МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 338.48

Костинець В.В.,
кандидат економічних наук,
доцент кафедри бізнес-економіки та туризму,
Київський національний університет технологій та дизайну

ТЕХНОЛОГІЯ BLOCKCHAIN У ТУРИЗМІ ТА ІНФОРМАЦІЙНІ ЗАГРОЗИ ЇЇ РЕАЛІЗАЦІЇ

Костинець В.В. Технологія blockchain у туризмі та інформаційні загрози її реалізації. Статтю присвячено аналізу інформаційних загроз реалізації технології блокчейн у туризмі. Автором досліджено глобальних посередників, які провадять свою діяльність на онлайн-ринку туристичних послуг. Висвітлено особливості використання блокчейну на ринку туристичних послуг. Визначено принципи роботи блокчейн-платформи бронювання туристичних послуг. Проведено аналіз інформаційної безпеки використання технології блокчейн у туризмі.

Ключові слова: блокчейн, ринок туристичних послуг, інформаційні загрози, інформаційна безпека, глобальні посередники.

Костинец В.В. Технология blockchain в туризме и информационные угрозы ее реализации. Статья посвящена анализу информационных угроз реализации технологии блокчейн в туризме. Автором исследованы глобальные посредники, осуществляющие свою деятельность на онлайн-рынке туристических услуг. Освещены особенности использования блокчейна на рынке туристических услуг. Определены принципы работы блокчейн-платформы бронирования туристических услуг. Проведен анализ информационной безопасности использования технологии блокчейн в туризме.

Ключевые слова: блокчейн, рынок туристических услуг, информационные угрозы, информационная безопасность, глобальные посредники.

Kostynets V.V. Blockchain-technology in tourism and information threats implementation. The article is devoted to the analysis of information threats to the implementation of the blockchain-technology in tourism. The author investigates global intermediaries, who conduct their activities on the online-market of tourist services. There are highlighted the peculiarities of the use of blockchain on the market of tourist services. There are determined the principles of work of the blockchain-platform for reservation of tourist services. There was carried out the analysis of the information security of the use of the block cock technology in tourism.

Key words: blockchain, market of tourist services, information threats, information security, global intermediaries.

Постановка проблеми. Провідний постачальник технологій для індустрії туризму і подорожей Sabre Corporation (NASDAQ: SABR) у квітні 2018 р. опублікував новий технологічний прогноз Emerging Technology Report-2018, підготовлений дослідницьким підрозділом Sabre Labs. У цьому звіті розглядаються перспективи інноваційних технологій та їхній вплив на туризм у наступному десятилітті. Головними трендами 2018 р. в туризмі стали автоматизація і блокчейн [1]. Саме блокчейн як інноваційна технологія відкриває нові можливості для суб'єктів економічної діяльності, у тому числі для учасників ринку туристичних послуг. Таким чином, проведення аналізу можливостей реалізації технології блокчейн у туризмі, а також інформаційних загроз її використання є актуальною проблемою.

Аналіз останніх досліджень і публікацій. Питанню використання технологій блокчейн в економіці присвячено публікації переважно зарубіжних учених, серед яких: Д. Аксенов [2], П. Вінья [3], Р. Воттенхофер [4], А. Купріков [2], С. Корчагін [5], М. Кейнсі [3], Б. Марр [6], А. Меньщиков [7], Д. Мигунов [8], І. Савельєв [9], К. Скіннер [10], М. Свон [11], Д. Тапскотт [12], А. Тапскотт [12] та деякі інші. Попри це маловивченою лишається проблема використання блокчейн на ринку туристичних послуг, із чим і пов'язана актуальність дослідження.

Формулювання цілей статті. Метою дослідження є аналіз інформаційних загроз реалізації технології блокчейн у туризмі.

Виклад основного матеріалу. Сьогодні у світовій туристичній галузі домінують кілька глобальних посередників, які поділили між собою ринок дистрибуції туристичних послуг:

1. GDS (Global Distribution Systems): Amadeus, Sabre, Travelport – глобальні системи дистрибуції, Інтернет-майданчики B2B, які з'єднують постачальників турис-

тичних послуг з їх продавцями (агентами). GDS дають змогу компаніям-постачальникам завантажити у свої бази даних актуальну інформацію про номерний фонд, авіарейси, доступні квитки, оренду автомобілів, налаштувати логіку і розклад, а агентствам – переглядати цю інформацію, здійснювати бронювання, проводити оплату. Як правило, GDS стягують абонентську плату за доступ до своєї інформаційної системи. З постачальників – для розміщення ресурсів, з агентів – для бронювання. Комісія з бронювань також не виключена. Таким чином, це додаткові витрати, які істотно підвищують вартість туристичних послуг, адже готелі й авіакомпанії закладають їх у ціну.

2. OTA (Online travel Agencies): Priceline, Expedia – Інтернет-турагентства, які відомі всім, це гіганти світового туристичного ринку типу Booking.com, Expedia.com і т. д. Онлайн-турагентства, про які йдеться, – це маркетплейси, передусім, для готелів. Вони з'єднують готель із кінцевим споживачем – туристом (тоді як GDS – з агентами), виконуючи функції продавця і стягнення комісії за бронювання. Багато OTA самі паралельно підключаються до GDS для доступу до авіаквитків і оренди автомобілів, щоб продавати їх на своїх сайтах (наприклад, Booking.com). OTA, як і GDS, надає готелям інструменти для управління номерним фондом.

У світі існує два провідних OTA: Priceline та Expedia. Booking належить Priceline, також як і Kayak, Agoda і Momondo, а, наприклад, Orbitz належить Expedia. OTA, усвідомлюючи своє домінуюче положення і відсутність реальної конкуренції, встановлюють свої правила на ринку туристичних послуг. OTA заробляють на комісії 10–30% із бронювання, коли споживач туристичних послуг безпосередньо бронює готель на сайті (наприклад, Booking.com). OTA зобов'язують готелі надавати їм мінімальну ціну за номер – так званий «паритет курсів», – нижче якої готелі не можуть продавати номери ні на своїх сайтах, ні оффлайн. За порушення – штрафи і відключення. Своєю чергою, сьогодні OTA – основний канал збуту для багатьох. У результаті споживачі і на інших сайтах отримують штучно завищену вартість, як і у випадку з GDS.

3. Channel Managers («менеджери каналів») – це інформаційні системи – своєрідні шлюзи, які підключаються по API до безлічі OTA і GDS, вони дають змогу готелю управляти каналами продажів і номерним фондом з одного місця і надають зручні інтерфейси для управління замовленнями. Як правило, один готель представлений відразу на безлічі онлайн-турагентствах, а також його номерний фонд розміщений одночасно в декількох GDS. Керувати бронюванням, оплатами, уникаючи овербукінгу, в десятках інтерфейсів нереально, для цього й існують Channel Managers. Вони також вносять свою комісію у ціну номерів, але на відміну від GDS і OTA вона не така суттєва. Channel Managers – більш прогресивні й інноваційні компанії, конкуренція мотивує їх розвиватися, збільшувати охоплення майданчиків для розміщення, швидкість обробки замовлень, пропонувати готелям безліч корисних функцій, таких як інтегровані CRM, віджети бронювання тощо. Конкуренція стримує їх від необгрунтованого підвищення цін.

GDS – монополісти, які усвідомлюють залежність готелів з авіакомпаніями від своїх інформаційних систем, із чим пов’язана відсутність інновацій, які, своєю чергою, дали б змогу GDS надати кращі сервіси постачальникам, що допомогло б знизити витрати, оптимізувати заповнюваність номерів і рейсів, економити на курсах валют. У кінцевому підсумку споживачі отримали б найкращу якість послуг за нижчими цінами.

Організацію ринку дистрибуції готельних номерів схематично наведено на рис. 1.

OTA більш інноваційні, ніж GDS, вони конкурують за туриста в онлайн-просторі, оптимізують сайти, роблять мобільні додатки, купують стартапи (які в підсумку й перетворюються на ще один дочірній бренд і створюють ілюзію вибору для туриста). Попри це вся конкуренція між найбільшими OTA зводиться до змагання маркетингових бюджетів та ставок за кліки в Google. Так, тільки в 2017 р. Priceline витратила більше $3,5 млрд. на контекстну рекламу, а маркетинговий бюджет Expedia виріс на мільярд доларів із 2016 р. – до $4,37 млрд. [7].

Стартапи і молоді IT-travel-компанії могли б скласти конкуренцію OTA і GDS як альтернативний канал збуту, запропонувавши постачальникам більш якісні сервіси з меншою комісією. Як наслідок, споживачі отримали б більш низькі ціни і більш релевантні пошукові видачі (наприклад, найбільш оптимальні комбінації перельотів). Водночас створити свою глобальну систему дистрибуції або онлайн-турагентство світового рівня і при цьому запропонувати невелику комісію є неможливим завданням для нової компанії. Таким чином, монополія GDS і гігантів онлайн-бронювання обмежує розвиток інноваційних рішень у туризмі, передусім на ринку дистрибуції туристичних послуг.

На думку низки практиків світового туристичного ринку, демократизація та інноваційність сфери туризму пов’язані з використанням блокчейну – децентралізованої бази даних, де пристрої, на яких зберігається загальна інформація, не підключені до загального єдиного сервера, тобто вся інформація у цій базі зберігається у вигляді списку упорядкованих записів (блоків), кожна з яких несе в собі інформацію про час створення блоку і посилання на попередній запис. Тому навіть у разі зміни останнього запису вихідна інформація не може бути втрачена. Суть блокчейн-платформи бронювання туристичних послуг у тому, щоб створити своєрідну відкриту глобальну систему дистрибуції, яка керувалася б спільнотою всіх учасників, а не одноосібно власником платформи. Постачальники туристичних послуг могли б максимально зручно і безкоштовно завантажувати їх у систему, самостійно призначаючи комісії за бронювання для агентів, а з іншого боку, будь-який агент (турагентство, сайт, тревел-стартап тощо) міг би підключитися і продавати ці ресурси, отримуючи призначену комісію. По суті, ця платформа ідентична GDS (єдина база даних турпродуктів і послуг). Відмінність від існуючих у тому, що ніхто не бере 10–30% комісії за управління і ніхто не володіє системою одноосібно. Це – громадська власність. Комісія для агентів залишається, але зникає більш істотна комісія і націнка посередників-монополістів. Рівноправний доступ агентів до такої платформи послужить стимулом для розвитку технологій, поліпшення якості сервісів та перешкоджатиме додатковим націнкам із боку самих агентів. Для постачальників туристичних послуг така платформа – новий, більш вигідний спосіб взаємодії з агентами на противагу Booking.com.

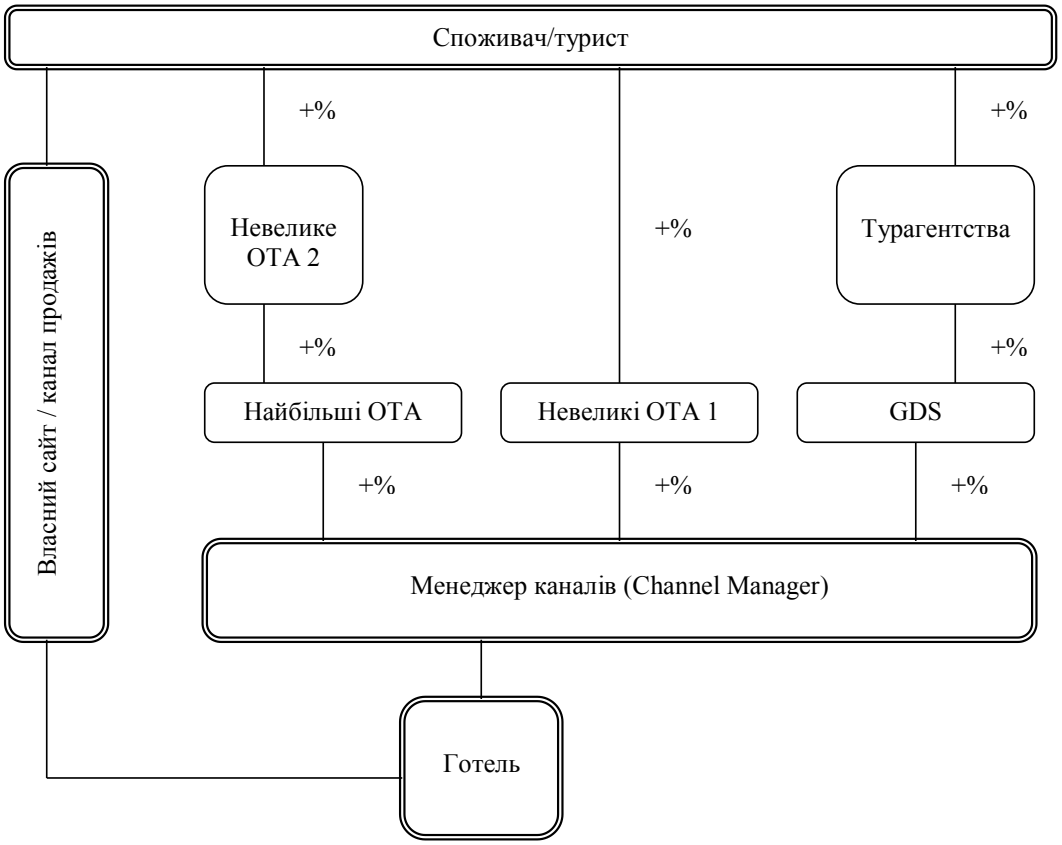

Рис. 1. Організація ринку дистрибуції готельних номерів на глобальному ринку туристичних послуг [7]

Вже сьогодні німецький гігант туристичної індустрії TUI Group тестує блокчейн для відстеження внутрішніх операцій і має намір надалі розширити сферу застосування даної технології на інші процеси. Нині компанія реалізує пілотний проект під назвою BedSwap, у рамках якого технологія блокчейн виступає центральним елементом системи обліку даних готельних номерів [13].

Водночас це не єдиний варіант використання блокчейну в туризмі. Технологічні можливості блокчейну дадуть змогу проходити паспортний контроль за допомогою зчитування відбитків пальців, накопичувати бали в бонусних програмах різних готельних мереж, авіакомпаній і сервісів з оренди автомобілів. Зокрема, технологія блокчейн може істотно спростити ідентифікацію пасажирів, не жертвуючи при цьому безпекою персональних даних, а також удосконалити процедури відстеження багажу, запропонувати клієнтам більш зрозумілі умови участі в програмах лояльності і спростити процес взаєморозрахунків між авіакомпаніями та агентствами [14], у тому числі і з використанням криптовалют. Так, зокрема, bitcoine все частіше використовується як платіж у різноманітних сферах туристичного відпочинку.

Попри це недоліки блокчейну в туризмі пов'язані саме з розрахунками в криптовалюті і наявністю хакерських атак на криптовалютні платежі. Так, популярною є хакерська атака DDoS – Distributed Denial of Service, або розподілена атака типу «відмова в обслуговуванні», яка проводиться відносно добре захищених компаній. Так, наприклад, у березні 2018 р. мережа платіжних каналів другого рівня для блокчейна біткоіни Litghtning Network піддалася DDoS-атаці. Організатором кібернападу стала анонімна група BitPico, у якій був набір автоматизованих інструментів із функцією підключення до сотень нодів. Уразливості розробники Lightning Network тоді не виявили, але з ладу було виведено 200 вузлів, або 20% мережі [15].

Інша відома атака – «атака Сивіли» – отримала свою назву в 2002 р. завдяки фахівцю Microsoft Research Брайану Зілу. «Атаку Сивіли» можна порівняти із психічною недугою, адже у цьому разі хакер привласнює одному ноду кілька ідентифікаторів і тим самим порушує роботу всієї мережі. У тимчасових мережах, таких як Bitcoin і Ethereum, немає довірених нодів, тому кожен запит пересилається кільком одержувачам. Водночас користувачі можуть мати кілька ідентифікаторів із різних нодів, які можна використовувати для розділення загальних ресурсів. Отримані копії створюють надмірність, дають змогу перевіряти прийняті з мережі незалежні дані. Але якщо дивитися на цей підхід з іншого боку, то виходить так, що всі доступні ноди, які повинні представляти різних одержувачів запиту, контролюються одним і тим же користувачем. Якщо він виявиться шахраєм, то такі транзакції замкнуться на нодах-псевдонімах. Дана атака набирає популярність, адже децентралізована мережа зростає і за великої кількості користувачів недоцільно вимагати від кожного учасника мережі підтверджувати володіння своїми ідентифікаторами, оскільки це перешкоджає масштабності і зручності мережі [15].

Ще один різновид атаки на рівні мережі – Eclipse attack, або «атака інформаційного затемнення». Даний вид кібернападу був детально описаний у доповіді групи вчених з університету Бостона та Єврейського університету на чолі з Ітаном Хейлманом у 2015 р. Дослідження описує причини першої атаки на мережу Bitcoin, а експеримент, проведений у рамках наукової роботи, демонструє вразливість технології. Пізніше І. Хейлман продемонстрував можливість ведення екліпс-атаки в мережі Ethereum і довів, що вся система вимагає доопрацювань [15].

«Атака інформаційного затемнення» дає змогу отримати контроль над доступом до ноду та інформації. За правильної маніпуляції в тимчасовій мережі хакер може «затьмарити» ноди так, щоб ті контактували тільки із зараженими нодами. По суті, цей кібернапад є першим щаблем в організації «Атаки 51%». Працює «інформаційне затемнення» так. Мережа містить три великих нода майнінга: два контрольних нода мають по 30% потужності майнінгу (загалом 60%), а третій нод у 40% відповідає за решту мережі. Якщо хакеру належить сорокавідсотковий нод, то зловмисник може розбити 40% на два майнера так, щоб вони не змогли скомпонувати блоки один одного. У результаті блокчейн зловмисника стає ланцюжком усього консенсусного блоку. Після цього можна маніпулювати нодом і зробити так, щоб усі його вихідні з'єднання були пов'язані з атакуючими IP-адресами. Для цього потрібно заповнити одноранговi таблиці нода зараженими адресами, перезапустити поточні з'єднання всіх користувачів (це відбувається часто через оновлення програмного забезпечення) і створити нові сполуки тільки для IP-злочинців.

Основним і найпростішим інструментом сучасного блокчейн-хакера є ботнети, які поширюються через дропери – спеціальні анонімні шкідливі програми, які маскуються під піратські версії ліцензійних програм. Як відомо, для майнінгу потрібні час і великі обчислювальні й енергетичні потужності. Для економії ресурсів криптохакери заражають комп'ютери інших користувачів мережі. У результаті сторонні люди приносять величезний дохід кіберзлочинцям і не підозрюють про це. Так, наприклад, ботнет під назвою Smominru для майнінгу Monero за півроку заразив понад півмільйона серверів по всьому світу і приніс 8 900 XMR, або $2 млн. [15].

Уразливість на рівні користувача з юридичного погляду пов'язана з деанонімізацією учасників ринку. Оскільки блокчейн-адреси не прив'язані до особистості й усі проведені транзакції не вимагають розкриття учасників угоди, криптошахраї починають користуватися цими перевагами у своїх корисливих цілях. Якщо зловмисник підключить заражені ноди до мережі, то з'явиться можливість простежити джерело здійснення транзакцій. Окрім того, анонімність блокчейна дає змогу здійснювати угоди між терористами та іншими злочинцями, які займаються незаконною діяльністю.

Висновки. Підводячи підсумки, відзначимо кілька напрямів туризму, де може бути використана технологія блокчейн. По-перше, це програми лояльності, де бали лояльності можуть бути приписані кожному клієнту через цифровий підпис, а їхні трансакції є прозорими. По-друге, онлайн-бронювання може стати набагато безпечніше, оскільки блокчейн зможе уникнути помилок у резервуванні, його раптової втрати або овербукінгу. При цьому всі транзакції будуть прозорі, а процес оплати – автоматизованим. По-третє, процес ідентифікації в аеропортах також може бути прив'язаний до блокчейну, якщо біометричні дані пасажира записані в системі, спеціалізований апарат зчитує їх, а інформація про це проходить далі шляхом звичайної транзакції. По-четверте, блокчейн дає змогу автоматизувати виконання контрактів зі страховими компаніями, щоб автоматично отримувати компенсацію у свій криптовалютний гаманець.

Перспективність блокчейна оскаржують експерти як туристичного, так і фінансового ринку. Так, головна проблема використання криптовалюти в туризмі як платіжної системи – це швидкість обробки транзакцій. Наприклад, Visa обробляє 60 тис. операцій на секунду, біткоіни – тільки сім транзакцій. Технічні вдосконалення системи тривають, але нині ефективність біткоінів становить трохи більше 0,01% від показника Visa. Ситуація з іншими криптовалютами принципово не відрізняється, а враховуючи обсяг туристичних операцій у світі, це є суттєвою проблемою використання блокчейну.

На блокчейн покладають особливі надії передусім ті, хто вважає, що угоди повинні здійснюватися без нагляду держави. Контроль органів влади дійсно може бути надто бюрократизованим, але держструктури за всієї їхньої неповоротності надають певний рівень надійності. Своєю чергою, власник криптогаманця не зможе звернутися за будь-якими гарантіями в разі крадіжки пароля: немає регулятора – немає гарантій. Причому подібний недолік системи знаходиться як на призначеному для користувача рівні, так і на рівні всієї системи. До того ж сама влада не захоче втрачати контроль над переміщенням коштів через необхідність протидіяти тероризму та організованій злочинності.

Проблемою майбутнього блокчейну можна назвати Selfish mining – стратегію видобутку біткоінів, коли користувачі мережі за окремою угодою об'єднуються в групи для збільшення власного доходу. Ця дія може централізувати мережу і розрушити початкову концепцію децентралізованої системи. Об'єднання всіх потужностей відбувається в Китаї, адже саме ця країна видобуває дві третини всіх біткоінів у світі. Якщо селфіш-майнінг не припиниться, то всі учасники блокчейн-ринку опиняться на тому ж місці, звідки пішли, тобто повернуть централізовану економіку в зміненому електронному форматі.

Список використаних джерел:

1. Emerging Technology in Travel. Report 2018 / Sabre Labs. URL: https://www.sabre.com/labs/emergingtech/2018/assets/files/SabreLabs_Emerging_Tech_Report_2018.pdf.

2. Направления и особенности применения блокчейн-технологии в экономике / Д.А. Аксенов, А.П. Куприков, П.А. Саакян. Научно-технические ведомости СПбГПУ. Экономические науки. 2018. Т. 11. № 1. С. 30–38.

3. Кейнси М., Винья П. Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок. 2017. 125 с.

4. Wattenhofer R. The Science of the Blockchain. Createspace Independent Publishing Platform. 2016. 124 p.
5. Корчагин С. О текущих трендах в развитии технологии блокчейн. Свободная мысль. 2016. № 4. С. 31–38.
6. Marr B. Practical Examples Of How Blockchains Are Used In Banking And The Financial Services Sector. Forbes. 2017. № 10. URL: https:// www.forbes.com/sites/bernardmarr/2017/08/10/practic al-examples-of-how-blockchains-are-used-in-bankingand-the-financial-services-sector/#22168ae51a11.
7. Меньщиков А. Блокчейн в туризме. URL: https://vc.ru/31535-blokcheyn-v-turizme-chast-1.
8. Мигунов Д. Блокчейн совершенно бесполезен. И вот почему. URL: https://lenta.ru/articles/2018/01/24/blockchain/.
9. Савельев И.Е. Технология blockchain и ее применение. Прикладная информатика. 2016. № 6. С. 19–23.
10. Скиннер К. ValueWeb. Как финтех-компании используют блокчейн и мобильные технологии для создания интернета ценностей. 2018. 320 с.
11. Свон М. Блокчейн: Схема новой экономики. М.: Олимп-Бизнес, 2017. С. 12–18.
12. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, London Portfolio. Penguin, 2016. 348 p.
13. Крупнейший туроператор Европы задействует блокчейн для внутренних операций. URL: https://forklog.com/krupnejshij-turoperator-evropy-zadejstvuet-blokchejn-dlya-vnutrennih-operatsij/.
14. Как блокчейн изменит тревел-индустрию. URL: http://turprofi.com.ua/novosti/ot-kompanij/2130-kak-blokchejn-izmenit-trevel-industriyu.
15. Flaws of the Flawless System, or Blockchain Vulnerabilities. URL: https://decenter.org/blockchain/555-crimes-in-blockchain-en.