

## ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА ЗМІНУ ВОЛАТИЛЬНОСТІ, ФОРМУВАННЯ ЦІНИ І ОБСЯГИ ТОРГІВ НА РИНКУ ВІРТУАЛЬНИХ АКТИВІВ

Кучерявий А.О., здоб. ступ. PhD

*Державна навчально-наукова установа  
«Академія фінансового управління»*

Цифрова революція із появою електронних комунікативних технологій безповороттно змінила природу фінансів. Розвиток сучасної економіки визначає курс на цифровізацію банківської системи, обігу грошей і платіжних систем. Із появою першої криптовалюти 2008 року, після світової економічної кризи доткомів інвестори отримали абсолютно новий технологічний інструмент. Відомо, що криптовалюти використовують технологію блокчейн, або «розподілений реєстр». Вони стали популярними завдяки ефективним швидким платіжним системам, що не залежать від політичного процесу або державної регуляції. Технологія блокчейн є незмінною, дозволяючи додавати інформацію, але не видаляти її. Транзакції в системі блокчейн мінімізують витрати на пошук, юридичні витрати і транзакційні витрати, а також знижують ризики фальсифікації даних.

Поширення використання віртуальних активів значно впливає на фінансові технології, трансформуючи способи обміну, зберігання та інвестування капіталу. За прогнозами аналітиків, до 2050 року частка криптоактивів у глобальній економіці суттєво зросте, що відкриє нові можливості та виклики для учасників ринку. Разом із популярністю криптовалют, таких як біткоїн і ефіріум, зростає і загроза кіберзлочинності.

В основі популярності криптовалют лежить їх здатність полегшувати транзакції без посередників, як-от банки або державні органи, і забезпечувати анонімність для обох сторін угоди. Однак ця анонімність і децентралізація також створили умови для поширення кіберзлочинів. За даними Федеральної торгової комісії США, кількість шахрайств із криптовалютами значно зросла з жовтня 2020 року по березень 2021 року, що призвело до втрат у понад 80 мільйонів доларів. Найбільш масштабні хакерські атаки, як-от злом біржі Mt. Gox у 2014 році, підривають довіру до криптовалют, викликаючи значні коливання їх цін та негативно впливаючи на ринок [1]. Для протидії цим загрозам необхідно підсилювати регуляторний контроль і кібербезпеку в усіх сферах використання криптоактивів. Кіберзлочини, пов'язані з криптоактивами, становлять значну небезпеку, оскільки вони підривають довіру до ринку та спричиняють фінансові втрати. Розуміння масштабів і видів цих злочинів, а також шляхів їхнього запобігання, є важливим аспектом захисту інвесторів та стабілізації ринку віртуальних активів [2].

Крадіжка криптоактивів має значний вплив на їхню волатильність. Коли відбувається кіберзлочин, що призводить до втрати великої кількості активів, це може спричинити масовий розпродаж серед інвесторів, що призводить до різких коливань і зниження ціни. Відсутність довіри до бірж і криптовалют

погіршує ситуацію, викликаючи ще більшу волатильність. У свою чергу, це впливає на всі активи на біржі, а інвестори можуть виводити свої кошти, шукаючи безпечніші місця для інвестування. Наприклад, після великої крадіжки у 2021 році, коли було викрадено більше \$3.2 мільярдів у криптовалюті, ціни на криптоактиви знизилися на короткий час, але згодом відновилися. Це показує, що ринок може бути досить стійким до подібних подій, якщо інвестори відчують, що ситуація під контролем

Учасники ринку віртуальних активів в Україні повинні дотримуватися вимог FATF, норм Цивільного кодексу та закону «Про віртуальні активи» [3]. А головним регулятором політики у сфері віртуальних активів визначено Національну комісію з цінних паперів і фондових ринків. Розробку алгоритму деанонізації учасників підозрілих операцій з обміну криптовалют покладено на Міністерство цифрової трансформації і НБУ [4].

Кіберзлочинність у сфері криптовалют має значний вплив на волатильність зламаних валют і збільшує кореляцію між зламаними валютами та іншими криптовалютами. Це систематично завдає шкоди ринкам криптовалют, хоча ефекти можуть бути специфічними для конкретного випадку. Злам криптовалют часто призводить до зниження відкриття ціни приблизно на 10-20% та до аномальних прибутків, які можуть варіюватися від -2% до -24% залежно від конкретної події [5]. Ці прибутки спостерігаються за кілька годин до злomu і повертаються до нуля після оголошення про злом.

Криптовалюти, як відносно новий клас активів, створили унікальні можливості для здійснення великих кіберзлочинів. Незважаючи на різні регуляторні обговорення, існує багато каналів, через які злочинність може розвиватися, уникаючи відповідальності. Різні хакерські атаки, як на рівні бірж, так і на рівні окремих криптовалют, значно впливають на довіру до цього класу активів. Саме тому необхідно приділяти більше уваги регуляторному контролю та підвищенню безпеки криптовалют. Для захисту від кіберзлочинів у сфері віртуальних активів різними регуляторами і було запропоновано низку рекомендацій, що наведено в таблиці нижче. Впровадження цих рекомендацій може значно знизити ризики кіберзлочинності та стабілізувати ринок криптоактивів.

**Таблиця – Рекомендації по запобіганню і боротьби зі злочинами для учасників ринку криптоактивів**

Регулятор	Рекомендація
Верховна Рада України [6]	Розробка і впровадження строгих регуляторних рамок для транзакцій з криптоактивами.
Європейський парламент [7]	Сприяння міжнародній співпраці у розслідуванні та боротьбі з кіберзлочинністю.
Комісія з торгівлі товарними ф'ючерсами США [8]	Підтримка приватно-державних партнерств для обміну інформацією про загрози для криптоактивів.
Інтерпол [9]	Створення міжнародних груп для боротьби з масштабними крадіжками криптоактивів.
FATF [10]	Розробка і впровадження на міжнародному рівні заходів і стандартів з боротьби щодо відмивання грошей у криптоіндустрії
МіСА [11]	Зобов'язання постачальників криптопослуг дотримуватися строгих заходів безпеки, розкривати інформацію про учасників транзакцій.

*Джерело: узагальнено автором.*

З огляду на виклики, пов'язані з регулюванням криптовалют на державному та міжнародному рівнях, фінансова цифровізація потребує ретельного врегулювання. Це важливо не лише для захисту інвесторів, а й для зниження можливості використання криптовалют у злочинних цілях. Зокрема, необхідно впроваджувати деанонімізацію операцій з криптоактивами та створення міжнародних стандартів для відстеження транзакцій, що допоможе зменшити використання криптовалют у незаконних цілях та стабілізувати ринки.

#### Інформаційні джерела:

1. Štefan Lyócsa, Peter Molnár, Tomáš Plíhal, Mária Širaňová, Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin, *Journal of Economic Dynamics and Control*, Vol. 119 (2020). URL: <https://www.sciencedirect.com/science/article/pii/S0165188920301482> (дата звернення: 22.10.2024).
2. Yoichi Tsuchiya, Naoki Hiramoto, How cryptocurrency is laundered: Case study of Coincheck hacking incident, *Forensic Science International: Reports*, Vol. 4 (2021). URL: <https://www.sciencedirect.com/science/article/pii/S2665910721000724> (дата звернення: 24.10.2024).
3. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.11.2019 року, № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text> (дата звернення: 26.10.2024).
4. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р. URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#top> (дата звернення: 24.10.2024).
5. Corbet, Shaen and Cumming, Douglas J. and Lucey, Brian M. and Peat, Maurice and Vigne, Samuel, Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in Cryptocurrency Markets (2019). URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3384707](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384707) (дата звернення: 26.10.2024).
6. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення: 26.10.2024).
7. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L\\_202302841](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302841) (дата звернення: 27.10.2024).
8. Final Interpretive Guidance for Retail Commodity Transactions Involving Certain Digital Assets. URL: <https://www.cftc.gov/sites/default/files/2020/06/2020-11827a.pdf> (дата звернення: 27.10.2024).
9. Cryptocurrency crime: preventing the misuse of virtual assets by organized crime for money laundering. URL: <https://www.interpol.int/en/News-and-Events/News/2021/Cryptocurrency-crime-preventing-the-misuse-of-virtual-assets-by-organized-crime-for-money-laundering> (дата звернення: 27.10.2024).
10. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (дата звернення: 28.10.2024).
11. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&qid=1730149482439> (дата звернення: 27.10.2024).