ПРИКЛАДНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК,
БЕЗПЕКИ ТА МАТЕМАТИКИ, 2025, № 4

УДК 519.816

# РЕАЛІЗАЦІЯ NFT НА BINANCE SMART CHAIN ТА ETHEREUM З ДОДАВАННЯМ ТОКЕНУ ДЛЯ ШВИДКОСТІ ТРАНЗАКЦІЙ ТА КІБЕРБЕЗПЕКА БЛОКЧЕЙНУ

Онищук О.О.(ORCID: 0000-0002-8342-3011),
*Волинський національний університет імені Лесі Українки, Луцьк, Україна*

# IMPLEMENTATION OF NFT ON BINANCE SMART CHAIN (BSC) AND ETHEREUM WITH TOKEN FOR IMPROVED SPEED TRANSACTIONS AND CYBERSECURITY FOR BLOCKCHAIN

Onyshchuk O.O. (ORCID: 0000-0002-8342-3011),
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine*

**Abstract.** The article analyzes the security aspects of two leading blockchain platforms, Binance Smart Chain and Ethereum. Special attention is given to the overview of standard transactions using an NFT smart contract as an example. The implementation of a basic NFT marketplace on Binance Smart Chain and Ethereum is examined, with the addition of a token designed to enhance transaction processing speed. The study identifies the key advantages and disadvantages of each platform in terms of information security and capabilities. The article includes tables comparing the main characteristics, such as transaction speed, transaction costs, scalability, consensus technology, popularity, and cross-chain support for a basic NFT marketplace, both without additional tokens and with a token for improved speed. Additionally, the main cybersecurity techniques that can be adapted depending on the specifics of the blockchain platform, goals, and infrastructure have been analyzed. The application of multiple layers of security is critical for protecting assets and ensuring user trust.

**Keywords:** transactions, NFT marketplace, Binance Smart Chain (BSC), Ethereum, blockchain, blockchain cybersecurity.

**Вступ.** Світ криптовалют і блокчейн-технологій стрімко розвивається, відкриваючи нові можливості для інновацій та фінансової свободи. Серед ключових інструментів цього цифрового ренесансу є смарт-контракти та NFT (невзаємозамінні токени), які стали основою багатьох проєктів у таких екосистемах, як Binance Smart Chain (BSC) та Ethereum [1, 2, 3]. Токеном називають такий цифровий актив, який створений на блокчейні, який може представляти право власності, доступ до продуктів чи послуг або використовуватись як засіб обміну в певній екосистемі. Binance Smart Chain, відома своєю швидкістю та низькими комісіями, пропонує зручне середовище для створення смарт-контрактів і запуску NFT-проєктів. У той же час Ethereum залишається флагманом блокчейн-індустрії, задаючи стандарти для смарт-контрактів і NFT, таких як ERC-721 та ERC-1155 [3]. Детальніше розглянемо, як ці концепції реалізуються в блокчейн-платформах, а також їхній вплив на розвиток смарт-контрактів і NFT.

BSC та Ethereum сьогодні є популярними блокчейн-платформами, кожна з яких має свої унікальні характеристики. BSC є новою платформою, яка швидко розвивається завдяки підтримці від Binance та підтримує мову Solidity, що полегшує перехід dApp-додатків з Ethereum [1-3]. Крім того, BSC має значно нижчі комісії або газові витрати (Gas Fees), які користувачі сплачують за виконання транзакцій або смарт-контрактів у блокчейні. Вони визначаються обсягом обчислювальних ресурсів, потрібних для операції, залежать від завантаженості мережі (близько $0.01) і забезпечують більш швидкі транзакції (3–5 секунд на блок), що робить дану платформу дешевшою та швидшою альтернативою для багатьох користувачів [1], [2], [3]. Ethereum відомий високими комісіями (близько $5–$50), що виникають через механізм консенсусу Proof of Stake (PoS) [1]. Ethereum має високий рівень децентралізації з численними валідаторами

у мережі, що використовують PoS [3]. Binance Smart Chain використовує Proof of Stake Authority (PoSA), яка являється гібридною технологією консенсусу та поєднує механізми делегованого PoS і авторитету валідаторів, що забезпечує високу продуктивність і низькі транзакційні витрати. Це робить BSC менш децентралізованою, порівняно з Ethereum, що дозволяє досягти швидких транзакцій [1], [3]. Ethereum має одну з найбільших і найактивніших спільнот розробників у криптопросторі та величезну екосистему децентралізованих додатків (dApps), які працюють на блокчейні без централізованого управління. Вони забезпечують прозорість, безпеку і дозволяють користувачам взаємодіяти напряму без посередників. Дана платформа призначена для створення складних смарт-контрактів та децентралізованих додатків [1], [3].

Загалом, вибір між Ethereum та BSC залежить від пріоритетів. Якщо віддавати перевагу високій децентралізації та великій екосистемі, то Ethereum є кращим вибором. Якщо ж важлива швидкість транзакцій і низькі комісії, то BSC може стати ідеальним варіантом для реалізації проекту [4]. Крім того, важливими критеріями при виборі є вибір технології консенсусу, тобто механізму, який забезпечує погодження між учасниками мережі щодо актуальності даних у блокчейні, та крос-чейн підтримки, тобто здатності блокчейнів взаємодіяти між собою, дозволяючи обмін активами або даними без посередників [4]. Наприклад, Ethereum використовує PoS, а BSC – PoSA та підтримує інтеграцію з Ethereum, забезпечуючи безшовну передачу активів.

NFT (невзаємозамінний токен) смарт-контракт - це програмований код, реалізований на блокчейні, який використовується для створення, управління та взаємодії з унікальними токенами [5],[6]. Ці токени можуть представляти цифрові чи фізичні активи, такі як мистецтво, музика, відео, предмети колекціонування, ігрові предмети та навіть нерухомість. Основні функції NFT смарт-контракту: створення токенів (Minting), управління власністю, передача (Transfer), метадані (Metadata), події, роялті. Смарт-контракт дозволяє створювати унікальні токени із заданими атрибутами, такими як ім'я, опис та метадані (наприклад, посилання на зображення або інші файли). Кожен NFT пов'язаний із унікальним власником, адреса якого записується в блокчейні. NFT можна передавати між власниками за допомогою функцій, наприклад transferFrom або safe TransferFrom [7], [8]. NFT включає інформацію про токен (наприклад, зображення, опис, властивості), що часто зберігається через URI (наприклад, IPFS). Смарт-контракт генерує події (наприклад Transfer, Mint), які фіксують взаємодії з NFT в блокчейні і має можливість автоматично виплачувати творцю відсотки з кожного наступного продажу токена. Прикладом є контракт ERC-721 (Ethereum) та BEP-721 і BEP-1155 (BSC), які визначають основні функції для NFT та мають унікальний токен. Передача токенів здійснюється між власниками. Лише власник контракту (той, хто його розгорнув) може створювати нові токени (only Owner) [9]. Розробка базового NFT-маркетплейсу передбачає створення функціоналу для купівлі, продажу та управління NFT. Транзакції в такому маркетплейсі обробляються через смарт-контракти, які забезпечують прозорість та безпеку взаємодій. Популярними маркетплейсами є OpenSea, Rarible і Binance NFT Marketplace. [11, 12]. Досить часто розглядають концепцію інтеграції токену швидкості, яка описує використання токенів для стимулювання частого використання платформи або додатка, наприклад, через знижки, винагороди чи ексклюзивний доступ [1], [3], [8], [9], [12].

**Результати досліджень.** Для дослідження особливостей транзакцій у блокчейні застосовано аналіз та порівняння швидкості створеного стандартного проекту на BSC та Ethereum, а також емпіричним методом відстежено безпеку блокчейнів та захист транзакцій.

Для порівняння стандартного підходу до створення базового проекту та з додаванням токену для швидкості обробки транзакцій на даних платформах використано

бібліотеки Open Zeppelin Contracts[13]. Крім того, показано у таблиці 2 кібербезпеку блокчейнів та методи захисту транзакцій на BSC та Ethereum.

Розглянуто реалізацію базового NFT-маркетплейсу на BSC та Ethereum з додаванням токену для швидкості обробки транзакцій. Використано наступні аспекти: створення смарт-контрактів для NFT, розгортання контрактів, інтеграція токену швидкості та використання бібліотеки Open Zeppelin Contracts. Реалізацію NFT-маркетплейсу показано на платформах BSC та Ethereum, оскільки вони мають різні механізми та підходи. В якості інструментів мову програмування для смарт-контрактів взято solidity, тобто бібліотеку для створення стандартів токенів Open Zeppelin, та фреймворки для тестування та розгортання смарт-контракті Truffle / Hard Hat. Сценарій створення токену на BSC наведено у лістингу 1 [10], [13]:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import
"@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol
";
import "@openzeppelin/contracts/access/Ownable.sol";

contract MyBSCNFT is ERC721URIStorage, Ownable {
    uint256 public tokenCounter;

    constructor() ERC721("MyBSCNFT", "BSCNFT") {
        tokenCounter = 0;
    }

    function createToken(string memory tokenURI) public onlyOwner
returns (uint256) {
        uint256 newTokenId = tokenCounter;
        _safeMint(msg.sender, newTokenId);
        _setTokenURI(newTokenId, tokenURI);
        tokenCounter += 1;
        return newTokenId;
    }
}
```

Лістинг 1

Для створення NFT смарт-контракту з інтеграцією токена швидкості на BSC додано логіку використання токена швидкості (SpeedToken) для прискорення або винагороди за створення NFT [10], [13]. Сценарій створення токену на BSC для швидкості обробки представлено у лістингу 2.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract SpeedToken is ERC20 {
    constructor() ERC20("SpeedToken", "SPT") {
        _mint(msg.sender, 1000000 * (10 ** decimals()));
    }

    // Використання токену для спеціальних функцій
    function useSpeedToken(address to, uint256 amount) external {
        _transfer(msg.sender, to, amount);
    }
}
```

Лістинг 2

Користувачі, які хочуть збільшити швидкість обробки своїх транзакцій на маркетплейсі, можуть використовувати Speed Token, враховуючи додаткову комісію за прискорену обробку.

Для створення базового NFT смарт-контракту на Ethereum використано аналогічний підхід, однак враховано більш високі комісії в порівнянні з BSC [10], [13]. Сценарій створення токену на Ethereum наведено у лістингу 3.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import
"@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol
";
import "@openzeppelin/contracts/access/Ownable.sol";

contract MyNFT is ERC721URIStorage, Ownable {
    uint256 public tokenCounter;

    constructor() ERC721("MyNFT", "MNFT") {
        tokenCounter = 0;
    }

    function createToken(string memory tokenURI) public onlyOwner
returns (uint256) {
        uint256 newTokenId = tokenCounter;
        _safeMint(msg.sender, newTokenId);
        _setTokenURI(newTokenId, tokenURI);
        tokenCounter += 1;
        return newTokenId;
    }
}
```

Лістинг 3

При додаванні токену швидкості обробки для Ethereum механізм прискорення схожий, що використовується в BSC, але враховуючи вищі комісії на Ethereum, токен буде мати більшу вартість для користувачів [10], [13].

Використання токенів для прискорення може бути корисним у тих системах, де надаються додаткові переваги, наприклад, знижки на комісії. Даний механізм прискорення "SpeedToken" може використовуватися як інструмент винагороди або додаткового заохочення для швидшого виконання певних транзакцій у вашій системі [10], [13]. Сценарій створення токену на Ethereum для швидкості обробки представлено у лістингу 4.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract SpeedToken is ERC20 {
    constructor() ERC20("SpeedToken", "SPT") {
        _mint(msg.sender, 1000000 * (10 ** decimals()));
    }
    // Функція для використання токенів для прискорення транзакцій
    function useSpeedToken(address to, uint256 amount) external {
        _transfer(msg.sender, to, amount);
    }
}
```

Лістинг 4

Порівняння базового NFT-маркетплейсу на BSC та Ethereum, а також базового NFT-маркетплейсу з додаванням токену для підвищення швидкості обробки транзакцій подані у таблиці 1, а також загальні критерії блокчейн платформ представлено на рис.1.

*Таблиця 1*

Базовий NFT-маркетплейс

| Характеристика | BSC без додаткових токенів | BSC з токеном для підвищення швидкості | Ethereum без додаткових токенів | Ethereum з токеном для підвищення швидкості |
|---|---|---|---|---|
| Швидкість транзакцій | Висока (3-5 сек.) | Дуже висока 1-2 сек (завдяки оптимізації) | Повільніша (15-30 сек.) | Помірна 10-20 сек (але може бути покращена за допомогою додаткових токенів) |
| Вартість транзакцій | Низька (~$0.1-$0.5) | Низька (~$0.1-$0.3, залежить від токену) | Висока (~$5-$30 залежно від навантаження) | Помірна (~$1-$10 з додатковим токеном для прискорення) |
| Масштабованість | Висока (може обробляти більше транзакцій) | Висока (покращена за допомогою токену) | Обмежена (залежить від навантаження) | Обмежена, але токен може знижувати навантаження |
| Технологія консенсусу | Proof of Staked Authority (PoSA) | Proof of Staked Authority (PoSA) | Proof of Stake (PoS) | Proof of Stake (PoS) |
| Популярність | Поміркована, але зростаюча | Поміркована, з можливістю зростання через інновації | Висока (найпопулярніша блокчейн мережа для NFT) | Висока, але може мати більшу конкуренцію з іншими рішеннями |
| Кросс-чейн підтримка | Підтримка міжмережевих операцій | Підтримка міжмережевих операцій | Обмежена підтримка міжмережевих операцій (але існують рішення на другому рівні) | Обмежена підтримка міжмережевих операцій, але з рішеннями на другому рівні |

BSC підходить для швидких, бюджетних рішень із високою ефективністю для стартапів чи невеликих проєктів. Ethereum обирають для більш масштабних або критично важливих проєктів, де децентралізація та безпека є пріоритетами, попри високу вартість. Звісно, що вибір платформи залежить від бюджету, потреб у швидкості, та рівня необхідної децентралізації (рис. 1).

Блокчейн, як децентралізована технологія, має ряд переваг, зокрема прозорість і стійкість до маніпуляцій. Однак вона також стикається з низкою загроз, зокрема атаками на смарт-контракти, компрометацією ключів та експлуатацією вразливості протоколів. Кібербезпека блокчейнів є критичним аспектом, який впливає на захист транзакцій, даних користувачів, смарт-контрактів і загальної мережі. Розглянуто ключові аспекти безпеки на поданому прикладі реалізації NFT-маркетплейсу на BSC і Ethereum (табл. 2).

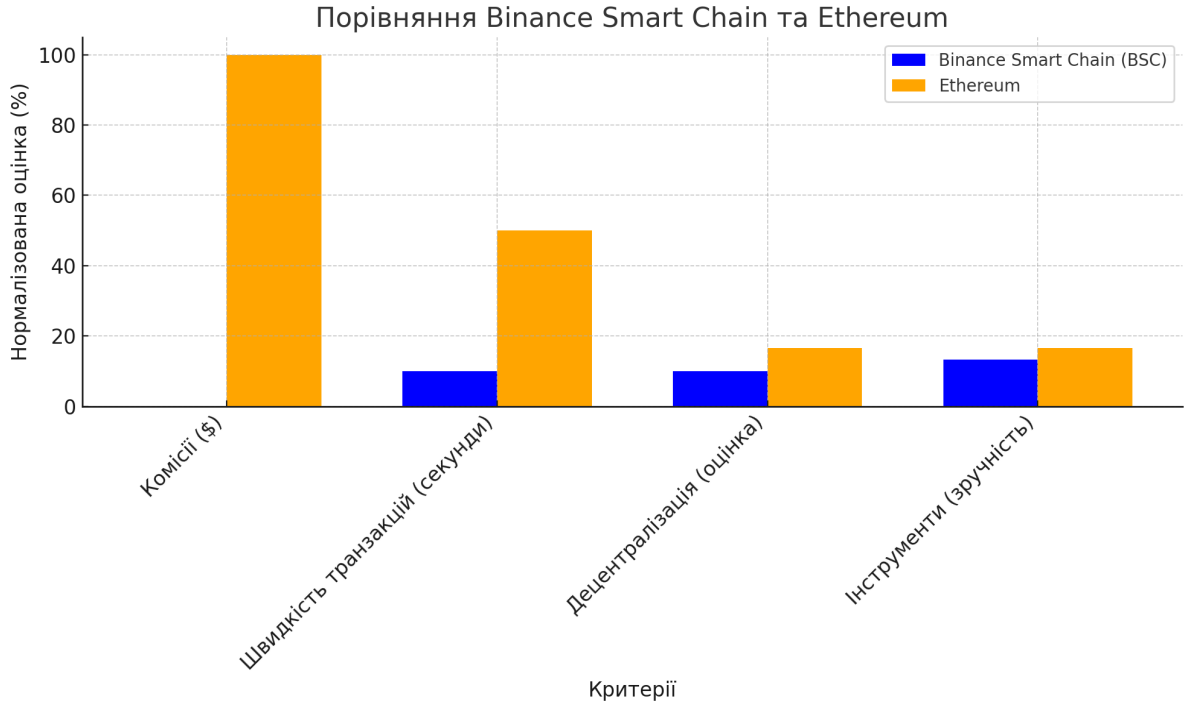


Рис.1 Порівняння Binance Smart Chain (BSC) та Ethereum за основними критеріями

По-перше, можливі атаки на рівні мережі у BSC, яка використовує механізм консенсусу PoSA і кількість валідаторів обмежена. Ця централізація збільшує вразливість до атак на валідаторів або компрометації їх ключів, порівняно невисока кількість вузлів робить мережу потенційно більш вразливою до DoS-атак, при цьому інтеграція з Binance дозволяє швидко реагувати на аномальну активність. В той час Ethereum при можливих атаках на рівні мережі використовує PoS, що менш енергозатратно. Проте також може бути вразливим до атак на валідаторів із великою часткою токенів (ризик 51%-атаки). Уникати цього дозволяє більша кількість вузлів, яка підвищить безпеку, але зробить систему чутливою до атаки Sybil. Крім того, захист можливо реалізувати через високу децентралізацію, що забезпечує стійкість до атак на рівні мережі [14], [15].

По-друге, щодо безпеки смарт-контрактів, то BSC має ризики через низькі комісії BSC, що часто приваблює менш досвідчених розробників, і це призводить до помилок у коді смарт-контрактів. Існує велика кількість зловмисних проектів або "rug pull" атак, які можливо захистити через використання перевірених бібліотек, таких як OpenZeppelin, для написання контрактів. При цьому важливим є аудит коду, що є обов'язковим для захисту. Щодо безпеки смарт-контрактів, то Ethereum має більш тривалий досвід розробників та знижує ймовірність помилок, але популярність платформи робить її мішенню для атак. Відомі атаки на Ethereum, вказують на вразливість у складних смарт-контрактах, при цьому захист можливий через розвинені інструменти для автоматичного аналізу вразливостей та часті аудити від провідних компаній [14], [15].

По третє, через популярність платформ DeFi у BSC існує велика кількість фішингових атак на користувачів. Крім того відслідковується менший рівень освіти користувачів щодо безпеки через низький бар'єр входу. Запобігти цього допомагає захист через навчальні матеріали від Binance для підвищення обізнаності та вбудовані функції захисту в інструменти Binance Wallet. Ethereum має велику кількість гаманців і додатків, що підвищує ймовірність атаки на користувачів. Такі підроблені додатки

можуть викрадати закриті ключі і захиститися можна через розвинені інструменти, такі як MetaMask, що мають вбудовані механізми виявлення фішингу [14], [15]..

Щодо ризику масштабованості та перевантаження на BSC, то це обмежена кількість валідаторів, який створює ризик перевантаження мережі під час пікового використання. Тут може допомогти захист з високою пропускною здатністю завдяки PoSA, що знижує ризик затримок. Ethereum також періодично стає перевантаженою мережею, що робить транзакції дорогими та повільними [14], [15].

Існують специфічні методи кіберзахисту для BSC і Ethereum, враховуючи їхні особливості та механізми консенсусу (таблиця 2). Варто звертати увагу на захист смарт-контрактів на Ethereum, проводити їх регулярний аудит з допомогою інструментів, які дозволяють виявляти вразливості на ранніх етапах. Щоб знизити ризик впровадження вразливостей важливо використовувати перевірені бібліотеки, наприклад OpenZeppelin Contracts, для реалізації стандартів ERC-20, ERC-721 та реалізації базового NFT маркетплейсу. Поряд із загальним аудитом смарт-контрактів на BSC, користувачам слід використовувати інструменти для перевірки контрактів перед їх розгортанням. Оскільки BSC є EVM-сумісною платформою, аудити, виконані для Ethereum, можуть бути корисними для контрактів на BSC [14], [15].

Наступним етапом кіберзахисту є захист приватних ключів та керування доступом для Ethereum і BSC. Зокрема, рекомендовано використовувати гаманців з мультипідписом для зменшення ризиків від компрометації приватних ключів та механізми багатофакторної аутентифікації (MFA) для доступу до важливих облікових записів чи функцій. Мультипідписні гаманці потребують кількох підписів для виконання транзакцій, що робить їх більш безпечними. ля великих сум активів на обох платформах важливо використовувати холодне зберігання. Токени і криптовалюти можуть бути збережені в офлайн-гаманцях для зниження ризику злому [15], [16]. Ethereum 2.0 використовує консенсус PoS, що значно знижує ризик атак , оскільки для їх проведення зловмиснику потрібно володіти значною часткою всіх ETH, що вимагає величезних ресурсів. BSC використовує модель PoSA, яка поєднує в собі елементи PoS і PoA, і тому це робить мережу менш вразливою до атак 51% [15], [16]. .

Обидві мережі мають механізми для обмеження та моніторингу витрат газу: Ethereum з його газовими лімітами, BSC з використанням швидких транзакцій. Однак захист від DoS-атак все ще вимагає моніторингу мережі та обмежень на надмірні витрати газу. Це допомагає запобігти атакам на мережу, що можуть призвести до зниження її продуктивності. Виявлення аномальних або потенційно шкідливих транзакцій у реальному часі є важливою стратегією для запобігання DoS-атак. Це можна здійснити через моніторинг транзакцій за допомогою аналітичних інструментів [15], [16].

Користувачі повинні бути обізнані про методи соціальної інженерії, фішинг-атаки, скам-проєкти, щоб не дати змогу зловмисникам отримати доступ до приватних ключів. Використання антивірусних програм та спеціальних додатків для безпеки гаманців, які запобігають фішингу та інших шкідливих спроб доступу [16], [17].

Блокчейн-платформи, такі як Ethereum та BSC, можуть організовувати програми винагород для дослідників безпеки (баунті-програми), щоб стимулювати знаходження вразливостей у смарт-контрактах. Страхування на основі блокчейну від таких платформ, як Nexus Mutual, може допомогти знизити фінансові ризики, що виникають через вразливості у смарт-контрактах [16], [17].

Наостанок, якщо використовуються крос-чейн протоколи (наприклад, Wrapped Tokens або Cross-chain Bridges), важливо забезпечити їх безпеку, щоб уникнути атак, таких як replay attacks або помилки в передаванні активів між мережами. Крос-чейн мости часто є вразливими до атак, тому важливо здійснювати аудит кожного моста, особливо якщо він передає великі суми. BSC має механізм PoSA, який забезпечує

швидкий консенсус і більшу безпеку за рахунок зменшення кількості валідаторів. Однак важливо зберігати збалансованість у кількості та різноманітті валідаторі [15], [16], [17].

*Таблиця 2*

Методи кіберзахисту для Ethereum та BSC

| Метод | Ethereum | BSC |
|---|---|---|
| Захист смарт-контрактів | Регулярний аудит смарт-контрактів, використання бібліотек Open Zeppelin, формальна верифікація. | Аудит смарт-контрактів, використання специфічних для BSC інструментів аудиту, бібліотеки Open Zeppelin. |
| Управління приватними ключами та доступом | Використання мульти підписних гаманців, холодне зберігання, багатофакторна аутентифікація. | Мультипідписні гаманці, холодне зберігання, списки доступу. |
| Захист від атак 51% | PoS знижує ризик атак 51%, велика мережа валідаторів. | Механізм консенсусу PoSA знижує ризики атак 51%, диверсифікація валідаторів. |
| Захист від атак DoS та експлуатації мережі | Моніторинг газових витрат, виявлення аномалій у реальному часі, моніторинг мережі. | Моніторинг газу, ліміти транзакцій, виявлення аномальної поведінки. |
| Захист від соціальної інженерії | Освітні програми для користувачів щодо фішингу, скамів та захисту ключів. | Освітні програми для користувачів BSC щодо фішингу та скамів. |
| Використання страхування смарт-контрактів | Страхування смарт-контрактів через децентралізовані платформи (наприклад, Nexus Mutual). | страхування, винагороди за виявленні вразливості. |

**Висновок.** Транзакції базового NFT-маркетплейсу демонструють унікальне поєднання безпеки, прозорості та децентралізації. Вони забезпечують високу довіру завдяки криптографічним методам і консенсусу Proof-of-Work. Однак певні обмеження, як-от низька масштабованість і висока енергозатратність, вимагають вирішення для підвищення ефективності системи. BSC пропонує більш швидку та дешеву обробку транзакцій у порівнянні з Ethereum завдяки більш ефективному консенсусу. Ethereum має більшу популярність та надає більше рішень для забезпечення безпеки і стабільності, але вартість транзакцій значно вища. Додавання спеціального токену для оптимізації швидкості транзакцій може зробити Ethereum більш конкурентоспроможним у порівнянні з BSC, при цьому знижуючи витрати на транзакції та підвищуючи ефективність. Вибір користувача залежить від пріоритетів, оскільки BSC підходить для швидких і економних рішень, тоді як Ethereum є оптимальним для децентралізованих проєктів із високими вимогами до безпеки.

Платформи Ethereum та Binance Smart Chain мають свої особливості у механізмах консенсусу, а також специфічні виклики для кібербезпеки. Найефективніша стратегія захисту передбачає використання багаторівневих підходів, включаючи захист смарт-контрактів, керування ключами, захист від атак на мережу та інтеграцію заходів безпеки між блокчейнами.

**Бібліографія**

1. Binance Smart Chain vs Ethereum. Режим доступу до ресурсу: URL: https://changenow.io/blog/binance-smart-chain-vs-ethereum
2. Comparing Binance Smart Chain and Ethereum. Режим доступу до ресурсу: URL: https://protos.com/comparing-binance-smart-chain-and-ethereum/
3. Binance Smart Chain vs Ethereum: Differences Explained. Режим доступу до ресурсу: URL: https://cointelegraph.com/learn/articles/binance-smart-chain-vs-ethereum-differences-explained
4. What is Consensus Algorithm In Blockchain & Different Types Of Consensus Models [Електронний ресурс] BangBit Technologies. 2018. Режим доступу до ресурсу: https://medium.com/@BangBitTech/what-is-consensusalgorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77.
5. Григорчук К. Огляд алгоритмів блокчейн консенсуса [Електронний ресурс] Digital Forest. 2018. Режим доступу до ресурсу: https://digiforest.io/blog/blockchain-consensus-algorithms.
6. What Are Public Keys and Private Keys? [Електронний ресурс] Ledger Academy. 2019. Режим доступу до ресурсу: https://www.ledger.com/academy/blockchain/what-are-public-keys-and-privatekeys
7. Haber S. How to Time-Stamp a Digital Document ] Morristown, Bellcore, 1991. 19 с.
8. Williams S. 20 Real-World Uses for Blockchain Technology [Електронний ресурс] The Motley Fool. 2018. Режим доступу до ресурсу: https://www.fool.com/investing/2018/04/11/20-real-world-uses-forblockchain-technology.aspx
9. Clavin J. Blockchains for Government: Use Cases and Challenges [Електронний ресурс] DGOV. 2020. Режим доступу до ресурсу: https://dl.acm.org/doi/fullHtml/10.1145/3427097
10. Solidity Documentation [Електронний ресурс] Режим доступу до ресурсу: https://docs.soliditylang.org/en/v0.5.3/index.html.
11. Thomas L. Blockchain Applications in Healthcare [Електронний ресурс]. Режим доступу до ресурсу: https://www.newsmedical.net/health/Blockchain-Applications-in-Healthcare.aspx.
12. How Walmart used blockchain to increase supply chain transparency [Електронний ресурс] The Leadership Network. 2020. Режим доступу до ресурсу: https://theleadershipnetwork.com/article/how-walmart-used-blockchainto-increase-supply-chain-transparency
13. URL: https://github.com/OpenZeppelin/openzeppelin-contracts
14. Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia.Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB)..*Future Generation Computer Systems*, 102:259–277, 2020.
15. Fynn, E.; Bessani, A.; Pedone, F. Smart contracts on the move. *In Proceedings of the 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Valencia, Spain, 29 June-2 July 2020. pp. 233–244. [Google Scholar]
16. Hafid, A.; Hafid, A.S.; Samih, M. Scaling blockchains: A comprehensive survey. *IEEE Access* 2020, *8*. [Google Scholar] [CrossRef]
17. Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. Dissecting ponzi schemes on ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 10, 2020.

**References**

1. Binance Smart Chain vs Ethereum. URL: https://changenow.io/blog/binance-smart-chain-vs-ethereum
2. Comparing Binance Smart Chain and Ethereum. URL: https://protos.com/comparing-binance-smart-chain-and-ethereum/
3. Binance Smart Chain vs Ethereum: Differences Explained. URL: https://cointelegraph.com/learn/articles/binance-smart-chain-vs-ethereum-differences-explained
4. What is Consensus Algorithm In Blockchain & Different Types Of Consensus Models. BangBit Technologies. 2018. URL: https://medium.com/@BangBitTech/what-is-consensusalgorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77.
5. Hryhorchuk K. Overview of blockchain consensus algorithms [Electronic resource] Digital Forest. 2018. Available: https://digiforest.io/blog/blockchain-consensus-algorithms.

6. What Are Public Keys and Private Keys? [Electronic resource] Ledger Academy. 2019. Available: https://www.ledger.com/academy/blockchain/what-are-public-keys-and-privatekeys
7. Haber S. How to Time-Stamp a Digital Document. Morristown, Bellcore, 1991. 19 p.
8. Williams S. 20 Real-World Uses for Blockchain Technology [Electronic resource] The Motley Fool. 2018. Available: https://www.fool.com/investing/2018/04/11/20-real-world-uses-forblockchain-technology.aspx
9. Clavin J. Blockchains for Government: Use Cases and Challenges [Electronic resource] DGOV. 2020. Available: : https://dl.acm.org/doi/fullHtml/10.1145/3427097
10. Solidity Documentation [Electronic resource] Available: : https://docs.soliditylang.org/en/v0.5.3/index.html.
11. Thomas L. Blockchain Applications in Healthcare [Electronic resource]. Available: https://www.newsmedical.net/health/Blockchain-Applications-in-Healthcare.aspx.
12. How Walmart used blockchain to increase supply chain transparency [Electronic resource] The Leadership Network. 2020. Available: https://theleadershipnetwork.com/article/how-walmart-used-blockchainto-increase-supply-chain-transparency
13. URL: https://github.com/OpenZeppelin/openzeppelin-contracts
14. Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia.Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB)..*Future Generation Computer Systems*, 102:259–277, 2020.
15. Fynn, E.; Bessani, A.; Pedone, F. Smart contracts on the move. *In Proceedings of the 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Valencia, Spain, 29 June-2 July 2020. pp. 233–244. [Google Scholar]
16. Hafid, A.; Hafid, A.S.; Samih, M. Scaling blockchains: A comprehensive survey. *IEEE Access* 2020, *8*. [Google Scholar] [CrossRef]
17. Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. Dissecting ponzi schemes on ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 10, 2020.