

Тетяна Дмитренко

кандидат економічних наук, ст. дослідник,
завідувач відділу міжнародних фінансів та фінансової безпеки
відділення глобальної економіки і міжнародних фінансів НДФІ
ДННУ «Академія фінансового управління», м. Київ, Україна
AML-консультант Управління ООН з наркотиків і злочинності,

м. Відень, Австрія

tetiana.dmytrenko@umdigital.science

ORCID ID: 0000-0002-2632-2986

Валерія Волкова

аспірантка

ДННУ «Академія фінансового управління», м. Київ, Україна

valeriya.vodus@gmail.com

ORCID ID: 0000-0001-8270-042X

АНАЛІЗ РИЗИКІВ БЕЗПЕКИ У ВИКОРИСТАННІ МАЙНІНГУ КРИПТОВАЛЮТ В ОПЕРАЦІЯХ З ВІДМИВАННЯМ ДОХОДІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ, ТА ПЕРСПЕКТИВИ ЇХ ПОДОЛАННЯ

Цифрові фінанси стають однією з найважливіших частин економічної та фінансової екосистем світу. Попит на криптоактиви і пов'язані з ними продукти/послуги стрімко зріс за останні роки та стає все більше взаємопов'язаним з регульованою фінансовою системою, оскільки потенційно він кардинально змінює її та всю економічну систему держави.

В той час, як суспільство зосередило свій погляд на темі криптовалют, майнінг цих же монет для багатьох залишається незрозумілою темою. Саме майнінг криптовалют (від англ. «mining» – видобуток) і створює цифрові валюти. Це певним чином децентралізований «випуск» грошей, і всі транзакції в мережі не випускаються однією установою у вигляді звичайного

для нас національного або центрального банку, а генеруються будь-яким користувачем, підключеним до мережі Інтернету. Це певна децентралізована система, яка виконує функції та ставить завдання для виконання, а майнер (власник) отримує винагороду у вигляді криптовалюти або її частини за певну кількість оброблених транзакцій в цій системі.

У 2022 році обсяг світового ринку майнінгу криптовалют становив 1,92 млрд дол. США. Очікується, що до 2032 року обсяг світового ринку майнінгу криптовалют досягне 7 млрд дол. США, а у 2032 році CAGR (сукупний річний темп зростання) збільшиться на 12,90% [4].

Майнінг є важливою операцією для створення, передачі та підтвердження криптовалютних транзакцій. Це гарантує стабільну, безпечну і надійну передачу валюти від платника до одержувача. Криптовалюти працюють в одноранговій мережі й тому вони є децентралізованими, на відміну від фіатних грошей, в яких центральний орган їх емісії контролює та регулює весь їх оборот. У 2022 році майнінговий сектор ринку віртуальних активів приніс понад 76% частки всього його доходу [4].

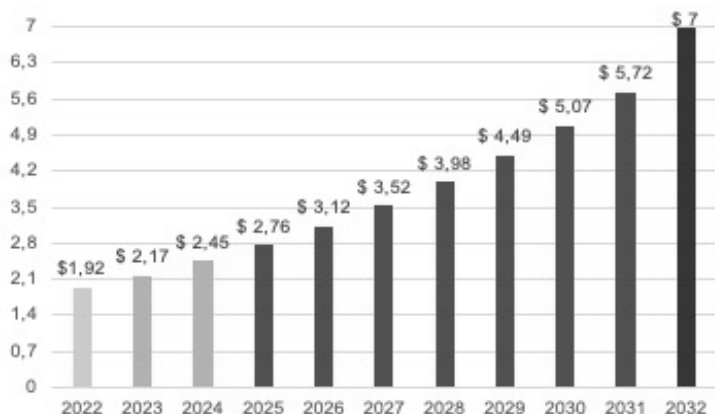


Рис. 1. Динаміка ринку майнінгу криптовалюти у 2022-2032 рр.

Джерело: Precedence research <https://www.precedenceresearch.com/cryptocurrency-mining-market>[4].

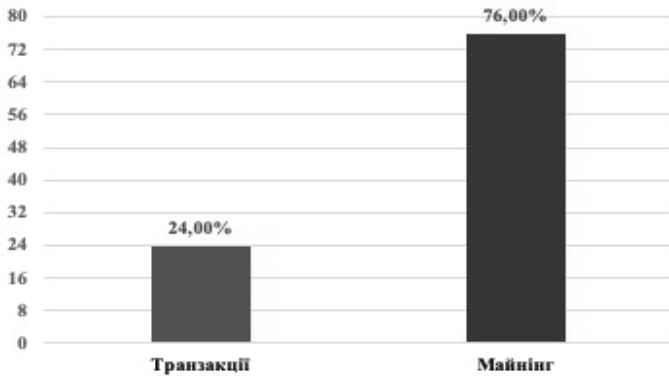


Рис. 2. Ринок майнінгу криптовалют у 2022 р.

Джерело: Pregelence research [4].

З появою першої криптовалюти популярність її видобутку з кожним роком все більше зростала, все більше людей долучалося до цього процесу як у легальний, так і в нелегальний спосіб. Саме використання майнінгу в незаконний спосіб і є одним з інструментів, за допомогою якого приховуються злочинні доходи через відмивання коштів. Як регулятори, так і спеціалісти з боротьби зі фінансовими злочинами повинні знати та розуміти ризики майнінгу криптовалюти.

Фахівці з боротьби із фінансовими злочинами та регулятори ринку різних юрисдикцій все більше приділяють посилену увагу ризиковим операціям з криптовалютами, в тому числі останні рекомендації Міжнародної організації з протидії відмиванню злочинних доходів (FATF) (2023) [11] зосереджені на дотриманні країнами Рекомендації 15 FATF та пояснювальної записки до неї (R.15/INR.15), особливо в частині моніторингу операцій зі стейблкоїнами, DeFi (децентралізованих фінансових систем) і одноранговими операціями та ліцензуванні діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів (VASPів). Майнінг як діяльність не належить до діяльності з високими криптовалютними ризиками, хоча такі організації, як Мережа боротьби з фінансовими

злочинами (FinCEN) та FATF, прискіпливо вивчають показники його ризикованості й формують рекомендації щодо пом'якшення таких ризиків.

Майнінг у системі криптовалют є однією зі складових безпеки самої системи і має три важливі характеристики: значна швидкість, низька вартість транзакції та надійність. Ще одна виняткова особливість майнінгу – це забезпечення мережі від різного виду атак, таких як подвійне витрачання, спам-атаки та атаки 51% в разі онлайн контролю більшої частини децентралізованої мережі. Останні спостереження ґрунтуються на тому, що майнери криптовалют не просто створюють нову криптовалюту або захищають мережу, вони також цілеспрямовано виконують функції грошових переказів, і до них треба ставитися в окремих випадках як до постачальників послуг, пов'язаних з оборотом віртуальних активів (VASP).

Випуск незабезпечених криптоактивів у більшості здійснюється децентралізовано. Здебільшого емітенти невідомі, що підвищує ризики та регуляторні загрози. Незважаючи на те, що децентралізація емісії має на меті децентралізацію фінансових послуг без центрального управління та більшої «демократизації» вартості, вона також підвищує ризики для користувачів і необґрунтованого розширення ринку. Децентралізація ускладнює розробку підходів до нормативних актів щодо діяльності емітентів криптоактивів. Більшість державних регуляторів обмежила свій вплив на формування ринку віртуальних активів шляхом відсутності надання рекомендацій та попереджень споживачам і/або користувачам, відсутності освітніх програм та заходів. Відсутність інформації щодо відомих емітентів часто призводить до труднощів у розкритті інформації про незабезпечені криптоактиви, що випускаються. Відсутність такої інформації формує загрози щодо визначення типу технології, що використовується, цільового призначення токена або будь-якої інформації про бенефіціарів прибутку чи доходу, які можуть бути отримані від продажу криптоактиву.

Криптоактиви, випущені в децентралізованій загальнодоступній мережі, мають меншу вірогідність мати ризик маніпулювання емісією, оскільки вузли і валідатори (оператори) потенційно

зосереджені по всьому світу. Це покращує безпеку обігу віртуальних активів та діяльності з нею. Однак такі мережі все ще вразливі до певних кібератак, наприклад, 51% атак (атака 51% відбувається, коли злоумисник у мережі отримує контроль над продуктивністю майнінгу блокчейну; 27% токенів продаються зацікавленим сторонам за узгодженою ціною перед збільшенням обсягу токенів). У випуску віртуальних активів суттєвим питанням є розкриття інформації щодо її цілей створення та використання. Централізовані складові інфраструктури крипторинку, такі як біржі криптоактивів та постачальники послуг, пов'язаних з оборотом віртуальних активів, також чутливі до кіберризиків і операційних ризиків.

Криптовалюта сама по собі не є засобом захисту інформації. Однак вона може вважатися такою, якщо ця криптовалюта застосовується для перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

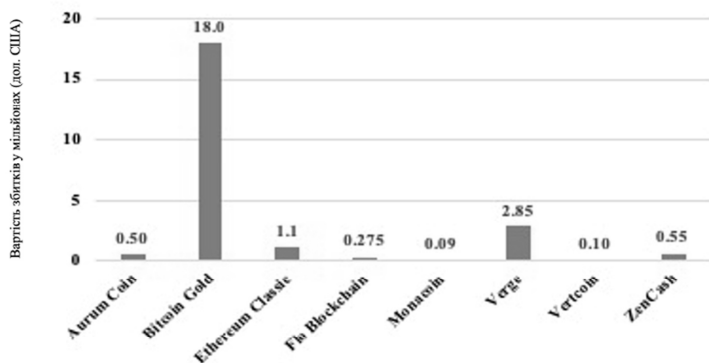


Рис. 3. Втрати від 51% атаки на вісім криптовалют, які були використані

Джерело: Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin [3].

На рис. 3 представлено суму збитків через 51% атаку з квітня 2018 року по січень 2019 року. Монета Verge (XVG) зазнала двічі атак протягом цих 9 місяців, втративши спочатку 1,1 млн дол. США, а потім 1,75 млн дол. США. Біткойн золото (BTG) також зазнав збитків та є

найбільш постраждалою монетою, яка призвела до втрат майже 18 млн дол. США в результаті своєї вразливості до кібератак. Решта зазначених монет також втратила значну суму від таких атак. Загальний збиток становить в середньому 2,5 млн дол. від атак на окремі валюти [3].

Атака 51% – це малоймовірне подія, тому що об'єднати утримувачів нод блокчейну обсягом більше 50% потужності хешування криптовалютної мережі важко з причин мотивації таких дій і великої кількості цих утримувачів. Ця атака може відбуватись на менших за обсягами DLT-мережах, та, як правило, трапляються невдачі у великих, таких як біткойн, оскільки вони безпечніші.

Незважаючи на назву, для атаки не обов'язково мати 51% майнінгової потужності мережі. Однак атака меншим обсягом утримувачів нод DLT мережі має набагато менші шанси на успіх.

Егоїстичний майнінг – ще одна хеш-атака більшості, яка виконується з використанням приблизно 25% загального мережевого хешування [2]. Це може здійснюватися майнерами або майнінг-пулами (децентралізовані групи, організовані та керовані третіми сторонами для координації хеш-потужностей майнерів, а потім розподілу отриманих біткоїнів [17]), які містять велику кількість мережевого хешу. В цій техніці атаки майнери стають дуже вибірковими у трансляції своїх блоків у мережу. Вони можуть вирішити або скасувати свої блоки, відмовившись від винагороди, або транслювати кілька блоків одночасно. Це призведе до скасування блоків інших майнерів, через що вони втратять свою винагороду, а також комісію за транзакції. Під час процесу незалежні вузли мають намір приєднатися до зловмисника, щоб збільшити свої прибутки, а зловмисники отримують більше контролю над мережею, маючи більшу потужність хешування. Ще одна атака – це атака 34%. Така атака відбувається через більшість мережевого хешування. Наприклад, ІОТА – це криптовалюта, розроблена для Інтернету речей. ІОТА не базується на блокчейні та містить унікальне сховище, відоме як Tangle [6]. Tangle також є розподіленою книгою, яка виконує подібні операції, як і блокчейн. ІОТА містить централізовану складову в сутності свого обігу, тому вона також вразлива до атаки 34% [5].

Ризики егоїстичного майнінгу та цінності, які добувають майнери в певних DLT-мережах, також можуть призвести до ризиків, які впливають на цілісність ринку та його функціонування. Навіть якщо емітенти децентралізовані, то орган управління може існувати, якщо до складу таких входять ті, хто володіє найбільшими холдингами токенів або токенами з певними правами управління. Це може призвести до централізації більшості криптоактивів, і, як наслідок, знову запровадити єдину точку відмови або вимагати довіри до однієї сутності.

Ризики також виникають через різні способи випуску та розповсюдження криптоактивів. Існує кілька способів створення і випуску криптоактивів, з яких три найпопулярніші – попередній майнінг, безперервний майнінг та гібридний підхід.

При попередньому майнінгу всі токени генеруються в одній партії як єдина подія, тоді як при безперервному майнінгу криптоактиви, ймовірно, створюватимуться на постійній основі або через проміжки часу протягом визначеного періоду або до встановленого кінцевого терміну. Попередній майнінг потенційно може створити певний ризик для споживача. Маніпулювання цінами за допомогою схем «накачування та скидання» в цьому разі є ключовою проблемою (на практиці це стосується до тієї групи інвесторів-майнерів, яка штучно підвищує ціну на відносно неліквідні криптоактиви шляхом узгодженої покупки. Коли ціна зростає, інші роздрібні користувачі проявляють зацікавленість, що продовжує підвищувати ціну такого криптоактиву. На цьому етапі початкова група попередньо продасть усі свої активи за вищою ціною, залишивши наступних інвесторів зі збитками, оскільки ціна впаде) [10]. Варто зазначити, що за останні роки рівень використання попереднього майнінгу суттєво знизився.

Ризики кібербезпеки є одними з ключових ризиків у дослідженні ризикорієнтованого підходу в діяльності майнерів криптовалют, адже майнінгові установки можуть стати мішенню для хакерів та вірусів, спрямованих на викрадення криптовалюти або обчислювальної потужності, вимагаючи значних зусиль і ресурсів для захисту системи.

Зловмисне програмне забезпечення для майнінгу криптовалюти – це тип зловмисного програмного забезпечення, яке використовує ресурси комп'ютера для майнінгу криптовалюти. Процес передбачає розв'язання складних математичних задач та виробництво нових монет у відповідь.

Зловмисне програмне забезпечення криптоджекінг (cryptojacking) схоже на зловмисне програмне забезпечення для майнінгу криптовалют, за винятком того, що воно не потребує жодної взаємодії чи згоди користувача. Воно працює у фоновому режимі, видобуваючи криптовалюту з комп'ютерів нічого не підозрюючих користувачів без їх відома чи дозволу.

Криптоджекінг – це метод кібератаки, під час якого зловмисне програмне забезпечення використовується для отримання контролю над комп'ютером і використання його ресурсів для видобутку криптовалюти [16]. Криптозловмисники можуть діяти шляхом встановлення зловмисного програмного забезпечення в системі жертви або шляхом зламу вебсайту за допомогою коду, який захоплює комп'ютери відвідувачів з метою майнінгу.

Криптоджекінг може статися з будь-яким типом криптовалюти, але найчастіше це відбувається з Monero (XMR), оскільки це анонімна валюта та має більше функцій конфіденційності, ніж інші монети, такі як біткойн або ефір.

Зловмисне програмне забезпечення криптоджекінг можна встановити через фішингові електронні листи, що містять посилання на заражені вебсайти або файли. Крім того, він може надходити в комплекті з іншими завантаженнями програмного забезпечення, про які користувачі не підозрюють, що вони містять шкідливий код, доки не стане надто пізно (наприклад, підроблені інсталятори Adobe Flash Player).

У період з 2018 по 2022 рік кількість спроб криптоджекінгу в усьому світі поступово зростає. У 2022 році кількість таких шахрайських діянь наблизилася до 140 млн дол. США. Це означає зростання викрадень криптоактивів на 43% порівняно з попереднім роком [1].

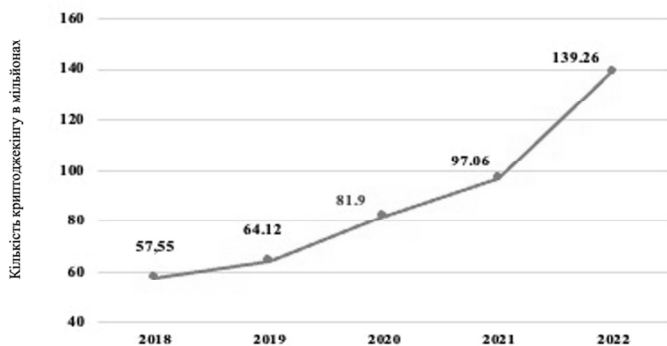


Табл. 4. Річна кількість атак криптоджекінгу в усьому світі у 2018-2022 рр.

Джерело: Global annual number of cryptojacking attempts 2018-2022 [1].

Схеми криптоджекінгу можуть залишатися непоміченими протягом тривалого часу, дозволяючи хакерам абсолютно безкарно здійснювати майнінг із пристроїв нічого не підозрюючих жертв.

Скрипти криптоджекінгу можуть призвести до затримки працездатності пристроїв або навіть до поломки через знос. Крім того, існує клас сценаріїв криптоджекінгу, які мають здатність проникнення, що дає змогу їм швидко тиражуватися, заражаючи кілька пристроїв та серверів у мережі.

Більшість юрисдикцій і органів влади ще не ввела в дію закони, що регулюють криптовалюти, а це означає, що для більшості країн законність майнінгу криптовалют як частини віртуальних активів залишається незрозумілою.

Відповідно до визначення Мережі боротьби з фінансовими злочинами (FinCEN), криптомайнери вважаються суб'єктами переказу грошей, тому на них можуть поширюватися закони, які регулюють таку діяльність.

В Ізраїлі, наприклад, майнінг криптовалют розглядається як бізнес та обкладається податком на прибуток підприємств. В Індії та в інших країнах зберігається регуляторна невизначеність, хоча Канада і США здаються дружніми до майнінгу криптовалют.

Однак, окрім юрисдикцій, які спеціально заборонили діяльність, пов'язану з криптовалютою, дуже мало країн забороняють майнінг криптовалют.

Японія була однією з провідних країн світу, яка дозволила майнінг та торгівлю криптовалютою. Видобуток криптовалюти є законним в Японії, але оператори повинні зареєструватися в Агентстві фінансових послуг і дотримуватися ряду правил безпеки, захисту клієнтів та боротьби з відмиванням грошей. Для забезпечення прозорості уряд також вимагає від майнінгових компаній розкривати свою операційну і фінансову інформацію.

Керівництво FATF з ризикорієнтованого підходу «Віртуальні валюти. Ключові визначення та потенційні ризики ПВК/ФТ» [11] дає визначення поняттю «майнер». Майнер – це фізична або юридична особа, яка бере участь у децентралізованій мережі віртуальних валют, запуску спеціального програмного забезпечення для розв'язання складних алгоритмів у розподіленій системі, підтвердження роботи чи іншій розподіленій системі доказів, яка використовується для перевірки транзакцій у системі віртуальної валюти. Майнери можуть бути користувачами, якщо вони самостійно генерують конвертовану віртуальну валюту виключно для власних цілей, наприклад, для зберігання, інвестування або використання – для оплати існуючого зобов'язання або придбання товарів чи послуг. Майнери також можуть брати участь у системі віртуальної валюти як обмінники, створюючи віртуальну валюту як бізнес, щоб продати її за фіатну або іншу віртуальну валюту [11, с. 7]. Цим Керівництво визнає, що майнінг криптовалют прирівнюється до постачальників криптовалютних послуг (VASP) та має потенційні ризики, які властиві таким суб'єктам ринку.

Європейський Регламент MICA [9] охоплює криптоактиви, які не регулюються чинним законодавством про фінансові послуги. Ключові положення для тих, хто випускає та торгує криптоактивами (включаючи токени фінансових активів і токени електронних грошей), стосуються прозорості, розкриття інформації, авторизації та контролю за транзакціями. Крім того, нова правова база підтримуватиме цілісність ринку та фінансову стабільність

шляхом регулювання публічних пропозицій криптоактивів. Однак цей Регламент не містить чіткого визначення поняття «майнінг криптовалют» і способів регулювання такої діяльності [9].

Саме поняття «майнінг» в українському законодавстві ще не має чіткого визначення. Прийнятий Закон України «Про віртуальні активи» від 14.12.2021 р. № 1953-IX [12] і Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 р. № 361-IX [13] не містять ні поняття майнінгу, ні емітента криптовалют, а також умов і законних підстав діяльності емітентів криптовалют. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» визначає постачальника послуг як суб'єкта, який провадить один або більше вид діяльності: обмін віртуальних активів, переказ віртуальних активів, зберігання та/або адміністрування віртуальних активів або інструментів, що дають змогу контролювати віртуальні активи, участь і надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажем віртуальних активів.

Актуальним і не вирішеним питанням наразі є належність цього виду діяльності до певної класифікації видів діяльності (КВЕД), установлені законодавством, оскільки в існуючій класифікації майнінг прямо не передбачено [15]. В рамках чинної класифікації майнінг відповідає класу 63.11 «Оброблення даних, розміщення інформації на вебвузлах і пов'язана з ними діяльність». Цей клас містить «надання інфраструктури для розміщення (хостингу), оброблення даних і пов'язану з цим діяльність» та «оброблення даних: повне оброблення даних, отриманих від клієнта, складання спеціалізованих звітів на основі даних, отриманих від клієнта».

Чинне законодавство не передбачає спеціальної дозвольної системи щодо майнінгу криптовалют як такого. Разом з тим, відповідно до Постанови Кабінету Міністрів України від 16.11.2016 р. № 821 ліцензуванню підлягають такі послуги: «технічне обслуговування (супроводження)... криптосистем і засобів криптографічного

захисту інформації». Відповідно, якщо майнінг стосується технічного обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації, то надання послуг із нього є ліцензованим видом діяльності. Згідно з п. 2 згаданої постанови, «технічне обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації – операція або комплекс операцій з підтримання криптосистем і засобів криптографічного захисту інформації у справному і придатному для експлуатації стані під час їх використання за призначенням відповідно до вимог експлуатаційної документації розробника (виробника) щодо криптосистем і засобів криптографічного захисту інформації та нормативної документації щодо криптосистем і засобів криптографічного захисту інформації» [14].

Майнінг біткойна розвивається в національній криптосистемі завдяки мінливим потребам ентузіастів. Для залучення та розвитку великих компаній з ефективною економічною складовою необхідно розробити стандарти безпеки, законодавчі рамки і заходи відповідальності з мінімізацією впливу на навколишнє середовище, в тому числі й використання альтернативних джерел енергопостачання та запобіжні заходи щодо шахрайства в майнінгу криптовалют, виходячи з найкращих міжнародних практик майнінгу та рекомендацій міжнародних організацій.

Незважаючи на регулятивні проблеми і ризики, майбутнє майнінгу криптовалют виглядає перспективним, а майнінг біткойнів є одним з найприбутковіших варіантів на ринку криптовалют. Потреба в регулюванні криптовалют та регулюванні майнінгу криптовалют лише зростатиме. Тому є необхідність надати інвесторам чіткіше уявлення про те, як діяти в межах своєї правової юрисдикції в окремій країні. Оскільки цифрові рішення продовжують революціонізувати в різних галузях, очікується, що криптовалюта відіграватиме вирішальну роль у формуванні майбутнього фінансів і технологій, а видобуток криптовалют, безумовно, зробить значний внесок у цю еволюцію. Таким чином, видобуток криптовалют як життєво важливий компонент цієї екосистеми є невід’ємною частиною віртуальних активів.

Література

1. Annual number of cryptojacking attempts worldwide from 2018 to 2022. URL: <https://www.statista.com/statistics/1377860/worldwide-annual-number-cryptojacking/>
2. Bai, Q.; Zhou, X.; Wang, X.; Xu, Y.; Wang, X.; Kong, Q. A Deep Dive into Blockchain Selfish Mining. arXiv 2018, arXiv:1811.08263.
3. Bastiaan, M. Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin; 2015. URL: <https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf>
4. Cryptocurrency Mining Market (By Offering: Hardware, Software; By Process: Mining, Transaction; By Type: Bitcoin, Ethereum, Bitcoin Cash, Ripple, Litecoin, Dash, Others; By End-User: Trading, E-commerce and Retail, Peer-to-Peer Payment, Remittance) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023-2032. URL: <https://www.precedenceresearch.com/cryptocurrency-mining-market>
5. Daniel Barta. IOTA: The Currency of Skynet. 2018. URL: <https://hackernoon.com/iota-the-currency-of-skynet-281b6abaec5>
6. IOTA. What Is IOTA? URL: <https://www.iota.org/get-started/what-is-iota>
7. Fintech Notes. Regulations of crypto assets. Note/19/03. Cristina Cuervo, Anastasia Morozova, Nobuyasu Sugimoto. URL: <file:///Users/Valerii/Downloads/FTNEA2019003.pdf>
8. Guidance for a risk-based approach to virtual currencies / FATF-GAFI. URL: <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
9. Markets in crypto-assets (MiCA). URL: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2022\)739221](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221)
10. Matt. Bitcoin's Attack Vectors: 51% Attacks. 2018. URL: <https://medium.com/chainrift-research/bitcoins-attack-vectors-51-attacks-a96deac43774>.
11. Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. URL: <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html>

12. Закон України «Про віртуальні активи» від 14.12.2021р. № 1953-IX. URL:<https://zakon.rada.gov.ua/laws/show/2074-20#Text>
13. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 р. № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>
14. Зелена книга регулювання ринку криптовалют / Офіс ефективного регулювання. 2018. Травень. URL: <https://regulation.gov.ua/book/91-zelena-kniga-reguluvanna-rinku-kriptovalut>.
15. Класифікація видів економічної діяльності – 2010 (КВЕД). URL: http://kved.ukrstat.gov.ua/KVED2010/63/KVED10_63_11.html.
16. Що таке криптоджекінг? URL:<https://coinmarketcap.com/academy/uk/glossary/crypto-jacking>
17. ЦО ТАКЕ ПУЛИ ДЛЯ МАЙНІНГУ БІТКОЇНІВ? URL:<https://bitcoinmagazine.ua/guides/1671039757-shcho-take-puli-mayningu-bitkoiniv>