

## ЗАСТОСУВАННЯ БЛОКЧЕЙНУ ДЛЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Вінницький національний технічний університет

### Анотація

У цій роботі досліджується застосування технології блокчейн для підвищення безпеки телекомунікаційних мереж нового покоління. Розглянуто принципи функціонування блокчейну, його ключові властивості - децентралізацію, незмінність даних і прозорість транзакцій. Проаналізовано сучасні напрямки впровадження технології в галузі зв'язку: захист даних користувачів, автентифікація абонентів, запобігання шахрайству, управління ресурсами в мережах 5G/6G та безпечна взаємодія між операторами. Показано, що використання блокчейну дозволяє знизити ризики атак типу DDoS, підробки ідентифікаторів SIM та несанкціонованого доступу до мережеских вузлів. Разом із тим виявлено низку проблем, серед яких масштабованість, затримка транзакцій і потреба у стандартизації.

**Ключові слова:** блокчейн, телекомунікаційна мережа, безпека, 5G, автентифікація, децентралізація, кіберзахист.

### Abstract

*This paper examines the application of blockchain technology to enhance the security of telecommunication networks. The basic principles of blockchain operation are described, including decentralization, data immutability, and transaction transparency. The main implementation areas are analyzed - data protection, user authentication, fraud prevention, resource management in 5G/6G networks, and secure inter-operator interaction. It is shown that blockchain helps reduce the risks of DDoS attacks, SIM identity spoofing, and unauthorized access to network nodes. However, several challenges remain, such as scalability, transaction latency, and the need for interoperability standards.*

**Keywords:** blockchain, telecommunication network, security, 5G, authentication, decentralization, cyber protection.

### Вступ

Сучасні телекомунікаційні мережі - це складні децентралізовані системи, що передають величезні обсяги даних у режимі реального часу. Зі зростанням кількості підключених пристроїв (IoT), впровадженням 5G та розвитком хмарних сервісів значно зросли ризики кібератак, шахрайства та витоку даних. Традиційні методи захисту (централізовані сервери, сертифікати та фаєрволи) поступово втрачають ефективність через складність інфраструктури та відсутність прозорого механізму довіри між учасниками мережі [1, 2].

Технологія блокчейн, спочатку створена для криптовалют, довела свою надійність у забезпеченні децентралізованого зберігання та перевірки інформації. Завдяки властивостям незмінності, прозорості та відсутності єдиної точки відмови, блокчейн розглядається як один із найперспективніших інструментів для підвищення рівня безпеки телекомунікаційних мереж [3, 5].

### Аналіз результатів дослідження

Блокчейн - це розподілений реєстр, у якому всі транзакції зберігаються у вигляді ланцюга блоків, що захищені криптографічними алгоритмами. Кожен новий блок містить хеш попереднього, що забезпечує незмінність даних - зміна одного запису призводить до порушення всієї структури. Такий підхід дозволяє уникнути фальсифікації даних і забезпечує високий рівень довіри між учасниками мережі [1, 4].

У контексті телекомунікацій, блокчейн може виступати механізмом обліку, автентифікації та контролю доступу до мережеских ресурсів. Кожен вузол або пристрій має власний криптографічний ключ, що унеможливує підробку особистості користувача.

Одним із найважливіших напрямків є ідентифікація користувачів без центрального сервера. У традиційних системах автентифікації (наприклад, через SIM-центр) існує ризик компрометації даних. Блокчейн забезпечує зберігання записів автентифікації у розподіленій базі, до якої мають доступ лише авторизовані учасники. Це мінімізує ризики підробки SIM-ідентифікаторів і шахрайських схем із роумінгом [2, 6].

У 2024 році проведені пілотні проекти в ЄС показали, що впровадження блокчейн-автентифікації дозволило скоротити кількість шахрайських дій із SIM-заміною на 32 %. Оператори Vodafone, Deutsche Telekom і Orange використовують подібну модель для створення децентралізованої бази даних користувачів. Технологія блокчейн активно застосовується для виявлення та блокування фальшивих транзакцій у білінгових системах. Наприклад, платформи на базі Hyperledger Fabric дозволяють вести журнал усіх з'єднань між мережами операторів і перевіряти їх достовірність. Завдяки незмінності записів блокчейн виключає можливість прихованої зміни інформації про з'єднання, що особливо важливо для міжоператорських розрахунків. У звіті 360 Research Reports зазначається, що щорічні втрати операторів від шахрайства у сфері зв'язку перевищують 38 млрд доларів, а блокчейн-системи дозволяють зменшити цей показник на 20-25 % протягом перших двох років впровадження [3, 5].

З появою 5G мережі стали більш віртуалізованими, тобто логічно поділеними на сегменти (network slices), кожен із яких може обслуговувати окремий тип сервісів. Це створює складну задачу контролю доступу між сегментами.

У роботі Kouvakis V. et al. (2024) запропоновано архітектуру Hierarchical Blockchain RAN, у якій блокчейн використовується для реєстрації подій між вузлами та моніторингу стану мережі. Такий підхід дозволяє запобігати підробці даних конфігурації та мінімізує ризик внутрішніх атак.

Дослідження показало, що використання блокчейну в системі керування ресурсами 5G зменшує час виявлення несанкціонованих дій на 27 % і підвищує точність моніторингу трафіку. Основними перевагами використання технології блокчейн в телекомунікаціях : Децентралізація - відсутність єдиного вузла, який може стати точкою відмови. Прозорість і відстежуваність - усі транзакції фіксуються в реєстрі, доступному учасникам. Незмінність даних - виключає можливість несанкціонованої модифікації інформації. Автоматизація через смарт-контракти - забезпечує виконання політик без участі людини. Сумісність із IoT-пристроями - децентралізоване керування великими системами сенсорів [1, 3, 4, 6].

Попри переваги, технологія має низку обмежень: Масштабованість - публічні блокчейни не можуть обробляти тисячі транзакцій на секунду, що необхідно для телеком-мереж, затримка транзакцій (latency) - консенсус вимагає часу, що може бути критичним у реальному часі, високе енергоспоживання у деяких алгоритмах консенсусу (Proof-of-Work), інтероперабельність - відсутність єдиних стандартів для взаємодії між операторами [4, 5, 6].

Сучасні рішення спрямовані на створення приватних або гібридних блокчейнів, які поєднують безпеку публічних мереж і швидкість централізованих систем.

Очікується, що у 2025–2030 роках блокчейн стане ключовим елементом архітектури мереж 6G, забезпечуючи довіру між автономними пристроями та автоматичне розподілення ресурсів за допомогою смарт-контрактів [2, 4].

Дослідження Emergen Research (2025) прогнозує, що ринок блокчейн-рішень для телекомунікацій зросте з 0.7 млрд \$ у 2023 до 17.5 млрд \$ у 2033 році [6].

Таким чином, блокчейн уже переходить із експериментальної технології до реального інструмента кіберзахисту в галузі зв'язку.

## Висновки

Технологія блокчейн є перспективним напрямом забезпечення безпеки телекомунікаційних мереж нового покоління. Її використання дозволяє створити децентралізовану систему довіри між операторами, підвищити рівень захисту даних, мінімізувати шахрайство та автоматизувати управління ресурсами. Результати аналізу показують, що блокчейн-рішення здатні зменшити втрати від кіберзагроз і покращити прозорість операцій. Основними напрямками подальших досліджень є вдосконалення

масштабованості, інтеграція зі штучним інтелектом, розробка галузевих стандартів і створення енергоефективних механізмів консенсусу.

Отже, блокчейн — це не лише технологія зберігання транзакцій, а фундаментальний елемент безпеки майбутніх телекомунікаційних систем 5G/6G та IoT-інфраструктури.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nguyen D. C., Pathirana P. N., Ding M., Seneviratne A. Blockchain for 5G and Beyond Networks: A State of the Art Survey
2. [Електронний ресурс]. – Режим доступу: <https://arxiv.org/abs/1912.05062>
3. Popoviciu C., Zhang Y., Lee S. Blockchain for Telecom: Opportunities and Challenges. IEEE Communications Magazine, 2023.
4. Blockchain in Telecom – Global Strategic Business Report. Research & Markets [Електронний ресурс]. – Режим доступу: <https://www.researchandmarkets.com/reports/5303087/blockchain-in-telecom-global-strategic>
5. Kouvakis V., Trevlakis S. E., Boulogeorgos A.-A. et al. Hierarchical Blockchain Radio Access Networks: Architecture, Modelling, and Performance Assessment. arXiv, 2024. – Режим доступу: <https://arxiv.org/abs/2412.19838>
6. Blockchain in Telecom Market 2025–2033: Growth, Trends, and Market Share. 360 Research Reports [Електронний ресурс]. – Режим доступу: <https://www.360researchreports.com/press-release/blockchain-in-telecom-market-outlook-2025-2033>

**Онищук Вячеслав Олександрович** – студент групи РТ-23б, факультету інформаційних електронних систем, Вінницький національний університет, м. Вінниця, e-mail: [onushukvyatcheslav@gmail.com](mailto:onushukvyatcheslav@gmail.com)

**Кичак Василь Мартинович** – д.т.н., проф., завідувач кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: [kychak.v.m@vntu.edu.ua](mailto:kychak.v.m@vntu.edu.ua)

**Viacheslav O. Onyshchuk** – student of group RT-23b, faculty of information electronic systems, Vinnitsa National University, Vinnitsa, e-mail: [onushukvyatcheslav@gmail.com](mailto:onushukvyatcheslav@gmail.com)

**Vasyl M. Kychak** – Doctor of Technical Sciences, Professor, Head of the Department of infocommunication systems and technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: [kychak.v.m@vntu.edu.ua](mailto:kychak.v.m@vntu.edu.ua)