«АКТУАЛЬНІ ПРОБЛЕМИ ІННОВАЦІЙНОЇ ЕКОНОМІКИ»

Науковий журнал

(Свідоцтво про державну реєстрацію друкованого засобу масової інформації Міністерства юстиції України серія КВ № 21710-11610Р від 13.10.2015 р.).

Журнал включений до Переліку друкованих наукових фахових видань в галузі економічних наук наказом Міністерства освіти і науки України від 11.07.2016 № 820

Міжнародний Центр періодичних видань (ISSN International Centre, Париж) включив журнал до міжнародного реєстру періодичних засобів масової інформації і надав йому числовий код міжнародної ідентифікації: ISSN 2524-0455 (Print).

Журнал індексується в Міжнародній наукометричній базі Index Copernicus International

Видається мовами: українською, російською, англійською, 4 номери на рік.

Засновник і видавець:
Харківський національний технічний університет сільського господарства імені Петра Василенка (ХНТУСГ).

Адреса редакції:
Україна, 61002, м. Харків, вул. Алчевських, 44, каб. 309.
Тел.: (057) 7-164-168; (057) 7-164-154, E-mail: apie@ukr.net

Рекомендовано до друку Вченою радою Харківського національного технічного університету сільського господарства імені Петра Василенка. Протокол № 1 від 27.09.2018 р.

Підписано до друку 29.09.2018 р.
Формат 60×84 1/8. Папір офсетний. Гарнітура Book Antiqua. Офсетний друк.
Умовн. друк. арк. — 9,9. Наклад — 300 прим. Зам. № __.
Видавництво «Стильна типографія». Свідоцтво суб'єкта видавничої справи: серія ДК № 5493 від 22.08.2017 р.
61002, м. Харків, вул. Чернишевська, 28 А Тел.: (057) 754-49-42 e-mail: zebraprint.zakaz@gmail.com

ISSN 2524-0455

«Актуальні проблеми інноваційної економіки»

науковий журнал

№ 4 / 2018

ЗМІСТ

Конкурентні та організаційно-управлінські аспекти інноваційного розвитку

РАЙТЕР Н. І, ЖЕЛЄЗНЯК А. М., КРУПА О. М. Професійні покупці споживчих товарів як елемент конкурентного середовища підприємств оптової торгівлі 5

ГРИНЬ Є. Л. Програмно-проектний підхід до управління організаційними змінами на підприємстві 11

ХАЧАТУРЯН Б. О. Науково-теоретичні засади управління витратами у створенні цінових конкурентних переваг 16

ТЕРЕЩЕНКО Л. В. Методичний підхід щодо визначення готовності персоналу до проведення організаційних змін на підприємстві 22

Фінансовий інструментарій інноваційного розвитку

ОРЄХОВА А. І. Аналіз стану фінансового потенціалу аграрних підприємств 28

БОЙКО О. Г. Ризики для економічної безпеки з боку платіжних систем на основі технології розподіленого реєстру Блокчейн 32

ІВАНЧЕНКОВА Л. В. Методичні аспекти моніторингу фінансової стабільності підприємств корпоративного сектору харчової промисловості 41

Макроекономічні тенденції інноваційного розвитку

ГУТОРОВ А. О. Ґенеза формування парадигми інклюзивного розвитку національної економіки 47

НІЩЕНКО В. С., САГАЙДАК М. П., БЕРЕЖНА Ю. Г., ЦУКАНОВ О. Ю. Соціально-економічні імперативи стану та розвитку овочевого ринку: макроекономічний аспект 53

KOTLYK A. V., JAMAL Y. Methodical approach to analysis of volatility, uncertainty, complexity and ambiguity of the external environment 65

ЛАРІНА Т. Ф., ДАНИЛЕНКО В. В. Економіка України крізь призму інституційної теорії світового розвитку. 69

Розвиток сільських територій та земельних відносин

ГРОШЕВ С. В. Управління ланцюгами створення цінності в контексті підвищення ефективності використання земельних ресурсів фермерських господарств. 76

МОІСЄЄВА Н. І., ДІДЕНКО Д. Ф. Генезис та особливості формування регіонального ринку туристичних послуг. 83

ДОВГАЛЬ О. В. Стан та особливості використання природно-ресурсного потенціалу сільських територій 88

ОРЕЛ А. М. Мотиваційний процес децентралізації розвитку сільських територій. 95

«Actual problems of innovative economy»

the scientific journal

№ 4 / 2018

CONTENT

Competitive, organizational and managerial aspects of innovative development

REITER N. I., ZHELEZNYAK A. M, KRUPA O. M. Professional buyers of consumer goods as an element of the competitive environment wholesalers……..... 5

HRYN YE. L. Program-project approach to organizational changes management at the enterprise..... 11

KHACHATURIAN B. O. Cost management theoretical principles in creating price competitive advantages 16

TERESHCHENKO L. V. Methodical approach to determining the personnel readiness to make organizational changes at an enterprise 22

Financial instrument for innovation development

ORIEKHOVA A. I. Analysis of the state of financial potential of agrarian enterprises..... 28

BOIKO O. Risks for economic security from payment systems based on distributed ledger technology Blockchain 32

IVANCHENKOVA L. V. Methodological aspects of the financial stability monitoring enterprises of the food industry corporate sector 41

Macroeconomic trends of innovation development

HUTOROV A. O. Genesis of forming a paradigm of inclusive development of the national economy 47

NITSENKO V. S., SAHAIDAK M. P., BEREZHNA YU. H., TSUKANOV O. YU. Socio-economic imperatives of the state and the development of the vegetable market: the macroeconomic aspect. 53

KOTLYK A. V., JAMAL Y. Methodical approach to analysis of volatility, uncertainty, complexity and ambiguity of the external environment..... 65

LARINA T. F., DANYLENKO V. V. Ukraine`s economy through a prism of the world development institutional theory. 69

Rural territories and land relations development

GROSHEV S. V. Value chains creation management in the context of increasing efficiency of farms' land resources using..... 76

MOISEEVA N. I., DIDENKO D. F. Genesis and features of forming of regional market of tourist services. Actual problems of innovative economy.. 83

DOVGAL O. V. Status and features of the natural resource potential use of rural areas. 88

OREL A. M. Motivational process of decentralization of rural territories development 95

определить резервы улучшения его финансового состояния и платежеспособности, а также способствует повышению эффективности использования его финансовых ресурсов. Определено, что анализ финансового потенциала предприятий является необходимым этапом стратегического анализа и управления. Как следствие, обеспечивается системный подход к оценке предприятия и его потенциала.

***Ключевые слова**: потенциал, финансовый потенциал, анализ, аграрные предприятия, стратегическое управление.*

Abstract.

Oriekhova A. I. Analysis of the state of financial potential of agrarian enterprises.

It is proved that the management of the financial potential of the enterprise is inextricably linked with the approved strategic objectives of the entity, access to capital markets and the quality of the current management system. The analysis of the parameters of the financial potential of agrarian business entities of Ukraine is carried out, which allows to identify and eliminate deficiencies in the financial activity of the enterprise, to determine the reserves for improving its financial status and solvency, as well as to increase the efficiency of using its financial resources. It is determined that the analysis of financial potential of enterprises is a necessary stage of strategic analysis and management. As a consequence, a systematic approach to assessing the company and its potential is provided.

***Key words**: potential, financial potential, analysis, agrarian enterprises, strategic management.*

Стаття надійшла до редакції 15.09.2018 р.

Бібліографічний опис статті:

Орєхова А. І. Аналіз стану фінансового потенціалу аграрних підприємств. Актуальні проблеми інноваційної економіки. 2018. № 4. С. 28-32.

Oriekhova A. I. Analysis of the state of financial potential of agrarian enterprises. Actual problems of innovative econoty. 2018. No 4, pp. 28-32.

УДК 336.744

БОЙКО О. Г.
аспірант кафедри міжнародних фінансів
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана» (Київ, Україна)

РИЗИКИ ДЛЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ З БОКУ ПЛАТІЖНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ РОЗПОДІЛЕНОГО РЕЄСТРУ БЛОКЧЕЙН

Бойко О. Г. Ризики для економічної безпеки з боку платіжних систем на основі технології розподіленого реєстру Блокчейн.

Міжнародні платіжні системи дуже швидко розвиваються під впливом технологічних інновацій. Технологія розподіленого реєстру Блокчейн започаткувала новий напрямок в здійсненні міжнародних платежів – криптовалюти. Криптовалюти характеризуються високою варіативністю в технологічних, технічних та економічних характеристиках, що ускладнює аналіз їх корисності для суспільства. Стаття присвячена розгляду ризиків для економічної безпеки від використання платіжних систем на основі Блокчейн, використовуючи при цьому ієрархію економічної безпеки від мікро- до мегарівня. Наведено внутрішні ризики, притаманні криптовалютам, вказано на перспективність конкретизації ризиків окремо для централізованих, розподілених та децентралізованих криптовалют.

***Ключові слова:** криптовалюта, Блокчейн, економічна безпека, платіжні системи, майнинг, ризики, розподілений реєстр.*

Постановка проблеми у загальному вигляді. Вплив електронних технологій на життя людини є всеохоплюючим і міжнародна системи розрахунків не є винятком. Практика міжнародних платежів демонструє стрімкий розвиток, який знаходиться значно попереду свого теоретичного осмислення. Технологія розподіленого реєстру Блокчейн наразі знаходиться в основі криптографічних платіжних систем, до яких проявляється сильний інтерес як в світі, так і в Україні.

Розподілений реєстр включає набір технологічних рішень, які забезпечують єдиний, послідовний, стандартизований та криптографічно-захищений облік діяльності, що безпечно розподіляється та використовується мережею перевірених учасників. Наприклад, такий облік може стосуватися транзакцій або активів. Блокчейн є типом технології розподіленого реєстру, згідно якої записи збираються в

[1]*Наразі існує три законопроекти стосовно ринку криптовалют та їх похідних в Україні: 7246, 7183 та 7183-1.*

блоки, що пов'язуються за допомогою криптографічного підпису. Дана технологія представляє собою систему управління розподіленої бази даних, яка дозволяє учасникам обробляти, зберігати та ділитися даними між багатьма вузлами в мережі. Тобто численні суб'єкти мають доступ до одних і тих самих даних практично в реальному часі [1, с. 10–11].

Однак використання даної технології пов'язано з численними ризиками, яким і присвячене дане дослідження і саме тому в його центрі знаходиться технологія розподіленого реєстру в контексті міжнародних розрахунків та економічної безпеки.

Аналіз останніх досліджень і публікацій. Для виконання завдань дослідження використано ієрархію видів економічної безпеки від особистого до глобального рівнів, запропоновану В. Токарем [2]. Вітчизняними вченими, які вивчають феномен криптовалюти з позиції кількох економічних теорій є В. Варцаба та Е. Мостіпака [3]. Американські дослідники Дж. Бонно, А. Міллер, Е. Фелтен, С. Голдфедер та А. Нараянан [4] детально аналізують технологію Блокчейн, на якій побудовані криптографічні системи міжнародних розрахунків. С. Чапман [5] описує IT-концепцію слухання подій, а Б. Ластер [6] визначає методику роботи з омп'ютерним кодом «fork-and-pull», які використано для пояснення процесу емісії (майнингу) криптовалюти. Також посилаємося на власне дослідження криптовалюти з технологічної [7] та техніко-економічної [8] точок зору.

Формулювання цілей статті. Метою роботи є встановлення внутрішніх ризиків, які походять від провайдерів платіжних систем, на основі технології Блокчейн у контексті економічної безпеки. Завданнями даного дослідження є визначення економічної безпеки та технології розподіленого реєстру, описання процесу надання та емісії криптовалюти (майнингу) та моделювання відхилення поведінки провайдера платіжної системи від поведінки за замовчуванням.

Виклад основного матеріалу дослідження. Економісти-неокласики визначають економіку як виробництво, розподіл, перерозподіл, обмін та споживання благ, які у ринковій економіці існують у формі товарів та послуг. Вчені вказують, що під впливом електронних технологій також відбувається зміна форми цих процесів з фізичної на цифрову [9]. На нашу думку, поповнення арсеналу продуктивних сил технологією розподіленого реєстру, широко відомою під назвою Блокчейн, призводить до появи нових видів економічної взаємодії, які характеризуються тяжінням до децентралізації та цифровою формою. Разом з тим виникають і нові ризики, що доцільно розглядати в контексті економічної безпеки.

Ієрархія економічної безпеки від найнижчого до найвищого рівня вже детально розроблена [2, с. 17]. В межах даного дослідження економічна безпека визначається як ступінь включення суб'єкта відповідного рівня у процеси виробництва, розподілу, перерозподілу, обміну та споживання благ.

З точки зору економічної безпеки під ризиком від запровадження платіжних систем на основі Блокчейн варто розумітимемо виключення суб'єкта відповідного рівня або з економічного циклу в цілому, або з якоїсь його частини зокрема.

Розподілений реєстр (distributed ledger) – це результат реєстрації певних подій, повноваження на здійснення якої розподіляється певним чином серед провайдерів. Блокчейн (Blockchain) дослівно означає «ланцюг з блоками» і є однією із форм розподіленого реєстру, тому що зареєстровані події збираються в блоки, а блоки розміщуються на часовій основі в ланцюг, який має властивість append-only, тобто є відкритим лише на додавання, але не на зміну вже існуючих блоків (**Помилка! Джерело посилання не знайдено.**).

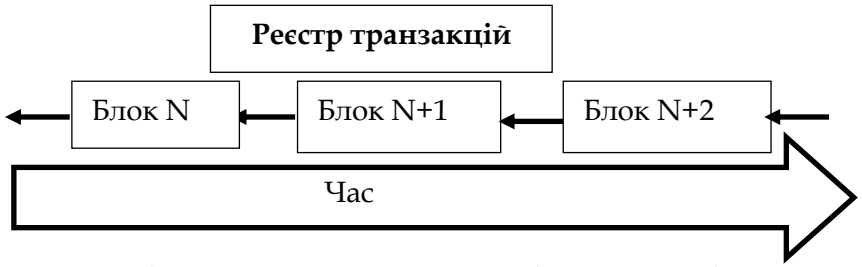

Рис. 1. Оформлення даних у вигляді ланцюга з блоками

Джерело: узагальнено автором на основі [4].

Так, події в блоці *N+1* беруть до уваги всі події, що записані у попередніх блоках, тому для валідації подій необхідно мати повний блоковий ланцюг, починаючи з Блоку *1* і закінчуючи Блоком *N*. У контексті криптовалюти подіями виступають платіжні транзакції, зареєстровані протягом певного часового інтервалу, які разом з емісійною транзакцією формуються в блок. Повноваження на формування блоків та їх додавання до ланцюга розподіляються або серед закритої, або відкритої групи суб'єктів. В першому випадку мова йтиме про централізовані та розподілені бази даних, а в другому – про децентралізовані. На Рис. 2 (зліва) зображено закриту централізовану систему, в центрі якої знаходиться один провайдер (який інколи ще називають нодом) з виключними повноваженнями з реєстрації транзакцій. На Рис. 2 (справа) зображена закрита розподілена система, в якій повноваження з реєстрації надані привілейованій групі нодів, приєднання до якої вимагає відповідного дозволу або неможливе. Тобто користувачі платіжної системи на основі Блокчейн, використовуючи ПК або смартфони, транслюють транзакції, які збираються, валідуються та додаються у вигляді блоків провайдерами до бази даних Блокчейн.

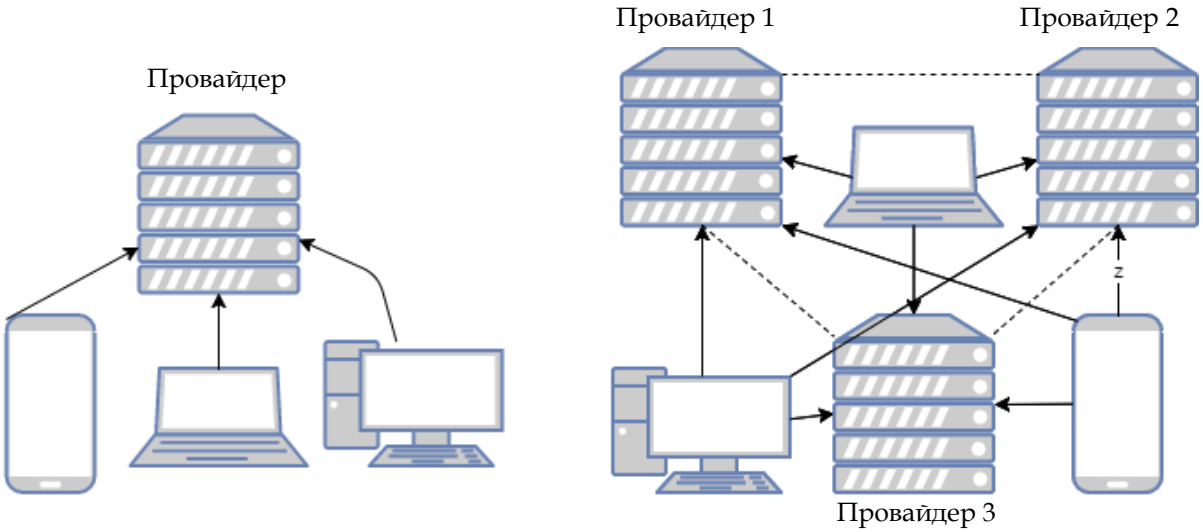

Рис. 2. Централізована і розподілена платіжні системи, в яких повноваження щодо зберігання та оновлення даних є закритими

Джерело: узагальнено автором на основі [6].

Також зазначимо, що централізовану систему можна розглядати як розподілену, в якій привілейована група складається всього з одного ноду, і так само розподілена система може виявитися в певному сенсі централізованою, якщо всі провайдери насправді підпорядковуються єдиному центру.

Рис. 3 демонструє відкриту децентралізовану систему, в якій повноваження з реєстрації є загальнодоступними. У децентралізованій системі будь-хто може отримати повноваження провайдера і здійснювати реєстрацію транзакцій разом з іншими нодами. Зі збільшенням рівня децентралізованості платіжна система функціонує більш автономно, в результаті чого виправлення помилок і колізій, які поширюються на всіх користувачів, стає складним завданням, тому що немає єдиного центру контролю, а повноваження концентруються здебільшого в розробників та девелоперів децентралізованої платіжної системи.

Через те, що кількість нодів-провайдерів реєстру транзакцій є здебільшого більшою за одного, передбачаються і відповідні правила вибору лідера, які часто називають консенсус-алгоритмом системи, тобто ті правила, згідно яких здійснюється вибір ноду, який додає наступний блок до ланцюга блоків Блокчейн. Для централізованої та розподіленої (тобто закритих) платіжних систем прийнятним консенсус-алгоритмом є, наприклад, такий, згідно якого вибір лідера кожен раз здійснюється випадковим чином. З іншого боку, для відкритих (децентралізованих) систем більш прийнятними правилами вибору лідера є ті, що базуються на обчислювальній потужності нодів. Наприклад, якщо обчислювальна потужність комп'ютера провайдера становить *25%*, то приблизно кожен четвертий блок буде реєструватися цим нодом. Якщо позначити частку обчислювальної потужності провайдера як *a*, то частота реєстрації складатиме *1/a*, що в даному прикладі становитиме кожен четвертий блок *1/0.25 = 4*. Таким чином, визначимо криптографічну валюту як віртуальну валюту, яка існує у формі розподіленого або децентралізованого ланцюга блоків Блокчейн, повноваження з підтримання якого належать певній групі провайдерів. Для більш детального ознайомлення з

технологічними характеристиками застосування Блокчейн у платіжних системах, які дістали назву криптографічних, посилаємося на наше попереднє дослідження даної технології за методом аналогії [7].

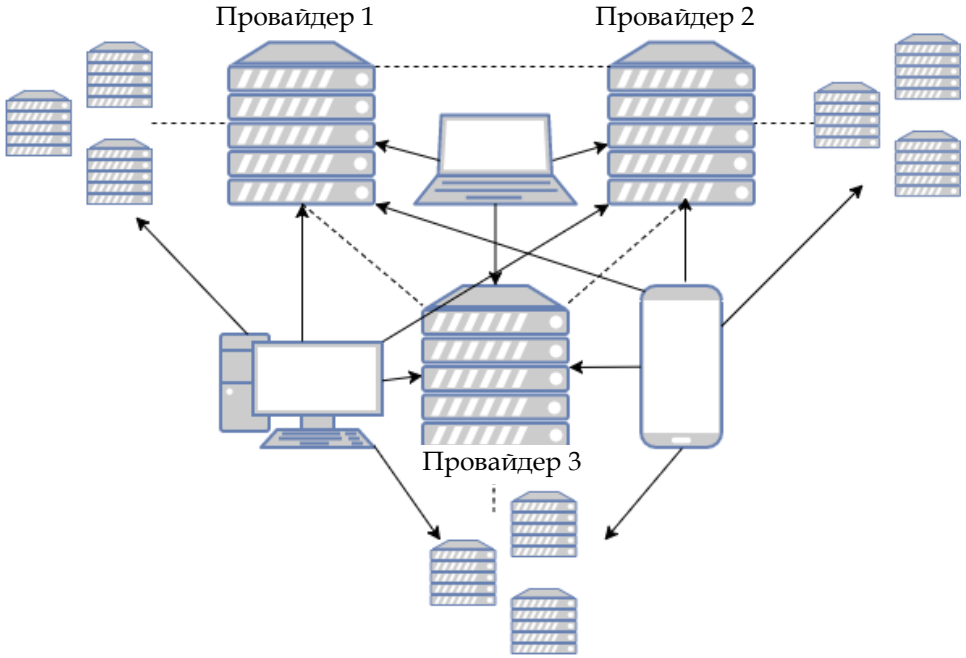

Рис. 3. Децентралізована платіжна система

Джерело: узагальнено автором на основі [6].

Управління по фінансовому нагляду і регулюванню, яке є головним наглядовим органом за ринком фінансових послуг Великобританії, досліджує вплив технології розподіленого реєстру на фінансову сферу. Дана установа визначає віртуальну валюту як будь-який публічно доступний електронний засіб обміну, який використовує розподілений реєстр та децентралізовану систему обміну вартістю [1, с. 11].

Слід відрізняти звичайних користувачів криптографічної системи розрахунків від її провайдерів: перші лише здійснюють транзакції, в той час як другі займаються зберіганням, реєстрацією, валідацією, групуванням транзакцій в блоки та трансляцією блоків. Програма-клієнт надає змогу здійснювати вищезгадані операції і має базові налаштування, які кожен провайдер може змінити і здійснювати обробку транзакцій «за власними правилами». Біткоін-майнер може обрати іншу модель поведінки, якщо вона буде в його інтересах і відповідно налаштувати свою програму-клієнт стосовно того:

- ✓ які з почутих транзакцій включати у власний блок, а які ігнорувати. Наприклад, можна ігнорувати всі транзакції, що забезпечать меншу комісійну винагороду за певне очікуване значення, або належать до "чорного списку";
- ✓ на основі якого почутого блоку здійснювати формування власного блоку. Типова поведінка передбачає продовження найдовшого почутого ланцюга;
- ✓ який слід обирати блок, якщо приблизно в один і той самий час було почуто одразу декілька блоків. У такому випадку тимчасово виникає "розгалуження" ("fork"), і за замовчуванням обирається той блок, який було почуто першим;
- ✓ коли транслювати власні створені валідні блоки [4, с. 130–131].

Тому постає питання, за яких умов відбудеться компрометація децентралізованої валюти, якщо кожен провайдер приймає стратегічне рішення стосовно того, які транзакції слід включати і як формувати ланцюг блоків. Крім того, чому провайдерів криптовалют часто порівнюють з золотошукачами та називають майнерами, а їх діяльність з формування блоків з транзакціями – майнингом? Та які ризики виникають при децентралізованому, а не централізованому дизайні платіжної системи?

В об'єктно-орієнтованому програмуванні під подіями ("events") розуміють оповіщення, які транслюються об'єктом, коли щось з ним відбувається. Прикладом може бути зміна значення однієї

з властивостей об'єкта або внесення користувачем даних за допомогою клавіатури або мишки. Слухачами ("listeners") прийнято називати об'єкти, які виконують певний метод, будучи оповіщенні про настання очікуваної події. Програми використовують події для комунікації того, що трапляється з об'єктами та відповідають на ці події шляхом виконання методів (функцій зворотного виклику), які належать об'єктам-слухачам [5, с. 501].

У платіжній системі Біткоін програма-клієнт майнера криптовалюти «слухає» нові транзакції в мережі та виконує у відповідь валідаційні методи, які перевіряють коректність цифрових підписів в транзакціях та наявність грошей на рахунках, з яких здійснюються платежі. Програма-клієнт також актуалізує базу даних, слухаючи нові блоки з транзакціями та додаючи їх до блокового ланцюга. Почувши про блок, майнер виконує у відповідь валідаційний метод над всіма транзакціями в почутому блоці, а також перевіряє відповідність хешу блоку певному критерію, наприклад, що даний хеш дійсно починається з *N*-ї кількості 0. Остання перевірка має на меті засвідчити виконану майнерську роботу тим провайдером, який створив блок. Маючи актуальний блоковий ланцюг, майнер починає будувати свій власний блок, групуючи почуті перевірені транзакції. Якщо ним випадково або навмисно включиться в блок невалідна транзакція (транзакція вважається невалідною, якщо виплату з публічного ключа-рахунка не було підписано відповідним йому приватним ключем), то такий блок не зможе пройти перевірку і бути прийнятим іншими провайдерами. Сформувавши блок, починається виконання трудомісткого ітеративного процесу з пошуку такого значення хеш-функції, яке відповідає певному критерію, як-то починатися за *N*-ї кількості 0. Аргументами в хеш-функцію слугують зібрані платіжні і одна емісійна транзакції та довільний одноразовий код («nonce»). Емісійна транзакція додається майнером в блок для створення абсолютно нових грошових одиниць на користь адреси, що йому належить.

Зараз опишемо суть майнингу, тобто виконання певної обчислювальної роботи, яка засвідчує обчислювальну потужність провайдера. Нижчеописана модель визначає типову поведінку провайдера децентралізованої криптовалюти біткоін, яка побудована на найпоширенішому консенсус-алгоритмі proof-of-work.

Перш за все, слід вказати, що властивістю хеш-функції *H()* є відсутність колізій, тобто неможливо знайти два відмінні аргументи *x* і *y*, та отримати однакове значення функції: якщо $x \neq y$, то $H(x) \neq H(y)$. Тому підбір значень хеш-функції здійснюється за допомогою ітерування над підконтрольними майнеру змінними – довільного одноразового коду, який для цього і включається в блок, та запису в емісійній транзакції. Слід також зазначити, що змінюючи вимоги до хешу блоку, наприклад зменшуючи кількість 0, на які може починатися валідний хеш, в криптографічній платіжній системі можна варіювати складність майнингу. В Біткоін таке калібрування здійснюється раз на два тижні, при якому спочатку оцінюється сукупна обчислювальна потужність всіх підключених майнерів, а потім встановлюються такі вимоги до хешу блоку, щоб в системі створення блоку відбувалося в середньому один раз кожні 10 хвилин. Дослідники вказували, що в 2016 році приблизно 1 з 2^{68} майнингових ітерацій в Біткоін призводила до отримання валідного хешу блоку. Нарешті, створивши валідний блок, провайдер транслює його в мережу та очікує на прийняття свого блоку іншими майнерами при здійсненні ними майнингу наступних блоків. Після укорінення блоку в Блокчейн, майнер не лише отримує змогу використати земітовані гроші з емісійної транзакції, а і додатково збирає комісійну винагороду, яка як-правило включається користувачами в платіжні транзакції. Таким чином можна побачити, що саме ітеративний процес пошуку прийнятного хеш-значення власного блоку і є майнингом, а не просто підрахунок хеш-значення відібраних транзакцій, як може здатися на перший погляд. Підсумовуючи вищесказане, майнинг можна визначити як процедуру вибору лідера з-поміж провайдерів для додавання наступного блоку в ланцюг, що здійснюється на основі виконаної обчислювальної роботи. Така процедура дістала назву proof-of-work, оскільки майнери визнають лише ті почуті блоки, створення яких потребувало достатніх обчислювальних затрат.

Як зазначають дослідники біткоін, винагорода від майнингу на 99% складається з емітованої криптовалюти і лише на 1% з «чайових», які в довільному порядку

надаються ініціаторами платіжних транзакцій. Тобто тіснота зв'язку між емісійним механізмом і стимулом до майнингу має братися до уваги архітекторами платіжних систем, особливо при необхідності контролювати грошову пропозицію. Темп емісії біткоін, тобто приріст криптовалюти за певний період, нагадує логарифмічну функцію, оскільки кожні 4 роки розмір майнерської винагороди зменшується на половину і номінал емісійної транзакції відповідно становитиме 25, 12.5, 6.25... біткоіна за блок [10, с. 33–34].

Провайдери криптовалюти транслюють створені блоки, в результаті чого створюється ланцюг блоків, який і становить децентралізовану базу даних Блокчейн. Правила створення блокового ланцюга – це ще один компонент технології розподіленого реєстру, який описано з використанням терміну «розгалуження».

Взагалі, термін «розгалуження або вилка («fork») запозичено з методики розробки програмного забезпечення під назвою «fork-and-pull», яку доцільно використовувати при роботі багатьох програмістів над комп'ютерним кодом одного проекту. Так, у віддаленому репозитарії на сервері розміщено актуальний код проекту разом з усіма попередніми його версіями. Власник коду, здійснюючи якісь зміни, створює нову версію, зберігаючи при цьому попередні версії коду. Фактично, кожна нова версія базується на попередній і має свою унікальну назву – хеш. Можна провести аналогію з таким написанням тексту в редакторі MS Word, при якому автором час від часу, наприклад при завершенні або корегуванні абзацу, створювалася б копія всього документу у форматі «.doc», якій присвоювалося б унікальне ім'я так, що через деякий час у автора назбиралося б чимало версій його твору, які логічно можна поєднати в ланцюг. Дану конструкцію вже можна порівняти з блоковим ланцюгом, але спершу зробимо розширення, змоделювавши роботу молодшого співавтора, який не є власником твору, над цим самим проектом за моделлю fork-and-pull. Щоб внести зміни, співавтор розгалужує віддалений репозитарій, тобто отримує повну копію проекту, що дозволяє обом авторам незалежно працювати над текстом вищеописаним чином, час від часу створюючи нові копії твору [6, с. 369]. Таким чином, виникають дві гілки – основна і додаткова. Здійснивши корективи, співавтор здійснює pull-запит до автора на злиття своєї гілки в основну, який автор може або прийняти, або відхилити, якщо зміни його не влаштують. Це ілюструє ситуацію, коли молодший співавтор копіює авторську версію файлу, розгалужуючи при цьому репозитарій, і вносить зміни в додатковій гілці, після чого ним робиться запит на злиття розгалуження в основну гілку, так що в результаті як зміни головного автора, так і молодшого співавтора потрапляють в єдиний файл.

Слід вказати на подібність fork-and-pull та Блокчейн, в якій також трапляються розгалуження, але не злиття гілок, оскільки завжди існуватиме одна головна гілка з блоками, яка і вважатиметься майнерами валідною. Відповідно, лише транзакції в блоках головної гілки відображатимуться в базі даних, а транзакції, які потрапили лише до допоміжної гілки – ні.

В Блокчейн операційні розгалуження постійно відбуваються на рівні майнингу криптовалюти, оскільки гілки конкурують між собою за право називатися основним блоковим ланцюгом (див. Рис. 4).

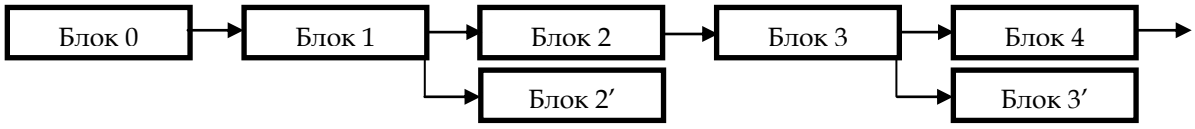

Рис. 4. Операційні розгалуження в Блокчейн [11]

Крім операційних розгалужень існують також слабкі та сильні розгалуження («soft and hard forks»). Слабкі розгалуження відбуваються внаслідок апгрейду програми-клієнта, після якого правила валідації транзакцій програми-клієнта стають жорсткішими так, що нові майнери не акцептуватимуть блоки, створені старими майнерами, оскільки вони можуть містити невалідні транзакції згідно нових правил.

Сильні розгалуження виникають тоді, коли після зміни параметрів і правил криптографічної системи з виходом нової версії клієнт-програма починає акцептувати блоки, які вважаються невалідними в старій версії. Таким чином, фактично найдовша гілка міститиме блоки, які вважатимуться

невалідними старими майнерами, що залишаться працювати на іншій гілці [4, с. 73–74]. У 2017 році в Біткоін вперше відбулися два сильні розгалуження, в результаті чого започаткувалися дві криптовалюти, які також були оформленні під власними брендами Bitcoin Cash і Bitcoin Gold, а в 2018 році відбулося ще одне сильне розгалуження з утворенням Bitcoin Private (рис. 5).

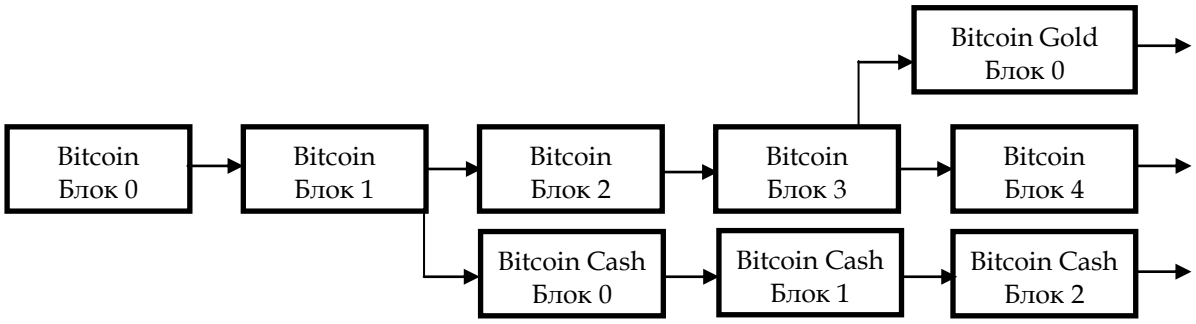

Рис. 5. Перманентні розгалудження в Bitcoin Блокчейн в 2017 році
Джерело: узагальнено автором на основі [12].

Вартує уваги є, що власники криптовалюти після сильного розгалуження можуть незалежно здійснювати транзакції на обох гілках, тобто їх кошти подвоюються. Умовно кажучи, на рис. 5 залишок криптовалюти в блоці 1 стає доступним як Bitcoin, так і Bitcoin Cash.

Ознайомившись з механізмом функціонування криптографічної валюти, можна встановити ризики, що походять від її провайдерів, коли ті відхиляються від поведінки за замовчуванням.

Вищезгадані поняття розгалуження та гілки дозволяють більш широко розкрити термін майнерської атаки – прибуткового відхилення від очікуваної поведінки, яку потенційно може здійснити провайдер криптовалюти, припускаючи, що його частка в обчислювальній потужності системи становить $0 < a \leq 1$. З однієї сторони, атака є суттєвим фактором ризику, оскільки може призвести до тимчасової або перманентної відмови сервісу та панікою на форекс-ринку такої криптовалюти. З іншої сторони, слід наголосити на тому, що провайдер ніяк не в змозі ініціювати валідну транзакцію, не маючи для цього відповідного закритого ключа, а відтак він не може «вкрасти» криптогроші з рахунків користувачів.

Атака здійснюється тоді, коли відправник криптовалюти одночасно є і її майнером, який здійснює подвійну витрату криптогрошей, виконуючи для цього дві однакові транзакції зі свого рахунку: першу – на адресу жертви, а другу – на підконтрольну йому адресу. При цьому майнером ініціюється тимчасове операційне розгалуження, тому що перша транзакція включається в блок однієї гілки, а друга – в блок конкуруючої гілки. Суть атаки подвійного витрачання полягає в тому, що спочатку найдовшою гілкою (тобто гілкою з найбільшою кількістю блоків) тимчасово буде та, в якій знаходиться транзакція на адресу жертви. Однак атакуючий провайдер здійснюватиме майнинг на конкуруючій гілці, додаючи нові блоки виключно до неї так, що в перспективі вона може виявитися найдовшою гілкою і всі інші майнери автоматично переключаться на неї. Дослідники вказують, що успіх атаки стає можливим, якщо частка обчислювальної потужності майнера становить більше 50%, тобто при $a \geq 0.5$ жертва втратить псевдо-переведені гроші, навіть попередньо отримавши підтвердження про їх зарахування.

Іншим різновидом атаки є включення певних адрес (тобто рахунків користувачів) в чорний список, тобто відмова майнера приймати ті почуті блоки, які містять транзакції з адрес в чорному списку. Успіх цієї атаки, внаслідок якої кошти заморожуються і не можуть біти використані, також залежить від частки атакуючого майнера a. Саме тому рівномірний розподіл обчислювальної потужності є важливим фактором безпеки децентралізованих криптовалют з консенсус-алгоритмом proof-of-work. Подібний чорний список може формуватися в цілях шантажу, критерієм потрапляння до якого може бути надання меншої за певний рівень комісійної винагороди. Більш того, можна припустити законодавчо ініційований чорний список, який майнери були б змушені брати до уваги [4, с. 131–136]. Крім того, також існує як ризик підвищення провайдером транзакційної комісії (транзакції, які не надаватимуть достатніх «чайових» не

включатимуться в блок, не зважаючи на їх валідність), так і вилучення майнером обчислювальної потужності з децентралізованої платіжної системи, що призведе до збільшення її вразливості внаслідок можливої концентрації обчислювальної потужності та здійсненні так званих «майнерських атак».

Висновки. Вищенаведені ризики від застосування технології розподіленого реєстру в платіжних системах хоча і характеризують в загальному криптографічні валюти, вони ще не можуть безпосередньо використовуватися для ризик-аналізу конкретних криптовалют через високу техніко-економічну варіативність останніх. У зв'язку з цим, доцільним вбачається встановлення груп ризиків окремо для децентралізованих, розподілених та централізованих платіжних систем на основі Блокчейн, тому що рівень централізації є однією із визначальних характеристик віртуальної валюти.

Більшість криптовалют побудовано на алгоритмі, який дозволяє її провайдерам відхиляються від поведінки за замовчуванням, тобто здійснювати атаки зсередини, у зв'язку з чим існують ризики нав'язування провайдером транзакційної комісії (валідні транзакції, які не надаватимуть достатніх «чайових» не включатимуться в блок) та сторнування вже зарахованих коштів, якщо провайдер, який має достатньо обчислювальної потужності, одночасно є платником і здійснює атаку подвійного витрачання. Відповідно поведінка провайдерів децентралізованих, розподілених чи централізованих платіжних систем на основі технології розподіленого реєстру багато в чому визначатиме включення їх користувачів в економічний кругообіг. Перспективним для майбутніх досліджень є розгляд віртуальних валют в якості привабливої цілі для зовнішніх атак, через що нашою пропозицією є актуалізація питання протекціонізму віртуальної валюти з боку держави чи корпорації, що створило б політичні та економічні витрати для потенційних опонентів. Значущим також було б використання контексту ієрархії економічної безпеки окремо для децентралізованих, розподілених та централізованих криптовалют з метою порівняння загроз в таких системах, починаючи від рівня особистості і закінчуючи глобальним рівнем економічної безпеки.

Література.

1. ***Bauer M.*** Discussion Paper on distributed ledger technology. Financial Conduct Authority. London, April. 2017.
2. ***Токар В.*** Еволюція наукових поглядів на ієрархізацію економічної безпеки. *Формування ринкових відносин в Україні*. 2013. 142. № 3. С. 12–17.
3. ***Варцаба В., Мостіпака О.*** Альтернативні грошові системи в контексті управління національною економікою. Проблеми економіки. 2017. № 4. С. 351–362.
4. ***Narayanan A.*** Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton: Princeton University Press, 2016. 304 с.
5. ***Chapman S. J.*** MATLAB programming for engineers. Australia: Cengage Learning, 2015.
6. ***Laster B.*** Professional git. Indianapolis IN: John Wiley and Sons, 2016. 454 с.
7. ***Бойко О.*** Аналіз технологічних інновацій в системі міжнародних розрахунків криптовалютою. *Інноваційна економіка*. 2018. № 75. 5-6. С. 143–153.
8. ***Бойко О.*** Експансія криптографічної валюти в систему міжнародних розрахунків під впливом технології Блокчейн: свідчення та причини. *Глобальні та національні проблеми економіки*. 2018. № 22. С. 31–38.
9. ***Бойко О.*** Можливості та ризики при використанні криптографічної валюти. Цифрова економіка: тренди та перспективи. Под ред. Осадца Ю. В. Тернопіль, 25/10/2018. С. 44–47.
10. ***Бойко О.*** Експансія криптографічної валюти в систему міжнародних розрахунків. ***Вісник ВІЕМ***. 2016. №16. С. 28–38.
11. ***Sikorski J. J., Haughton J., Kraft M.*** Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*. 2017. №195. С. 234–246.
12. Wikipedia contributors. List of Bitcoin forks, 21.11. URL: https://en.wikipedia.org/w/index.php?title=List_of_bitcoin_forks&oldid=860559039.

References.

1. ***Bauer, M.*** (2017). *Discussion Paper on distributed ledger technology*. Financial Conduct Authority. London, April.

2. ***Tokar, V.*** (2013). «Evolution of scientific views on the hierarchy of economic security». *Formuvannia rynkovykh vidnosyn v Ukraini*. 142. no. 3. pp. 12–17.

3. ***Vartsaba, V. and Mostipaka O.*** (2017). «Alternative monetary systems in the context of national economy management» *Problemy ekonomiky*. 2017. no. 4. pp. 351–362.

4. ***Narayanan, A.*** (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press. Princeton. USA.

5. ***Chapman, S. J. (2015).*** *MATLAB programming for engineers*. Cengage Learning. Australia.

6. ***Laster, B.*** (2016). *Professional git*. John Wiley and Sons. Indianapolis IN. USA.

7. ***Boiko, O.*** (2018). «Analysis of technological innovations in the system of international calculations of cryptography». *Innovatsijna ekonomika*. no. 75. 5-6. pp. 143–153.

8. ***Boiko, O. G.*** (2018). «Expansion of the cryptographic currency into the system of international payments under the influence of Blokcain technology: evidence and reasons». *Global`ni ta nacional`ni problemy` ekonomiky`*. no. 22. pp. 31–38.

9. ***Bojko, O.*** (2018). Mozhly`vosti ta ry`zy`ky` pry` vy`kory`stanni kry`ptografichnoyi valyuty`. [Opportunities and risks when using cryptographic currency]. Cy`frova ekonomika: trendy` ta perspekty`vy`. [Digital Economy: Trends and Prospects]. In ***Osadcza, Yu. V.*** Ed. Ternopil`, 25/10/2018. S. 44–47.

10. ***Boiko, O.*** (2016). «Expansion of the cryptographic currency into the system of international payments.» *Visnyk VIEM*. no. 16. pp. 28–38.

11. ***Sikorski, J. J., Haughton, J. and Kraft, M.*** (2017). «Blockchain technology in the chemical industry: Machine-to-machine electricity market». *Applied Energy*. no. 195. C. 234–246.

12. Wikipedia contributors. List of Bitcoin forks, 21.11. Available at: https://en.wikipedia.org/w/index.php?title=List_of_bitcoin_forks&oldid=860559039.

Аннотация.

Бойко О. Г. Риски для экономической безопасности со стороны платежных систем на основе технологии распределенного реестра Блокчейн

Международные платежные системы очень быстро развиваются под влиянием технологических инноваций. Технология распределенного реестра Блокчейн начала новое направление в осуществлении международных платежей - криптовалюта. Криптовалюта характеризуются высокой вариативностью в технологических, технических и экономических характеристиках, что затрудняет анализ их полезности для общества. Статья посвящена рассмотрению рисков для экономической безопасности использования платежных систем на основе Блокчейн, используя при этом иерархию экономической безопасности от микро- к мегауровня. Приведены внутренние риски, присущие криптовалюта, указано на перспективность конкретизации рисков отдельно для централизованных, распределенных и децентрализованных криптовалюта.

Ключевые слова: *криптовалюта, Блокчейн, экономическая безопасность, платежные системы, майнинг, риски, распределенный реестр.*

Abstract.

Boiko O. Risks for economic security from payment systems based on distributed ledger technology Blockchain.

International payment systems are developing rapidly under the influence of technological innovations. The technology of the distributed register of Blockchain has begun a new direction in the implementation of international payments - cryptocurrency. Cryptocurrency fluctuations are characterized by high variability in technological, technical and economic characteristics, which complicates the analysis of their utility for society. The article is devoted to the consideration of risks for economic security from the use of payment systems based on the Blockchain, using the hierarchy of economic security from micro to mega-level. The internal risks inherent in cryptographic currencies are indicated, and it is indicated on the prospect of specificity of risks separately for centralized, distributed and decentralized cryptographic currencies.

Key words: *cryptocurrency, Blockchain, economic security, payment systems, mining, risks, distributed ledger.*

Стаття надійшла до редакції 15.09.2018 р.

Бібліографічний опис статті:

Бойко О. Г. Ризики для економічної безпеки з боку платіжних систем на основі технології розподіленого реєстру Блокчейн. Актуальні проблеми інноваційної економіки. 2018. № 4. С. 32-40.

Boiko O. Risks for economic security from payment systems based on distributed ledger technology Blockchain. Actual problems of innovative economy. 2018. No 4, pp. 32-40.