DOI 10.31891/2307-5732-2020-289-5-101-105
УДК 004.75:336.744

Г.І. РАДЕЛЬЧУК, М.Л. ХОРОШУН
Хмельницький національний університет

КОНЦЕПЦІЇ ПРОЕКТУВАННЯ ДЕЦЕНТРАЛІЗОВАНОЇ ПЛАТІЖНОЇ СИСТЕМИ З ВЛАСНОЮ ЦИФРОВОЮ ВАЛЮТОЮ НА БАЗІ БЛОКЧЕЙН-ПЛАТФОРМИ ETHEREUM

У роботі представлено концепції проектування децентралізованої платіжної системи з власною криптовалютою на базі блокчейн-платформи Ethereum. У дослідженні удосконалено метод створення цифрових платіжних засобів шляхом проектування комплексного рішення, яке складається з клієнтської частини та системи розумних контрактів. Обґрунтовано доцільність проектування власної обмінної платформи поряд з інтеграцією зовнішніх криптовалютних бірж для можливості купівлі розробленої криптовалюти за інші популярні цифрові валюти. Удосконалено методи опрацювання транзакцій, що дозволило оптимізувати пропускну здатність системи у порівнянні з існуючими рішеннями. Розглянуто алгоритми функціонування блокчейн-систем та обрано оптимальний алгоритм консенсусу. Результатом дослідження є покращені методи проектування децентралізованих платіжних систем.

Ключові слова: блокчейн, децентралізована платіжна система, цифрова валюта.

G. RADELCHUK, M. KHOROSHUN
Khmelnytskyi National University

CONCEPTS OF DESIGNING A DECENTRALIZED PAYMENT SYSTEM WITH ITS OWN DIGITAL CURRENCY BASED ON THE BLOCKCHAIN PLATFORM ETHEREUM

The study is devoted to the research of design concepts for the development of decentralized payment systems with its own cryptocurrency based on the blockchain platform Ethereum. The study examines the problems associated with traditional models of decentralized payment systems, analyzes the shortcomings in the industry, and proposes approaches to their solution. During the research, the method of creating digital assets was improved by designing a comprehensive solution consisting of a smart contracts part and a web-client part. Also, the expediency of designing its own exchange platform along with the integration of external cryptocurrency exchanges for the possibility of buying developed cryptocurrency for other popular digital currencies was substantiated and visual schemes of the traditional payment system structure with the method of exchange platform integration were presented. The paper substantiates the use of dynamic block size as a method of optimizing system efficiency, which can increase or decrease the maximum block size at the algorithm level, depending on the number of pending transactions, thus providing the required level of bandwidth. Also, the need for one-to-many transfers is justified, which involves the development of new methods of smart contracts for the cryptocurrency transfer from one user to a large number of addresses within a single transaction in order to reduce the load on the network. The problem of high energy consumption required for the functioning of the consensus system in the traditional model was solved by developing a model based on protocols that do not use the computational power of participants as a parameter to maintain consensus. Thus, the results of this study present improved methods for designing decentralized payment systems. The obtained results and generated recommendations can be used in the design of decentralized payment systems.

Keywords: blockchain, decentralized payment system, digital currency.

Вступ. Постановка проблеми

На сучасному етапі розвитку людства гроші втратили товарну сутність і сприймаються лише як розрахункова одиниця. Але еволюція грошей продовжується – паперові гроші перетворюються на цифрові, і все більше виокремлюються децентралізовані платіжні системи як альтернатива центральним банкам. Децентралізовані платіжні системи дозволяють виключити банківську систему з процесу емісії грошей і проведення транзакцій та довірити це комп'ютерним алгоритмам. Такі системи не мають обмежень у формуванні обмінних курсів та здійсненні операцій та дозволяють виконувати вільне переміщення коштів. Транзакції у таких системах не піддаються цензурі та є незворотніми. Поява децентралізованих платіжних систем продемонструвала, що криптовалюти можуть бути ефективним інструментом інвестування. Випуск віртуальної цифрової валюти, яку далі можна використовувати як платіжний засіб усередині сервісу або компанії, виявився найпростішим і найпривабливішим способом як для залучення інвестицій, так і для інвестування. Таким чином, з'явився попит на створення децентралізованих платіжних систем з власними цифровими валютами. Зазвичай, криптовалюта в таких системах виступає в ролі внутрішньої валюти додатку. Однак, методи реалізації подібних систем різняться за показниками ефективності, безпеки коштів та цінністю валюти на глобальному ринку.

Аналіз останніх досліджень та публікацій

Криптовалюти − одна з найновітніших технологій у сфері фінансів. Сьогодні наукова спільнота активно проводить дослідження у сфері криптовалютних платіжних систем. Серед робіт на тему криптовалют у першу чергу варто відзначити працю [1], у якій автори детально дослідили більше сотні популярних криптовалют та їхні ключові характеристики, а також ситуацію на ринку криптовалют у цілому та на криптовалютних біржах зокрема. У роботі [2] дослідники розглянули ефективність алгоритму консенсусу Proof-of-Work (PoF), який застосовується у більше ніж 90% сучасних децентралізованих систем. У роботі [3] здійснено ґрунтовний аналіз популярних криптовалют та визначені їхні переваги та недоліки у порівнянні з фіатними валютами.

Виділення невирішених частин загальної проблеми

У передових економіках світу цифрові платіжні системи розвиваються активними темпами, і безумовною перевагою криптовалют є можливість здійснення прямих платежів між користувачами, відсутність національних кордонів для здійснення переказів та зниження операційних витрат у порівнянні з традиційними банківськими системами [4]. Але, окрім внутрішніх витрат за перекази коштів між користувачами мережі для здійснення оплати в криптовалюті, користувачу, який не має її у своєму розпорядженні, необхідно спершу обміняти наявні у нього гроші на криптовалюту, що потребує використання онлайн-бірж або обмінників. Така конвертація валют містить додаткові комісійні витрати. Наприклад, найпопулярніша в Україні онлайн-біржа KUNA встановлює 1,5% комісійних від суми платежу при купівлі криптовалюти за фіатні гроші та 0,25% на обмін криптовалют [5]. При здійсненні платежу у криптовалюті з рахунку на біржі встановлюються фіксовані комісійні. Таким чином, при здійсненні платежів із використанням криптовалют транзакційні витрати всередині децентралізованої платіжної системи можуть бути досить низькими та, враховуючи можливості транскордонного переміщення коштів, більш привабливими у порівнянні із банківськими платежами. Але якщо користувачу необхідно здійснювати обмін або купувати криптовалюту для здійснення такого платежу, то додаткові комісійні витрати можуть перевищувати аналогічні витрати у банківській системі.

Також однією з головних проблем для децентралізованих платіжних систем залишається масштабованість. Наприклад, у рамках протоколу Bitcoin блок транзакцій обмежений розміром в 1 мегабайт і швидкість їх обробки становить приблизно сім операцій в секунду (у той же час Visa обробляє в середньому 2000 операцій за секунду). Розмір блоку впливає на кількість транзакцій, які можна додати у блок. Протокол Bitcoin передбачає, що блок формується в середньому 10 хвилин, і при збільшення активності у мережі збільшуються як комісійні, що пропонуються відправниками, так і час підтвердження окремої транзакції вузлами мережі.

Ще одним важливим моментом при здійсненні платежів є спосіб підтвердження транзакцій. При використанні централізованих банківських платіжних систем банк виступає посередником і гарантом переміщення коштів між рахунками клієнтів. У децентралізованих платіжних системах визначення, чи є транзакція вірною, відбувається на основі консенсусу учасників такої системи (тобто її підтвердження здійснюється «більшістю голосів»). Понад 90% існуючих систем використовують алгоритм консенсусу Proof-of-Work [2]. Суть цього алгоритму зводиться до двох основних пунктів:

- необхідності виконання певного, досить складного і тривалого завдання;
- можливості швидко і легко перевірити результат.

Необхідність постійного розрахунку рішення робить вирішення задачі дуже ресурсномістким, у зв'язку з чим десятки тисяч комп'ютерів витрачають власні обчислювальні ресурси на виконання протоколу консенсусу і при цьому лише один з них наприкінці отримує можливість створити блок. У результаті це призводить до великих енергозатрат, що є проблемою.

Таким чином, проаналізувавши наукові дослідження та публікації, можна зробити висновок, що основними проблемами, пов'язаними з існуючими децентралізованими платіжними системами є наступні: низька швидкість проходження транзакцій; необхідність залучення третьої сторони (криптовалютних бірж) для купівлі/обміну власної криптовалюти; функціонування системи на алгоритмі консенсусу Proof-of-Work, що вимагає значних енергозатрат. Тому основною задачею даного дослідження є покращення методів створення децентралізованих систем задля вирішення існуючих проблем.

Формулювання цілей

Для проведення дослідження сформульовано наступні цілі: провести теоретичний аналіз процедур функціонування децентралізованих платіжних систем; охарактеризувати базову модель організації процесів функціонування децентралізованих платіжних систем; описати існуючі механізми реалізації децентралізованих платіжних систем; виділити наявні проблеми в галузі та описати шляхи їх вирішення; покращити існуючі алгоритми функціонування децентралізованих систем.

Виклад основного матеріалу

Децентралізована платіжна система – цифрова пірингова платіжна система, яка використовує криптовалюту як розрахункову одиницю для обліку операцій. Така комп'ютерна мережа заснована на рівноправ'ї учасників (тобто відсутні виділені сервери), а кожний вузол є як клієнтом, так і виконує функції сервера. На відміну від архітектури «клієнт-сервер» така організація дозволяє зберігати працездатність мережі при будь-якій кількості та будь-якому поєднанні доступних вузлів. Функціонування та захист системи забезпечуються використанням криптографічних методів. При цьому вся інформація про транзакції між адресами системи доступна у відкритому вигляді. Серед популярних децентралізованих платіжних систем можна виділити мережі Bitcoin, Litecoin, Ethereum, Stellar, серед яких найпоширенішою є Ethereum.

Традиційні децентралізовані платіжні системи складаються з двох архітектурних компонентів. Основна логіка роботи системи працює на блокчейн-платформі (наприклад, на розумних контрактах). Для забезпечення зручних інтерфейсів розробляється веб-частина, до складу якої найчастіше входять наступні інструменти: оглядач блоків і транзакцій для показу статистичної та службової інформації про платіжну систему; відділ адміністрування, де здійснюється керування платформою; криптогаманець, за допомогою якого кінцевий користувач здійснює операції надсилання криптовалютних коштів чи отримує інформацію про їх отримання.

При такій формі організації системи існує очевидна проблема − після закінчення емітування монет у мережі користувачі можуть отримати криптовалюту, лише купивши її в інших учасників системи або на криптовалютних біржах. Це призводить до появи небажаних комісій та додаткових ризиків для користувачів, які вимушені користуватись сторонніми додатками для придбання криптовалюти. Рішенням цієї проблеми може стати розробка власної обмінної платформи у комплексі однієї платіжної системи. Таким чином, користувач матиме вибір − здійснювати переказ через зовнішні біржі на ринку чи скористатись офіційною обмінною платформою. В той час, як на офіційній обмінній платформі ціна на криптовалюту буде вищою за ринкову, користувачі, які нею користуватимуться, будуть впевнені у безпеці проведення своїх операцій, оскільки їм не потрібно покладатись на сторонні платформи. На рис. 1 наочно продемонстровано схему платформи і те, як компонент обмінної системи інтегрується в неї.

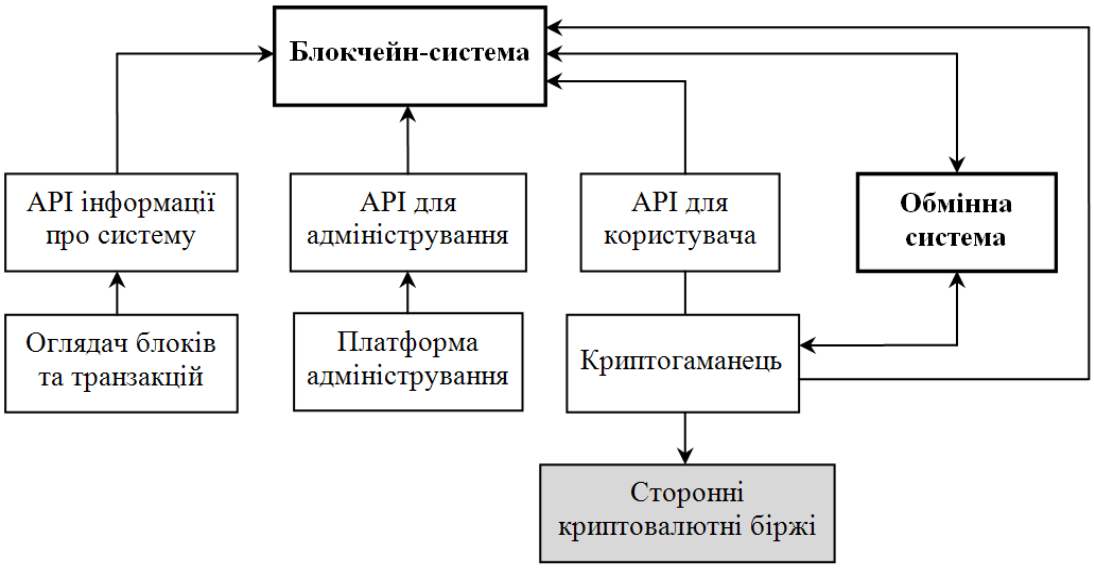

Рис. 1. Взаємодія компонентів системи

Розглянемо детальніше компоненти на представленій схемі. Очевидно, що основним її компонентом є блокчейн-система, яку використовують інші частини платформи для виконання операцій. Блокчейн-система реалізовує головний функціонал системи − збереження даних про криптовалюту та користувацькі рахунки, емітування монет, опрацювання переказів між користувачами. Інші компоненти системи лише звертаються до методів розумних контрактів для отримання даних чи для виконання певних операцій.

В той час, як операції для отримання даних з блокчейну відбуваються за допомогою звичайних методів читання бази даних смарт-контрактів (які миттєво повертають результат), виконання операцій на модифікацію існуючих даних (таких, наприклад, як перекази між рахунками) відбуваються за визначеним алгоритмом (рис. 2). Всі транзакції у системі зберігаються у спеціальних структурах даних − блоках. Під час роботи системи через деякий визначений часовий інтервал у блокчейн додається новий блок. Цей блок може бути порожнім або містити інформацію про деяку кількість транзакцій, обмежену розміром блоку. Кожний наступний блок зберігає посилання на попередній, формуючи таким чином єдиний нерозривний ланцюг. При додаванні нового блоку до ланцюга, транзакції, що містяться в ньому, почергово виконуються на розумних контрактах.

Очевидно, що з таким алгоритмом опрацювання транзакцій неможливо здійснювати горизонтальне масштабування системи. Незважаючи на те, що блокчейн є розподіленою системою, у підсумкову базу даних записується лише один блок, від одного вузла, тому що опрацювання блоків може здійснювати лише один канал обслуговування. Оскільки збільшення кількості каналів обробки є неможливим, то для підвищення пропускної здатності системи у роботі запропоновані наступні методи оптимізації.

1 Використання динамічного розміру блоку. Кожний блок у системі має фактичний та максимальний розмір. Фактичний розмір блоку відповідає об'єму транзакцій, які в ньому знаходяться. Максимальний розмір блоку відповідає максимальному значенню сукупного розміру транзакцій, які можуть розміститися в ньому, та визначається системою під час її старту. Передбачивши можливість збільшення максимального розміру блоку вже після запуску мережі, можна масштабувати пропускну здатність системи: при збільшенні навантаження на систему значення максимального розміру блоку буде зростати, а при зменшенні навантаження − зменшуватись. Таким чином, з'явиться змога опрацьовувати більшу кількість транзакцій за той самий часовий період. Реалізація цього функціоналу полягатиме у підтриманні консенсусної зміни конфігурацій. Створювачу блоків має бути надана можливість змінювати максимальний розмір для свого блоку, але не більше ніж на 1% від розміру попереднього блоку. Таким чином, значення максимального розміру блоку в системі відповідатиме навантаженню на систему.

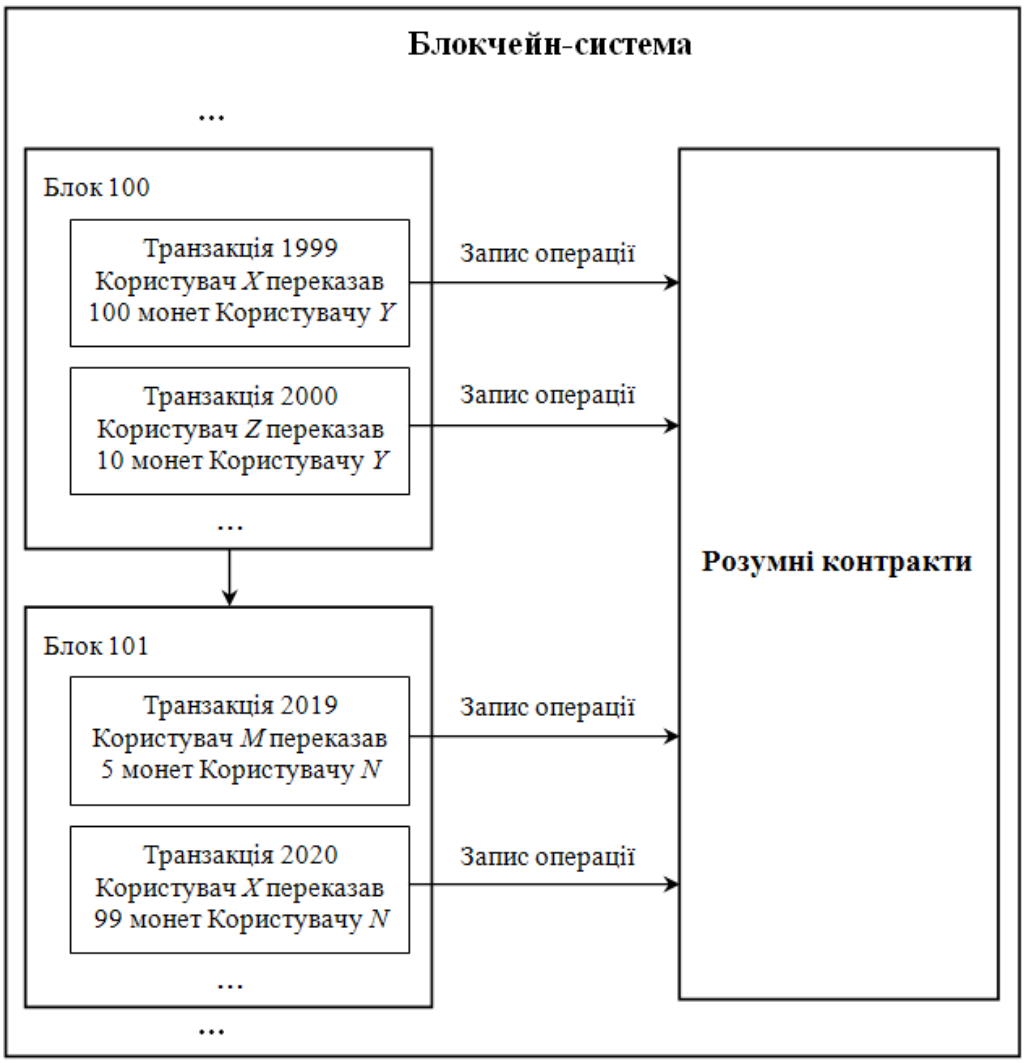

Рис. 2. Опрацювання транзакцій всередині блокчейн-системи

2 Перекази «один до багатьох». Також для того, щоб зменшити навантаження на мережу, доцільно розробити функціонал виклику трансферу криптовалюти, при якому в якості вхідних аргументів методу смарт- контракту можна було б передати список адрес отримувачів та необхідні суми переказу кожному з отримувачів. Таким чином, при здійсненні переказу на значну кількість адрес, користувач зможе це зробити всередині лише однієї транзакції, що зменшить навантаження на мережу.

У процесі застосування технології блокчейн виникає також питання підбору ефективного протоколу консенсусу. Консенсус блокчейна полягає в тому, що всі вузли підтримують однаковий розподілений реєстр. У традиційній архітектурі програмного забезпечення це не є проблемою через існування центрального сервера, з яким узгоджуються інші вузли. Однак, у розподіленій мережі (такій як блокчейн) кожен вузол є і хостом, і сервером, і, щоб досягти консенсусу, йому потрібно обмінюватися інформацією з іншими вузлами. Інколи деякі вузли можуть працювати у режимі офлайн. Окрім того, можуть з'явитись деякі шкідливі вузли, які будуть негативно впливати на процес консенсусу і, навіть, можуть зашкодити йому. Тому потрібен протокол, який не допустить виникнення подібних ситуацій та мінімізує негативний вплив шкідливих вузлів таким чином, щоб вони не впливали на кінцевий результат консенсусу.

Аналіз предметної області показав, що близько 90% існуючих децентралізованих систем використовують алгоритм консенсусу Proof-of-Work. Однак, значним недоліком PoW-алгоритму є те, що його функціонування потребує постійних значних затрат електроенергії на процес створення блоків. Цей недолік яскраво видно на прикладі Біткоіна, який реалізовує вказаний алгоритм. За один рік на функціонування мережі витрачається більше електроенергії, ніж використовує Швейцарія за цей же період. Проблему значних енергозатрат можна вирішити шляхом розробки моделі на основі протоколів, що не використовують обчислювальну здатність учасників як параметр підтримання консенсусу. У роботі [6] автори здійснили порівняльний аналіз найпопулярніших алгоритмів консенсусу, розглянувши методи обчислення значень основних характеристик алгоритмів: відмовостійкість, ресурсоємність, масштабованість та придатність для публічних мереж. На основі результатів цього аналізу сформовано порівняльну таблицю 1.

Таблиця 1

Характеристика різних алгоритмів консенсусу

Характеристика	PoW	PoS	PBFT	Ripple
Тип алгоритму	Ймовірнісно-кінцевий	Ймовірнісно-кінцевий	Абсолютної остаточності	Абсолютної остаточності
Відмовостійкість	50%	50%	33%	20%
Ресурсоємність	Висока	Середня	Низька	Низька
Масштабованість	Добра	Добра	Погана	Погана
Придатність для публічних мереж	Придатний	Придатний	Не придатний	Придатний

Як бачимо з табл. 1, серед алгоритмів, придатних для публічної мережі, алгоритми PoW і PoS (Proof of Stake) відрізняються лише за показником ресурсоємності. При цьому PoS набагато менш ресурсоємний, тому він є кращим вибором для публічного блокчейну. Вибір цього алгоритму консенсу для системи дозволить зменшити її ресурсоємність та забезпечить необхідними інструментами персоналізації.

Висновки

Таким чином, у роботі досліджено процедури залучення криптовалютних інвестицій, охарактеризовано структуру предметної області та виділено основні невирішені проблеми. Розглянуто та описано моделі, за якими працюють традиційні децентралізовані платіжні системи. Запропоновано методи та рішення, які дозволять оптимізувати їхню роботу: підвищити швидкість проходження транзакцій; забезпечити відсутність необхідності залучення «третьої» сторони (сторонніх криптовалютних бірж) для купівлі/продажу власної криптовалюти; оптимізувати використання енергозатрат для підтримки функціонування системи шляхом вибору та застосування ефективного алгоритму консенсусу.

Література

1. Hileman G. Global cryptocurrency benchmarking study / G. Hileman, M. Rauchs. – Cambridge, 2017. – 114 p.

2. Gervais A. On the Security and Performance of Proof of Work Blockchains / A. Gervais, G. Karame, K. Wüst etc. // CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – № 10. – P. 3–16.

3. Dorofeyev M. Trends and Prospects for the Development of Blockchain and Cryptocurrencies in the Digital Economy / M. Dorofeyev, M. Ksov, V. Ponkratov // European Research Studies Journal. – 2018. – № 21. – P. 429–445.

4. Олешко А. А. Інноваційні тенденції розвитку безготівкової економіки / А. А. Олешко // Інвестиції: практика та досвід. – 2018. – № 10. – С. 22–25.

5. Бойко В. П. Переваги та недоліки використання децентралізованих платіжних систем як інноваційного способу транскордонних розрахунків / В. П. Бойко // Інвестиції: практика та досвід. – 2019. – № 8. – С. 75–82.

6. Золотарьова І. О. Інформаційні технології оптимізації роботи приватного блокчейн за допомогою вибору алгоритму консенсусу / І. О. Золотарьова, Г. О. Плеханова // Системи обробки інформації. – 2020. – № 1. – С. 107–114.

References

1. Hileman G. Global cryptocurrency benchmarking study / G. Hileman, M. Rauchs. – Cambridge, 2017. – 114 p.

2. Gervais A. On the Security and Performance of Proof of Work Blockchains / A. Gervais, G. Karame, K. Wüst etc. // CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – № 10. – P. 3–16.

3. Dorofeyev M. Trends and Prospects for the Development of Blockchain and Cryptocurrencies in the Digital Economy / M. Dorofeyev, M. Ksov, V. Ponkratov etc. // European Research Studies Journal. – 2018. – № 21. – P. 429–445.

4. Oleshko A. A. Innovatsiyni tendentsiyi rozvytku bezhotivkovoyi ekonomiky / A. A. Oleshko // Investytsiyi: praktyka ta dosvid. – 2018. – № 10. – S. 22–25.

5. Boyko V. P. Perevahy ta nedoliky vykorystannya detsentralizovanykh platizhnykh system yak innovatsiynoho sposobu transkordonnykh rozrakhunkiv / V. P. Boyko // Investytsiyi: praktyka ta dosvid. – 2019. – № 8. – S. 75–82.

6. Zolotar'ova I. O. Informatsiyni tekhnolohiyi optymizatsiyi roboty pryvatnoho blokcheyn za dopomohoyu vyboru alhorytmu konsensusu / I. O. Zolotar'ova, H. O. Plekhanova // Systemy obrobky informatsiyi. – 2020. – № 1. – S. 107–114.

Надійшла / Paper received : 17.10.2020 Надрукована/Printed :27.11.2020