УДК 004.72.056.523 **DOI:** 10.31673/2412-9070.2025.019556
А. О. ТВЕРДОХЛІБ, аспірант;
ORCID: 0000-0002-6591-2866
С. С. КОРОТКОВ, PhD, доцент,
ORCID: 0000-0002-4090-5934
Державного університету інформаційно-комунікаційних технологій, Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

У сучасному світі, де цифрова безпека є критично важливою, технологія блокчейн відкриває нові горизонти для захисту даних. Унікальна здатність цієї технології до створення непорушних ланцюгів інформації робить її ідеальною для розробки систем авторизації та автентифікації, які вимагають надійності та прозорості. Дана стаття розглядає питання, яке стосується можливостей блокчейну трансформувати традиційні підходи до управління доступом. Зокрема, аналізується й те, як блокчейн-технології можуть забезпечити більш безпечну та ефективну систему верифікації та прав доступу у контексті застосування авторизації та автентифікації. Можна також спрогнозувати, що блокчейн-рішення у сфері авторизації та автентифікації набудуть ширшого розповсюдження, оскільки вони не тільки підвищують безпеку та прозорість процесів, але й сприяють поліпшенню аудиту, інтерактивності з користувачами та надають їм більше контролю над власними даними.

Ключові слова: блокчейн, авторизація, автентифікація, смарт-контракти.

Вступ

Наразі цифровізація стрімко проникає у кожен аспект життя людини, онлайн-сервіси стають невід'ємною частиною повсякденності. Від онлайн-банкінгу, що дозволяє нам управляти фінансами з комфорту дому, до електронних урядових послуг, які спрощують бюрократичні процедури — цифровізація відкриває нові горизонти зручності.

З іншого боку ця зручність несе в собі виклики. Автентифікація користувача стає критичною задачею, адже від її надійності залежить безпека особистих та фінансових даних. Традиційні методи, такі як паролі та PIN-коди, вже не викликають довіри, особливо на тлі численних випадків витоку даних. Це ставить під загрозу не лише особисту інформацію, а й фінансову стабільність користувачів.

Блокчейн пропонує альтернативний підхід до автентифікації та безпеки даних. Завдяки децентралізованій природі та смарт-контрактам, блокчейн може забезпечити надійну верифікацію користувачів та транзакцій. Це відкриває двері до створення уніфікованої системи цифрової ідентифікації, яка може служити надійним засобом захисту від шахрайства та зловживань [1].

Проте, навіть з блокчейном, точність даних залишається важливою. Неправильно введені дані можуть призвести до помилок, які ускладнюють отримання послуг. Тому, розробка міцної інфраструктури, яка може ефективно обробляти та коригувати такі помилки, є ключовою для створення дійсно надійної цифрової системи.

Децентралізація та блокчейн мають потенціал радикально змінити спосіб, яким ми взаємодіємо з цифровими послугами, пропонуючи більш безпечні та прозорі механізми для захисту наших цифрових прав. Це стане не лише новим стандартом у сфері цифрової безпеки, а й кроком до створення більш відкритого та довірливого цифрового суспільства [2].

Мета статті – дослідження потенціалу блокчейн-технологій для реформування систем управління доступом та виявлення переваг та викликів, пов'язаних з інтеграцією блокчейну в існуючі системи, а також визначити можливі напрямки подальших досліджень у цій області.

Крім того, стаття має на меті також оцінити можливості блокчейну у сприянні створенню більш надійних та ефективних механізмів верифікації та управління правами доступу, з особливим акцентом на авторизацію та автентифікацію у цифровому просторі.

Основна частина

Авторизація та автентифікація є фундаментальними щаблями цифрової безпеки. Вони забезпечують захист ідентичності та контролюють доступ до ресурсів. Автентифікація — це процес перевірки особи, який підтверджує, що користувач або пристрій є тим, за кого себе видає. Авторизація ж визначає, які дії дозволені після успішної автентифікації.

У контексті розробки програмного забезпечення, рівні авторизації відіграють ключову роль у захисті конфіденційної інформації. Вони встановлюють, який доступ має користувач у системі, виходячи з його ролі або атрибутів. Ці рівні можуть варіюватися від базового доступу для читання до повного адміністративного контролю. Розробники мають визначити чітку політику авторизації, щоб забезпечити, що лише уповноважені особи мають доступ до певних дій або даних. Важливо також ефективно керувати ролями та дозволами, а також обробляти помилки контролю доступу, щоб уникнути несанкціонованого доступу [3].

Рівні авторизації можуть бути реалізовані через різні методи, зокрема через авторизацію на основі ролей, де користувачам призначаються ролі з певними дозволами або через авторизацію на основі атрибутів, яка враховує характеристики користувача для надання дозволів. Авторизація на основі ролей або рольова авторизація включає визначення ролей, зв'язування дозволів з кожною роллю та забезпечення виконання відповідних перевірок для перевірки доступу користувачів. Це досягається за допомогою платформ або бібліотек, які підтримують керування доступом на основі ролей. Вибір методу авторизації залежить від потреб програми та її користувачів. Завдяки авторизації на основі ролей адміністратори мають можливість визначати ролі та керувати ними, надаючи відповідні дозволи кожної ролі. Наприклад, роль адміністратора може мати повний доступ і адміністративні привілеї, а роль користувача може мати обмежений доступ і дозволи. Рольова авторизація забезпечує простоту управління, тоді як авторизація на основі атрибутів пропонує більшу гнучкість [4].

При авторизації на основі атрибутів дозволи призначаються на основі атрибутів користувача, таких як розташування користувача, відділ, посада або будь-яка інша відповідна інформація. Наприклад, користувач з атрибутом «менеджер» може мати додаткові дозволи порівняно з користувачем без цього атрибута.

Перевагами авторизації на основі атрибутів можна зазначити наступні характеристики:

- Гнучкість - дозволяє точно визначити, які дії може виконувати користувач в залежності від його атрибутів;
- Деталізація – завдяки високому рівню деталізації через авторизацію на основі атрибутів отримуються кращі результати у сценаріях зі змінними вимогами безпеки.

Важливо, що авторизація на основі атрибутів використовується разом з надійними механізмами автентифікації, щоб запобігти несанкціонованому доступу та захистити конфіденційні дані. Крім того, ефективне управління ролями та дозволами користувачів є ключовим для успішної реалізації рівнів авторизації. Розробники мають визначити чітку політику авторизації та ретельно керувати доступом, щоб забезпечити безпеку даних [5].

Варто зазначити, що обробка помилок контролю доступу є важливою для ідентифікації та виправлення ситуацій, коли користувачі намагаються виконати дії, на які вони не мають дозволу, забезпечуючи цілісність системи. Цей підхід до авторизації дозволяє створювати масштабовані та адаптивні системи, які можуть відповідати змінним вимогам безпеки та управління доступом у складних програмних середовищах.

Автентифікація – це ключовий елемент цифрової безпеки, який дозволяє переконатися в ідентичності користувача або пристрою. Цей процес зазвичай включає в себе введення унікальних облікових даних, таких як ім'я користувача та пароль або використання цифрового сертифіката. Важливість автентифікації не можна недооцінювати, адже вона є першим захисним

бар'єром, який запобігає доступу неавторизованих осіб до системи або програми, тим самим захищаючи конфіденційні дані.

Методами автентифікації є:

- Пароль є найпоширенішим методом, але він може бути вразливим до атак взлому.
- Біометрична автентифікація, яка використовує унікальні фізичні характеристики, такі як відбитки пальців або розпізнавання облич.
- Двофакторна автентифікація комбінує щось, що користувач знає (пароль), з чимось, що він має (телефон або токен).
- Багатофакторна автентифікація включає в себе два або більше методів для забезпечення додаткового рівня безпеки.
- Автентифікація на основі сертифікатів використовує цифрові сертифікати, які видаються довіреними центрами сертифікації.

Централізовані системи, які керують авторизацією та автентифікацією за допомогою імені користувача та пароля, часто стають мішенями для кібератак. Якщо хакери проникають до такої системи, вони можуть отримати доступ до великої кількості облікових даних. Рішеннями даної проблеми можна зазначити:

- Фізичні токени та картки, що забезпечують додатковий рівень автентифікації, але можуть вимагати спеціального обладнання.
- Цифрові сертифікати, які надають високий рівень безпеки, але вимагають спеціалізованих знань для реалізації та управління.

Вибір методу автентифікації залежить від потреб системи, чутливості даних та користувачів. Крім того, важливо знайти баланс між безпекою та зручністю для користувачів, щоб забезпечити ефективну та надійну автентифікацію [6].

Блокчейн технологія відкриває нові горизонти у сфері авторизації та автентифікації, пропонуючи революційні зміни у способах, якими компанії управляють цими критично важливими процесами. Такими змінами є:

- *Децентралізоване управління:* блокчейн пропонує децентралізований підхід, де дані розподілені по мережі вузлів, значно ускладнюючи потенційний злом системи. Хакерам потрібно було б одночасно атакувати численні вузли, щоб отримати доступ до облікових даних користувачів, що робить такі атаки надзвичайно складними.
- *Передові криптографічні методи:* використання блокчейну включає застосування складних криптографічних технік, таких як цифрові підписи та шифрування, що забезпечують лише уповноважених осіб доступом до певної інформації.
- *Смарт-контракти:* автоматизація процесів авторизації та автентифікації можлива завдяки смарт-контрактам, які виконуються автоматично, коли виконуються певні умови, дозволяючи користувачам отримувати доступ до ресурсів без необхідності ручного втручання.
- *Аудиторський слід:* блокчейн створює незмінний, прозорий аудиторський слід усіх транзакцій, що полегшує відстеження доступу до інформації та допомагає запобігати несанкціонованому доступу.
- *Підтвердження нульового розголошення:* така технологія дозволяє користувачам підтверджувати володіння певними даними без необхідності розкривати самі ці дані, зменшуючи ризик витоку конфіденційної інформації.
- *Інфраструктура відкритих ключів:* блокчейн використовує принципи інфраструктури відкритих ключів для підвищення надійності автентифікації та захисту комунікацій.
- *Управління доступом на основі блокчейну:* створення децентралізованих систем управління доступом, які забезпечують безпечний та перевірений контроль над дозволами.

Так, завдяки блокчейну, рішення для авторизації та автентифікації стають більш безпечними, прозорими та ефективними, забезпечуючи оптимізовану взаємодію з користувачами та надаючи їм більший контроль над процесом [7]. Однак, як і будь-яка передова технологія,

блокчейн стикається з рядом викликів, які потребують уваги для її широкого прийняття. Можна навести такі приклади викликів:

Досвід користувача: Наразі, блокчейн може здатися складним для звичайних користувачів. Ключовим аспектом є спрощення управління ключами та інтерфейсів, щоб зробити технологію більш доступною для всіх, незалежно від їх технічного досвіду.

Нормативна база: Регулювання блокчейну та цифрової ідентифікації є непостійним і різноманітним у різних країнах. Це створює необхідність розробки глобальних стандартів, які б забезпечували конфіденційність, безпеку та відповідність національному законодавству.

Довіра до механізмів консенсусу: Новітні алгоритми консенсусу, такі як Proof-of-Stake і Proof-of-Authority, вимагають довіри спільноти та доведення своєї надійності. Це вимагає часу, ретельного тестування та перевірки, щоб стати загальноприйнятими [8].

Для подолання зазначених викликів, необхідно зосередитися на розробці інтуїтивно зрозумілих користувацьких інтерфейсів, створенні міцної нормативної основи та побудові довіри через прозорість та відкритість. З таким підходом блокчейн має потенціал не просто вдосконалити існуючі системи, а й створити нову еру цифрової безпеки, де доступ та авторизація керуються непорушними принципами децентралізації та прозорості.

Разом із тим, ця технологія відкриває нові можливості для багатьох секторів, від фінансів до охорони здоров'я, вносячи зміни, які важко переоцінити. Крім того, блокчейн пропонує децентралізоване рішення, яке використовує передові криптографічні технології та смарт-контракти для забезпечення безпеки та ефективності. У таблиці наведені сфери застосування блокчейну у частині покращення авторизації та автентифікації.

Сфери застосування технології блокчейну

Фінанси та банківська справа	Технологія блокчейну внесла значні зміни у фінансовий сектор, пропонуючи безпечні та прозорі механізми для переказу коштів. Він виключає необхідність у посередниках, забезпечуючи безпеку транзакцій та захист конфіденційної інформації.
Охорона здоров'я	У сфері медицини блокчейн гарантує безпеку даних пацієнтів, створюючи надійну платформу для обміну інформацією між лікарями та пацієнтами. Це сприяє цілісності медичних записів та ефективності ланцюгів постачання ліків.
Логістика	Блокчейн революціонізує управління ланцюгами поставок, підвищуючи прозорість та відстежуваність товарів. Це забезпечує чесну торгівлю та зменшує ризики підробки.
Інтернет Речей (IoT)	Завдяки блокчейну забезпечується надійна автентифікація пристроїв IoT, запобігаючи несанкціонованому доступу та забезпечуючи безпечне спілкування між пристроями у різних промислових секторах.
Право інтелектуальної власності	Блокчейн служить надійним інструментом для захисту творчості, дозволяючи авторам безпечно реєструвати свої твори та управляти правами на інтелектуальну власність.
Урядовий сектор	Уряди використовують блокчейн для підвищення прозорості та ефективності державних служб, включаючи процеси голосування та ідентифікації громадян.

Автентифікація та авторизація в блокчейні – це дві частини основи, що підтримує цілісність та безпеку цієї перспективної технології. У світі блокчейну, де учасниками можуть бути користувачі, вузли зберігання, обчислювальні вузли, автентифікація забезпечує впевненість у тому, що кожен учасник є достовірним і виконує визначену роль. Авторизація ж надає цим учасникам право виконувати певні дії, від читання даних до їх модифікації [9].

Ці процеси не лише сприяють безпеці та конфіденційності у розподіленому середовищі блокчейну, але й відіграють важливу роль у встановленні відповідальності у разі конфліктів або суперечок. Невідмовність від автентифікації та авторизації є ключовою для забезпечення прозорості та довіри між учасниками.

У контексті бездротових мереж шостого покоління, які вимагають нових підходів до автентифікації та авторизації, блокчейн пропонує розподілене управління, адже відсутність централізованого органу управління вимагає прозорого управління з боку розподіленої мережі, а також ефективність та конфіденційність, тобто змінні ролі учасників вимагають гнучких механізмів для оновлення та відкликання облікових даних, а також забезпечення конфіденційності за необхідності.

Блокчейн використовує децентралізований механізм співпраці для відстеження поведінки учасників, забезпечуючи довіру до кожної транзакції. Це створює систему, де інформація є непідробною та незмінною, допоки більшість обчислювальної потужності є законною. У разі спроби несанкціонованого втручання, система швидко ідентифікує та ізолює аномалії, забезпечуючи цілісність ланцюжка. Процес транзакції показано рис. 1.

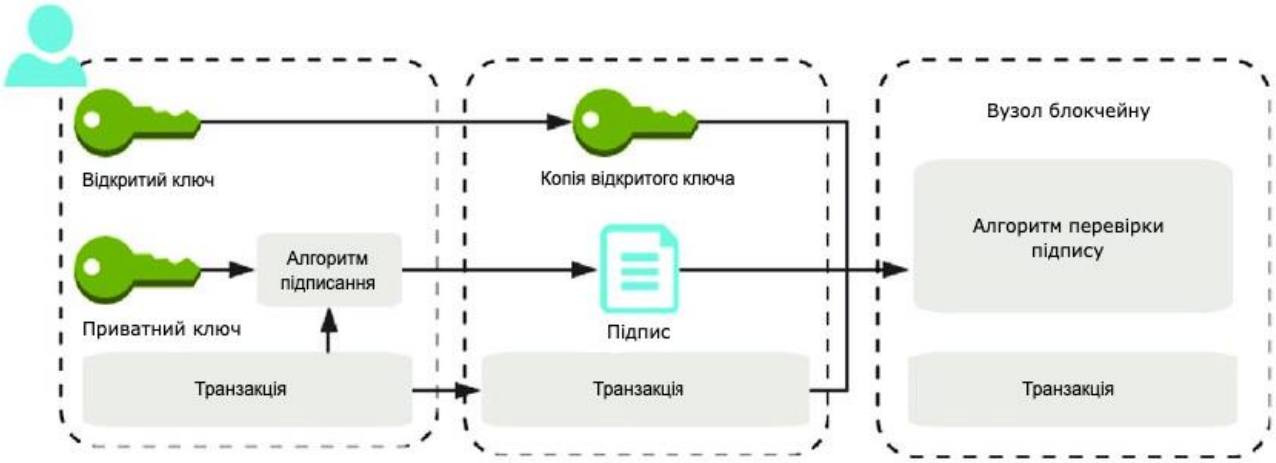

Рис. 1. Процес автентифікації для транзакцій у блокчейні

У високонавантажених системах, де безліч зацікавлених сторін мають можливість створювати унікальні ідентифікатори для своїх користувачів та управляти доступом до даних, виникає потреба в ефективному міждоменному управлінні (незалежне управління ідентифікацією показане на рис. 2). Традиційні централізовані моделі управління сертифікатами можуть стати надмірно складними та вразливими до компрометації, що підвищує ризики безпеки та витрати на управління [10].

У зв'язку з цим централізоване управління ідентифікацією пропонує введення єдиного менеджера, як-от постачальника послуг єдиного входу, може спростити процес, але вимагає консенсусу між усіма зацікавленими сторонами, що може бути непрактичним у динамічних мережах шостого покоління. Натомість, децентралізоване управління ідентифікацією на основі блокчейну пропонує альтернативний підхід, де зацікавлені сторони можуть колективно управляти ідентифікаційними даними користувачів та автентифікацією, як показано на рис. 2. Блокчейн, керований комітетом консорціуму, може надавати послуги автентифікації та авторизації, забезпечуючи прозорість та відстежуваність оновлень членства та операцій відкликання.

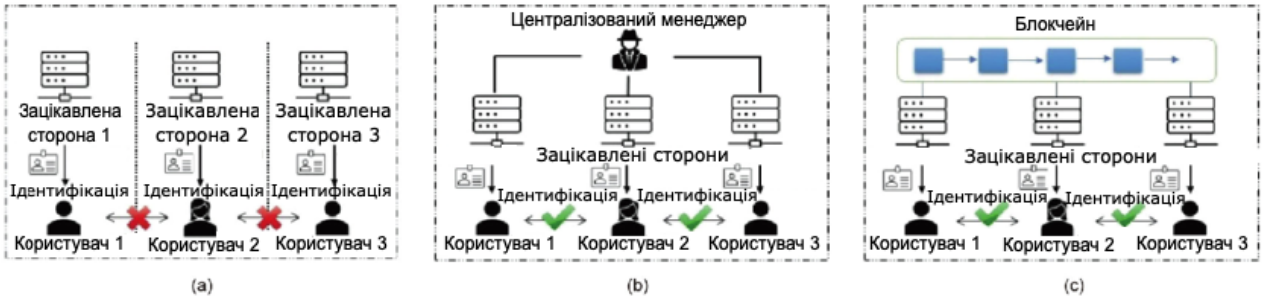

Рис. 2. Еволюція управління ідентифікацією: від незалежності до децентралізації: (a) незалежне управління; (b) централізоване управління ідентифікацією; (c) децентралізоване управління ідентифікацією

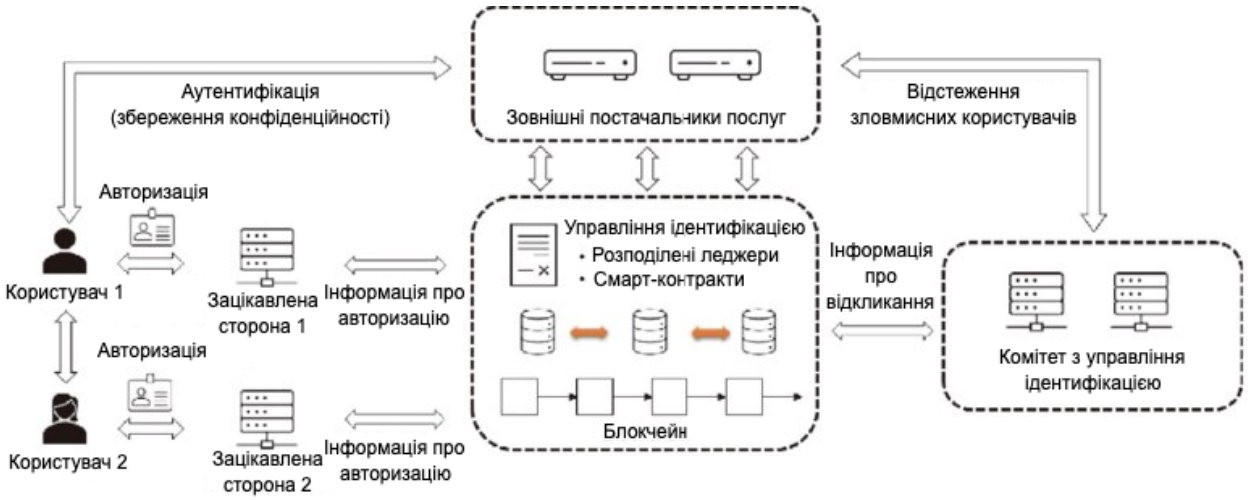

Рис. 3. Загальні процедури блокчейн-аутентифікації та авторизації

Таким чином, можна виділити деякі переваги блокчейну, а саме: прозорість – всі транзакції та оновлення політик авторизації є відкритими для перевірки всіма учасниками; відстежуваність – навіть у випадку компрометації деяких зацікавлених сторін, блокчейн забезпечує можливість відстеження та підзвітності всіх змін; розподілене управління знижує ризики, пов'язані з централізованими системами та дозволяє гнучке оновлення політик [11].

Разом із цим, постає ряд викликів, для яких доцільним є визначити приклади їх вирішення. Зокрема серед таких викликів можна виділити наступні: компрометація – необхідна розробка механізмів для швидкого виявлення та реагування на компрометацію зацікавлених сторін; управління консенсусом – потрібне забезпечення надійності та безпеки механізмів консенсусу у блокчейні; інтеграція – гармонізація блокчейн-рішень з існуючими системами та протоколами [12].

У сфері традиційної сертифікації, блокчейн-базові методи були запропоновані для забезпечення видимості та відкликання сертифікатів. Центри сертифікації виступають як публікатори сертифікатів у загальнодоступному блокчейні, тоді як валідність сертифікатів підтримується добросовісністю більшості учасників. Деякі дослідження фокусувалися на створенні структур прозорості повноважень, які дозволяють аудитувати процеси автентифікації та управління авторизацією.

На відміну від сертифікат-базованих систем, самостійна ідентифікація використовує блокчейн для дозволу користувачам самостійно керувати своїми посвідченнями, зменшуючи залежність від централізованих центрів сертифікації. Це знижує ризик збоїв і підвищує контроль доступу до даних через інтеграцію з механізмами на основі атрибутів, такими як шифрування на основі атрибутів, які вбудовуються у блокчейн через реєстри та смарт-контракти. Користувачі можуть отримувати ключі дешифрування, основані на їх атрибутах, що дозволяє динамічно оновлювати доступ до даних [13].

Блокчейн пропонує значні переваги у керуванні ідентичністю користувачів, але також створює виклики для конфіденційності через свою прозорість. Інтеграція механізмів збереження конфіденційності з блокчейн-базованими системами автентифікації та авторизації дозволяє захистити приватність. Основні методи включають використання псевдонімів, які представлені у блокчейні відкритими ключами, дозволяючи користувачам залишатися анонімними, поки вони не порушують правил. Інші методи, такі як групові та кільцеві підписи, допомагають зберегти анонімність особистості користувачів у блокчейні, дозволяючи їм використовувати одну ідентичність для багаторазового використання у різних додатках. Ці методи захисту конфіденційності були прийняті деякими блокчейн платформами, такими як Moreno [14].

Схеми групових та кільцевих підписів, основані на алгоритмах Фіата-Шаміра, можуть бути використані для самостійного управління ідентифікацією у блокчейнах. Анонімні облікові дані можуть бути делеговані на різних рівнях, що сприяє розширенню використання. У таких умовах конфіденційність особистих даних захищена, а відповідальність за відстеження зловмисників забезпечена. Існують схеми автентифікації та авторизації на основі блокчейну, які дозволяють відстежувати особистість користувачів під вимогливими умовами. Захист конфіденційності та забезпечення відповідальності можуть бути досягнуті одночасно. У контексті управління доступом на основі атрибутів, загальний підхід до збереження конфіденційності полягає у приховуванні політик доступу через шифрування на основі атрибутів, яке приховує атрибути, забезпечуючи захист не лише ідентифікаторів користувачів, а й політик даних [15].

Таким чином, блокчейн технологія виступає як децентралізований механізм, що забезпечує підвищену безпеку у процедурах авторизації та верифікації особистості. Завдяки використанню сучасних криптографічних рішень, автоматизації через смарт-контракти, надійному аудиту, механізмам підтвердження без розкриття інформації, інфраструктурі громадських ключів та блокчейн-орієнтованому управлінні доступом, організації мають можливість радикально трансформувати методи доступу до чутливих даних та ресурсів.

У контексті зростаючого фокусу на безпеку з боку провідних корпорацій прогнозується, що блокчейн-базовані системи авторизації та аутентифікації набудуть ширшого розповсюдження. Проте, для ефективного впровадження таких систем необхідно враховувати аспекти масштабованості, інтеграції та відповідності до регулятивних вимог, що забезпечить їхню широку адаптацію та зручність у використанні [16].

У таблиці представлено аналітичне порівняння механізмів авторизації та аутентифікації, що базуються на блокчейні, у порівнянні з конвенційними методами.

Порівняння підходу на основі технології блокчейн та традиційного підходу для авторизації та автентифікації

Показник	Блокчейн підхід	Традиційний підхід
Децентралізація	Так	Ні
Масштабованість	Середня	Середня
Безпека	Висока	Низька
Швидкість	Середня	Висока
Прозорість	Так	Ні
Вартість	Висока	Низька
Незмінність	Так	Ні
Ефективність	Висока	Висока

Затримка	Середня	Низька
Можливість збоїв	Низька	Середня

Огляд даних демонструє, що обидва підходи володіють унікальними перевагами та обмеженнями. Відтак, вибір відповідної технології для авторизації та аутентифікації залежить від специфічних вимог та контексту застосування, а також від тих аспектів безпеки, які є пріоритетними для даної системи.

Висновки

У контексті сучасної цифрової економіки, авторизація та аутентифікація, що базуються на блокчейні, виступають як важливі інструменти, що задовольняють зростаючий попит на безпеку, прозорість та оптимізацію транзакційних процесів. Ці механізми впроваджують криптографічні ключі та цифрові підписи для верифікації особистостей, мінімізації шахрайства та підсилення довіри, особливо у сфері фінансових операцій.

Незважаючи на значні переваги, такі як збільшення рівня безпеки, підвищення прозорості та ефективності, блокчейн також стикається з викликами. Ці виклики охоплюють технологічну складність, змінність регуляторного середовища та перешкоди, пов’язані з прийняттям та довірою до технології.

Попри існуючі перепони, з поступом у технологічному освоєнні та розвитку правових рамок, трансформаційний потенціал блокчейн-автентифікації у різноманітних галузях стає все більш виразним. У кінцевому підсумку, ця інноваційна технологія обіцяє значні можливості для майбутнього безпечних та надійних цифрових транзакцій.

Список літератури

1. Alilwit, Norah, "Authentication Based on Blockchain" (2020). Doctoral Dissertations and Master's Theses. *548. URL: https://commons.erau.edu/edt/548*

2. Blockchain Authentication. Overview, How It Works, Factors. Finance Strategists. URL: https://www.financestrategists.com/wealth-management/blockchain/blockchain-authentication/

3. Dominick Baier and Vittorio Bertocci, “A Guide to Claims-Based Identity and Access Control: Authentication and Authorization for Services and the Web”, 2013.

4. Gerardus Blokdyk, “Authentication Authorization Third Edition”, 2022.

5. Nigel Chapman, “Authentication and Authorization on the Web”, 2012.

6. Sambit Kumar Dash, “Ultimate Web Authentication Handbook”, 2023.

7. Elad Elrom, “The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects”, 2019.

8. Joaquin Garcia-Alfaro and Jose Luis Muñoz-Tapia, “Data Privacy Management, Cryptocurrencies and Blockchain Technology”, 2022.

9. Marco Fanti, “Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA”, 2023.

10. NeoNomad. Revolutionizing Authorization and Authentication: The Power of Blockchain Technology. Medium. URL: https://medium.com/@NeoNomadFinance/revolutionizing-authorization-and-authentication-the-power-of-blockchain-technology-51dc63da3e07

11. Sanjay Misra and Amit Kumar Tyagi, “Blockchain Applications in the Smart Era”, 2022.

12. Singh Garewal, “Practical Blockchains and Cryptocurrencies: Speed Up Your Application Development Process and Develop Distributed Applications with Confidence”, 2020.

13. What Is Blockchain Authentication. WooCommerce Plugins by JEM Products. URL: https://jem-products.com/what-is-blockchain-authentication/

14. Yu, Linsheng & He, Mingxing & Liang, Hongbin & Xiong, Ling & Liu, Yang. (2023). A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services. Sensors. 23. 1264. DOI: 10.3390/s23031264

15. Yuen TH, Sun SF, Liu JK, Au MH, Esgin MF, Zhang Q, et al. RingCT 3.0 for blockchain confidential transaction: shorter size and stronger security. In: Bonneau J, Heninger N, editors. Financial cryptography and data security. Cham: Springer; 2020. p. 464–83.

16. Шахід Шейх, "Створення децентралізованих блокчейн програм: дізнайтеся, як використовувати блокчейн як основу для програм нового покоління", 2021.

A. Tverdokhlib, S. Korotkov

IMPROVING THE EFFICIENCY OF AUTHORIZATION AND AUTHENTICATION USING BLOCKCHAIN TECHNOLOGY

In the contemporary research landscape, blockchain technology is garnering recognition as an innovative solution that enhances the security and transparency of operations across various sectors. Its application is particularly significant in the realms of authorization and authentication, where blockchain introduces innovative approaches to managing these critical processes. Research in this domain indicates a trend towards increasing adoption of blockchain-based solutions due to their ability to enhance security, ensure transparency, improve audit capabilities, optimize user interaction, and expand user control over processes.

Given the widespread use of online services such as online banking, which enables users to conduct transactions directly and efficiently, there is a growing need for robust authentication mechanisms to prevent fraud. Traditional methods like passwords and PIN codes are proving insufficient in the face of modern cybersecurity challenges. Blockchain offers alternative solutions that allow users to have independent and secure ownership of their information and facilitate safe data exchange among various service providers.

This article examines how blockchain can address data accuracy issues and provide a robust infrastructure for handling incidents and scenarios related to identification and authorization. It also considers the prospects of decentralization as a key element in all digital solutions provided by governments and private enterprises, with an emphasis on information confidentiality.

Ultimately, blockchain technology emerges as a potentially revolutionary tool for ensuring the security and reliability of digital transactions, considering the necessity for scalability, integration, and compliance with regulatory requirements for its effective implementation and widespread application.

Keywords: blockchain, authorization, authentication, smart contracts.