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

БЛОКЧЕЙНОВІ ЗАСТОСУВАННЯ У ФІНАНСАХ
THE BLOCKCHAIN APPLICATIONS IN FINANCE

УДК 519.8
https://doi.org/10.32843/infrastruct35-77

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
Сирку А.А.
магістр, аспірант
Інститут кібернетики
імені В.М. Глушкова
Національної академії наук України
Сулейманов Сеїт-Бекір
магістр, аспірант
Інститут кібернетики
імені В.М. Глушкова
Національної академії наук України

За досягнення децентралізованого консенсусу блокчейни залучають для верифікації множину реєстраторів, якими є розподілені (децентралізовані) учасники блокчейну. Даний аналіз відрізняється від традиційних застосувань інформаційної економіки до фінансів і торгівлі. Ключовою є унікальна функціональність блокчейну у генеруванні децентралізованого консенсусу шляхом розподілу інформації на множині реєстраторів. У торговельно-фінансовому сценарії ця функціональність спирається на децентралізацію: система залучає реєстраторів (торгових партнерів, порти, інших продавців або покупців), які своїми діями формують консенсус, схвалений громадою. Потім цей консенсус часто поширюється далі серед усіх агентів на блокчейні. Незважаючи на технологічні досягнення у низці сфер фінансових послуг, велика частина таких послуг для торгівлі здійснюється вручну і на папері багатьма учасниками в різних юрисдикціях усього світу, а тому є вразливою до помилок людей уздовж ланцюга постачання.

Ключові слова: *криптоактиви, реєстри, якість зламостійкого консенсусу, довіра, Інтернет речей, змова, розподіл інформації.*

При достижении децентрализованного консенсуса блокчейны привлекают для верификации множество регистраторов, которыми являются распределенные (децентрализованные) участники блокчейна. Данный анализ отличается от традиционных применений информационной экономики к финансам и торговле. Ключевой является уникальная функциональность блокчейна в генерировании децентрализованного консенсуса путем распределения информации на множестве регистраторов. В торгово-финансовом сценарии эта функциональность опирается на децентрализацию: система привлекает регистраторов (торговых партнеров, порты, других продавцов или покупателей), которые своими действиями формируют консенсус, одобренный обществом. Потом этот консенсус часто распространяется далее среди всех агентов на блокчейне. Несмотря на технологические достижения в ряде областей финансовых услуг, большая часть таких услуг для торговли совершается вручную и на бумаге многими участниками в разных юрисдикциях всего мира, а поэтому является уязвимой к ошибкам людей вдоль цепи снабжения.

Ключевые слова: *криптоактивы, реестры, качество взломостойкого консенсуса, доверие, Интернет вещей, сговор, распределение информации.*

While achieving a decentralized consensus and verifying blocks, blockchains involve a set record keepers – distributed (decentralized) blockchain participants. The analysis given differs from the traditional applications of information economics to finance and trade. The key difference is a unique functionality of blockchain in generating a decentralized consensus by sharing information over set of record keepers. In the basic case of trade and finance scenario, that functionality is based on decentralization: a system involves record keepers (trade partners, ports, other sellers or buyers), which act to form a consensus approved by the community. Then that consensus is often distributed further among all the agents on a blockchain. Despite of technology advances in some areas of financial services, a significant part of such services for trade is implemented by handwork and paperwork across many parties in various jurisdictions around the world, and therefore is vulnerable to human errors along with a supply chain. Every record keeper on a blockchain observes a realization expressing the status of shipment in the case of trade and finance scenario. While payment verifications on the Bitcoin largely concern the double-spending issues, requiring a limited information distribution (for instance, by hiding real identities of transaction parties), validations of general economic activity typically are more complicated, demanding more information. For example, many trade and finance blockchains use the information from local ships, ports, banks, and border customs in order to trace a status of shipment (potentially with assistance of sensors and the Internet of Things devices), though the information details are not fully distributed (similar to the Corda and Hyperlydger blockchains). In such complicated business situations, record keepers most probably observe a noised signal on the true state of world, and the policy of public information disclosure on an arbitrary blockchain might influence on the signal quality of record keepers and the decentralized consensus quality as well.

Key words: *cryptoassets, ledgers, quality of tamper-proof consensus, trust, Internet of Things, collusion, information distribution.*

Постановка проблеми. Майнінг криптоактивів як спосіб підтримки консенсусного запису є характерною особливістю прихильників Bitcoin та Ethereum. Криптоактиви Ripple та R3 CEV використовують свій власний процес консенсусу, покладаючись на громаду реєстраторів. Цей різноманітний процес типово передбачає конкуренцію, призначення на реєстрацію, підтвердження доданих блоків (post-block validations).

Аналіз останніх досліджень і публікацій. Нехай продавець постачає товари клієнту. Тоді дослідимо потік інформації у генеруванні консенсусу про постачання товарів, позначаючи $\tilde{\omega}$ умову успішності постачання. Реєстратори (надавачі логістики, міжнародні порти, митниці, нотаріати, фінансові посередники), потенційно із сенсорами Інтернету речей (Internet of Things, IoT) [1], ведуть моніторинг постачання і надають свої звіти $\tilde{y}_k(\tilde{\omega})$. Протокол блокчейну агрегує ці звіти для формування децентралізованого консенсусу $\tilde{z}$ про стан товарів, положення торгівлі, обсяги платежів тощо. Цей консенсус разом з інтелектуальним контрактом зберігається у блоці (скажімо, xbh53hflojs), якому передує блок (jsf9875htsvx), якому, своєю

чергою, передує ще один блок (wjshfk873gt) [2]. Консенсус є сигналом для проведення платежу за контрактом. Позначимо наступний блок bxfpos76f35r.

Після того як залучені сторони надали свої звіти $\tilde{y}_k$ на блокчейн, блокчейновий протокол генерує децентралізований консенсус $\tilde{z}$ стосовно умовного результату (contingency), основаного на цих звітах. Потім створюється новий блок, який додається до всього ланцюга (chain, чейну). Новостворений блок має пройти певні перевірки на сумісність відносно історії існуючого блокчейну (такими перевірками можна вважати приєднання минулих звітів як входів для генерування поточного консенсусу) перед тим, як додаються наступні блоки. Доданий блок може вимагати подальшої верифікації, як у випадку біткойна формується фіналізований (finalized) або підтверджений (confirmed) блок.

У зазначеному сценарії інші продавці можуть отримувати інформацію двома шляхами на блокчейні: через термінали, зв'язані з датчиками Інтернету речей (Internet of Things, IoT), та шляхом залучення для верифікації трансакції. Ці шляхи відіграють різні ролі, але шлях залучення як істотний крок у генеруванні консенсусу є важливішим для технології блокчейну. Не беручи до уваги питання змови, чим більше інформації мають галузеві експерти (скажімо, інші продавці), тим більша ймовірність формування консенсусу вищої якості у процесах даного сценарію. Обсяг необхідної для консенсусу інформації задає нижню межу на її розподіл. Якщо трансакція, яку треба верифікувати, є зашифрованою, то сам факт залучення експерта фактично розкриває деяку інформацію.

Постановка завдання. Щоб проілюструвати, як децентралізація веде до ефективнішого консенсусу за рахунок більшого розподілу інформації, формалізуємо згаданий сценарій як для публічних, так і ексклюзивних (permissioned) блокчейнів. Припустимо, що інтелектуальний контракт посилається на результат $\tilde{\omega}$ за його умовами, який називатимемо доставкою послуги чи товару. Випадкова змінна $\tilde{\omega}$ приймає значення 1, якщо доставка є успішною, і 0, якщо доставка не є успішною. Позначимо $\tilde{z} \in \{0,1\}$ децентралізований консенсус щодо $\tilde{\omega}$ на блокчейні.

У згаданому сценарії учасники на блокчейні (агенти) дістають різні сигнали за допомогою технологій IoT в реальному часі. Хоча ці технології не стосуються верифікації суб'єктивного досвіду, для простоти припустимо, що всі агенти мають досконалі спостереження $\tilde{\omega}$. Випадок неправдивого звітування охоплює формування інформаційного середовища у міру того, як агенти дістають сигнали, що загалом відрізняються від істинної умови $\tilde{\omega}$. У такому разі для великого класу лінійних моделей можна показати робастність взаємообмінів.

Виклад основного матеріалу дослідження. У мережі Bitcoin (токен – BTC) реєстраторами є майнери, які підтверджують трансакції і гарантують мережу; майнери опосередковано впливають на врядування (governance), маючи деякий контроль над оновленнями протоколу (BTC-BCH) [3]. Майнери є також реєстраторами у мережах Tezos (XTZ) (здійснюють майнінг статків і управління протоколом, пряме голосування статками (stake-voting) на чейні з пропозицій щодо протоколу, включаючи вдосконалення і нові застосування), Dfinity (DFINITIES) (здійснюють майнінг статків і управління протоколом через блокчейнову нервову систему (Blockchain Nervous System, BNS), пряме голосування на чейні з елементами штучного інтелекту, які evolve і навчаються з часом), Filecoin (FIL) (здійснюють зберігання і retrieval файлів, зважаючи на persistency та latency, але не мають безпосереднього врядування щодо протоколу).

У мережах Raiden (RDN) та 1protocol (CRED) реєстраторами є оператори: у RDN оператори здійснюють пошук шляхів, моніторинг каналів, gateway тощо; у CRED оператори здійснюють майнінг статків від імені капіталістів (capitalists), а також безпосереднє врядування мережі.

У мережах Cosmos (ATOM) та Polkadot (DOT) реєстраторами є валідатори: в ATOM валідатори здійснюють доведення статків і валідацію трансакцій, пряме голосування статками на чейні щодо оновлень протоколу; у DOT валідатори (а також номінатори й рибалки) здійснюють валідацію трансакцій та оголошення поміж блокчейнів або інтелектуальних контрактів, дисциплінування процесу валідації, а також безпосереднє врядування мережі.

У мережі Augur (REP) реєстраторами є репортери, які здійснюють звітування про наслідки подій, а також опосередковане врядування мережі.

У мережі 0x (ZRX) опорники (relayers) здійснюють гарантію ліквідності, розвиток ринку (market making), пошук арбітражу, пряме голосування статками на чейні щодо оновлень протоколу.

У мережі Truebit (TRU) вирішувачі (solvers) та претенденти (challengers) здійснюють верифікацію обчислень і дисциплінування системи, а також безпосереднє врядування мережі.

У мережі Maker (MKR, Dai) пошукувачі (seekers) арбітражу, позичальники Dai, закривачі (closers) заставленої боргової позиції (Collateralized Debt Position, CDP) здійснюють пошук можливостей арбітражу, підтримуючи стабільність Dai; найбільші держателі MKR є водночас реєстраторами.

Для моделювання процесу консенсусу припустимо, що блокчейновий протокол залучає множину $\mathrm{K} = \{1,\ldots,K\}$ потенційних реєстраторів, яких уважаємо однорідними. Нехай ефективність консенсусу для укладення угод (чи інших суспільних цілей) вимірюється дисперсією $Var(\tilde{\omega} - \tilde{z})$. На

практиці ефективність залежить від мети і використання консенсусу на кожному конкретному блокчейні. Дисперсія якісно враховує загальну думку про те, що консенсус завжди не є ефективним, коли неточно виражає істину. Крім того, дисперсія є робастною мірою ефективності при введенні штрафів за зсуненість із моментами вищих порядків. Багато фірм фінтеху (Fintech) вважає, що ефективний консенсус є наріжним каменем довіри.

Під час свого залучення кожний реєстратор $k \in \mathrm{K}$ надає звіт $\tilde{y}_k \in \{0,1\}$, породжуючи набір звітів $\vec{y} = \{\tilde{y}_k\}_{k\in\mathrm{K}}$. Якщо $\tilde{y}_k \neq \tilde{\omega}$, то реєстратор k надав неправдивий звіт. Нехай, наприклад, функція консенсусу задається

$$\tilde{z}(\vec{y}) = \begin{cases} 1 \text{ з імовірністю } P = \sum_{k=1}^{K} w_k \tilde{y}_k, \\ 0 \text{ в інших випадках} \end{cases}$$

де сума невід'ємних ваг $w_k \geq 0$ для y_k дорівнює 1. Припущення $w_k \to 0$ за $K \to \infty$ характеризує ключову рису децентралізації. Якщо реєстратори більше звітують про успішну доставку, то значення функції консенсусу ближче до 1. Дослідимо, як метрика децентралізації множини K впливає на якість децентралізованого консенсусу та загальносистемний розподіл інформації. Загалом

$$\tilde{z}(\vec{y}) = \tilde{Z}\left(\sum_{k=1}^{K} w_k \tilde{y}_k\right) \in [0,1], \qquad (1)$$

а математичне сподівання (expectation) $E(\tilde{Z})$ є диференційованою і зростаючою функцією, причому $E(\tilde{Z}) = \tilde{Z}$ для $\tilde{Z} \in \{0,1\}$ (якщо всі звіти є точними, то консенсус відбиває істинний стан світу). Зазначені риси спостерігаються на багатьох існуючих блокчейнових протоколах.

В альтернативній постановці змінні $\tilde{\omega}$, $\tilde{z}$, $\tilde{y}_k$ можуть приймати континуум значень, а не тільки бінарні значення. Залежно від конкретного блокчейнового протоколу консенсус $\tilde{z}(\vec{y})$ є перетворенням входів $\tilde{y}_k$, зібраних від залучених реєстраторів. Співвідношення (1) охоплює багато відомих блокчейнів (наприклад, Bitcoin), де майнер, який розв'язує важку NP-повну проблему першим (це стається цілком випадково, коли майнери мають однакові обчислювальні потужності), здійснює блок записів. Іншими словами, блокчейновий протокол випадково вибирає один звіт від усіх залучених реєстраторів (майнерів).

Для простоти дослідимо великий клас лінійних моделей, які зазвичай використовуються у просторі континууму сигналів, де децентралізований консенсус є простим середнім [4] усіх вибраних звітів:

$$\tilde{z}(\vec{y}) = \frac{1}{K}\sum_{k=1}^{K} y_k. \qquad (2)$$

Можна показати, що тоді багато результатів є робастними до гетерогенних і стохастичних ваг для сигналів для компромісу між більшою децентралізацією (для поліпшення якості консенсусу) і меншою децентралізацією (для зниження розподілу інформації).

Припустимо, кожний реєстратор на блокчейні спостерігає реалізацію $\tilde{\omega}$ – статус доставки. Якщо платіжні верифікації на Bitcoin здебільшого торкаються питань подвійних витрат, потребуючи обмеженого розподілу інформації (скажімо, маскуються реальні ідентичності сторін трансакції), то валідації загальної економічної діяльності типово є складнішими, вимагаючи більше інформації. Наприклад, багато торговельно-фінансових блокчейнів використовують інформацію від місцевих суден, портів, банків і прикордонних митниць для відстеження статусу доставки, потенційно за допомогою датчиків і приладів IoT, деталі якої повністю не розголошуються (як у блокчейнах Corda чи Hyperlydger). У подібних ускладнених ділових ситуаціях реєстратори, мабуть, спостерігають лише зашумлений сигнал про істинний стан, а політика розкриття публічної інформації на будь-якому блокчейні, ймовірно, впливає на якість сигналу реєстраторів, а отже, на якість децентралізованого консенсусу.

Щоб доєднати потенційно зашумлене спостереження, припустимо, що кожний реєстратор i на блокчейні має приватний сигнал $\tilde{x}_i = \tilde{\omega} + \tilde{\eta}_i$, де для простоти вважаємо шуми $\tilde{\eta}_i$ незалежно однаково розподіленими з нульовим середнім і дисперсією σ_η^2. У шумі враховується істинний стан, оснований на публічній інформації, наявній інформації про блокчейн поза чейном, додатковій інформації за генерування консенсусу.

Позначимо $\vec{1}_k$ подію залучення реєстратора k, після якої його сигналом стає

$$\tilde{x}_k = \tilde{\omega} + \tilde{\eta}_k, \qquad (3)$$

де випадкова величина $\tilde{\eta}_k$ має нульове середнє і дисперсію $\sigma_{\mathrm{K}}^2 \leq \sigma_\eta^2$ (нерівність має місце завдяки додатковій (потенційно зашифрованій) інформації). Тоді інформаційну множину реєстраторів на блокчейні задає набір K, $\{\tilde{x}_i\}_{i\notin\mathrm{K}}$, $\{\tilde{x}_k, \vec{1}_k\}_{k\in\mathrm{K}}$, $\tilde{z}$.

Ураховуючи рівність (2), запишемо нормалізовану корисність кожного нейтрального до ризику реєстратора, який надає звіт $\tilde{y}_k$, у вигляді

$$U(y_k; \vec{y}) = \tilde{b}_k(\tilde{z}(\vec{y}) - \tilde{x}_k) - \frac{1}{2h}(y_k - \tilde{x}_k)^2 =$$
$$= \frac{\tilde{b}_k}{K}\sum_{k=1}^{K} y_k - \tilde{b}_k\tilde{x}_k - \frac{(y_k - \tilde{x}_k)^2}{2h}, \qquad (4)$$

де зсуненість (bias) реєстратора k у неправдивому звітуванні, відома цьому реєстратору перед тим, як він надає свій звіт, визначається

$$\tilde{b}_k = \tilde{b} + \tilde{\varepsilon}_k. \qquad (5)$$

Тут спільна (серед залучених реєстраторів) випадкова зсуненість $\tilde{b}$ має нульове середнє і дисперсію σ_b^2; $\tilde{b}$ ураховує спільну упередженість на блокчейні, яку можна інтерпретувати як вибір валідаторів однією інституційною стороною тран-

сакції у своїй власній (proprietary) мережі (колегіальний відбір на Ripple чи нотаріальний вибір на Corda), тобто спробу держателів криптоактивів пригальмувати виникнення інфляції валюти та/або загальносистемний мотив хакінгу. Подібна зсуненість зустрічається в традиційній економіці: арбітри у діловому арбітражі винагороджуються лише тоді, коли вибираються їхніми клієнтами і можуть систематично cater до головних клієнтів. Окрім того, специфічні члени $\tilde{\varepsilon}_k$ є незалежно однаково розподіленими з нульовим середнім і дисперсією σ_ε^2. Член $\frac{1}{2h}(y_k - \tilde{x}_k)^2$ враховує приватну вартість маніпуляції, де h – параметр швидкості підвищення вартості з величиною неправдивого звітування, залежної від проекту протоколу консенсусу.

Кожний залучений реєстратор (record keeper) обирає $y_k = y_k^*$, щоб максимізувати функцію корисності (4):

$$0 = \frac{\partial U(y_k; \vec{y})}{\partial y_k} = \frac{\tilde{b}_k}{K} - \frac{2}{2h}(y_k^* - \tilde{x}_k),$$

$$y_k^* = \tilde{x}_k + \frac{h\tilde{b}_k}{K} = \tilde{\omega} + \tilde{\eta}_k + \frac{h\tilde{b}_k}{K}, \qquad (6)$$

ураховуючи рівність (3). Тоді рівності (2) і (5) дають

$$\tilde{z}(\vec{y}) = \frac{1}{K}\sum_{k=1}^{K} y_k = \frac{1}{K}\sum_{k=1}^{K}\left(\tilde{\omega} + \tilde{\eta}_k + \frac{h\tilde{b}_k}{K}\right) =$$

$$= \tilde{\omega} + \frac{1}{K}\sum_{k=1}^{K}\tilde{\eta}_k + \frac{1}{K}\sum_{k=1}^{K}\frac{h}{K}(\tilde{b} + \tilde{\varepsilon}_k) =$$

$$= \tilde{\omega} + \frac{1}{K}\sum_{k=1}^{K}\tilde{\eta}_k + \frac{h}{K}\left(\tilde{b} + \frac{1}{K}\sum_{k=1}^{K}\tilde{\varepsilon}_k\right),$$

звідки

$$E(\tilde{z} - \tilde{\omega}) = 0,$$

$$Var(\tilde{z} - \tilde{\omega}) = \frac{\sigma_\text{К}^2}{K} + \frac{h^2}{K^2}\left(\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right) \qquad (7)$$

дисперсія є сумою двох доданків з різною інтерпретацією.

Доданок $\frac{\sigma_\text{К}^2}{K}$ безпосередньо пов'язаний з якістю сигналу. Наприклад, залучення для верифікації шляхом надання деяких деталей інформації про трансакції може знижувати $\sigma_\text{К}$, поліпшуючи якість консенсусу. Крім того, цей доданок показує, що за збільшення розміру K вибірки згладжуються шуми $\tilde{\eta}_k$ спостережень, також покращуючи консенсус.

Доданок $\frac{h^2}{K^2}\left(\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right)$ пов'язаний із процесом генерації децентралізованого консенсусу. Коли блокчейн залучає все більше реєстраторів (збільшуючи K), то кожний усвідомлює про свій менший вплив на кінцевий результат консенсусу. Тоді звіти y_k^* зазнають менше маніпуляцій (у силу співвідношення (6)), збільшуючи ефективність консенсусу з множником $\frac{1}{K^2}$ (у силу співвідношення (7)) і безпечність блокчейну. Крім того, безпечності блокчейну сприяють технічні досягнення кібербезпеки. Авжеж, агрегація сприяє кращому консенсусу, зменшуючи вплив idiosyncratic-компонентів неправдивого звітування.

Проте залучення більшої кількості реєстраторів впливає на інформаційне середовище, яке агенти займають на блокчейні: залежно від деталізації блокчейнових протоколів збирання звітів включає передачу певної інформації про трансакції до залучених реєстраторів, змінюючи $\sigma_\text{К}$ (як у згаданій мережі Corda); хоча зміст інформації може шифруватися, власне подія залучення реєстратора (позначена $\vec{1}_k$) несе інформацію. З погляду індустріальної організації, це несе публічну інформацію про агреговану економічну діяльність за залучення всіх агентів, що полегшує змову і загрожує конкуренції.

Реєстратори можуть діставати додаткову інформацію про трансакцію після укладення контракту. Наприклад, IBM працює над торговельно-фінансовими блокчейнами, які забезпечують реєстраторів додатковою інформацією про статус поставки, бо генерування консенсусу про доставку вимагає співробітництва поза чейном і перехресних перевірок із shipping-компаніями й установами експортно-імпортного контролю.

Реєстратори можуть мати стимули до надання неправдивих звітів. Наприклад, у торговельно-фінансових застосуваннях реєстратори є також сторонами, залученими до трансакції: майнери біткойну можуть приховувати звіти шляхом егоїстичного майнінгу чи витрачати певні койни двічі. У наведеній моделі неправдиве звітування є деяким шумом унаслідок можливості зламу реєстраторів. Подібні стимули існують також у традиційній економіці: арбітри (третейські судді) справ могли надавати перевагу певному клієнту, а подвійні витрати були проблемою у традиційних онлайнових платежах, яка, власне, спричинила створення біткойну. Фактично повідомлення засобів масової інформації та обговорення практиків здебільшого зосереджувалися на тому, як блокчейн допомагає знижувати фальсифікацію, маніпуляцію та злам.

Припустимо, що кожний нейтральний до ризику реєстратор k надає звіт $y_k \in \{0,1\}$, щоб максимізувати свою нормалізовану корисність

$$U(y_k; \vec{y}) = b_k \mid \tilde{z}(\vec{y}) - \tilde{\omega} \mid - h_k \mid y_k - \tilde{\omega} \mid =$$

$$= b_k \left| \tilde{Z}\left(\sum_{i=1}^{K} w_i y_i\right) - \tilde{\omega} \right| - h_k \mid y_k - \tilde{\omega} \mid, \qquad (8)$$

де b_k, h_k є додатними та рівномірно обмеженими нулем коефіцієнтами $\forall k$: b_k є виграшем реєстратора k за досягнення хибного консенсусу (коли замість істинного стану $\tilde{\omega}$ формується стан $(1 - \tilde{\omega})$); h_k охоплює вартість неправдивого звітування. Залежно від проектування протоколу в конкретних торговельно-фінансових застосуваннях h_k може відповідати вартості репутації у блокчейновій групі чи вартості контрафактних сигналів у сенсорах IoT. Неточні записи у випадку біткойну потребують тривалішого підтвердження і мають вищу ймовірність своєї відміни, а у випадку сис-

тем PoW потребують надзвичайно великої обчислювальної потужності.

Кожний залучений реєстратор, максимізуючи функцію (8), вибирає

$$\tilde{y}_k^* = \begin{cases} \tilde{\omega} \text{ при } h_k \geq b_k w_k, \\ 1-\tilde{\omega} \text{ в інших випадках.} \end{cases}$$

Виграш від неправдивого звітування становить $b_k w_k$, бо воно зсуває консенсус на w_k за заданих рівноважних стратегій решти гравців, а втрати від такого звітування становлять h_k. Тоді рівноважним консенсусом є

$$\tilde{z} = \begin{cases} \tilde{\omega} \text{ з імовірністю } \sum_{k \in \mathrm{K}^*} w_k, \\ 1-\tilde{\omega} \text{ в інших випадках,} \end{cases} \quad (9)$$

де $\mathrm{K}^* = \{k \in \mathrm{K}: \ h_k > b_k w_k\}$ – множина реєстраторів, які надають правдиві звіти. У силу співвідношення (9) за даного розподілу інформації результуюча якість децентралізованого консенсусу вимірюється дисперсією

$$Var(\tilde{\omega} - \tilde{z}) = Var[\tilde{\omega} - (1-\tilde{\omega})]\left(1 - \sum_{k \in \mathrm{K}^*} w_k\right)^2$$

$$= Var(2\tilde{\omega} - 1)\left(1 - \sum_{k \in \mathrm{K}^*} w_k\right)^2, \quad (10)$$

де $Var(2\tilde{\omega}-1)$ не залежить від K. Отже, чим більша множина K^*, тим менша дисперсія (10) і вища якість децентралізованого консенсусу. Виграш децентралізації виражається тим, як обсяг K залучених реєстраторів поліпшує якість консенсусу шляхом зменшення стимулів кожного реєстратора до маніпуляції та розширення множини K^* до всієї множини K. Наприклад, у випадку однорідних симетричних реєстраторів з $b_k = b > 0$, $h_k = h > 0$, $w_k = \frac{1}{K}$ маємо $\mathrm{K}^* = \left\{k \in \mathrm{K}: h > \frac{b}{K}\right\} = \left\{k \in \mathrm{K}: K > \frac{h}{b}\right\}$ і вищу якість консенсусу за більшого K.

Загалом децентралізований консенсус стає досконалим ($\tilde{z} = \tilde{\omega}$) при $K \to \infty$, що сприяє укладенню контрактів, входу в ринок і конкуренції.

У літературі з фінансової економіки часто вивчається саме поширення наявної інформації. Прикладом розкриття інформації, яке типово стосується прозорості, є система звітування TRACE на ринку корпоративних облігацій [5; 6]. Ринкові гравці (market makers) можуть користуватися торговою інформацією для підтримування поведінки змови [7]. Процеси трейдингу й агрегації відбуваються, незважаючи на вплив вимог TRACE для прозорості на мотивацію кожного трейдера й ефективність ринкової функції. Іншими словами, коли великий обсяг публічної інформації є шкідливим, то регулятори чи агенти можуть вирішити поширювати менше інформації.

Зосередимося на генеруванні децентралізованого консенсусу: поширення інформації під час генерування консенсусу є ключовою функцією блокчейну для забезпечення децентралізованого консенсусу і протизламної стійкості. Чим більший ступінь поширення інформації, тим вища якість децентралізованого консенсусу: спроби обмеження децентралізації з метою зменшення ступеня поширення інформації часто знижують операційну стійкість, яка вважається перевагою технології над централізованими системами [2]. Загалом якість консенсусу й обсяг розподілу інформації на блокчейнах залежать від їхніх конкретних протоколів. Є багато алгоритмів для побудови консенсусу, основаному на таких вимогах, як продуктивність (performance), масштабованість, сумісність, місткість даних, урядування, безпека, завадостійкість (failure tolerance). Не маючи на меті деталізацію різних механізмів консенсусу чи поліпшення проектування блокчейну, торкнемося блокчейнових застосувань до фінансової галузі та думок практиків про обмін інформацією.

Виходячи з функціонування блокчейну, обговоримо різні реальні блокчейнові проекти. Коло застосування інтелектуальних контрактів і технології блокчейну часто виходить за межі галузі фінтеху. Наприклад, аналіз 834 інтелектуальних контрактів від Bitcoin та Ethereum з 1 673 271 трансакцією виявив п'ять основних категорій застосування (фінансову, нотаріальну, ігрову, бібліотечну, розрахункову), три з яких пов'язуються з грошовими трансфертами і трансакціями, а дві – з реєстрацією інформації консенсусу [2]. Більшість застосувань пов'язана з управлінням, збором і розподілом грошей.

За даними Світової організації торгівлі, міжнародна торгівля у 2015 р. становила понад 10 трлн дол. США. Якщо продавець (експортер) може вимагати від покупця (імпортера) передоплати за поставлені товари, то покупець (імпортер) може бажати знижувати ризик, вимагаючи від продавця документування товарів, які були відправлені. Типово банки можуть надавати різні форми підтримки як продавцям, так і покупцям. Наприклад, банк імпортера може надати акредитив (letter of credit, LC) експортеру чи його банку, забезпечуючи платіж після отримання певних документів, наприклад, накладної (bill of lading). Банк експортера може надати позику (через аванс) експортеру на підставі експортного контракту. Малі постачальники мають чекати від 60 до 90 днів оплати за поставлені товари, що заважає їхньому доступу до робочого капіталу. Імпортеру може не вдатися укласти угоду (fail to strike a deal), коли банк, який надав акредитив, не має відповідної репутації в країні експортера. Експортер може не отримати аванс, коли банк не впевнений в успішному та своєчасному постачанні товарів і забезпеченні платежів від імпортера.

Технологія блокчейну може допомагати вирішувати вищезазначені проблеми торгівлі. Ця технологія може запропонувати два класи рішень.

Перший клас стосується потоку товарів, бо децентралізований реєстр може краще відстежувати товари під час процесу, в якому ці товари відправляються, зберігаються і доставляються (скажімо, фізичні місця розташування і пересування, температурні умови зберігання тощо), застосовуючи такі комунікаційні технології, як IoT та експертні системи, що обробляють офлайну інформацію. Другий клас рішень торкається взаємозв'язку між грошима і торгівлею (наприклад, акредитивів і фінансів торгівлі, пов'язаних із довірчими платежами). Хоча обидва класи рішень розвивалися окремо, галузеві практики планують на майбутнє повністю інтегровану систему, яка може бути кращою для мережі вантажовідправників, експедиторів (freight forwarders), морських перевізників, портів, митних органів і банків, які взаємодіють на блокчейні в реальному часі.

У 2016 р. банк Barclays і фінтех-стартап Wave повідомили, що стали першими організаціями, які виконують глобальну торговельну трансакцію з використанням нової блокчейнової платформи Wave – трансакцію LC між Ornua (колишньою Irish Dairy Board (Ірландською молочною радою)) та Seychelles Trading Company (Сейшельською торговельною компанією). Також у 2016 р. фірма IBM започаткувала застосування блокчейнів та інтелектуальних контрактів до фінансів торгівлі, запропонувавши рішення для транснаціональної Indian Mahindra Group (Індійської групи Махіндра) у партнерстві з данською транснаціональною компанією Maersk. У 2017 р. IBM та Maersk за співробітництва з Hyperledger Fabric оголосили про завершення пілотного проекту наскрізного (end-to-end) цифровізованого ланцюга постачання з використанням технології блокчейну, який включає сторони торгівлі, різні порти і митні органи [2]. Цим проектом була партія вантажу (консигнація) від транснаціональної компанії Schneider Electric з м. Ліон (Франція) до м. Ньюарк (США), включаючи порт Роттердам (Нідерланди), порт Ньюарк (США), Митну адміністрацію Нідерландів (Customs Administration of the Netherlands), Директорат науки і технології Міністерства внутрішньої безпеки США (U.S. Department of Homeland Security Science and Technology Directorate), Службу митного і прикордонного контролю США (U.S. Customs and Border Protection). Продовжуючи новітні проекти, у 2017 р. IBM розгорнула Yijian Blockchain Technology Application System для фармацевтичного сектору Китаю. IBM також співпрацювала з групою компаній для розроблення фінансової платформи торгівлі сирою нафтою, основаної на блокчейні. Інші основані на блокчейні платформи, які підтримують трансакції надання позик, емітування LC, експортного кредитування, страхування, включають HK Blockchain для фінансів торгівлі, TradeSafe, Digital Trade Chain (DTC). Блокчейновий стартап R3, фінтех-провайдер TradeIX і група великих банків перевели свою платформу Marco Polo фінансів торгівлі у пілотну стадію [2].

Спостерігається прогрес у застосуванні технології блокчейну до галузі вантажоперевезень і логістики. У 2017 р. Maersk у партнерстві з консалтинговою компанією Ernst & Young, софтверною компанією Microsoft, страховою компанією Willis Towers Watson та іншими страхувальниками організувала безпечний обмін даними поставок на KSI – блокчейні, розробленому Guardtime. У 2017 р. асоціація Blockchain in Transport Alliance, куди входить такий блокчейновий стартап, як ShipChain, залучила відомі софтверну компанію SAP і поштову компанію UPS [2].

Платежі на великі відстані чи невідомій стороні утруднюються проблемою недостатньої довіри. Товариство світових міжбанківських телекомунікацій (Society for Worldwide Interbank Financial Telecommunications, SWIFT) зменшує цю проблему, але нерідко передбачає неефективну координацію між багатьма інституціями і значні внески. Водночас координація і трансакційні видатки істотні для цифрових платежів, які несуть ризики подвійних витрат. За побудовою підтримування децентралізованого консенсусу на блокчейні Bitcoin вимагає від майнерів розв'язання NP-повних обчислювальних задач (тобто майнінгу біткойнів, або форми доведення роботи (proof-of-work, PoW)), рівень важкості яких зростає з обчислювальною потужністю, утруднюючи обробку великих обсягів фінансових трансакцій. Наступні платформи (такі як Lightning (основана на блокчейні Bitcoin) та Stellar (окремий блокчейн)) допомагають поліпшувати потужність обробки через локальні канали та багатопідписні рахунки таким чином, що зайва інформація не є потрібною для децентралізованого консенсусу. Платформа Counterparty теж основана на блокчейні Bitcoin, але дозволяє гнучкіші інтелектуальні контракти і підтримує консенсус через доведення знищення (proof-of-burn), тобто через руйнування внесків у криптоактиві, сплачених клієнтам, і відповідну ревальвацію цього криптоактиву для вузлів за валідації. Біткойни стали першим рішенням, яке запропонувало анонімні рівноправні (peer-to-peer) трансакції, записані на блокчейні Bitcoin для безпеки, часової мітки (time stamp) і протизламної стійкості [8]. Мова кодування таких блокчейнів є обмеженою. Друга (після Bitcoin) за ринковою капіталізацією блокчейнова платформа Ethereum допускає використання повної (за Тюрінгом (Turing)) мови і складніших умовних операцій, забезпечуючи класичне здійснення інтелектуальних контрактів із валідними оновленнями контрактних станів.

Висновки з проведеного дослідження. Після того як багато роздрібних торгівців Японії стали

приймати біткойни, подібна практика швидко поширилася по всьому світу, включаючи Україну. Важливо, що розподілений реєстр Bitcoin забезпечує децентралізований консенсус щодо події транзакції, публічно транслюючи про всі кандидатури на трансакції і підтримуючи майнерів, які постійно конкурують за коректний запис нових блоків для здобуття біткойнів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

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

2. Cong L.W., He Z. Blockchain disruption and smart contracts. *National Bureau of Economic Research Working Paper*. 2018. № 24399. 52 p.

3. Zurrer R. KeepersWorkers that maintain blockchain networks. *Medium*. 2017. August 5. URL: https://medium.com/@rzurrer/keepers-workers-that-maintain-blockchain-networks-a40182615b66 (дата звернення: 27.09.2019).

4. Knopov P.S., Kasitskaya E.J. *Empirical estimates in stochastic optimization and identification*. Dordrecht, Netherlands : Kluwer, 2002. 250 p.

5. Goldstein M.A., Hotchkiss E.S., Sirri E.R. Transparency and liquidity: a controlled experiment on corporate bonds. *Review of financial studies*. 2006. № 20. P. 235–273.

6. Bessembinder H., Maxwell W. Markets transparency and the corporate bond market. *Journal of economic perspectives*. 2008. № 22. P. 217–234.

7. Bloomfield R., O'Hara M. Market transparency: who wins and who loses? *Review of financial studies.* 1999. № 12. P. 5–35.

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

REFERENCES:

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

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

3. Zurrer R. (2017) KeepersWorkers that maintain blockchain networks. Medium, August 5. Available at: https://medium.com/@rzurrer/keepers-workers-that-maintain-blockchain-networks-a40182615b66 (accessed 27 September 2019).

4. Knopov P. S., Kasitskaya E. J. (2002) Empirical estimates in stochastic optimization and identification. Dordrecht, Netherlands: Kluwer.

5. Goldstein M. A., Hotchkiss E. S., Sirri E. R. (2006) Transparency and liquidity: a controlled experiment on corporate bonds. Review of financial studies, no. 20, pp. 235–273.

6. Bessembinder H., Maxwell W. (2008) Markets transparency and the corporate bond market. Journal of economic perspectives, no. 22, pp. 217–234.

7. Bloomfield R., O'Hara M. (1999) Market transparency: who wins and who loses? Review of financial studies, no. 12, pp. 5–35.

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

Gorbachuk Vasyl
Doctor of of Physical and Mathematical Sciences, Senior Research Associate,
Leading Research Associate at
Department of Mathematical Methods of Operations Research
V.M. Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine
Syrku Andrij
Master, Postgraduate Student
V.M. Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine
Suleimanov Seit-Bekir
Master, Postgraduate Student
V.M. Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine

THE BLOCKCHAIN APPLICATIONS IN FINANCE

The purpose of the article is achieving a decentralized consensus and verifying blocks when blockchains involve a set record keepers – distributed (decentralized) blockchain participants. Those participants may form the functional role groups.

Methodology. The analysis given differs from the traditional applications of information economics to finance and trade. The key difference is a unique functionality of blockchain in generating a decentralized consensus by sharing information over set of record keepers. In the basic case of trade and finance scenario, that functionality is based on decentralization: a system involves record keepers (trade partners, ports, other sellers or buyers), which act to form a consensus approved by the community. Then that consensus is often distributed further among all the agents on a blockchain.

Results. Despite of technology advances in some areas of financial services, a significant part of such services for trade is implemented by handwork and paperwork across many parties in various jurisdictions around the world, and therefore is vulnerable to human errors along with a supply chain. Every record keeper on a blockchain observes a realization expressing the status of shipment in the case of trade and finance scenario. While payment verifications on the Bitcoin largely concern the double-spending issues, requiring a limited information distribution (for instance, by hiding real identities of transaction parties), validations of general economic activity typically are more complicated, demanding more information. For example, many trade and finance blockchains use the information from local ships, ports, banks, and border customs in order to trace a status of shipment (potentially with assistance of sensors and the Internet of Things devices), though the information details are not fully distributed (similar to the Corda and Hyperlydger blockchains). In such complicated business situations, record keepers most probably observe a noised signal on the true state of world, and the policy of public information disclosure on an arbitrary blockchain might influence on the signal quality of record keepers and the decentralized consensus quality as well.

Value/originality. Payments to distant or unknown parties are complicated by the problem of insufficient trust. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) mitigates that problem, but often entails inefficient coordination among multiple institutions and significant service fees. At the same time, coordination and transaction costs are important for digital payments bearing the risks of double- spending. Bitcoins become the first solution suggesting anonymous peer-to-peer transactions recorded on the Bitcoin blockchain to get security, time stamp and tamper-proofness. As a result, today many retailers in Japan accept bitcoins. The most important is that a distributed ledger of Bitcoin provides a decentralized consensus regarding to the fact of transaction, publicly broadcasting all candidate transactions and supporting miners, which constantly compete for a correct record of new blocks to gain bitcoins.