КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018
ISSN 2663 - 4023

УДК 004.031.43: 004.056

Спасітєлєва Світлана Олексіївна
канд. ф.-м. наук, доцент, доцент кафедри комп'ютерних наук та математики
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID: 0000-0003-4993-6355
spasiteleva@gmail.com
Бурячок Володимир Леонідович
доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка
OrcID: 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

ПЕРСПЕКТИВИ РОЗВИТКУ ДОДАТКІВ БЛОКЧЕЙН В УКРАЇНІ

Анотація. Стаття присвячена визначенню проблем, пов'язаних з використанням блокчейн технологій, та шляхів їх подолання при створенні розподілених, безпечних додаткі . В роботі розглянуті теоретичні основи блокчейн технології та блокчейн додатків, нові моделі блокчейн бізнесу, платформи розробки, безпека блокчейн додатків, проблеми розвитку та перспективи подальших досліджень блокчейн технології. У статті зроблено аналіз останніх досліджень та публікацій у сфері блокчейн технологій. На основі цього аналізу визначено, що у блокчейн-індустрії поки не завершився процес формування загальновизнаного багаторівневого опису технології. В роботі зроблено огляд існуючих моделей блокчейн бізнесу, визначені їх характеристики та сфери застосування. Розглянуті програмні засоби створення та підтримки блокчейн додатків. В роботі розглядаються особливості, переваги та проблеми використання блокчейн технологій для створення розподілених, безпечних корпоративних додатків. Розглянута проблема інтеграції нових та існуючих приватних систем з відкритим блокчейном. Одним із варіантів вирішення цієї проблеми є створення служби аутентифікації на основі блокчейну для реалізації глобального рівня безпеки. Така служба може стати стандартною інфраструктурою безпеки для нових моделей змішаних приватних і публічних систем, яка принесе користь всім зацікавленим сторонам в різних сферах економіки. На основі аналізу сучасного стану розвитку блокчейн, визначені напрямки розвитку захищених блокчейн додатків та першочергові задачі, які необхідно вирішити для успішного впровадження технології у сферу державного управління та приватного бізнесу в Україні. Зважаючи на проблеми розвитку блокчейн систем, визначені перспективи подальших досліджень в трьох головних напрямках: стандартизації, безпеки додатків та інтеграції блокчейн систем з існуючими приватними системами та сучасними технологіями штучного інтелекту, великих даних та інтернету речей.

Ключові слова: блокчейн технологія; блокчейн додатків; однорангова мережа; алгоритми консенсусу; розумні контракти; безпека додатків.

1. ВСТУП

Нова парадигма інформаційного простору блокчейн (blockchain) набула широкого розповсюдження в усьому світі, в тому числі в Україні. Інтернет виходить на наступний виток розвитку. Всесвітня Павутина (World Wide Web) дала можливість швидко обмінюватися інформацією. Її можна назвати «Всесвітньою Павутиною Інформації». Другий етап – впровадження технології блокчейн, яка дає можливість обмінюватися цінностями, створивши «Всесвітню Книгу Обліку Цінностей» (World Wide Ledger). Тепер віртуально можна обробляти все, що для людини важливо та може бути представлено в цифровому форматі: гроші, свідоцтва, договори, права на власність,

ISSN 2663 - 4023

дипломи та наукові звання, фінансові рахунки, медичні процедури, страхові випадки, результати голосування, походження продуктів харчування. Почалася нова ера цифрової економіки. Попередній етап ознаменувався поєднанням обчислювальних і комунікаційних технологій. Новий етап базується на інженерії комп'ютерних систем, математики, криптографії та поведінковій економіці [1].

«Blockchain» (block – блок, chain – ланцюг) є способом зберігання даних, який ще називається цифровим реєстром будь-яких операцій, впорядкований у блоки за ланцюговим принципом. У світі вже існують та успішно працюють ефективні рішення побудовані на базі блокчейн, такі як, наприклад, Bitcoin – інноваційна мережа платежів та цифрова валюта, Brave – браузер, який має можливість проводити анонімні платежі власникам сайтів та багато інших успішних реалізацій. Ринок стартапів на базі використання технології блокчейн, за оцінками експертів, залучить у 2018 році інвестицій на суму 3 млрд. доларів. Використання технології блокчейн викликає зацікавлення в Україні. Україна уклала угоду з міжнародною технологічною компанією Bitfury Group про переведення всіх електронних державних даних на блокчейн [2]. Bitfury почне з пілотного проекту, в рамках якого на блокчейн перейдуть державні реєстри, соціальне страхування, держпослуги і охорону здоров'я. Після завершення пілотної стадії, на розподілений реєстр будуть переведені всі сфери, включаючи кібербезпеку.

Постановка проблеми. У зв'язку з бурхливим розвитком блокчейн сервісів, API для розробників блокчейн систем, засобів статистики та моніторингу блокчейн мереж, виникає потреба в аналізі переваг та недоліків існуючих підходів та реалізацій для застосування в різних галузях економіки, управління, соціальній сфері. Виникає потреба у визначенні напрямків розвитку захищених корпоративних блокчейн додатків та вирішенні таких проблем як безпека, висока доступність та швидкість виконання транзакцій. У блокчейн-індустрії поки не завершився процес формування загальновизнаного багаторівневого опису технологій, тому виникає потреба в аналізі та однозначному визначенні трьох частин концепції: базової блокчейн технології, протоколу передачі даних та цифрового ресурсу для корпоративного блокчейну.

Аналіз останніх досліджень і публікацій. Концепція першого блокчейну була розроблена в 2008 році людиною (або групою людей), відомою як Сатоши Накамото. У 2008 році було описано протокол електронних платежів для однорангової мережі (peer-to-peer network, P2P). Це математичний алгоритм, який дозволяє безпечно і приватно обмінюватися цінностями через однорангові мережі. Протокол, створений Накамото, називають «протоколом довіри» [3]. Так була закладена основа для технології блокчейн. У 2009 році ця технологія була реалізована в рамках цифрової валюти — біткоїна. Таким чином, першою успішною практичною реалізацією блокчейн технології стала мережа біткойн. У 2015 році журнал The Economist опублікував статтю «Машина довіри», в якій йдеться про те, що технологія мережі біткойн, може повністю змінити економіку. Саме ця технологія стала першою, яка змогла вирішити інформаційну проблему, таку як забезпечення довіри між сторонами до отриманої інформації без залучення зовнішніх гарантів – банків, посередників тощо. Автори багатьох публікацій з блокчейну Дон Тапскотт та Алекс Тапскотт проаналізували програми, сервіси, бізнес-моделі, ринки, організації і навіть уряди, які оперують блокчейн. Виявили закономірності і сформулювали 7 принципів, на які спираються послідовники технології [1].

Мета статті. Метою статті є визначення проблем, пов'язаних з використанням блокчейн технологій, та шляхів їх подолання при створенні розподілених, безпечних корпоративних додатків.

ISSN 2663 - 4023

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Блокчейн в найпростішому розумінні це розподілена база даних, до якої кожен може безпечно приєднатися та виконати транзакційний код. Інформація про транзакції знаходиться в глобальній, загальнодоступній блокчейн базі даних. У ній відбувається підтвердження і прийняття операцій P2P-мережі. Ієрархія таких систем повністю горизонтальна [4]. Всі учасники рівноправні, будь-який учасник системи є точкою управління (рис. 1).

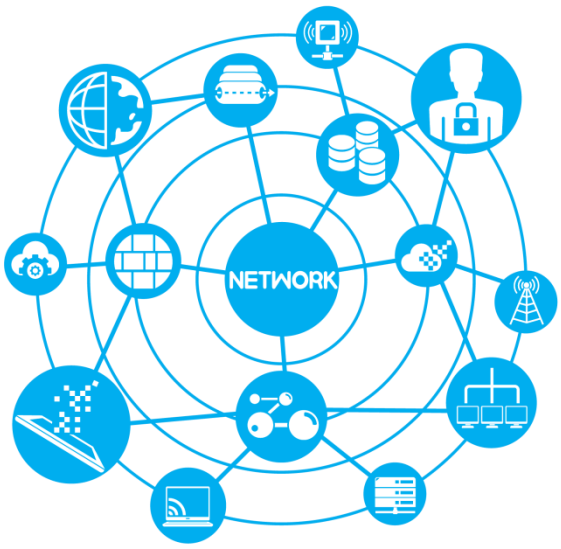

Рис. 1. Розподілена блокчейн мережа

Одноранговa (peer-to-peer) мережа. Щоб використовувати блокчейн для запису транзакцій, необхідно мати можливість перевірити блокчейн. Поточний стан блокчейна завантажується, синхронізується і надається багатьом комп'ютерам з усього світу. Ці комп'ютери називаються «вузлами» або «нодамі» (nodes), і вони працюють спільно в одноранговій мережі, щоб гарантувати, що блокчейн є безпечним і актуальним. Кожен з цих вузлів зберігає повну, оновлену (актуальну) версію блокчейну. Кожен раз, коли додається новий блок, всі вузли оновлюють свій блокчейн. Використання одноранговоі мережі має певні переваги:

• завжди можна перевірити стан блокчейну, використовуючи програму-проводир (blockchain explorer);
• не треба покладатися тільки на одну сторону, щоб знати справжній стан блокчейна;
• не треба покладатися на безпеку одного сервера, щоб знати, що блокчейн захищений;
• зловмиснику доведеться одночасно зламати тисячі комп'ютерів, а не один сервер;
• завжди є впевненість, що блокчейн ніколи не зникне, тому що для цього його треба буде знищити в усіх вузлах.

Усі транзакції зберігаються в блоках даних, які створюються таким чином, що ними досить складно маніпулювати після того, як вони вже потрапили до системи блокчейн. Для того, щоб блок потрапив до блокчейн потрібно здійснити верифікацію цього блоку і додати його до системи. Транзакції зашифровані двома ключами, публічним і приватним, що гарантує безпеку. Блоки – це дані про транзакції, угоди і контракти всередині системи, представлені в криптографічній формі. У ланцюжку витримується строга послідовність. Кожен з блоків містить масив певних даних. Усі блоки пов'язані між собою. Для запису нового блоку, необхідно послідовне зчитування інформації про старі блоки. Кожна ланка ланцюжка містить певний ключ. Поки він не буде розшифрований, блок не закриється. На рисунку 2 наведено опис послідовності виконання транзакцій. Послідовність дій така:

- користувач А хоче здійснити операцію (транзакцію) з користувачем В;
- маючи відкритий ключ для здійснення операції, користувач А задає відомості про операцію для формування блоку і передає його у мережу;

ISSN 2663 - 4023

- відбувається перевірка операції всіма учасниками мережі. Якщо немає помилок, то кожен учасник додає блок до свого екземпляру розподіленої бази даних. Блок додається до ланцюжка блоків, операція вважається підтвердженою;
- відповідь про підтвердження транзакції разом із закритим ключем для отримання ресурсу надходить до користувача В.

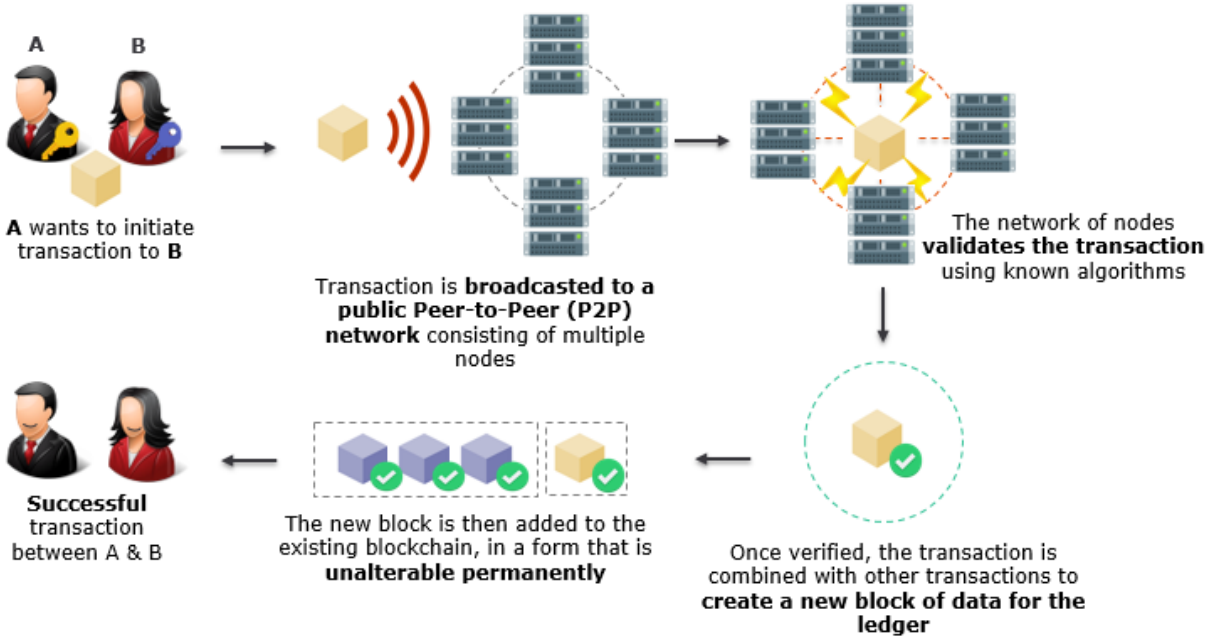

Рис. 2. Послідовність виконання транзакції блокчейн

Всі ланцюги блоків розподілені, вона обробляються комп'ютерами по всьому світу. Центрального сервера, який можна було б зламати, не існує. Блокчейн публічний і дуже надійний одночасно, так як використовує зашифровані дані. З цієї бази даних неможливо нічого видалити або провести заміну/підміну блоку. І вона «безмежна» – в неї можна записати нескінченну кількість транзакцій. Це одна з головних особливостей блокчейна. Всі операції проводяться між суб'єктами безпосередньо. А здійснюються вони за рахунок того, що всі учасники підключені до однієї мережі. Блокчейн має змогу вирішувати проблеми такі як: безпека, висока доступність та швидкість виконання транзакцій.

Механізм консенсусу. Сатоши Накамото, засновник біткойна, об'єднав блокчейн з консенсусним механізмом, заснованим на криптографії. Консенсусний механізм дозволяє вузлам в одноранговій мережі працювати разом, не знаючи і не довіряючи один одному. Метою консенсусного алгоритму є виконання безпечного оновлення стану відповідно до деяких конкретних правил, при цьому право на виконання зміни стану розподіляється серед користувачів, яким надається право колективно виконувати ці зміни через алгоритм. Механізм консенсусу – це просто набір правил, який узгоджується вузлами в мережі, запускаючи програмне забезпечення мережі. Ці правила дозволяють мережі працювати за призначенням і залишатися синхронізованою. Консенсусний протокол встановлює правила:

- яким чином блоки повинні бути додані в блокчейн;
- коли блоки вважаються дійсними;
- як вирішуються конфлікти.

ISSN 2663 - 4023

Найбільш відомими механізмом консенсусу є доказ роботи (PoW), який використовується в мережі біткойн, доказ стану (PoS), який використовується в Coin [4], Proof of Elapsed Time – доказ минулого часу (PoeT), який використовується в проектах Hyperledger. Головним недоліком алгоритмів є те, що вони вимагають великих обчислювальних потужностей. Триває широка дискусія про те, які консенсусні механізми є кращими, також створюються нові алгоритми.

Структура блоку транзакцій. Структура даних блокчейн – це упорядкований «назад» пов'язаний між собою список блоків транзакцій (рис.3). Блокчейн може зберігатися у будь-якому файлі або просто в базі даних. Клієнт Bitcoin Core зберігає метадані блокчейн використовуючи БД LevelDB від Google [3]. Кожен блок у блокчейн ідентифікується хешем, який генерується з використанням криптографічного алгоритму SHA256, застосованого до заголовка блоку. Кожен блок також посилається на попередній блок, відомий як батьківський блок, через поле «хеш попереднього блоку» в заголовок блоку. Іншими словами, кожен блок містить хеш свого батька всередині власного заголовка. Послідовність хешей, що зв'язують кожен блок з його батьком утворює ланцюг, який тягнеться до самого першого блоку з коли-небудь створених, відомому як блок генезису. Змінений хеш батьківського блоку вимагає зміни посилання «хешу попереднього блоку» в дочірньому блоці. Це каскадний ефект гарантує, що якщо блок має багато поколінь, він не може бути змінений без перегляду всіх попередніх блоків. Так як для подібного перерахунку потрібна величезна кількість обчислень, то довгий ланцюг блоків робить глибоку історію в блокчейні незмінною, що є ключем до безпеки цифрового ресурсу. Ті блоки, які вже записані в блокчейн, змінити неможливо. Взагалі, будь-яке редагування в блокчейн інформації (транзакцій) заборонено. Можна тільки дописувати нові блоки. Це важлива властивість блокчейна, як розподіленого реєстру транзакцій.

Блок складається із заголовка (Head), що містить метадані, далі за ним іде довгий список транзакцій (Payload), які займають більшу частину всього обсягу блоку (Рис.3.). Заголовок блоку містить таку інформацію: версію блоку, дата і час створення блоку, хеш-код заголовка блоку, хеш-код попердднього блоку, хеш-код всіх транзакцій в блоці, спеціальні параметри nonce і bits. Хеш-код заголовка блоку пов'язує попередній блок з наступним у ланцюжку блокчейна. Розмір блоку займає 80 байт, в той час як середня транзакція займає не менше 250 байтів, а середній блок містить понад 500 угод [4]. Відповідно, повністю заповнений транзакціями блок в 1000 разів більше заголовка.

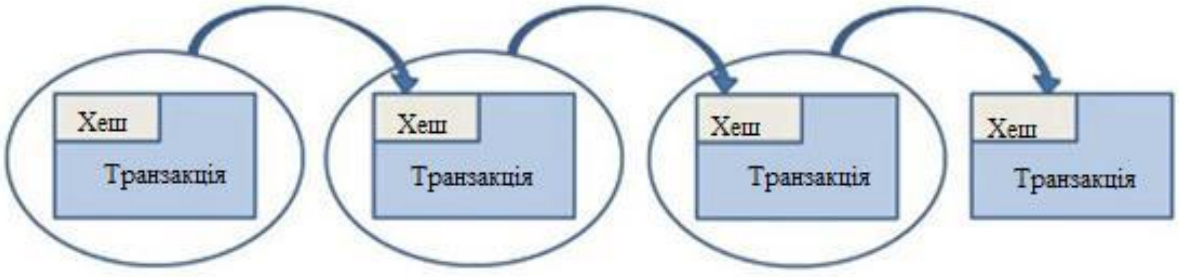

Рис. 3. Ланцюг блоків

ISSN 2663 - 4023

Метафорично, блокчейни (ланцюжки блоків) є кінцевими універсальними комп'ютерами. Після запуску вони демонструють неймовірну стійкість, що робить їх надійними та привабливими для роботи нового покоління децентралізованих служб та програмних додатків [3]. Таким чином, головними перевагами блокчейну є:

- децентралізація – в ланцюжку немає сервера, кожен учасник підтримує роботу всього блокчейна;
- прозорість – інформація про транзакції зберігається у відкритому доступі, при цьому ці дані неможливо змінити;
- надійність – для запису нових даних необхідний консенсус вузлів блокчейна, що дозволяє фільтрувати операції і записувати тільки легітимні транзакції, здійснити підміну хеша нереально;
- теоретична необмеженість – теоретично блокчейн можна доповнювати записами до нескінченності.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Корпоративні блокчейни. Складністю практичної імплементації технології блокчейн в бізнес є те, що вона передбачає зміну парадигми управління і перехід від ієрархічної моделі до плоскої. При цьому рішення приймаються децентралізовано, а весь процес прозорий для всіх учасників. Очевидно, що це вимагає переосмислення бізнес-процесів, підходів до управління і захисту інформації. Business Blockchains – це нові технологічні шари, які перекривають Інтернет і загрожують старішим конструктивним рішенням та централізованому обслуговуванню бізнесу [3]. По суті, блокчейн вводить довіру в мережу, відстороняючи посередників від виконання цієї функції і творчого порушення старих технологій. Криптотехнологічна економіка має стати економікою, яка базується на децентралізованій довірі [4].

Багато галузей промисловості децентралізовані вкрай неефективно: у кожної компанії є своя інфраструктура, через яку взаємодіють користувачі, проводяться транзакції і обмін даними і яка вимагає узгодження з іншими компаніями при кожній взаємодії. З появою децентралізованих баз даних, які можуть технологічно відтворити мережевий ефект, раніше доступний тільки монополіям, кожен може приєднатися до них і діяти собі на благо, не створюючи монополію з усіма її негативними сторонами. Саме тому технології блокчейна так затребувані в сфері фінансів, індустрії поставок і системах ідентифікації. Всі вони використовують децентралізовані бази даних, реалізуючи свої цілі на одній платформі, без витрат на те, щоб домовитися про те, хто отримає контроль над цією платформою, а потім примиритися з тим, що вони спробують зловживати своїм монопольним становищем.

Поширення блокчейна відбувається поступово, починаючи з розробників стартапів до великих компанії різних галузей економіки, які відкрили для себе величезний потенціал блокчейна (рис. 4). Яскравим прикладом перебудови великого бізнесу під нову парадигму є банківський консорціум R3CEV (об'єднання понад 70 найбільших фінансових компаній і банків світу), який створено з метою розробки і застосування технології блокчейна у фінансовій сфері. Крім R3CEV існує декілька десятків блокчейн-консорціумів і постійно з'являються нові об'єднання. Починаючи з 2016 року кількість створюваних нових проектів за технологією блокчейн зросла феноменально.

ISSN 2663 - 4023

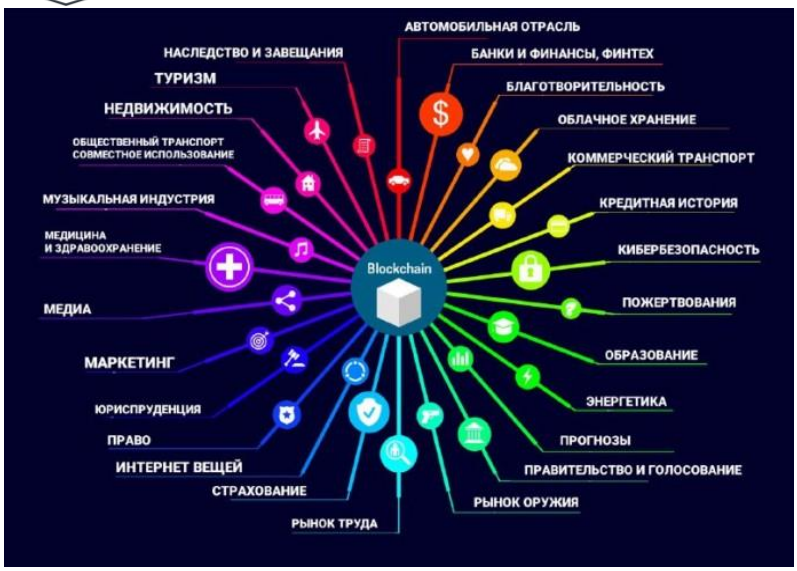

Рис. 4. Сфери застосування Blockchain

Одним із прикладів української розробки є блокчейн проект електронних аукціонів з оренди та продажу держмайна e-Auction 3.0 [5]. Сервіс був протестований в ряді українських міст і отримав підтримку окремих адміністрацій.

ДП «СЕТАМ» 7 вересня 2017 року провело перший у світі аукціон за допомогою технології блокчейн. Для впровадження блокчейну була обрана платформа EXONUM міжнародної компанії BitFury Group. З вересня 2017 року по лютий 2018 року з використанням блокчейну було проведено 24 202 аукціонів, серед них успішних – 4 471. Загальна сума продажів склала 692 млн грн. [6].

Нові моделі блокчейн бізнесу. Немає єдиного «офіційного» блокчейна, а є різні типи блокчейнів, які існують незалежно і взаємодіють між собою. Таким чином, у блокчейна можуть виявлятися специфічні технічні особливості використання в різноманітних додатках. Умовно всі інноваційні моделі бізнесу можна поділити на 4 типи: «розумні» контракти, відкриті мережеві підприємства, автономні агенти, розподілені автоматичні підприємства [1]. Вони відрізняються ступенем автоматизації і складністю функціоналу моделі. Автоматизація відображає, якою мірою потрібна участь людини: низька – участь людини необхідно, висока – модель працює без людей. Складність говорить про кількість функцій моделі: низька – одна функція, висока – різноманітність функцій.

Таблиця 1.

Характеристика моделей блокчейн бізнесу

Модель бізнесу	Автоматизація	Складність
«Розумні» контракти	низька	низька
Відкриті мережеві підприємства (ВМП)	низька	висока
Автономні агенти	висока	низька
Розподілені автоматичні підприємства (РАП)	висока	висока

«Розумні» контракти – базова форма компанії, побудована на блокчейн [3]. Це спеціальний код, який містить набір інструкцій для блокчейн. Звичайний контракт – це домовленість між учасниками угоди, записані на папері. Узгодження умов угоди, врегулювання спірних питань, якщо виникли різночитання, вимагає зусиль. «Розумні» контракти прибирають всі підготовчі дії для підписання контракту і виконання його умов. Ведення бізнесу спрощується.

Відкриті мережеві підприємства – об’єднання «розумних» контрактів, наступний крок на шляху ускладнення їх функціоналу. Компанії стають частиною мережі. В

ISSN 2663 - 4023

результаті знижуються витрати на координацію діяльності, з'являються постачальники і партнери, які раніше були неможливими.

Автономний агент – це пристрій або програма, які збирають інформацію і можуть робити незалежний вибір. Можливість визначати спосіб досягнення мети відрізняє агента від звичайного додатку. Агент реагує на зміну навколишнього середовища. До цієї категорії відносять цікаві програми, які можуть здійснювати транзакції, купувати ресурси, здійснювати платежі, іншими словами, створювати цінності користувачам на правах творця – агента. Як приклад автономного агента можна назвати сервіс хмарних обчислень або безпілотний автомобіль. Автомобіль належить людині або групі людей, а можливо, пересувається по місту самостійно, надає послуги перевезення, сам сажає пасажирів, відвозить, бере оплату.

Розподілені автоматичні підприємства – це об'єднання відкритих мережевих підприємств і автономних агентів. Система приймає рішення і функціонує без участі людини – більшість щоденних рутинних операцій може бути запрограмоване. Всі діють згідно з процедурами «розумних» контрактів. Завдання персоналу, показники ефективності його роботи стануть простими і зрозумілими. В результаті знизиться корпоративна бюрократія, оплата топ-керівників стане прозорою. Клієнти мають зворотний зв'язок. Підприємство постійно враховує їх думку, покращуючи сервіси і продукти. Акціонери отримують дивіденди частіше, ніж один раз на рік, оскільки фінансовий облік компанії відбувається в реальному часі.

Програмні засоби створення та підтримки блокчейн додатків. За Blockchain стоїть реальна технологічна платформа і її різні версії. Проектів, які пропонують платформи для створення блокчейн додатків існує дуже багато і постійно з'являються нові. Для блокчейн-додатків, які будують інфраструктуру криптоекономіки, потрібна величезна кількість програмістів. В основному це блокчейн-розробники зі знанням основних мов програмування: C ++, Golang, Scala, Java і Python. Особливу увагу останнім часом виділяють мови Solidity, якими пишуться смарт-контракти під мережу Ethereum.

Ethereum (Ефіріум) – конструктор для створення рішень на блокчейн [7]. Дозволяє побудувати будь-який додаток з верифікацією на блокчейн. Основною ідеєю «Ефіріума» є використання розумних контрактів – записів, які містять умови виконання певних дій. Умовою може стати будь-яка дія, наприклад, передача товарів замовнику. Розробник, який використовує блокчейн Ethereum, може запрограмувати необхідні тригери і дії за допомогою вбудованої мови сценаріїв. При цьому кожен запис може бути перевірений всіма зацікавленими сторонами: реєстр даних залишається відкритим і децентралізованим. Завдяки високій гнучкості розумних контрактів саме Ethereum став однією з найбільш популярних платформ для створення нових блокчейн-проектів з використанням мови Solidity. Розробникам більше не потрібно придумувати власну реалізацію ланцюжка блоків: достатньо створити потрібну надбудову над вже існуючою системою.

На сьогоднішній день однією із найбільш популярних відкритих платформ для створення блокчейн проектів є Hyperledger [8] від Linux Foundation, Intel, IBM та інших (більше 100 крупних фірм). Платформа пропонує набір інструментів для розробки: Fabric, Iroha, Sawtooth lake, blockchain explorer, Fabric chaintool (Caliper, Cello, Composer, Quilt), Fabric SDK Py, Corda. На сьогоднішній день однією із найбільш популярних інструментів є Hyperledger Fabric – це блокчейн-фреймворк, який призначений для створення основи для розробки рішень на блокчейні і заснований на модульній архітектурі. Fabric представляє собою модуль для розробки масштабованих

ISSN 2663 - 4023

блокчейн додатків з гнучким рівнем дозволів до якого в разі необхідності можуть бути приєднані різні компоненти, наприклад, алгоритми консенсусу. Основна вимога Hyperledger – це модульна структура. Різні служби повинні підключатися і відтворюватися, користувачі повинні мати можливість легко видалити і додати модуль відповідно до специфіки свого бізнесу.

Консорціум R3CEV підтримує створення и тестування роботи блокчейн-платформи Corda. Corda – це блокчейн-платформа для банківського сектора.

Проект NEM, створений великої командою розробників з Японії, багато в чому схожий на Ethereum і є платформою для розробки різних блокчейн-проектів. Однак, на відміну від Ефіріума, цей проект основну увагу приділяє швидкості обробки транзакцій: підтвердження дії в системі займає лічені секунди.

Проект Aragon реалізує концепцію децентралізованих організацій, існуючих виключно в межах блокчейна: жодних паперів і бюрократичних процедур, тільки цифрові дані. На сайті Aragon вже доступна альфа-версія програмного забезпечення, яка успішно справляється із завданнями, що виникають при створенні стартапів та інших приватних онлайн-проектів.

Sia – проект децентралізованого хмарного сховища. На відміну від традиційних сервісів типу Google Drive або Amazon S3, що зберігають призначені для користувача дані на власних серверах, Sia пропонує механізм розподілу зашифрованої інформації на багатьох незалежних комп’ютерах. Перевага Sia перед традиційними хмарними сервісами полягає у вартості передплати: витрати на зберігання файлів у децентралізованому сховищі в 10-15 разів нижче, ніж у традиційних файлових хостингах. Крім того, зашифровані файли не можуть бути розкриті на вимогу поліції та інших державних структур. Ще один проект, практично ідентичний Sia – розподілене сховище Storj.

Безпека блокчейн додатків. В технологію блокчейн від початку закладено безпеку на рівні бази даних. Безпека в технології блокчейн забезпечується через децентралізований сервер, проставлені мітки часу і однорангові мережні з’єднання. В результаті формується база даних, яка керується автономно, без єдиного центру. Це робить ланцюжки блоків дуже зручними для реєстрації подій та операцій з даними, управління ідентифікацією та перевірки походження. Блокчейн є механізмом, що забезпечує високий ступінь обліку та ідентифікації. Більше не буде пропущених транзакцій, помилок людини або машини, або навіть змін, що зроблені без згоди залучених сторін. Блокчейн гарантує законність транзакції шляхом запису її не лише в головному реєстрі, а в розподіленій системі реєстрів, пов’язаних через захищений механізм перевірки. За рахунок самого принципу роботи мережі неймовірно складно зробити підробки блоку. Для того щоб блок вважався справжнім з ним повинні погодитися 51% всіх існуючих вузлів. Отже виникає загроза «Атака 51%» – якщо в блокчейн мережі 51% обчислювальних потужностей буде належати одному пристрою, то цілісність порушиться.

Шифрування блоків гарантує, що користувачі можуть користуватися лише тими частинами ланцюжка блоків, до яких вони мають закриті ключі, без яких зчитування зміна запису є неможливою. Шифрування гарантує синхронізацію копій розподіленого ланцюжка блоків у всіх користувачів. Кожен учасник мережі повинен використовувати шифрування. Заходи безпеки вбудовані в мережу. Вони забезпечують конфіденційність і автентичність.

Замість того, щоб звертатися до третіх осіб, вузли блокчейн-мережі використовують спеціальний протокол консенсусу для узгодження вмісту реєстру, а

ISSN 2663 - 4023

також криптографічні алгоритми хешування і електронно-цифрового підпису для забезпечення цілісності транзакції і передачі її параметрів.

Механізм консенсусу гарантує, що розподілені реєстри є точними копіями, що знижує ризик появи шахрайських транзакцій, оскільки стороннє втручання може виникнути в багатьох місцях одночасно. Криптографічні алгоритми хешування, такі як алгоритм обчислень SHA256, гарантують, що будь-яка зміна вхідних даних транзакції, навіть сама незначна, призведе до появи іншого значення хешу в результатах розрахунків, що вказує на ймовірність компрометації вхідних даних транзакції. Електронно-цифрові підписи гарантують, що транзакції здійснюються легітимними відправниками (підписані закритими ключами), а не зловмисниками.

Сучасні платформи розробки, такі як Hyperledger [8] надають широкий спектр криптографічних протоколів і алгоритмів. Також пропонується гнучка модель PKI (інфраструктури відкритих ключів), яка може використовуватися для управління функціями контролю доступу. Таким чином, сила и тип криптографічних механізмів будуть варіюватися в залежності від потреб користувачів.

На цей час вже існує ряд бізнес-сервісів на блокчейні, що забезпечують:

- безпечне адміністрування мереж, запобігання хакерським атакам і знімає проблему «єдиного адміністратора»;
- зберігання цифрових сертифікатів, що робить повністю захищеним доступ користувачів до сайтів (зокрема, виключаючи перехоплення паролів);
- безпечні двосторонні угоди без залучення гарантуючої третьої сторони (юридичної фірми, нотаріуса, банку та ін.);
- фіксацію часу розміщення документів, що дозволяє вирішувати питання патентування, авторського права та інше;
- підтвердження достовірності продукту (товару) за допомогою надійно захищеного сертифікату;
- підтвердження прав на будь-яку власність;
- створення загальнодоступних електронних реєстрів, інформація на яких автоматично оновлюється навіть після «роздачі» по Інтернет-ресурсам;
- систему DNS, що є невразливою для DDOS-атак.

Як приклад, наведемо BAASIS ID і Civic – платформи з управління ідентифікацією на базі блокчейн, послуги якої спрямовані на вирішення проблеми крадіжки особистих відомостей клієнтів. Сервіс дозволяє користувачам реєструвати, підтверджувати персональну інформацію і захищати свою кредитну історію від шахраїв. UniquID Wallet надає безпечне рішення з управління ідентифікацією, інтегроване з сканерами відбитків пальців і іншими біометричними персональними пристроями. Працювати з додатком UniquID Wallet можна на нестандартних пристроях, серверах, персональних комп'ютерах або смартфонах, планшетах та інших пристроях з обмеженим часом роботи без перезарядження. У з-поміж заявлених можливостей можна виділити індивідуальне блокчейн-сховище для інформації про використовувані «девайси» без паролів, які замінені алгоритмами розпізнавання користувача по підключеним до системи персональних об'єктів. Це дозволяє отримати максимально високий рівень цілісності і оперативної сумісності в межах будь-якої інфраструктури. Identifi об'єднує всі особисті мережеві профілі і персональні дані в єдиний ідентифікаційний інструмент. У блокчейн можна записувати дати народження людей, відбитки пальців, зберігати відомості про дипломи, паспорти, водійські права. У перспективі це може допомогти в боротьбі з різного роду шахрайством.

ISSN 2663 - 4023

Проблеми розвитку блокчейн додатків. Впровадження блокчейн технології гальмується багатьма факторами. Перерахуємо основні з них.

Інерція гравців ринку і необхідність досягати консенсусу між великою кількістю учасників, відсутність законодавчої бази значно гальмує розвиток ринку. Відсутність законодавчої бази призводить до невизначеності в безлічі питань. Щоб технологія набула довіри, вона повинна відповідати стандартам (державним, наприклад). Немає стандартів – немає відповідності. У технології немає керуючого органу і невизначено хто буде визначати шляхи її розвитку.

Складність існуючих прототипів рішень на блокчейні для розуміння масового бізнес-споживача. Сьогодні бізнес, який цікавиться практичним застосуванням технології, задається питанням, які капіталовкладення потрібні для реалізації блокчейн-проекту в корпоративному секторі. У цьому випадку немає однозначної відповіді. Порядок цифр в значній мірі залежить від області застосування; складності бізнес-логіки, яку потрібно створити під конкретний проект; кількості зав'язків зі сторонніми сервісами; використовуваної інфраструктури зберігання ключів; кількості ролей і користувачів в системі тощо. Також компанії буде потрібний штатний фахівець з безпеки, який буде вести проект, навіть якщо всю побудову системи візьме на себе спеціалізований блокчейн-розробник. В середньому вартість побудови системи обліку для підприємства можна оцінити в десятки і сотні тисяч доларів.

Серед основних проблем можна виділити «масштабованість». В цей час всі протоколи блокчейна збудовані так, що кожен комп'ютер в мережі повинен обробити кожну транзакцію, – це властивість забезпечує максимальну відмовостійкість і безпеку ціною того, що обчислювальна потужність мережі фактично обмежується обчислювальною потужністю одного комп'ютера. Необхідно подолати ці обмеження і досягти рівня, достатнього для його масового поширення.

Також існує проблема інтеграції нових та існуючих приватних систем з відкритим блокчейном. Одним із варіантів вирішення цієї проблеми є створення служби аутентифікації на основі блокчейну для реалізації глобального рівня безпеки. Така служба може стати стандартною інфраструктурою безпеки для нових моделей змішаних приватних і публічних систем, яка принесе користь всім зацікавленим сторонам в різних сферах економіки. Прикладом такого підходу є блокчейн Гідро Рейндроп (Hydro Raindrop) [9].

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Можна зробити висновки, що блокчейн, насамперед, це інструмент для вирішення питань безпеки, надійності та прозорості трансакцій, тому використання його у різних сферах ділової активності набирає обертів. Зважаючи на проблеми розвитку блокчейн додатків, необхідно продовжувати розвиток технології в напрямку стандартизації, безпеки додатків та інтеграції блокчейн систем з іншими сучасними технологіями.

Стандартизація технології блокчейн – важливий крок до єдиного понятійного апарату, інтероперабельності, масштабування, аудиту, а також можливого подальшого регулювання технології. Саме тому в 2016 Міжнародна організація по стандартизації (ISO – International Organization for Standardization) сформувала комітет для розробки стандарту технології блокчейна і почала працювати над міжнародним стандартом ISO/TC 307 – Blockchain and distributed ledger technologies (Блокчейн і технології розподілених реєстрів). В Україні розпочата процедура зі створення національного

ISSN 2663 - 4023

комітету зі стандартизації блокчейн технології через Українське агентство зі стандартизації. Потрібно визначити базові терміни і спростити прийняття технології для усіх учасників ринку. Маючи стандарти і погоджену усталену термінологію отримаємо можливість говорити про якісне законодавче регулювання блокчейну. Маючи стандарт, можна буде проводити аудит блокчейн-платформ.

Також необхідно системно підходити до питання безпеки блокчейн додатків. В цьому напрямку необхідно проводити серйозні дослідження. На сьогодні немає великого практичного досвіду використання блокчейн систем. Єдиною мережею, яка довгий час працює без істотних збоїв є блокчейн біткойн. Проблеми, що пов'язані з мережею біткойну, були через злам сервісів, побудованих поверх блокчейну. Також, була успішно виконана атака у мережі Ethereum [10].

Блокчейн веде облік цінностей в режимі реального часу. Скоро мільярди «розумних» речей будуть взаємодіяти один з одним, тому Інтернету речей (англ. Internet of Things, IoT) потрібна технологія блокчейн. В наш час зростає потреба у виконанні операцій з великими потоками даних. Технологія блокчейн дозволяє ідентифікувати і систематизувати бази bigdata, які стосуються різних сфер бізнесу. При цьому спрощується процес складання графіків, систематизації інформації, фіксації пересувань ресурсів в процесі діяльності компанії. Компанії, що користуються рішеннями блокчейн, можуть бути впевнені в безпеці й збереженні всіх даних, їх відповідності до юридичних вимог. Такі рішення дозволяють зберігати інформацію і записи з даними у вигляді блокчейнів, роблячи часову мітку. На цьому етапі розглядаються проекти (наприклад, Woroom.network) для побудови мережі, в який об'єднуються технології блокчейн, штучного інтелекту, big data, IoT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Dan Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, New York, USA, Penguin Random House, 2016.
[2] «Украина переведет все государственные данные на блокчейн». [Онлайн]. Режим доступу: https://hightech.fm/2017/04/14/us-ukraine-bitfury-blockchain [18 черв. 2018].
[3] W. Mougayar, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology," New York, USA, John Wiley & Sons Inc., 2016.
[4] Лоран Лелу, *Блокчейн от А до Я. Все о технологии десятилетия*, Москва, Россия, Изд-во «Эксмо», 2018.
[5] "EAuction 3.0". [Онлайн]. Режим доступу: https://forklog.com/tag/eauction-3-0 [19 черв. 2018].
[6] «OpenMarket (ДП „СЕТАМ")». [Онлайн]. Режим доступу: https://minjust.gov.ua /news/ministry/openmarket-dp-setam-proviv-24-tisyachi-auktsioniv-z-vikoristannyam-tehnologii-blockchain-na-mayje-700-mln-grn [19 черв. 2018].
[7] "What is Ethereum? A Step-by-Step Beginners Guide". [Онлайн]. Режим доступу: https://blockgeeks.com/guides /ethereum [19 черв. 2018].
[8] "A Blockchain Platform for the Enterprise". [Онлайн]. Режим доступу: https://hyperledger-fabric.readthedocs.io/en/ latest [19 черв. 2018].
[9] «Гідро Рейндроп відкрита аутентифікація на блокчейні». [Онлайн]. Режим доступу: https://www. Hydrogenplat form.com/white-papers/ Hydro_Raindrop_White_Paper_Ukranian.pdf [19 черв. 2018].
[10] "Ethereum Classic". [Онлайн]. Режим доступу: http://uacoin.club/coin/ETC [19 черв. 2018].

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018
ISSN 2663 - 4023

UDC 004.031.43: 004.056

Svitlana O. Spasiteleva
PhD, Associate Professor, Associate Professor of the Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID: 0000-0003-4993-6355
spasiteleva@gmail.com
Volodymyr L.Buriachok
Doctor of Technical Sciences, Professor, Head of the Department of Information and cyber security,
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

PERSPECTIVES FOR DEVELOPMENT OF BLOCKCHAIN APPLICATIONS IN UKRAINE

Abstract. The article is devoted to the definition of problems using of blockchain technologies, and ways to overcome them to create distributed, secure applications. The paper considers the theoretical fundamentals of blockchain technologies and blockchain applications, new models of blockchain business, blockchain applications development platform, blockchain applications security, blockchain applications development problems, prospects for further research.
The analysis of recent research and publications in the field of blockchain technologies are made in the article. Based on this analysis, it was determined that the blockchain industry has not yet completed the process of generating a generally accepted multilevel technology description. The overview of existing models of business blockchain, their characteristics and areas of application are done in the article. Software tools for creating and maintaining blockchain applications are considered.
The article deals with the features, advantages and problems of using blockchain technology for creating distributed, secure applications. The problem of integration of new and existing private systems with an open blockchains is considered. A possible solution to this problem is the creation of a blockchain authentication service to implement a global security level. Such a service can become a standard security infrastructure for new models of mixed private and public systems that will be useful to all participants in different areas of the economy.
The directions of development of protected blockchain applications in the sphere of public administration and private business in Ukraine are determined. In addition, the priority tasks that need to be solved for successful implementation of technology in Ukraine are determined based on the analysis of the current state of development of blockchains. There are three main areas of development of blockade technology: standardization, application security and integration of block systems with existing private systems and modern technologies of artificial intelligence, large data and the Internet of things, and described prospects for further research for them.

Keywords: blockchain technology; enterprise blockchain; peer-to-peer network; consensus algorithms; smart contracts; application security.

REFERENCES

[1] Dan Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, New York, USA, Penguin Random House, 2016.
[2] "Ukraina perevedet vse gosudarstvennye dannye na blokchein [Ukraine will transfer all state data to the blockbuster]." [Online]. Available: https://hightech.fm/2017/04/14/us-ukraine-bitfury-blockchain [Jun. 18, 2018]. (In Russian).
[3] W. Mougayar, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology," New York, USA, John Wiley & Sons Inc., 2016.

[4] Loran Lelu, *Blokchein ot A do Ya. Vse o tekhnologii desyatiletiya* [*Block from A to Z. All about the technology of the decade*], Moskva, Rossiya, Izd-vo "Eksmo," 2018. (In Russian).
[5] "EAuction 3.0". [Online]. Available: https://forklog.com/tag/eauction-3-0 [Jun. 19, 2018].
[6] "OpenMarket (DP 'SETAM')." [Online]. Available: https://minjust.gov.ua /news/ministry/openmarket-dp-setam-proviv-24-tisyachi-auktsioniv-z-vikoristannyam-tehnologii-blockchain-na-mayje-700-mln-grn [Jun. 19, 2018]. (In Ukrainian).
[7] "What is Ethereum? A Step-by-Step Beginners Guide". [Online]. Available: https://blockgeeks.com/guides /ethereum [Jun. 19, 2018].
[8] "A Blockchain Platform for the Enterprise". [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/ latest [Jun. 19, 2018].
[9] "Hidro Reyndrop vidkryta autentyfikatsiya na blokcheyni [Hydro Rainbow is open for blockade authentication]." [Online]. Available: https://www.Hydrogenplatform.com/white-papers/Hydro_Raindrop_White_Paper_Ukranian.pdf [Jun. 19, 2018]. (In Ukrainian).
[10] "Ethereum Classic". [Online]. Available: http://uacoin.club/coin/ETC [Jun. 19, 2018].