РОЗДІЛ 8. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

ПИТАННЯ ДЕЦЕНТРАЛІЗОВАНОГО КОНСЕНСУСУ БЛОКЧЕЙНІВ
THE ISSUES OF DECENTRALIZED CONSENSUS IN BLOCKCHAINS

УДК 519.8
https://doi.org/10.32843/infrastruct34-47

Горбачук В.М.
д.ф.-м.н., старший науковий співробітник, провідний науковий співробітник відділу математичних методів дослідження операцій
Інститут кібернетики імені В.М. Глушкова Національної академії наук України
Ляшко В.І.
к.ф.-м.н., доцент, доцент кафедри інформатики
Національний університет «Києво-Могилянська академія»
Сирку А.А.
магістр, аспірант
Інститут кібернетики імені В.М. Глушкова Національної академії наук України

Блокчейн як розподілена реєстрова технологія з децентралізованим чи автономним менеджментом набула популярності завдяки криптоактиву біткойн, основаному на цій технології. Згодом ця технологія постала у багатьох інших формах, часто здатних зберігати та виконувати комп'ютерні програми. Це породжує такі застосування, як інтелектуальні контракти, характерні платежами внаслідок зламостійкого консенсусу щодо умовних результатів і фінансовані через первинні койнові пропозиції. Багато галузевих практиків вважає, що технологія блокчейну має потенціал до розмивання ділових і фінансових послуг аналогічно до того, як сучасний Інтернет розмив офлайнову комерцію. Водночас деякі фахівці сумніваються у справжній інноваційності та реальній практичності технології блокчейну, вважаючи основним застосуванням блокчейну проведення фінансових операцій, малопомітних для державних функціонерів законності і правопорядку.
Ключові слова: *реєстр, зламостійкий консенсус, умовні результати, блокчейн, довіра, Інтернет речей, змова, розподіл інформації.*

Блокчейн как распределенная реестровая технология с децентрализованным или автономным менеджментом приобрела популярность благодаря криптоактиву биткойн, основанному на этой технологии. Со временем эта технология возникла во многих других формах, часто способных хранить и выполнять компьютерные программы. Это порождает такие приложения, как интеллектуальные контракты, характерные платежами вследствие взломостойкого консенсуса относительно условных результатов и финансированные через первичные койновые предложения. Много отраслевых практиков считает, что технология блокчейна имеет потенциал к размыванию деловых и финансовых услуг аналогично тому, как современный Интернет размыл офлайновую коммерцию. В то же время некоторые специалисты сомневаются в действительной инновационности и реальной практичности технологии блокчейна, считая основным применением блокчейна проведение финансовых операций, малозаметных для государственных функционеров законности и правопорядка.
Ключевые слова: *реестр, взломостойкий консенсус, условные результаты, блокчейн, доверие, Интернет вещей, сговор, распределение информации.*

Blockchain as a distributed ledger technology with a decentralized or autonomous management has become popular due to the Bitcoin cryptoasset based upon that technology. Subsequently, this technology has emerged in many other forms often able to store and execute computer programs. It creates such applications as smart contracts characterized by payments as results of tamper-proof consensus on contingent outcomes and financed via initial coin offerings. Many industry dealers assume that blockchain technology has a potential to disrupt business and financial services similar to the modern Internet has disrupted offline commerce. Some specialists are doubtful regarding the genuine innovationess and real practicality of blockchain technology believing that major blockchain application area is carrying out financial operations invisible for state functioners in law and order. Despite of various definitions, descriptions, and applications of blockchain and decentalized ledger, this technology and its clowns have a common function to povide a decentralized consensus. A decentralized consensus within a system is defined as a state of the world, in the terms of supplying goods and making payments, which is accepted unanimously and enforced by all the system agents. The economists recognize that consensus allows agents interaction with various ideas and incentives as it provides the truth with chain reactions in a social organism, including ethics, contract law, law enforcement, and so on. The specific feature of blockchain technology is that consensus is generated and maintained in a decentralized way capable of improving the system resilience and reduce the rent gained by centralized third parties. For instance, on the Bitcoin blockchain, given history of transactions, the participants can examine and verify records on transactions by a digital way in order to avoid double spending of digital assets and to free everyone from the need in a centralized trustworthy arbiter or a third party. The majority of blockchains has communities of different generations consisting of record keepers and users overlapped in the time. Similar to the third party arbiters in real world, these communities, receiving signals on true state of the world, may have incentives to fabricate, manipulate, or tamper reports.
Key words: *ledger, tamper-proof consensus, contingent outcomes, blockchain, trust, Internet of Things, collusion, information distribution.*

Постановка проблеми. Постановка проблеми полягає в необхідності цілісного аналізу новітньої революційної технології – технології блокчейну. Технологія блокчейну (blockchain) забезпечує децентралізований консенсус і потенційно розширює простір традиційних контрактів за рахунок інтелектуальних (smart) контрактів із протизламною стійкістю (tamper-proofness) та алгоритмічним виконанням. Водночас генерація такого консенсусу передбачає розподілення інформації та відповідну зміну інформаційного середовища. Слід проаналізувати вплив децентралізації на ефективність консенсусу, а також залежність галузевої організації та концентрації від характерних рис блокчейну. Інтелектуальні контракти можуть зменшувати інформаційну асиметрію, поліпшувати суспільний добробут і споживчий надлишок шляхом сприяння входу в ринок і конкуренції, але згадане розподілення інформації може заохочувати змови. Тому є інтерес до антимонопольних стратегій, наприклад, розділення реєстраторів (record-keepers) консенсусу і користувачів. Загалом блок-

чейни можуть підтримувати ринкові рівноваги з ширшим колом економічних результатів.

Аналіз останніх досліджень і публікацій. Британський журнал «Economist» 31 жовтня 2015 р. називає блокчейн машиною довіри і вважає, що технологія, на якій оснований біткойн, торкнеться всіх економічних процесів. Співзасновник відомого браузера Netscape Марк Андріссен (Marc Andreessen) вважає, що блокчейн – це розподілена мережа довіри, якої завжди потребував Інтернет, але не мав (президентом Netscape був Джеймс Барксдейл (James Barksdale), випускник університету Міссісіпі (Ole Miss), де у 2000 році стажувався один з авторів цієї роботи, виграви стипендію за програмою «Contemporary Issues» США, а завдяки благодійним внескам Барксдейла Школа бізнесу цього університету у тому ж році вперше увійшла у топ-100 США за рейтингом U.S. News & World Report).

У період від 30 березня 2014 р. до 30 березня 2018 р. кількість пошуків технології блокчейну через Google помітно зростала порівняно з кількістю пошуків S&P500 [1]. У період від січня 2013 р. до квітня 2018 р. за експонентою зростало число проектів щодо блокчейнів та інтелектуальних контрактів, які мали хостинг на GitHub, головній світовій платформі для розробок на основі відкритих кодів.

Постановка завдання. Незважаючи на розмаїття визначень, описів і застосувань блокчейну та децентралізованого реєстру (ledger), ця технологія та її різновиди мають спільну функцію забезпечення децентралізованого консенсусу. Децентралізований консенсус – це стан світу (постачання товарів і здійснення платежів), який приймається одностайно і втілюється всіма учасниками системи. Економісти визнають, що консенсус дозволяє взаємодіяти учасникам із різноманітними уявленнями і мотиваціями, оскільки він забезпечує істинний запис із глибокими наслідками для функціонування суспільства, включаючи етику, контрактне право, втілення законодавства тощо. Відмітна риса технології блокчейну полягає у тому, що консенсус генерується і зберігається децентралізованим способом, який може поліпшувати стійкість (resilience) системи і знижувати ренту, яку дістають централізовані треті сторони. Засновник біткойну Сатоші Накамото зазначав: «Багато людей автоматично відкидає електронну валюту як втрачену справу через усі компанії, які зазнали невдачі, починаючи з 1990-х років. Сподіваюся, що лише централізовано керована природа тих систем була причиною втрат. Думаю вперше спробувати децентралізовану систему, що не втрачає довіру» [2]. Наприклад, на блокчейні біткойна, за цієї історії трансакцій, учасники можуть перевіряти і верифікувати записи про трансакції цифровим способом, щоб запобігати подвійним витратам цифрової валюти і вивільнювати кожного від потреби у централізованому надійному арбітрі чи третій стороні. Подвійні витрати є потенційною вадою у системі цифрової готівки, в якій та сама цифрова валюта може витрачатися принаймні двічі, коли немає реєстрації консенсусу про історії трансакцій, бо відповідний цій валюті цифровий файл може дублюватися чи фальсифікуватися.

Виклад основного матеріалу дослідження. Блокчейни взаємодіють з розподіленими реєстраторами, щоб досягати децентралізованого консенсусу, використовуючи новітні технології. Тоді природним чином виникають дві економічні сили: 1) програмований децентралізований консенсус, коли він досягнутий, має тенденцію до полегшення укладення залежних контрактів (contracting on contingencies) завдяки своїй зламостійкій та автоматизованій природі; 2) водночас досягнення такого консенсусу вимагає достатнього розподілення інформації для верифікації. Тому застосування блокчейну типово вирізняються засадничою розбіжністю між 1) децентралізованим консенсусом і 2) розподілом інформації. Якщо 1) сприяє укладенню контрактів з поліпшенням добробуту, то 2) може бути згубним для суспільства. Вказана засаднича суперечність визнається урядами, засобами масової інформації, галузевими дослідженнями. Наприклад, проект Jasper Банку Канади у 2017 р. звітував: «Більш робастна верифікація даних вимагає ширшого поділу інформацією. Потрібний баланс між прозорістю і приватністю висуває базове питання до життєздатності системи з такими рисами, коли обмежується її ключова та визначальна властивість». Це питання заслуговує окремої уваги.

Під час дослідження блокчейну є два економічні питання: а) механізми блокчейну для генерування та підтримування децентралізованого консенсусу; б) наслідки для реального світу при цій функціональності блокчейну. На відміну від аналізу стратегічних ігор майнінгу (mining), характерних для протоколу Bitcoin, вивчення цих питань зосереджується на балансуванні питань 1) і 2), а також на впливі технології блокчейну на індустріальну організацію.

Це вивчення слід почати з простої моделі досягнення децентралізованого консенсусу під час застосування блокчейну для торгівлі та фінансів. Більшість блокчейнів має громади різних поколінь реєстраторів і користувачів, які перетинаються в часі. Подібно до арбітрів третьої сторони в реальному світі, ці громади, отримуючи сигнали про істинний стан світу, можуть мати стимули до фальсифікації, маніпуляції чи викривлення звітності. За допомогою все новіших технологій комунікації в реальному часі серед децентралізованих реєстраторів, ретельно спроектований протокол на блокчейнах може знижувати індивідуальний

стимул до згаданих маніпуляції та фальсифікації, сприяючи ефективнішій агрегації інформації. Порівняно з традиційним укладенням контрактів, блокчейни мають потенціал виробляти консенсус, який краще відбиває істину про умовні зобов'язання (contingencies), істотні для ділових операцій, а тому блокчейни сприяють укладенню контрактів щодо цих умовних зобов'язань. Проте генеруванню ефективнішого консенсусу (ближчого до істини) передує спостереження й отримання більшого обсягу інформації децентралізованими реєстраторами. Деяка така інформація може бути зашифрованою. У разі публічних блокчейнів (наприклад, біткойнів) консенсус типово генерується всіма користувачами. Вирішальним є те, що процес розподілу інформації змінює інформаційне середовище, а відтак економічну поведінку учасників блокчейнів [3].

Зміна інформаційного середовища технологією блокчейну впливає на конкуренцію й організацію галузі. У простій моделі досягнення децентралізованого консенсусу виділяємо двох наявних продавців, кожний з яких є аутотентичним на 100%, і нового продавця, який є аутотентичним з деякою ймовірністю. Якщо аутотентичний продавець виконує контракт завжди, то неаутотентичний (фальшивий) – не завжди. У кожний період часу з постійною ймовірністю (залежною від агрегованих ділових умов) з'являється група покупців, яка закуповує продукти у продавців відповідно до цінових котирувань, а потім виходить з ринку. Кожний продавець має спостереження стосовно своїх клієнтів, але не має спостережень стосовно цін або клієнтів інших продавців. Таке економічне середовище називається традиційним світом, в якому неможливо передавати інформацію поміж учасників.

У такому традиційному світі, внаслідок неповноти контрактів, продавці не можуть пропонувати ціни залежно від успіху постачання товарів. Тому входу у такий ринок заважає проблема неякісних продуктів [4, с. 154]. З іншого боку, два наявні продавці можуть увійти у змову за рівноваги. Оскільки кожний наявний продавець не може розрізняти подію відсутності продавців від події повної втрати своєї частки ринку, то частіше трапляються агресивні цінові війни, що ускладнює змову серед наявних продавців.

На відміну від традиційного ринку, блокчейни шляхом децентралізованого консенсусу дають змогу своїм агентам укладати контракт про результати постачання й автоматизувати умовні (contingent) трансферти. Тоді аутотентичний новий продавець здатний сигналізувати про свою повну аутентичнність, усуваючи асиметрію інформації як бар'єр для входження в ринок і бар'єр для зростання конкуренції, сприяючи добробуту і споживчому надлишку на так званому блокчейновому ринку.

Проте генерування децентралізованого консенсусу також веде до збільшення знань про агреговані ділові умови на блокчейні, яке може заохочувати неявну змову серед продавців. На відміну від традиційного світу, де продавці не спостерігають ділову діяльність один одного, у блокчейновому світі вони можуть принаймні визначати агреговані ділові умови на блокчейні, виконуючи функції реєстраторів, а тому вони здатні знаходити відхилення від будь-якої (кооперативної) рівноваги змови. Можна показати, що на блокчейнових ринках, в яких можуть брати участь лише наявні продавці, завжди є не менша кількість рівноваг змови, ніж на традиційних ринках.

Згадана модель досягнення децентралізованого консенсусу враховує компроміс між потенційно вищою конкуренцією та потенційно більш загрозливішою змовою, які породжує технологія блокчейну. Загалом при блокчейновому ринку (доступному наявним і новим продавцям) та інтелектуальних контрактах розширюється множина можливих динамічних рівноваг, у яких суспільний добробут і споживчий надлишок можуть бути більшими чи меншими, ніж при традиційному ринку.

Висновки [1] пов'язані з поширеним занепокоєнням про те, що блокчейни можуть серйозно погіршувати ринкову конкурентність. Воно насамперед стосується ексклюзивних (permissioned) блокчейнів з потужними фінансовими інститутами як особливими членами. Оскільки є фундаментальний економічний механізм, яким блокчейн сприяє змові, то мають бути відповідні регулювання [1]. Прикладом такого регулювання може бути поділ процесів користування та генерування консенсусу на блокчейні, щоб для збереження змови продавці не могли скористатися інформацією, отриманою під час генерування консенсусу. Докладний економічний аналіз блокчейну й інтелектуальних контрактів показує, що блокчейни є не просто технологіями баз даних, які знижують витрати на зберігання чи розподіл даних, але й технологіями, властивості яких можуть мати глибокі економічні наслідки для генерування консенсусу, проектування інтелектуальних контрактів, індустріальної організації та антимонопольної політики. Отже, технологія блокчейну містить величезний потенціал до зменшення асиметрії інформації та заохочення входу в ринок, але при цьому створює передумови до поведінки змови.

Крім досліджень з комп'ютерних наук, блокчейнам присвячено публікації з економічних механізмів генерування і підтримування децентралізованого консенсусу, а також публікації з реальними застосуваннями блокчейнової функціональності. Серед публікацій з економічних механізмів виділяють вивчення загального процесу генерування децентралізованого консенсусу для більшості блокчейнів з децентралізованими взаємодіями (взаємообмі-

нами) і вивчення теоретико-ігрових тем, включаючи забезпечення стимулів і ринкової мікроструктури, на основі конкретного блокчейнового протоколу, скажімо, майнінгового протоколу Bitcoin.

Серед публікацій про застосування й економічний вплив блокчейну відомі огляд криптофінансів, зокрема огляд фінансів на основі біткойну, роботи про трейдинг цифровими активами і про потенційний вплив технології блокчейну на корпоративне управління, емпіричні документи про інтерпретування і програмування інтелектуальних контрактів на різних блокчейнових платформах, звіт про вплив найвизначальніших рис блокчейну на асиметрію інформації та ринкову конкуренцію.

Аналіз базового механізму для генерування децентралізованого консенсусу пов'язаний з іграми майнінгу біткойнів. Майнери (miners), які дотримуються правила найдовшого ланцюга, перебувають у ситуації рівноваги Неша. Згадані ігри можуть мати кілька рівноваг. Вивчалися егоїстичний майнінг і впертий (stubborn) майнінг, в якому майнер пулу (pool) не повідомляє про знайдений вірний хеш (hash) блоку з метою зниження прибутковості цього пулу (запускає атаку затримки блоку). Проводився аналіз трансакційних внесків біткойну, перенавантаження та неефективності майнінгу. Вивчалися організація та компенсація у пулах майнінгу. Не обмежуючись конкретними блокчейновими протоколами (скажімо, протоколом Bitcoin), під час аналізу стратегічної поведінки майнерів або ринкової мікроструктури варто виходити з цілісного підходу до загальних рис блокчейнів, зосереджуючись на співвідношенні між розподілом інформації під час децентралізації та якістю генерації консенсусу. Найважливіше, що ключове поняття децентралізації у технології блокчейну має як переваги, так і недоліки. Занепокоєння про розподіл інформації у блокчейновій децентралізованій системі є природною думкою на користь централізації. Деякі роботи присвячені поділу ризиків і розподілу інформації.

Аналіз блокчейнової змови [1] розвиває дослідження індустріальної організації та повторюваних ігор із моніторингом. Цей аналіз ґрунтується на вивченні змови при конкуренції Курно з недосконалим громадським моніторингом. Емпіричні дослідження вказують на зв'язок змови зі стратегіями фірм щодо розкриття фінансової інформації (financial disclosure) чи розподілу інформації. Досліджується конкуренція за Бертраном, пов'язуючи додаткову спостережувану чи контрактну інформацію з типом моніторингу у повторюваних іграх при технологічній інновації. Проводиться аналіз самопідтримуваних рівноваг. Застосування блокчейнів та інтелектуальних контрактів до фінансових послуг ґрунтується на укладенні оптимальних контрактів та отриманні неповних контрактів за асиметрії інформації [4–6].

Блокчейн як децентралізований консенсус ґрунтується на певних інститутах, економічних взаємодіях, інформаційних процесах, інтелектуальних контрактах, реальних застосуваннях. Блокчейни забезпечують багато таких функцій, як зберігання розподілених даних, анонімність, приховування даних, спільне використання реєстрів тощо. Оскільки ці функції можуть здійснюватися незалежно від блокчейну, то слід зосередитися на їхній взаємодії при забезпеченні децентралізованого консенсусу. Не вдаючись до аналізу технічних характеристик різних протоколів або додаткових виграшів технології блокчейну, варто дослідити економічні наслідки децентралізованого консенсусу та природні процеси розподілу інформації, які супроводжують генерування такого консенсусу.

Від першої роботи з блокчейну до його першої концептуалізації й реалізації [2] пройшло 17 років. Ця концептуалізація стала поширюватися завдяки криптоактиву з назвою біткойн. Досліджувалися принципи проектування, властивості, ризики й регулювання цього криптоактиву, а також технічні характеристики блокчейну Bitcoin. Відповідно до закону Стівена Стіглера (Stephen Stigler) про епоніми («Будь-яке наукове відкриття не назване ім'ям свого першовідкривача»), складники та принципи для біткойна були започатковані значно раніше публікації [2], а інновація автора [2] полягала в системній інтеграції відомих складників і принципів. Біткойн у найпростішій формі передбачає розподілену базу даних, яка автономно підтримує неперервно зростаючий перелік записів про трансакції, що вимірюється у блоках (блок – одиниця вимірювання) і захищається від викривлення та перегляду. Кожний блок містить часову відмітку і ланку до попереднього блоку. Після біткойна виникли інші форми блокчейнів з різними конструкціями винятковості, прозорості та підтримки записів.

Всі блокчейни до різної міри спрямовані на створення системи бази даних, яку сторони можуть спільно підтримувати і редагувати децентралізованим способом, причому будь-яка сторона не здійснює централізованого управління. Отже, визначальна риса блокчейнових аріхтектур – це їхня здатність підтримувати порівняно ефективним шляхом однорідний погляд на стан речей і порядок подій, тобто консенсус.

Оскільки консенсус є суттєвим для багатьох соціально-економічних функцій, то є виграш і розширення можливостей для кожного, хто поділяє однаковий звіт (перелік записів) і довіряє цьому звіту. Тоді врегулювання у деяких випадках тривають не більше кількох днів, проблеми неякісних продуктів і шахрайства можуть бути зменшені, ймовірно, впливаючи на ex-ante стимули агентів економіки. Традиційно суди, уряди, нотаріальні агентства забезпечують такий консенсус, але шляхом, який іноді вважається трудомістким,

часовитратним, підвладним фальсифікації і монополізації. Тому багато людей виступає на захист технології блокчейну, вважаючи, що вона обіцяє порушити низку традиційних видів діяльності, забезпечуючи консенсус більш децентралізованим способом, хоча потенційно дорожчим способом за споживанням енергії та інформації.

Щоб виробляти і підтримувати децентралізований консенсус без централізованого органу влади, блокчейнові протоколи проектуються з мотивуванням до відповідальної і точної реєстрації записів громадою розподілених реєстраторів, типово конкурентним способом, знижуючи маніпулювання і викривлення. У певному сенсі децентралізований консенсус має наближатися до деякої форми голосування більшістю, хоча алгоритми генерування такого консенсусу у різних проектах і застосуваннях можуть істотно відрізнятися.

Два широко відомі проекти для підтримки децентралізованого консенсусу – це доведення роботи (proof-of-work, PoW) і доведення статків (proof-of-stake, PoS). PoW винагороджує реєстраторів, які розв'язують складні криптографічні ребуси для підтвердження трансакцій і створення нових блоків (здійснюють майнінг). PoW запобігає таким атакам, як відмова обслуговування (denial-of-service, DoS), і гарантує, що коли хтось спостерігає підтверджений стан звіту (переліку записів), то не можна нехтувати трансакціями певного віку: цей алгоритм потребуватиме від зловмисника конкурувати з усією мережею за обчислювальною потужністю [7]. Як наслідок, блокчейн досягає зламостійкого консенсусу про підтвердженість (валідність) цих трансакцій. На відміну від PoW, у PoS агент як творець наступного блоку вибирається детерміністичним способом, а ймовірність такого вибору залежить від багатства (статків) цього агента. Інші відомі проекти включають практичний алгоритм задачі візантійських генералів (byzantine fault tolerance, BFT) та алгоритм делегованого доведення статків (delegated proof-of-stake, DPoS). DpoS працює так само, як PoS, за винятком того, що особи (агенти) віддають (делегують) свої голоси керівній установі пропорційно своїм статкам у системі. Практичний алгоритм BFT має справу з робастною синхронною домовленістю за присутності деяких вузлів із зловмисними помилками. Не вдаючись до порівняння конкретних проектів (для підтримки децентралізованого консенсусу), моделюється загальний для більшості існуючих проектів алгоритм децентралізованого консенсусу.

Слід зазначити, що багато проектів алгоритмів швидко та суттєво вдосконалюється. Наприклад, після кількох випадків хакінгу (hacking) на блокчейнах і критики майнінгу біткойнів за марнування енергії, у відповідь на це з'явилося багато пропозицій поліпшення проекту протоколу і поглиблення децентралізації: для збільшення обчислювальної потужності Lightning на Bitcoin знижує обсяг інформації, яку треба записувати на блокчейні; аналогічно LITEX сприяє використанню різних криптоактивів як засобу платежу серед роздрібних торгівців; Phi (розробка String Lab) на Ethereum забезпечує вищі безпеку і швидкість роботи; такі стартапи, як BOINC, каналізують майнінгові обчислення для розв'язання наукових завдань. Важливим питанням для практиків є відсутність одностайності про розвиток блокчейнових протоколів, які наразі допускають розгалуження і тимчасові неясності щодо того, яких саме протоколів мають дотримуватися користувачі блокчейну.

Сучасний розвиток технології блокчейну відновив інтерес до інтелектуальних контрактів, передбачених у 1990-х роках [8]. Хоча загальноприйняте визначення інтелектуальних контрактів перебуває у процесі розроблення, їхня мета, очевидно, полягає в укладенні угод про досягнення умовних зобов'язань, виходячи з децентралізованого консенсусу, мінімізації витрат і автоматизації виконання.

Інтелектуальні контракти – це цифрові контракти, які допускають умовні зобов'язання, залежні від децентралізованого консенсусу, є зламостійкими і самовтілюваними шляхом автоматизованого виконання. Наведене означення відповідає визначенням, зазвичай вживаним ученими-правниками. Важливо сказати, що інтелектуальні контракти, незважаючи на свою роботизацію, не є просто цифровими контрактами (багато з яких покладається на довірений орган влади для досягнення консенсусу і свого виконання) чи елементами штучного інтелекту.

За відсутності децентралізованого консенсусу, сторона, яка надає централізований консенсус, часто користується великою ринковою владою (наприклад, третя сторона з монополією даних). Традиційні рішення третіх сторін (судів чи арбітражів) до великої міри включають не завжди раціональне втручання людини [6], що супроводжується значними невизначеностями і витратами. Інтелектуальні контракти можуть підвищувати здатність до укладення угод і сприяти обміну грошима, нерухомістю, акціями, послугами чи будь-чим вартісним, використовуючи алгоритмічну автоматизовану і безконфліктну процедуру. Якщо виконання інтелектуальних контрактів проводиться третіми сторонами (без автоматизації), то у сусідній Грузії наявності консенсусної реєстрації землі було достатньо для зменшення розбіжностей під час укладення угод і їх виконання.

Що стосується теорії укладення контрактів, то децентралізований консенсус, досягнутий технологією блокчейну, має потенціал до значного розширення кола умов контрактів і звуження сфери дії неповних контрактів. Інтелектуальні контракти можуть змінювати здатність до укладення угод та

їхнього втілення, залежних від певних умов, наприклад, від вимоги блокування (lock-in) для зняття коштів або автоматизованого платежу після успішного отримання товарів імпортером. Таким чином, здатність до укладення угод стає кращою за рахунок більшого розподілу інформації, але це не обов'язково покращує загальний стан економіки.

Досягнення децентралізованого консенсусу вимагає розподілу інформації серед учасників системи. З практичної і регуляторної позиції дуже суттєвими є економічні взаємообміни (компроміси) під час розподілу інформації, необхідного для генерування децентралізованого консенсусу. Оскільки у разі біткойна консенсус досягається і підтримується через всю інформацію про трансакції (з шифруванням за допомогою публічного ключа (public-key-encrypted) для адрес власників) всієї популяції на блокчейні, то публічною є інформація про всі деталі трансакцій (за винятком ідентичностей), записані за консенсусом. Очевидне питання в блокчейнових застосуваннях для реального світу – це ділова приватність. Наприклад, фінансові установи типово є чутливими до розкриття деталей трансакцій непов'язаних сторін. Наприклад, трейдери можуть бажати приховувати свої ідентичності, щоб запобігати довчасному розголошенню (front-running), а більший розподіл інформації може також впливати на індустріальну організацію та конкуренцію.

Через згадані взаємообміни з'явилося багато пропозицій кращого шифрування, яке ефективно маскує чутливу інформацію у процесі генерації консенсусу. Інший очевидний компроміс полягає у досягненні децентралізованого консенсусу на підмножині важливих станів світу чи запитуванні верифікації від меншої кількості вузлів (реєстраторів) у блокчейновій мережі. Наприклад, обговорювався хешінг (hashing) першого етапу для забезпечення пріоритету у часі без подальшого розкриття докладної інформації, щоб запобігати довчасному розголошенню трансакції перед тим, як вона буде записана на блоці розподілених звітів. Із згаданим компромісом безпосередньо пов'язане так зване «доведення з нульовим знанням» у комп'ютерних науках: простими словами, учасники можуть домовитися про певні факти без розкриття корисної інформації. Варто дослідити, як розподіл інформації впливає на приватні та суспільні інтереси, а також на ефективність блокчейнового консенсусу.

Можна побудувати просту економічну модель механізму генерації консенсусу, висвітлюючи роль реєстраторів і природу розподілу інформації. Постановка моделі зумовлена застосуванням до торгівлі та фінансів, яке широко використовується на практиці.

Багато основоположників блокчейну вивчає сценарій, де низка потенційно міжнародних експортерів (продавців) певних продуктів потребує доставки з певними умовами (скажімо, доставка вина потребує дотримання температурного режиму). Успішність продажу цих продуктів імпортерам (клієнтам) потребує різних інших сторін, таких як надавачі логістики, міжнародні порти, митниці (для товарних потоків), нотаріати, фінансові посередники (для платіжних потоків).

Учасники такого процесу постачання, включаючи обов'язково продавця і покупця, можуть вести моніторинг фізичних умов (наприклад, місцезнаходження і температури) товарів через наскрізний збір інформації на основі Інтернету речей (Internet of Things, IoT) – датчиків, інтелектуальних механізмів входів, обробки даних в реальному часі. Для кращих моніторингу і прозорості ці датчики IoT можуть встановлюватися по всьому ланцюгу постачання [9]. Тоді інформацію цих датчиків отримуватиме як продавець, так і покупець.

Інші сторони на блокчейні можуть отримувати потрібну інформацію, яка може сприяти моніторингу процесу. Наприклад, інші продавці можуть теж встановлювати датчики IoT, здатні визначати доставку товарів. Інші клієнти, забираючи інші товари у тому самому порту, без датчиків IoT можуть діставати корисну для себе інформацію про цю доставку. Проте ці сигнали не реєструються на блокчейні.

Висновки з проведеного дослідження. Вирішальний крок на блокчейні – генерування децентралізованого консенсусу про те, чи товари успішно доставлені, з таким агрегуванням відповідної інформації від багатьох залучених сторін (продавця, покупця, надавачів логістики, портів, фінансових посередників), яке задовольняє всю громаду (всі сторони) і реєструється на блокчейні за допомогою залучення верифікаторів. Аналогічно залучаються також інші продавці з IoT, які мають експертизу у верифікації успішності доставки на випадок спорів. У блокчейнових застосуваннях такі залучені сторони (агенти) називаються реєстраторами. Оскільки залучені агенти можуть надавати неправдиві звіти, то залучаються також інші покупці (споживачі) для перевірки сумісності. Тому принцип «клієнт завжди правий» справедливий як на традиційних, так і на блокчейнових ринках.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Cong L.W., He Z. Blockchain disruption and smart contracts. *National Bureau of Economic Research Working Paper*. 2018. 24399. 52 p.

2. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008. 9 p. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 30.08.2019).

3. Narayanan A., Clark J. Bitcoin's academic pedigree. *Communications of the ACM*. 2017. 60. P. 36–45.

4. Горбачук В.М. Методи індустріальної організації. К.: А.С.К., 2010. 224 с.

5. Горбачук В.М., Бойко В.В., Русанов И.А. Проектирование контрактов в условиях риска. *Теория оптимальных решений*. 2011. № 10. С. 116–122.

6. Горбачук В.М., Макаренко О.С. Особливості прийняття рішень людиною для розв'язання складних міждисциплінарних проблем. *Системні дослідження та інформаційні технології*. 2017. № 3. С. 73–87.

7. Горбачук В.М., Дунаєвський М.С., Морозов О.О. Рівноважні інвестиції у кібербезпеку мережі ланцюгів постачання. *Вісник Київського національного університету імені Тараса Шевченка. Серія: фізико-математичні науки*. 2017. № 2. С. 47–52.

8. Szabo N. Formalizing and securing relationships on public networks. *First Monday*. 1997. 2 (9). September 1. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First (дата звернення: 30.08.2019).

9. Горбачук В.М., Кошулько А.І., Сирку А.А. Розподілені децентралізовані мережі сенсорів для спостережень Землі. *16-th Ukrainian conference on space research (August 22–27, 2016, Odessa)*. Kyiv: State Space Agency of Ukraine, 2016. P. 192.

REFERENCES:

1. Cong L.W., He Z. (2018) Blockchain disruption and smart contracts. National Bureau of Economic Research Working Paper. 24399. 52 p.

2. Nakamoto S. (2008) Bitcoin: a peer-to-peer electronic cash system. 9 p. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 30 August 2019).

3. Narayanan A., Clark J. (2017) Bitcoin's academic pedigree. Communications of the ACM, 60, pp. 36–45.

4. Gorbachuk V.M. (2010) Metody industrialnoi orhanizatsii [Methods of industrial organization], Kyiv: A.S.K., 224 p.

5. Gorbachuk V.M., Boiko V.V., Rusanov Y.A. (2011) Proektyrovanye kontraktov v uslovyiakh ryska [Contract design under risk]. Teoryia optymalnykh reshenyi [Theory of optimal decisions], 10, pp. 116–122.

6. Gorbachuk V.M., Makarenko O.S. (2017) Osoblyvosti pryiniattia rishen liudynoiu dlia rozviazannia skladnykh mizhdystsyplinarnykh problem [The features of human decision making for complex interdisciplinary problems solution]. Systemni doslidzhennia ta informatsiini tekhnolohii [System research & information technologies], 3, pp. 73–87.

7. Gorbachuk V.M., Dunaievskyi M.S., Morozov O.O. (2017) Rivnovazhni investytsii u kiberbezpeku merezhi lantsiuhiv postachannia [Equilibrium investments to cybersecurity of supply chain network]. Visnyk Kyivskoho univepsytetu. Sepiia: fizyko-matematychni nauky [Herald of Taras Shevchenko National University of Kyiv. Series: physical and mathematical sciences], 2, pp. 47–52.

8. Szabo N. (1997) Formalizing and securing relationships on public networks. First Monday, 2 (9), September 1. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First (accessed: 30 August 2019).

9. Gorbachuk V.M., Koshulko A.I., Syrku A.A. (2016) Rozpodileni detsentralizovani merezhi sensoriv dlia sposterezhen Zemli [Distributed decentralized sensor networks for Earth observation]. 16-th Ukrainian conference on space research (August 22–27, 2016, Odesa), Kyiv: State Space Agency of Ukraine, p. 192.

Gorbachuk Vasyl
Doctor of Physical and Mathematical Sciences, Senior Research Associate,
Leading Researcher at Department of Mathematical Methods
of Operations Research
V.M. Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine
Lyashko Volodymyr
Candidate of Physical and Mathematical Sciences, Associate Professor,
Senior Lecturer at Department of Informatics
National University of «Kyiv-Mohyla Academy»
Syrku Andrij
Master, Postgraduate Student
V.M. Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine

THE ISSUES OF DECENTRALIZED CONSENSUS IN BLOCKCHAINS

The purpose of the article. The detailed economic analysis of blockchains and smart contracts shows that blockchains are not only the database technologies reducing the costs of data storage or distribution but also the technologies having properties with profound economic implications for generating consensus, designing intellectual contracts, industrial organization, and antitrust policy. The blockchain technology contains a significant potential for reduction of information asymmetry and motivation of market entry but creates preconditions of collusive behavior. This article is devoted to economic analysis of such preconditions.

Methodology. Blockchain as a distributed ledger technology with a decentralized or autonomous management has become popular due to the Bitcoin cryptoasset based upon that technology. Subsequently, this technology has emerged in many other forms often able to store and execute computer programs. It creates such applications as intellectual contracts characterized by payments as results of tamper-proof consensus on contingent outcomes and financed via initial coin offerings.

Results. Despite of various definitions, descriptions, and applications of blockchain and decentalized ledger, this technology and its clowns have a common function to povide a decentralized consensus. A decentralized consensus within a system is defined as a state of the world, in the terms of supplying goods and making payments, which is accepted unanimously and enforced by all the system agents. The specific feature of blockchain technology is that consensus is generated and maintained in a decentralized way capable of improving the system resilience and reduce the rent gained by centralized third parties. For instance, on the Bitcoin blockchain, given history of transactions, the participants can examine and verify records on transactions by a digital way in order to avoid double spending of digital assets and to free everyone from the need in a centralized trustworthy arbiter or a third party. The majority of blockchains has communities of different generations consisting of record keepers and users overlapped in the time. Similar to the third party arbiters in real world, these communities, receiving signals on true state of the world, may have incentives to fabricate, manipulate, or tamper reports.

Practical implications. Many industry dealers assume that blockchain technology has a potential to disrupt business and financial services similar to Internet disrupted offline commerce. Some specialists are doubtful regarding the genuine innovationess and real practicality of blockchain believing that major blockchain application area is carrying out financial operations invisible for state functioners in law and order.

Value/originality. The economists recognize that consensus allows agents interaction with various ideas and incentives as it provides the truth with chain reactions in a social organism, including ethics, contract law, law enforcement, and so on. Contemporary development of blockchain technology has renewed the interest to smart contracts. While a generally accepted concept of smart contracts is currently under development, their goal is to make agreements about contingent commitments based on decentralized consensus, minimal cost, and automated execution. Smart contracts are digital contracts allowing contingent commitments dependent on a decentralized consensus.