Model for IoT / S. M. Awan, M. A. Azad, J. Arshad [et al.] // Pervasive Computing in IoT. 16 February 2023 [Електронний ресурс]. URL:*
https://doi.org/10.3390/info14020129.

*4. **Ensuring** Information Security of Web Resources Based on Blockchain Technologies / A. Barakova; O. Ussatova, Y. Begimbayeva, I. Sogukpinar // International Journal of Advanced Computer Science and Applications (IJACSA). 2023 [Електронний ресурс]. URL:*
https://doi.org/10.14569/IJACSA.2023.0140689.

*5. **Shi Jinshan, Li Ru, Hou Wenhan.** A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control // IEEE Access. 24 August 2020 [Електронний ресурс]. URL:*
https://doi.org/10.1109/ACCESS.2020.3018783.

*6. **Chetverikov I. O., Petrenko A. I.** Blockchain technology in the information security system // ДВНЗ «Київський національний університет імені Вадима Гетьмана», 2020 [Електронний ресурс]. URL:*
https://doi.org/10.33111/mise.99.14.

*7. **Mahmood Samreen, Chadhar Mehmood, Firmin Selena.** Cybersecurity Challenges in Blockchain Technology: A Scoping Review // School of Engineering, Information Technology and Physical Sciences. 05 Apr 2022 [Електронний ресурс]. URL:*
https://doi.org/10.1155/2022/7384000.

*8. **A systematic** literature review of blockchain cyber security / P. J. Taylor, T. Dargahi, A. Dehghantanha [et al.] // Digital Communications and Networks. May 2020 [Електронний ресурс]. URL:*
https://doi.org/10.1016/j.dcan.2019.01.005.

*9. **Cybersecurity**, Data Privacy and Blockchain: A Review / V. Wylde, N. Rawindaran, J. Lawrence [et al.] // SN Computer Science. 12 January 2022 [Електронний ресурс]. URL:*
https://doi.org/10.1007/s42979-022-01020-4.

*10. **Rogue** Device Mitigation in the Internet of Things: A Blockchain-Based Access Control Approach / J. Uzair, J. Furqan, J. Umair [et al.] // Mobile Information Systems. October 2020 [Електронний ресурс]. URL:*
https://doi.org/10.1155/2020/8831976.

*11. **Collaborative** Cyber Attack Defense in SDN Networks using Blockchain Technology / M. Hajizadeh, N. Afraz, M. Ruffini, T. Bauschert // 2020 6th IEEE Conference on Network Softwarization (NetSoft), June 2020 [Електронний ресурс]. URL:*
https://doi.org/10.1109/NetSoft48620.2020.9165396.

I. Shakhmatov

BLOCKCHAIN TECHNOLOGY AS A TOOL FOR COUNTERING ILLICIT USE OF WEBSITE ACCESS

This paper introduces an innovative approach to cybersecurity, integrating blockchain technology with economic analysis to address the burgeoning challenges in website security, such as unauthorized access and data breaches. The study delves into the existing security measures, highlighting their limitations and proposing a robust solution through the unique features of blockchain, like immutability, decentralized data storage, and cryptographic encryption. To analyze the distribution of access to web resources, it employs the Gini coefficient and the Lorenz curve, which aids in identifying potential vulnerabilities and provides a quantitative foundation for evaluating the security system's effectiveness.

In a significant advancement, the paper describes the creation of a Unified Modeling Language (UML) diagram and a class structure design to conceptualize the integration of blockchain and economic analysis within the cybersecurity framework. Additionally, it discusses the development of a Python-based algorithm, illustrating its functionality and efficiency in real-world scenarios. The algorithm's performance was meticulously tested using authentic data sets, with the results demonstrating a marked improvement in websites' ability to counteract cyber threats.

By incorporating practical aspects such as UML schematics, class structure development, and Python coding into the research, this paper not only proposes a theoretical model but also showcases its application potential. The research has substantial practical implications, offering a new paradigm for website protection across diverse web applications, including corporate portals and e-commerce. It also makes a pivotal contribution to the academic community, merging cybersecurity, blockchain technology, and economic analysis, and opening new avenues for future research.

Keywords: blockchain; cybersecurity; Gini coefficient; decentralized data storage; unauthorized access; digital security; web resource access; UML diagram; class structure; Python coding.