

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

ФАКУЛЬТЕТ СОЦІОЛОГІЇ ТА УПРАВЛІННЯ

КАФЕДРА СОЦІАЛЬНОЇ ФІЛОСОФІЇ ТА УПРАВЛІННЯ

**Кваліфікаційна робота
магістра**

**ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ
ДЕРЖАВНОГО УПРАВЛІННЯ**

Виконав: магістрант 2-го курсу, групи 8.2810-з
спеціальності 281 «Публічне управління та
адміністрування»
освітньо-професійної програми «Публічне
управління та адміністрування»
Д.В. Заріпов

Керівник: професор кафедри соціальної філософії
та управління, доцент,
д.філос.н. Чайка І.Ю.

Рецензент: доцент кафедри соціальної філософії
та управління, доцент,
д.філос.н. Масюк О.П.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет соціології та управління
Кафедра соціальної філософії та управління
Рівень вищої освіти магістр
Спеціальність 281 «Публічне управління та адміністрування»
Освітньо-професійна програма «Публічне управління та адміністрування»

ЗАТВЕРДЖУЮ

Завідувач кафедри соціальної філософії та
управління

_____ Т.І.Бутченко
« ____ » _____ 2021 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРАНТУ

Заріпову Дмитру Вадимовичу

(прізвище, ім'я, по-батькові)

1. Тема роботи Впровадження Blockchain технології до системи
державного управління

керівник роботи Чайка Ірина Юріївна, д.філос.н, доцент,
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від «18» червня 2021 року № 914-с

2. Строк подання студентом роботи 8 грудня 2021 року

3. Вихідні дані до роботи Важинський С. Е., Щербак Т. І. Методика та
організація наукових досліджень : навч. посіб. Суми :СумДПУ, 2016. 260 с.; Atzori
M. Blockchain technology and decentralized governance: Is the state still necessary?
Journal of Governance and Regulation. 2017. No 6 (1). P. 45–62.; Strauss A., Corbin J.
Basics of qualitative research: Techniques and procedures for developing grounded
theory (2nd ed.). Thousand Oaks, CA: Sage. 1998.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Проаналізувати історію дослідження використання blockchain технології в системі державного управління. 2. Уточнити основні поняття у сфері впровадження blockchain технологій у державному управлінні. 3. Визначити принципи та методи дослідження впровадження blockchain технології до системи державного управління. 4. Визначити місце blockchain в системах технологій розподіленого реєстру. 5. Уточнити можливості використання blockchain технологій для реалізації функцій державного управління. 6. Дослідити впровадження blockchain технології до системи державного управління, як фактор розвитку інформаційного суспільства в сучасній Україні. 7. Обґрунтувати управлінські рішення для систем на основі blockchain у державному секторі. 8. Обґрунтувати використання blockchain для покращення управління даними у державному секторі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Чайка І.Ю., професор кафедри соціальної філософії та управління	17.06.2021	17.06.2021
Розділ 2	Чайка І.Ю., професор кафедри соціальної філософії та управління	30.08.2021	30.08.2021
Розділ 3	Чайка І.Ю., професор кафедри соціальної філософії та управління	14.10.2021	14.10.2021

7. Дата видачі завдання 18 червня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір теми кваліфікаційної роботи	Березень – квітень 2021	<i>виконано</i>
2.	Бібліографічний пошук	Травень 2021	<i>виконано</i>
3.	Розробка основних положень роботи	Травень 2021	<i>виконано</i>
4.	I розділ	Червень – липень 2021	<i>виконано</i>
5.	II розділ	Серпень – вересень 2021	<i>виконано</i>
6.	III розділ	Жовтень – листопад 2021	<i>виконано</i>
7.	Систематизація висновків	Листопад 2021	<i>виконано</i>
8.	Нормоконтроль	Листопад – грудень 2021	<i>виконано</i>

Студент _____ Д.В. Заріпов

Керівник роботи _____ І.Ю. Чайка

Нормоконтроль пройдено

Нормоконтролер _____ А.І. Васильєва

РЕФЕРАТ

Кваліфікаційна робота складається з 89 сторінок, 118 позицій у списку літератури, 4 додатків.

БЛОКЧЕЙН, ДЕРЖАВНЕ УПРАВЛІННЯ, ЛАНЦЮГ, МЕРЕЖА, ПРОТОКОЛ, СМАРТ-КОНТРАКТ, СИСТЕМА, ТЕХНОЛОГІЯ

Мета дослідження: теоретичний аналіз впровадження блокчейн технології, як елемента системи електронного врядування, у державному управлінні.

Об'єкт дослідження: технології електронного врядування в системі державного управління.

Предмет дослідження: блокчейн технології в системі державного управління.

Методи дослідження. Для реалізації визначеної мети використані методи порівняння, аналізу, синтезу та обґрунтованої теорії.

Наукова новизна полягає у теоретичному обґрунтуванні механізмів впровадження блокчейн технологій до системи державного управління.

Гіпотеза дослідження. Впровадження блокчейн технологій до системи державного управління сприятиме підвищенню ефективності її функціонування.

Висновки: 1. Стандартизація сфери блокчейну все ще знаходиться на ранніх стадіях. Уряду необхідно спочатку визначити больові точки в управлінні, а потім розглянути компроміси блокчейну як потенційного рішення в порівнянні з іншими альтернативами.

2. Для вивчення можливих варіантів застосування електронного уряду потрібні дрібномасштабні експерименти, щоб реалізувати потенціал і уникнути дорогих невдач. При великомасштабному впровадженні важливо забезпечити гнучкість – один з найважливіших критеріїв проектування систем електронного уряду. Це вимагає сильного управління, оскільки самі характеристики блокчейн-технологій мають вбудовані механізми, які суперечать гнучкості.

ABSTRACT

Qualification work consists of 89 pages, 118 items in citations, 4 supplements.

BLOCKCHAIN, GOVERNMENT, CHAIN, NETWORK, PROTOCOL, SMART CONTRACT, SYSTEM, TECHNOLOGY

The purpose of the study: theoretical analysis of the introduction of blockchain technology as an element of e-government in state administration.

Object of research: e-government technologies in the system of state administration.

Subject of research: blockchain technologies in the system of state administration.

Research methods. Methods of comparison, analysis, synthesis and grounded theory were used to achieve the goal.

The scientific novelty lies in the theoretical substantiation of the mechanisms of introduction of blockchain technologies in the system of state administration.

Research hypothesis. The introduction of blockchain technologies in the system of state administration will help to increase the efficiency of its operation.

Conclusions: 1. Standardization of the blockchain sector is still in its early stages. The government needs to first identify problem issues in the governance and then to consider blockchain trade-offs as a potential solution compared to other alternatives.

2. To study the possible options of using e-government, small-scale experiments are necessary to realize the potential and to avoid costly failures. In large-scale implementation, it is important to ensure flexibility which is one of the most important criteria for designing e-government systems. It requires strong management, as the very characteristics of blockchain technologies have built-in mechanisms that conflict the flexibility.

ЗМІСТ

ВСТУП.....	6
РОЗДІЛ 1. МЕТОДОЛОГІЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ.....	8
1.1. Історія дослідження використання blockchain технології в системі державного управління.....	8
1.2. Уточнення основних понять у сфері впровадження blockchain технології до системи державного управління.....	13
1.3. Принципи та методи дослідження впровадження blockchain технології до системи державного управління.....	19
РОЗДІЛ 2. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ.....	26
2.1. Blockchain як різновид технології розподіленого реєстру.....	26
2.2. Можливості використання blockchain для реалізації функцій державного управління.....	35
2.3. Впровадження blockchain технології до системи державного управління як фактор розвитку інформаційного суспільства в сучасній Україні.....	41
РОЗДІЛ 3. ПРАКТИЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ.....	49
3.1. Управлінські рішення для систем на основі blockchain в державному секторі.....	49
3.2. Використання blockchain для покращення управління даними у державному секторі.....	67
ВИСНОВКИ.....	76
СПИСОК ЛІТЕРАТУРИ.....	79
ДОДАТКИ.....	90

ВСТУП

Актуальність дослідження. Blockchain (блокчейн) – вибудований за певними правилами безперервний послідовний ланцюжок блоків, що містить інформацію. З'явившись у 2008 році володів такими основними принципами, як: функціонування до останнього активного мережевого вузла, доступ до повної історії ланцюжка, відсутність ієрархії, незмінність даних, відсутність посередників та централізованого контролю. Блокчейн – це технологія загального призначення, і в той же час блокчейн може забезпечити нову форму координації, як доповнення до ринків, мереж і ієрархій. Це вказує на те, що існує більш широкий спектр застосування технології блокчейн окрім криптовалют. Блокчейн в контексті державного управління відноситься до системи електронного уряду. З огляду на швидкість, з якою проводяться експерименти з блокчейном, існує брак наукової літератури з управління блокчейном, а більшість існуючих досліджень присвячено потенціалу та прийняттю блокчейну в неурядових секторах. Якщо казати в цілому, теоретико-методологічне підґрунтя закладено в наукових працях таких дослідників як: Д. Аллен, М. Атзори, В. Беккерс, К. Кащін, Ф. Даніель, А. Карвалхо, С. Девідсон, Г. Дімітропулус, В. Дрехслер, П. Філіппі, Д. Флуд, Л. Франк, Г. Говернаторі, Г. Гринспан, П. Джаячандран, М. Ласіту, І. Мартинович, О. Мазонка, С. Накамото, Д. Осборн, В. Шермін, А. Страус та Д. Корбін.

Об'єкт дослідження – технології електронного врядування в системі державного управління.

Проблемна ситуація дослідження – інформаційно-комунікаційні технології є важливою частиною сучасної реформи державного управління, змінюючи процес надання державних послуг і підвищуючи стандарти державних послуг. В той же час сьогодні бракує теоретичних досліджень, в яких би обґрунтовувались засади впровадження цифрових технологій, включаючи блокчейн, до практики діяльності органів державного управління всіх рівнів.

Предмет дослідження – блокчейн технології в системі державного управління.

Метою дослідження є теоретичний аналіз впровадження блокчейн технології, як елемента системи електронного врядування, у державному управлінні.

Завдання дослідження. Для досягнення вищевказаної мети поставлено такі завдання:

- проаналізувати історію дослідження використання blockchain технології в системі державного управління;
- уточнити основні поняття у сфері впровадження blockchain технологій у державному управлінні;
- визначити принципи та методи дослідження впровадження blockchain технології до системи державного управління;
- визначити місце blockchain в системах технологій розподіленого реєстру;
- уточнити можливості використання blockchain технологій для реалізації функцій державного управління;
- дослідити впровадження blockchain технології до системи державного управління, як фактор розвитку інформаційного суспільства в сучасній Україні;
- обґрунтувати управлінські рішення для систем на основі blockchain у державному секторі;
- обґрунтувати використання blockchain для покращення управління даними у державному секторі.

Наукова новизна полягає у теоретичному обґрунтуванні механізмів впровадження блокчейн технологій до системи державного управління.

Гіпотеза. Впровадження блокчейн технологій до системи державного управління сприятиме підвищенню ефективності її функціонування.

Структура роботи: кваліфікаційна робота складається зі вступу, трьох розділів, висновку, списку літератури, додатків.

РОЗДІЛ 1

МЕТОДОЛОГІЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ

1.1. Історія дослідження використання blockchain технології в системі державного управління

На даний момент існує лише кілька академічних досліджень, написаних спеціально по темі публічного управління і блокчейну, і кілька тематичних досліджень проєктів блокчейну, які забезпечують внесок в дослідження загальної перспективи управління. Проте, дослідження показали, що ця область має гостру потребу в аналізі з точки зору, не пов'язаної з інформаційними технологіями (ІТ). Існуюча література з управління блокчейном розглядає блокчейн з політичної або фундаментальної точки зору. Основний висновок полягає в тому, що блокчейн слід обговорювати як частину організаційної теорії, та слід відкинути як окрему політичну теорію [16, с. 1], але ці дослідження використовують досить широкий підхід до блокчейну, і обговорення блокчейну в державному управлінні не є всеосяжним. Ще одне ключове дослідження в галузі управління блокчейном стверджує, що блокчейн – це новий тип інститутів, що конкурує з ринками і мережами [32]. Ця точка зору дещо перегукується з висновком британської дослідниці Марсели Атзори про те, що блокчейн підпорядковується організаційній теорії, разом з тим стверджуючи, що блокчейн дозволяє обслуговувати людей, яких в даний час не обслуговують ринкові, ієрархічні або урядові механізми координації. Це поняття є вихідним матеріалом для перспективи публічного управління, де блокчейн використовується як інструмент для надання громадських послуг, що посилює необхідність обговорення управління блокчейном.

З 2008 року блокчейн розвивався як технологія загального призначення і знайшов різні сфери застосування, де в системі транзакцій спостерігається

проблема «довіри». Цифрова валюта та платежі, реєстрація землі, управління ідентифікацією, нотаріальне засвідчення, відстеження ланцюга поставок, охорона здоров'я, освіта, корпоративна реєстрація, управління даними, аудит, ринок енергетики, оподаткування, голосування та управління юридичними особами – це деякі сфери, де блокчейн зараз тестується для державних послуг.

Незважаючи на такий широкий інтерес, фактичне впровадження технології в державному секторі залишалося обмеженим. Більшість досліджень висвітлювали кілька проблем, пов'язаних із впровадженням, такі як відсутність регулювання, безпека та проблеми конфіденційності, недостатність та відсутність сумісної інфраструктури, неефективні та енергодорогі операції, необхідність змін у адміністративних процесах, орієнтованих на цінності, і останнє, але не в останню чергу, відсутність ефективних моделей управління [62; 85; 115]. Багато досліджень визначили управління як ключову проблему для впровадження блокчейну в державному секторі [16; 77; 85], а деякі відомі дослідження досліджують наслідки блокчейну для державного управління [16; 20; 41; 110; 115]. Тим не менш, здається, що управління блокчейном залишається одним із найбільш суперечливих аспектів для організацій державного сектору, і для вирішення проблем управління проектуванням, функціонуванням та обслуговуванням систем на основі блокчейну потрібен інструмент систематичного аналізу [62; 85]. Для впровадження в державному секторі технології блокчейну, найважливішою особливістю якої є формування довіри до процесів управління без потреби довіреної третьої сторони, розуміння того, чим керувати і як керувати, є основоположним.

У той час як деякі урядовці все ще перебувають у вичікувальному режимі, інші бачать значні переваги в тому, щоб рухатися вперед прямо зараз, пропонуючи негайні рішення та впровадження інноваційних технологій, які можуть окупитися у довгостроковій перспективі. Існує безліч прикладів використання в різних країнах, включаючи: Європейський Союз (ЄС – боротьба з контрафакцією), Естонія (цифровий уряд), США (FDA, DHS, NHS, GSA – безпека, боротьба з контрафакцією), Китай (платежі), Індія (платежі,

земельний кадастр), Швейцарія (ідентифікація), Данія (голосування), Дубай (цифровий уряд), Грузія (земельний кадастр), Гібралтар (фондова біржа) та багато інших [113]. Крім цих країн, варіанти використання блокчейну продовжують поширюватися по всьому світу, особливо в тих галузях, де ефективність державного сектору щосили намагається впоратися з попитом на різні послуги.

Блокчейн може не лише допомогти у підвищенні ефективності, але й запобігти шахрайству, забезпечуючи основу для безперебійних послуг та операцій, що охоплюють усі сфери життя. Деякі проблеми, з якими стикається більшість урядів – це корупція, фальсифікація або знищення документації. У разі використання блокчейну інформація може бути збережена та перевірена у офіційному бухгалтерському реєстрі. Це практично усуне необхідність у будь-яких документах (підроблених чи оригінальних). Існує широкий спектр програм, які впроваджуються або досліджуються урядами по всьому світу. Все інше може наслідувати впровадження цифрової ідентичності. Наприклад, естонська система управління цифровою ідентифікацією [56], її впровадження та використання у повсякденних транзакціях є основою довіри та платформою для реалізації сценаріїв використання блокчейну, деякі приклади наведені нижче як варіанти використання, які з самого початку здаються очевидними. Після того, як вони будуть повністю реалізовані та функціональні, ймовірно, з'являться нові ідеї для реалізації інших варіантів використання, особливо за рахунок конвергенції ідей та технологій, таких як штучний інтелект та інтернет речей.

Сценаріїв використання блокчейну:

- державні записи (особисті записи, земельна реєстрація, корпоративна реєстрація);

- надання атестатів на основі цифрових посвідчень та даних, що зберігаються в офіційній бухгалтерській книзі блокчейн;

- управління правами та послугами для громадян у галузі охорони здоров'я, освіти, екстрених служб, енергетики, комунальних послуг, інфраструктури та інших пілґ;

- управління ідентифікаторами виборців, голосування для прозорих виборів і підрахунку голосів;

- державні тендерні процеси;

- оподаткування;

- звичаї;

- ведення особистих записів: відомості про шлюб, розлучення, смерть, народження та страхування, паспорти, візи;

- реєстрація землі, документи, право власності, право власності на транспортний засіб, реєстрація транспортного засобу для протидії шахрайським претензіям на власність та продаж власності, що належить іншим особам, документи на ювелірні вироби, твори мистецтва.

- різні державні та приватні організації можуть використовувати офіційну інформацію реєстру блокчейну для підтримки та запуску своїх процесів та систем, а також для розробки нових наборів даних, які сприятимуть подальшому розширенню можливостей та додаткових послуг.

Деякі приклади в усьому світі, коли уряди впроваджують або тестують широкий спектр сценаріїв використання з метою надання низки послуг своїм громадянам:

- штат Андхра-Прадеш в Індії використовує блокчейн для реєстрації землі та реєстрації транспортних засобів. Вони також створили великий портфель сценаріїв використання блокчейну для підвищення ефективності операцій державного та приватного секторів [113];

- найвідоміша програма цифрового уряду на основі блокчейну – це програма електронного резидентства [42];

- у Швейцарії місто Цуг використало голосування на основі блокчейну з використанням цифрової ідентифікації на основі блокчейну;

– щоб задовольнити потребу громадян у ще більш швидкому реагуванні та наданні державних послуг, уряд Данії вивчає можливість використання штучного інтелекту та блокчейну у цифровій ідентифікації, охороні здоров'я, підтримці бізнесу та своїй системі соціального забезпечення [56];

– у 2016 році Естонський фонд електронної охорони здоров'я розпочав загальнонаціональний проект розгортання блокчейну, щоб зберегти медичні записи всього населення, щоб зберегти журнали активності та медичні записи в медичних записах населення Естонії [56];

– IBM та датська судноплавна компанія «Maersk» співпрацюють з більш ніж 90 партнерами, включаючи митні органи, операторів портів та терміналів та інших, щоб оптимізувати глобальний процес доставки. Блокчейн-платформа «Tradelens» робить ключову інформацію, необхідну для митних службовців, доступною в реальному часі. Ключові урядові групи, що беруть участь у програмі, включають митні органи Сінгапуру, Австралії, Саудівської Аравії, Перу, Нідерландів, Бельгії та США. Сьогодні, після виконання понад 150 мільйонів операцій з доставки, проект із підтримкою блокчейн повідомив про середню економію 40% порівняно зі застарілими системами [113];

– у жовтні 2018 року мер Сеула Пак Вон-Сун заявив, що столичний уряд Сеула має п'ятирічний план створити в Сеулі розумне місто, яке буде працювати на блокчейні. Запланована вартість розробки 123,3 мільярда корейських вон (108 мільйонів доларів). Планове завершення проекту до 2022 року, воно охоплюватиме 14 державних послуг у п'яти областях [9].

1.2. Уточнення основних понять у сфері впровадження Blockchain технології до системи державного управління

Державне управління – вид діяльності держави, що полягає у здійсненні нею управлінського, тобто організуючого впливу на ті сфери і галузі суспільного життя, які вимагають певного втручання держави шляхом використання повноважень виконавчої влади. В той же час державне управління здійснюється і за межами функціонування виконавчої влади, наприклад, на рівні державних підприємств, установ і організацій. Завдяки цьому поняття «державне управління» за змістом є ширшим, ніж поняття «виконавча влада». Для визначення змістовно поєднаних сфер або галузей суспільного життя, що потребують державного управління, використовується термін «сектор державного управління»[6].

Система державного управління – складне поняття, зміст якого охоплює такі складові елементи:

- суб'єкти управління, тобто органи виконавчої влади;
- об'єкти управління, тобто сфери та галузі суспільного життя, що перебувають під організуючим впливом держави;
- управлінська діяльність (процес), тобто певного роду суспільні відносини, через які реалізуються численні прямі та зворотні зв'язки між суб'єктами і об'єктами управління.

Досить поширений термін «адміністративна система» найчастіше характеризує поєднання двох згаданих елементів – суб'єктів управління та управлінської діяльності. Зміст останньої розкривається, зокрема, через поняття «цілі і завдання», «функції», «методи», «стадії», «процедури», «повноваження», «ефективність», «культура», «етика» тощо [6].

Блокчейн технологія – це концепція або протокол, що лежить в основі роботи блокчейну. В той же час блокчейн – є, по суті, розподіленою базою даних записів або загальнодоступного реєстру всіх транзакцій або цифрових подій, які були виконані та поширені між сторонами-учасниками. Кожна операція в публічному реєстрі перевіряється консенсусом системи. І після

введення інформація ніколи не може бути стерта. Блокчейн містить визначений і перевіряємий запис кожної окремої транзакції. Він об'єднує в собі протокол «peer-to-peer», технологію цифрового шифрування, механізм консенсусу, смарт-контракти і інші технології.

У блокчейні технологія криптографії в основному використовується для захисту конфіденційності користувачів і інформації про транзакції, забезпечення узгодженості даних, тощо [117]. Одним із методів захисту інформації в мережі є асиметрична техніка шифрування. В асиметричному алгоритмі шифрування ключ шифрування і ключ дешифрування відрізняються і називаються відкритим ключем і закритим ключем відповідно. Закритий ключ зазвичай потрібно генерувати за допомогою алгоритму випадкових чисел, а відкритий ключ обчислюється за допомогою незворотнього алгоритму. Алгоритм асиметричного шифрування має переваги окремих відкритих і закритих ключів, які можна передавати по незахищених каналах. Аналогічно, він має недоліки: низька швидкість обробки і низька міцність шифрування, необхідність забезпечити безпеку асиметричного алгоритму шифрування, заснованого на математичних задачах [116, с. 5].

Смарт-контракти – це механізми, які містять цифрові активи двох або більше залучених сторін, де активи розподіляються автоматично відповідно до попередньо визначених дій, коли виконуються умови запуску [52].

Смарт-контракти повинні розглядатися як функції програмного забезпечення в кожному аспекті, а механізми смарт-контракту блокчейну повинні бути детермінованими. Детермінізм смарт-контракту – це характеристика, яка підтримує реєстр у стабільному, несуперечливому стані, забезпечує остаточність транзакції та уникає софт і хард форків [29]. На основі емпіризму смарт-контракти можна розділити на три великі категорії:

- статичні;
- динамічні;
- керовані оракулами.

Статичні смарт-контракти не викликають інші смарт-контракти, не залежать від взаємодії з людиною, виконуються в один крок і ніколи не змінюють попередньо визначену кількість дій. Статичні смарт-контракти виконують примітивні математичні операції, такі як додавання, віднімання, множення та ділення. Інші смарт-контракти можуть викликати, отримувати та використовувати результати своєї роботи. Усі смарт-контракти отримують параметри для виконання дій і є певним чином динамічними. Однак у статичних смарт-контрактах немає додаткових умов, щоб змінити шлях їх дій. Математичні операції постійно досягають одного і того ж результату, а оператори щоразу дотримуються однакових правил пріоритету. Смарт-контракти можуть повертати відповідь «так/ні» на конкретне запитання або повертати стандартне зображення при виконанні дії. Приклад статичного смарт-контракту – це функція, яка приймає запит на перевірку академічного диплому, переглядає книгу для власника диплома, видає назву установи та дату видачі та повертає результат запитувачу.

У динамічні смарт-контракти вбудовані різні правила, згідно яких включаються функції, що відстежують певні умови та запускають заплановані дії. Людина може перешкоджати або скасувати функцію динамічної дії смарт-контракту. Внесок людини вважається динамічним з точки зору нестандартної кінцевої дії, зумовленої умовами. Динамічною природою смарт-контракту можна керувати за допомогою дій від машини до машини. Непередбачувані результати можуть виникнути, якщо розробка і реалізація смарт-контракту розробником помилкова, неповна або недетермінована. Приклад функції динамічного смарт-контракту є взаємозв'язок державних адміністрацій, що запитують обмін даними громадян. Наприклад, якщо податкова служба просить отримати доступ до земельних прав громадян, які належать службі земельного кадастру. Динамічний смарт-контракт, забезпечений номером ПДВ податкової служби, може отримати доступ до прав власності на землю, прив'язаних до цього номера ПДВ, якщо є відповідні дозволи громадян. Якщо універсальний блокчейн містить право власності на землю для всіх громадян, динамічний

смарт-контракт може допомогти протистояти шахрайству та ухилянню від сплати податків та стати посередником у безпечному обміні даними між країнами.

Оракул, третя основна категорія смарт-контрактів, призначена для роботи з даними із зовнішніх по відношенню до блокчейну джерел. Оракули є динамічними і включають інформацію, що поступає від так званих оракулів штучного інтелекту, які також є смарт-контрактами. Оракули діють як агенти штучного інтелекту з можливістю запитувати інформацію з реального світу та записувати її в блокчейн для використання іншими смарт-контрактами [31]. Особливістю категорії оракулів є те, що смарт-контракти, як правило, не мають права включати дані, зовнішні по відношенню до блокчейну через детермінізм функцій блокчейну. Детермінізм стверджує, що той самий результат повинен повертатися щоразу, коли викликається функція смарт-контракту, а зовнішні ресурси часто піддаються змінам. Оракули можливо застосовувати до юридичних заяв. Наприклад, закони про спадщину можуть змінюватися, і нотаріуси чи інші державні службовці, які виконують наглядові функції, повинні бути офіційно поінформовані щодо таких питань, як передача спадщини. Оракул з штучним інтелектом отримує доступ до інформації з державного сховища та записує у блокчейн, коли змінюється конкретний закон. Після цього через додаток блокчейну надсилається повідомлення, щоб підтвердити дату та час відправлення, повідомити зацікавлені сторони, а також запит і запис підтвердження отримання на блокчейні.

Концепцію смарт-контракту на основі блокчейну можна поширити на децентралізовану автономну організацію (DAO). DAO функціонує за допомогою набору комп'ютерних програм, у даному випадку смарт-контрактів, які заздалегідь визначають правила, що керують організацією [33]. Як і організація, DAO поводитьсь керуючись певними цілями, для досягнення визначеної мети. У теорії, DAO може бути створена з будь-яких причин або цілей [102, с. 27-29]. Зазвичай традиційна організація належить фізичній особі або зацікавленим сторонам і зареєстрована в централізованій системі,

наприклад в уряді. Цей тип організації керується в ієрархічних структурах. Директори в організації вирішують подальші дії, а інші члени просто виконують рішення. Наприклад, у компанії рада має право вирішувати, як поводитися з коштами та ставити мету; іншим працівникам буде доручено тільки завдання для досягнення цілей компанії. На відміну від цього, усі учасники DAO мають однакові права на ухвалення рішень. Це означає, що ніхто не має особливих привілеїв в роботі організації. Основною особливістю DAO є автономія. DAO вимагає автоматизованої програми, щоб гарантувати, що рішення будуть виконані без будь-якого ручного втручання [64]. Для смарт-контракту, якщо ініціюється набір подій у контракті, він буде виконуватися автоматично децентралізованою системою. Наприклад, якщо підрядник отримає достатньо голосів від членів DAO, йому будуть виділені кошти. Як правило, DAO також включає наступні функції:

- містить усі дані/вимоги (ресурси), необхідні для виконання завдання/процесу;
- може забезпечувати партнерські відносини між компаніями/організаціями без будь-якої фізичної взаємодії, оскільки смарт-контракт автоматично запускається на вузлах мережі і не вимагає взаємодії з людьми;
- може бути створена так само просто, як і компанія. Це глобальна організація, відкрита для усіх, яка регулюється смарт-контрактом і керується за допомогою комп'ютерних кодів/кодування.

При створенні блокчейн-мереж велику роль відіграє оновлення мережі. Існує два варіанти запровадження змін до структури блокчейну: софт форк та хард форк.

Хард форк в технології блокчейн – це радикальна зміна протоколу мережі, яка робить раніше недійсні блоки та транзакції дійсними, або навпаки. Хард форк вимагає, щоб усі вузли або користувачі оновили програмне забезпечення протоколу до останньої версії [48].

Софт форк в технології блокчейн – це зміна програмного протоколу, де недійсними стають лише раніше дійсні блоки транзакцій. Оскільки старі вузли розпізнають нові блоки як дійсні, софт форк зворотно сумісний [50].

Керування системами на основі блокчейну зазвичай включає в себе різноманітні правила та процедури, які можуть бути реалізовані як в ланцюжку, так і поза ланцюжком. Управління в ланцюжку відноситься до правил і процесів прийняття рішень, які були закодовані безпосередньо в базовій інфраструктурі системи на основі блокчейну. Цей тип управління визначає правила взаємодії між учасниками через інфраструктуру, в межах якої ці взаємодії відбуваються; ці взаємодії визначаються виключно правилами, вбудованими в базовий код блокчейну – так званім правилом коду [45]. Правила та процеси можуть бути багатошаровими; це означає, що один шар правил підпорядковується іншому. Наприклад, деякі правила можуть допускати інфраструктурні зміни, встановлюючи процедури зміни інших (нижчого рівня) правил і, можливо, навіть самих правил (вищого рівня). Управління в ланцюжку неможливо уникнути або обійти, оскільки воно діє відповідно до системи правил, які були закодовані безпосередньо в системі, яка відповідає за їх виконання. Управління поза ланцюжком включає всі інші (тобто не ланцюжкові) правила та процеси прийняття рішень, які можуть вплинути на роботу та майбутній розвиток систем на основі блокчейну.

Позаланцюжкове управління включає як ендогенні, так і екзогенні правила. Перша категорія відноситься до правил, прийнятих референтною спільнотою для забезпечення належного функціонування та постійного розвитку системи на основі блокчейну (включаючи процедури впровадження змін протоколу). Остання категорія включає всі правила, нав'язані третьою стороною референтній спільноті, наприклад, національні закони і правила, договірні угоди, технологічні стандарти, тощо.

1.3. Принципи та методи дослідження проблеми впровадження Blockchain технології до системи державного управління

Як зазначається в «Енциклопедичному словнику з державного управління», принцип – це «основні засади, вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю і відображають суттєві положення теорії, вчення, науки, системи права, державного устрою тощо» [3, с. 560].

У державному управлінні принципи розглядаються, вважає А. Кузнецов, «як прояви закономірностей, відношення або взаємозв'язки суспільно-політичного характеру та інших груп елементів державного управління, відображені як певне наукове положення, що застосовується в теоретичній і практичній діяльності людей у сфері державного управління. Принципи державного управління ґрунтуються на онтологічних, гносеологічних і методологічних аспектах державно-управлінської діяльності, відображають найбільш суттєві, основні, об'єктивно необхідні закономірності, відносини і взаємозв'язки в державному управлінні» [4, с. 561].

Сучасна наука керується трьома основними принципами пізнання: принципом детермінізму, принципом відповідності і принципом додатковості [1, с. 36].

Філософський енциклопедичний словник поняття «детермінізм» (лат. *determinare* – обмежити, визначити) тлумачить як філософське вчення про визначений (недовільний) характер буття і явищ, теорію відносин, опосередкування, завдяки яким продукуються речі і явища, визначається їх природа та спосіб існування. Детермінізм – принцип причинності, згідно з яким не існує нічим не зумовлених подій, кожне явище породжене певним попереднім явищем [7, с. 152].

Зосередимо увагу на одному із визначень, яке пропонує І. Шаталович. Вона вважає, що в основі принципу детермінізму лежать такі тези:

- кожне явище відбувається з необхідності;
- кожне явище має причину;

- кожне явище обумовлене;
- кожне явище відбувається певним чином;
- кожне явище відбувається закономірно;
- кожне явище взаємопов'язане з іншими явищами.

Цю сукупність тверджень умовно узагальнимо твердженням: незалежних одного від іншого явищ не існує [8, с. 193].

Детермінізм в технологіях блокчейну – це концепція, згідно з якою події в рамках даної парадигми пов'язані причинно-наслідковим зв'язком таким чином, що будь-який стан (об'єкта чи події) повністю визначається попередніми станами. Це означає, що ми досягаємо точно такого ж стану, як і всі інші, якщо виконуємо ті самі операційні кроки в тому ж порядку.

Принцип відповідності означає наступність наукових теорій. Нові теоретичні знання бувають корисні для розвитку науки, але якщо вони не будуть співвідноситися з колишніми, то наука перестане бути цілісною [1, с. 37].

Сутність принципу додатковості полягає в наступному: відтворення цілісності явища вимагає застосування в пізнанні взаємовиключних «додаткових» класів понять. За допомогою додатковості встановлюється еквівалентність між класами понять, комплексно описують суперечливі ситуації в різних сферах пізнання (загальне розуміння принципу додатковості) [1, с. 37].

«Науковий метод, згідно з визначенням науковців (Ю. Ковбасюк, Л. Ващенко, Ю. Сурмін та ін.), – це спосіб, підхід, інструмент, прийом, яким користується певна наука для дослідження закономірностей, що становлять її предмет. Це комплекс різноманітних засобів, який дає можливість знайти оптимальний шлях до наукової істини. Під методом теоретичного дослідження розуміється сукупність прийомів досягнення мети, поставленої наукою, чи вирішення конкретного дослідницького завдання, а під методологією – вчення про систему методів, що використовуються в певній науці» [2, с. 117].

Що стосується державного управління як самостійної галузі наукового знання, то воно спирається як на загальні наукові методи (абстрагування, аналіз, синтез, індукція, дедукція, систематизація, моделювання тощо), так і на спеціальні, що витікають із соціально гуманітарного, у своїй кінцевій якості, предмета дослідження [2, с. 117].

Порівняння – це метод виявлення відмінностей між процесами, явищами, об'єктами. Порівняльним є таке дослідження, в якому порівнюються певні характеристики двох об'єктів у даний момент часу або одного об'єкта в різних часових точках, з метою виділення та аналізу рис подібності та розбіжності між досліджуваними характеристиками [5, с. 30]. В основі порівняльного методу лежить процес індукції. В контексті технологій блокчейн в державному управлінні порівняння має на меті виявити схожості та відмінності між двома, або більше досліджуваними об'єктами, а також слугує засобом отримання інформації.

Аналіз – метод пізнання, при якому предмет дослідження (об'єкт, властивості тощо) розкладається на окремі складові частини. У зв'язку з цим аналіз лежить в основі аналітичного методу досліджень [1, с. 40]. Використовується для визначення особливостей впровадження блокчейн-технологій до сфери державного управління.

Синтез – це поєднання окремих сторін предмета дослідження в єдине ціле. В контексті дослідження використовується для пошуку можливостей впровадження блокчейн-технологій в умовах діджиталізації державного управління.

Аналіз і синтез взаємозв'язані та уособлюють єдність протилежностей. Розрізняють такі види аналізу і синтезу: прямий, або емпіричний, метод (використовують для виділення окремих частин об'єкта); елементно-теоретичний метод (базується на уявленнях про причинно-наслідкові зв'язки різних явищ); структурно-генетичний метод (вилучення із складного явища таких елементів, які створюють вирішальний вплив на решту сторін об'єкта) [1, с. 40].

Обґрунтована теорія є науковим методом. Її процедури складено таким чином, що якщо вони проводяться ретельно, то метод задовольняє критеріям «доброї» науки: значущості, сумісності теорії та спостереження, узагальнення, відтворюваності, точності, суворості та верифікації [101, с 24].

У роботі проведено систематичний огляд літератури, щоб вивчити та проаналізувати наявні знання в академічній літературі щодо управління блокчейном. За даними [57], лише 14 з 28 досліджених академічних пошукових систем добре підходять для систематичних оглядів, оскільки вони відповідають усім необхідним вимогам до ефективності щодо точності, запам'ятовування та відтворюваності. Беручи до уваги дисциплінарну спрямованість і кількість доступних звернень, було вибрано Scopus, ScienceDirect та Web of Science для пошуку дослідницьких статей. Пошуковий запит будується наступним чином: (blockchain або block chain або distributed ledger) та (governance).

Запит проводився шляхом пошуку за назвами, анотаціями та ключовими словами опублікованих журнальних статей, розділів книг та матеріалів конференції, що рецензуються. Не вибирався конкретний термін, були включені всі публікації, опубліковані на дату запиту. Після видалення дублікацій та статей з недоступністю повного рукопису склався зведений список із 495 публікацій.

Критерії включення до остаточної вибірки були встановлені наступним чином:

- публікація повинна містити концептуалізацію управління блокчейном;
- публікація повинна містити класифікацію управління блокчейном.

Після ретельної перевірки до остаточного списку було відібрано 67 публікацій, що розподілились по таким галузям як:

- економіка;
- інформатика/бібліотечна справа;
- бізнес;
- інформатика/інформаційні системи;
- інженерія/електроелектроніка;

- інформатика /міждисциплінарне застосування;
- право;
- менеджмент;
- інформатика/теоретичні методи;
- науки про землю та навколишнє середовище.

Щоб вирішити дослідницькі питання, дотримуючись підходу обґрунтованої теорії провели тематичний аналіз серед вибраних статей, щоб визначити, розробити та зв'язати концепції існуючої літератури з концептуальними рамками управління блокчейном. Підхід обґрунтованої теорії дотримується відкритих, осьових та вибіркового процесів кодування [101].

Перший набір кодів був створений з посиланням на управління блокчейном і застосований до даних після ітераційного процесу відкритого та осьового кодування. Фаза відкритого кодування дозволила визначити відповідні концепції, що стосуються управління блокчейном, а осьове кодування дозволило пов'язати ідентифіковані концепції з конкретними підкатегоріями в рамках управління блокчейном. У селективному кодуванні підкатегорії інтегруються та розвиваються в теорію.

Завдяки відкритому та осьовому кодуванню визначили три різні категорії в управлінні блокчейном. Перша категорія зосереджена на інфраструктурі блокчейну. У цих дослідженнях управління блокчейном вбудовано в технічний дизайн інфраструктури блокчейну, а дослідницька робота зосереджена на з'ясуванні того, як різні рішення системних дизайнерів щодо архітектури блокчейну, додатків блокчейну та технічних стандартів формують управління блокчейном. Цей підхід до управління блокчейном іноді концептуалізується як «управління за допомогою блокчейну» [85] або «управління за допомогою інфраструктури» [43].

Друга категорія пов'язана з операційними процесами управління блокчейном і охоплює вибір технічного дизайну та алгоритми, які впливають на обмін інформацією, транзакції та колективні дії між користувачами. Прийняття рішень за допомогою мережевих та автономних методів, ініціатив та

механізмів консенсусу знаходяться у центрі уваги цієї категорії. Цей підхід до управління блокчейном концептуалізується деякими дослідниками як «управління блокчейном» [85] або «управління інфраструктурою» [43].

У третій категорії блокчейн розглядається як технологія управління, яка дозволяє децентралізованим, алгоритмічним та автоматизованим формам управління реалізовувати політичні рішення. У цих дослідженнях управління блокчейном фокусується на регулюванні, організації та контролі системи, заснованої на блокчейні, у конкретній інституційній структурі. Деякі пов'язані з цим питання управління мають централізований характер порівняно з децентралізованими структурами, правилами та положеннями в реалізації політики та контролем управління блокчейном [55; 95].

При вибіркового кодуванні назвали ці три категорії відповідно мікро-, мезо- та макрорівнем управління. Ці три рівні часто використовуються в соціальних науках для класифікації об'єктів дослідження за розміром, масштабом або місцезнаходженням. У сфері державного управління ці рівні в основному відповідають рішенням та взаємодіям на індивідуальному, організаційному та інституційному рівнях. Коротко, управління на мікрорівні відноситься до вибору проектувальників систем щодо архітектури блокчейну та додатків. Мезорівневе управління відноситься до групових рішень та поведінки користувачів. Управління на макрорівні відноситься до вибору на інституційному рівні у конкретному політико-адміністративному середовищі.

На рівні синтезу даних розподілили вибраний список статей за виявленими категоріями. Статті з ширшим охопленням питань управління поділяються на кілька категорій. Огляд кодів та субкодів, взято з відповідної літератури та впорядковано за трьома рівнями управління (див. Додаток А).

Отже, проаналізувавши основні дослідження по темі публічного управління та блокчейну, визначили сутність блокчейну в контексті впровадження до систем державного управління на прикладі сценаріїв його використання. Провели аналіз світового досвіду використання блокчейну з метою надання низки послуг своїм громадянам.

Уточнено основні поняття у сфері впровадження блокчейн технології до системи державного управління. Визначено сутність терміну «блокчейн технологія» та «блокчейн» в контексті державного управління. Запропоновано категоризацію смарт-контрактів на: статичні, динамічні, керовані оракулами, та визначено їх роль в блокчейн технології державного управління. Поширено концепцію смарт контракту на DAO, що порівнюється з організацією без децентралізованого управління.

Дослідження впровадження блокчейн технології до системи державного управління потребувало використання в єдності основних принципів (детермінізму, відповідності, додатковості) та наукових методів (порівняння, аналізу, синтезу, обґрунтованої теорії), що дало змогу повно і всебічно визначити зміст, концептуальні підходи, пріоритетні напрями впровадження блокчейн технології до системи державного управління.

На основі методу обґрунтованої теорії запропонована категоризація управління блокчейном, що була заснована на систематичному огляді літератури. Структура припускає, що управління блокчейном в державному секторі передбачає прийняття рішень щодо архітектури інфраструктури, архітектури додатків, інтероперабельності, механізму прийняття рішень, механізму стимулювання, механізму консенсусу, організації, підзвітності та контролю управління.

РОЗДІЛ 2

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ

2.1. Blockchain як різновид технології розподіленого реєстру

Розподілений реєстр, який також називають спільним реєстром або технологією розподіленого реєстру або Distributed Ledger Technology (DLT) – це консенсус щодо тиражованих, спільних та синхронізованих цифрових даних, географічно розподілених між різними сайтами, країнами чи установами. На відміну від централізованої бази даних, центрального адміністратора немає.

Головна відмінність полягає в тому, що, хоча блокчейн вимагає загального консенсусу між усіма вузлами, DLT може досягти консенсусу без необхідності перевірки по всьому блокчейну.

Блокчейн – це тип DLT, децентралізованої бази даних, якою керують багато учасників (технологія розподіленого реєстру), в якій транзакції записуються з незмінним криптографічним підписом, який називається хеш. Блокчейн формується як безперервно зростаючий ланцюжок блоків із записами про всі транзакції. Копії бази або її частини одночасно зберігаються на безлічі комп'ютерів і синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блоці не шифрується і доступна у відкритому вигляді, а відсутність змін засвідчується криптографічно через хеш-ланцюжка.

Однією з ключових різниць між іншими типовими базами даних та блокчейном є спосіб структури даних. База даних структурує свої дані в таблиці, тоді як блокчейн, як випливає з назви, структурує свої дані в шматки (блоки), які з'єднані між собою. Це робить так, що всі блокчейни є базами даних, але не всі бази даних є блокчейнами. Ця система також за своєю суттю

робить незворотну хронологію даних, коли їх впроваджують децентралізовано. Коли блок заповнений, він вкладається в камінь і стає частиною цієї часової шкали. Кожному блоку в ланцюжку призначається точна позначка часу, коли він додається до ланцюжка.

Блокчейн публічно зберігає в незашифрованому вигляді інформацію про всі транзакції, що підписуються за допомогою асиметричного шифрування. Для запобігання багаторазової витрати однієї і тієї ж суми використовуються мітки часу, реалізовані шляхом розбиття бази даних на ланцюжок спеціальних блоків, кожен з яких, в числі іншого, містить в собі хеш попереднього блоку та дані транзакцій, подані як хеш-дерево.

Кожен новий блок здійснює підтвердження транзакцій, інформацію про які містить і додаткове підтвердження транзакцій у всіх попередніх блоках ланцюжка. Змінювати інформацію в блоці, який вже знаходиться в ланцюзі, не практично, так як в такому випадку довелося б редагувати інформацію в усіх наступних блоках. Найчастіше умисна зміна інформації в будь-якій з копій бази або навіть в досить великій кількості копій не буде визнана істинною, тому що не буде відповідати правилам. Деякі зміни можуть бути прийняті, якщо будуть внесені в усі копії бази (наприклад, видалення декількох останніх блоків через помилки в їх формуванні). Завдяки цьому успішне «подвійне витрачання» (повторна трата раніше витрачених коштів) на практиці вкрай мало ймовірна.

У блокчейні можливі ситуації, коли кілька нових блоків в різних частинах розподіленої мережі називають попереднім один і той же блок, створюються одночасно, тобто ланцюжок блоків може гілкуватися. У разі рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якої з'явився раніше. Порівняння технології блокчейн з іншими видами DLT (див. Додаток Б).

Переваги використання технології блокчейн:

- забезпечення високоефективних механізмів захисту цілісності та доступності інформації;

- створення повністю децентралізованої системи;
- стійкість системи щодо несанкціонованого втручання та зміни інформації, яка зберігається в реєстрі;
- економія коштів порівняно зі зберіганням інформації на паперових носіях та із застосуванням традиційних технологій зберігання даних на машинних носіях інформації;
- неможливість внесення змін до реєстру даних попередньою датою;
- підвищення рівня захисту державних баз даних від несанкціонованого втручання, зокрема від кібератак;
- зменшення випадків шахрайства, оскільки кожен запис буде унікально закодовано і прив'язано до інтелектуального ключа, який відомий тільки власнику майна;
- використання розумних смарт-контрактів, які є програмованими контрактами й виконуються самостійно з дотриманням певних умов.

Водночас при використанні технології блокчейн існують певні ризики:

- розкриття персональних даних та конфіденційної інформації;
- низька пропускна здатність і швидкість роботи бази даних;
- рівень безпеки та децентралізація системи прямо залежать від кількості учасників та обчислювальних потужностей;
- можливість введення недостовірних даних;
- людський чинник в управлінні доступом до реєстрів;
- ідентифікація користувачів бази даних;
- глобальна синергія (синхронізація) бази даних;
- захист системи в інфраструктурі мережі.

Основою технології розподіленого реєстру є протокол консенсусу. Вже протягом десятиліть математики та інженери розробляють розподілені мережі і протоколи консенсусу, але тільки з появою проекту Bitcoin ця технологія зробила значний ривок вперед. Цей крок уможливив створення додатків абсолютно нового типу.

Консенсус в загальному розумінні означає спосіб прийти до угоди. У блокчейні, який являє собою децентралізовану систему, яка не має єдиного керуючого органу, для досягнення консенсусу розроблені різні алгоритми. У блокчейн-мережі не має значення, чи довіряють учасники системи один одному чи ні. Вони повинні домовитись про певні принципи роботи, які стосуватимуться всіх. І це – пряма функція механізму консенсусу. Алгоритм консенсусу в блокчейні являє собою набір певних математичних правил і функцій, які дозволяють досягти угоди між усіма учасниками і забезпечити працездатність мережі. На даний час існує безліч видів досягнення консенсусу. Найбільш розповсюджені механізми консенсусу (див. Додаток В). Обрання алгоритму консенсусу залежить від цілі виконання майбутньої мережі, класу блокчейн мережі, потрібної продуктивності, масштабованості, можливості підтримувати смарт-контракти.

Платформи розподіленого реєстру можна поділити на три класи: платформи відкритого типу, закритого типу і комбіновані.

Платформи відкритого типу (permissionless), або публічні дозволяють стати учасниками платформи необмеженому колу осіб, ніякої реєстрації або відкликання повноважень не потрібно. Прикладами таких платформ є Bitcoin та Ethereum і абсолютна більшість інших криптовалютних платформ.

Платформи закритого типу (permissioned), або приватні, або корпоративні обмежують коло учасників межами спільноти, для участі потрібна реєстрація, при виході із товариства право доступу відзивається.

Прикладами таких платформ є всі платформи, створені в рамках проекту Hyperledger:

- Hyperledger Fabric;
- Hyperledger Iroha;
- Hyperledger Sawtooth;
- Corda;
- Tendermint;
- Quorum;

- Echonum;
- NEM Catapult та інші.

Платформи змішаного, або комбінованого, типу – це платформи відкритого типу, які використовують для досягнення консенсусу технології побудови платформ закритого типу. Поки такі платформи не знаходять широкого практичного застосування – в цій сфері переважають експериментальні розробки. Як приклади можна привести платформи як:

- Toda-Algorand;
- Omniledger;
- BitcoinNG та інші.

Відзначимо найважливіші особливості платформ розподіленого реєстру відкритого типу:

- учасники можуть легко додаватися і виходити з блокчейн-мережі, від присутності або відсутності конкретного учасника в цілому нічого не залежить, можлива анонімна участь (точніше, псевдонімна, оскільки транзакції, виконані під одним і тим же псевдонімом, відстежувані);

- формування нових блоків транзакцій на цих платформах відбувається за допомогою алгоритмів консенсусу, кожен з яких реалізує принцип лотереї;

- для роботи блокчейн-платформи відкритого типу потрібна криптовалюта, щоб стимулювати майнерів. Ця вимога зберігається незалежно від того, чи створюється сама по собі платформа розподіленого реєстру як криптовалюта або як універсальна. Таким чином, з'являється вимога наявності як «зовнішньої», так і «внутрішньої» криптовалюти. «Зовнішня» потрібна для врегулювання зобов'язань учасників в рамках виконання смарт-контрактів, «внутрішня» – для винагороди вузлів, що виконують корисну роботу в інтересах всієї спільноти. «Зовнішня» і «внутрішня» криптовалюта може бути однаковою (Bitcoin) або різною (Ethereum: ефір і газ);

- блокчейн-платформи відкритого типу дуже ресурсомісткі (електроенергія, машинний час).

Ключовою особливістю платформ відкритого типу є специфічний механізм досягнення консенсусу при записі нових блоків до реєстру. Оскільки для платформи відкритого типу невідома точна кількість її учасників в кожен конкретний момент часу, неможливо відрахувати, скільки вузлів має проголосувати для досягнення консенсусу. У зв'язку з цим в якості критерію досягнення консенсусу має використовуватися не просто достатня кількість учасників мережі, а будь-яка інша величина: достатня частка обчислювальної потужності мережі, достатня частка криптовалютних ресурсів, якої в сукупності володіють учасники, що прагнуть досягти консенсусу, або щось ще.

Головні особливості платформ розподіленого реєстру закритого типу полягають у наступному:

- учасники не можуть самостійно додаватися і виходити з блокчейн-мережі – для цього центр реєстрації, званий на різних платформах або підтверджуючим центром, або провайдером членства (MSP – membership service provider) і т.п., повинен видати учаснику його цифровий ідентифікатор і ключі;

- формування нових блоків транзакцій відбувається за 3 кроки:

- 1) виконання смарт-контрактів та валідація транзакцій;
- 2) впорядкування окремих транзакцій в блок;
- 3) виконання протоколу консенсусу.

- протоколи, що дозволяють досягти консенсусу шляхом голосування, набагато менш трудомісткі, ніж будь-який із способів, що використовуються для платформ відкритого типу (на кілька порядків величини). Як наслідок, блокчейн-платформи закритого типу мають високу швидкодію і хорошу масштабованість;

- для роботи блокчейн-платформи закритого типу не потрібна криптовалюта;

Як і у випадку з платформами відкритого типу, ключовою особливістю платформ закритого типу є реалізований в них механізм консенсусу. Оскільки

для платформ закритого типу число учасників точно відомо в кожен конкретний момент часу, для досягнення консенсусу може бути застосований принцип голосування. Строго кажучи, система розподіленого реєстру вимагає реалізації не просто протоколу консенсусу, а так званого протоколу атомарної ширококомовної розсилки [26], так як реплікам необхідно не просто узгоджувати додавання до реєстру одиночних записів, а й суворо зберігати порядок транзакцій, а значить, послідовність зміни станів реєстру. Проте, в повсякденній практиці прижилося саме поняття консенсусу, тому при несуворому аналізі питання можна користуватися і цим терміном. В даний час відомо більше 700 протоколів консенсусу, що працюють при різних припущеннях про моделі противника. Розрізняють два основних типи таких протоколів: відмовостійкі (CFT – crash fault-tolerant) і стійкі до «візантійських» атак (BFT – byzantine fault-tolerant) (принцип голосування). Під «візантійськими» розуміють атаки активного противника, який може вести себе довільним чином, в тому числі посилаючи іншим учасникам мережі некоректні і суперечливі повідомлення. Назва походить від так званого «завдання про візантійських генералів».

Використання протоколів, заснованих на голосуванні, надає велику гнучкість в побудові системи розподіленого реєстру. Так, ролі вузлів, які виконують смарт-контракти, що досягають консенсусу, що вносять зміни до реєстру і зберігають копії реєстру в принципі можуть бути розділені, що дозволяє підвищити швидкодію платформи і довіру до неї користувачів. Перераховані фактори роблять платформи закритого типу дуже привабливими інструментами забезпечення довіри бізнес-процесів рівня корпорацій, консорціумів, альянсів. На них також можуть бути реалізовані криптовалюти і додатки зі смарт-контрактами, які вимагають розрахунки в криптовалюті, але при цьому криптовалюта залишається тільки «зовнішньою» за своєю роллю в системі (див. табл 2.1).

Таблиця 2.1

Порівняння різних типів технології блокчейн

	Permissionless public	Permissioned public	permissionless private	Permissioned private
Участь	Кожен може завантажитись та діяти як вузол	Тільки користувачі, що відповідають заздалегідь визначеним критеріям, можуть завантажуватись та діяти як вузли	Кожен у приватній мережі може виступати в ролі вузла	Лише вибрані вузли приватного каналу можуть виконувати функції вузла
Споживання енергії	Високе	Середнє	Низьке	Низьке
Безпека	Дуже висока	Висока	Середня	Висока
Швидкість	Дуже повільна	Повільна	Швидка	Дуже швидка
Рівень довіри	Без довіри	Без довіри	З довірою	З довірою

До числа основних переваг DLT приписують безпеку, але поки що на цей рахунок не існує єдиної думки. Так, об'єднана група експертів в області безпеки з Гонконзького політехнічного університету, Університету електронної науки і технології Китаю, а також Пекінського університету виявила цілий ряд вразливих сторін блокчейна. Однією з них є продуктивність, яка може знижуватися через складні механізми консенсусу і некоректних даних. Прикладом є вже згадуваний PoW, який дослідники називають «марнотратством ресурсів» [76].

Ще одна проблема, яка заважає глобальному впровадженню технології – ризик «атаки 51%». Вона відбувається, коли у атакуючої сторони, в ролі якої може виступати порівняно невелика кількість майнерів, знаходиться «контрольний пакет» хешрейта, тобто обчислювальних потужностей. В результаті атаки майнери отримують контроль над всією мережею і можуть створювати блоки на свій розсуд. Чим більше обчислювальних потужностей знаходиться в розпорядженні майнерів, тим вищі шанси знайти вірне рішення

швидше за всіх і тим більше розмір винагороди. Також «атака 51%» може привести до того, що недобросовісні майнери зможуть використовувати одну і ту ж монету кілька разів, відкликаючи вчинені з нею транзакції (подвійне витрачанням).

При використанні блокчейну секретний ключ користувача розглядається як підтверджуючий реквізит для ідентифікації та безпеки, що генерується і зберігається самим користувачем. Оскільки блокчейн не залежить від якихось централізованих сторонніх довірчих організацій, то в разі крадіжки особистого ключа важко відстежити подальшу поведінку злочинців і відновити змінену ними блокчейн-інформацію.

Являє проблему анонімність, яка безпосередньо пов'язана з криптовалютою. Відмивання грошей, наркоторгівля, махінації з нерухомістю та зброєю – все це дуже важко відстежити. Окремо стоять проблеми зі смарт-контрактами. Підроблені смарт-контракти можуть спростити витік конфіденційної інформації, крадіжку криптографічних ключів. Проблеми зі смарт-контрактами можуть бути викликані програмними дефектами.

Крім цього згадується проблема мертвого коду та циклічність операцій у смарт-контрактах на базі Ethereum. Проблема викликана тим, що користувачеві дуже часто доводиться для оплати будь-яких операцій вдаватися до власної криптовалюти Ethereum, вартість якої для деяких операцій з інтенсивних введенням-виведенням встановлюється заниженою, що дозволяє виконувати велику кількість таких операцій за одну транзакцію. Завдяки цьому зловмисник може ініціювати DDoS-атаку на Ethereum.

По мірі розвитку сервісів, заснованих на технології блокчейн, зростає кількість атак, спрямованих на несанкціоноване внесення даних до реєстру, блокування роботи систем або на отримання зловмисниками контролю над ресурсами. Як об'єкти атак можуть бути розглянуті:

- криптографічні алгоритми;
- ключі (гаманці);
- алгоритми консенсусу;

- смарт-контракти;
- ноди (вузли) мережі;
- компоненти інтерфейсу користувача і додатків.

Докладний аналіз вразливостей технології блокчейн, де кожному з компонентів зіставлені можливі уразливості і наведені приклади здійснених атак (див. Додаток Г).

2.2. Можливості використання blockchain для реалізації функцій державного управління

Блокчейн як нова мережева технологія має безліч підходів для академічного обговорення. Теорія транзакційних витрат або теорія технологічного потенціалу можуть дати пояснення впливу блокчейну на конкретний організаційний або галузевий рівень. Проте технологія ще не досягла широкого поширення, а також знаходиться на ранніх стадіях розвитку і не має емпіричних доказів для підходу з точки зору технологічного потенціалу. Використання теоретичних основ реформи державного управління дозволяє зробити висновки про те, як технологія впишеться в сучасні рамки реформи, якщо взагалі впишеться. Винахід інтернету є хорошим аналогом для ілюстрації того, як технологія розвивалася, щоб доповнити надання державних послуг або трансформувати їх. Якщо спочатку інтернет використовувався як засіб зниження адміністративних витрат, то потім він перетворився на ширшу платформу для взаємодії уряду і громадян, в інструмент управління.

Управління, хоча і є ключовим поняттям з точки зору обговорення парадигми державного управління або рамок реформи, не має визначення, яке було б загально визнаним. Визначення управління варіюється залежно від контексту. Управління може відноситися до горизонтальних стосунків між організаціями державного сектора і іншими організаціями [87, с. 304] або до визначення – «механізми управління в певній політичній одиниці, що підкреслюють взаємодію гравців держави, бізнесу і суспільства» [38]. Кожне з

визначень управління фокусується на різних елементах одного і того ж кластера ідей. Загальним для більшості визначень є те, що вони розглядають його як загальну концепцію керівництва і управління державним сектором і його взаємовідносин з іншими суб'єктами. Хоча управління саме по собі є позитивною концепцією, воно часто тісно пов'язане з іншим ключовим терміном «добре врядування», який є нормативною концепцією [38, с. 388]. Концепція доброго врядування міняється з часом і часто диктується міжнародними організаціями, такими як Організація економічного співробітництва та розвитку (ОЕСР) [38, с. 389], і вченими в області державного управління. Виділемо чотири різні підходи до управління.

Управління як корпоративне управління: «управління відноситься до принципів правильно функціонуючої адміністрації. Така адміністрація характеризується справедливим відношенням до громадян і однозначною організацією, яка дотримується основних принципів верховенства закону. Тут акцент робиться на функціонуванні уряду, а не на тому, як воно організоване. Проте такий погляд на управління мало що додає до класичних уявлень про уряд або навіть бюрократію» [87, с. 303].

Управління як новий державний менеджмент: «засіб підвищення ефективності і підзвітності або форма ринкового управління [21; 86]. Згідно з цим визначенням, роль уряду полягає в тому, щоб управляти, а не гребти. У центрі уваги уряду має бути постановка цілей, а не контроль процесу реалізації» [86].

Управління як багаторівневе управління: відноситься до концепції досягнення консенсусу і результатів в багатосторонньому середовищі [87, с. 304]. Одним з найбільш очевидних прикладів є обговорення екологічних проблем, в якому бере участь безліч суб'єктів з державного, приватного і третього сектора, кожен з яких має різні стимули і наміри відносно результатів політики.

Управління як мережеве управління: «управління відбувається в основному у рамках рухливої мережі державних і недержавних суб'єктів, і

взаємодія між цими групами робить процеси управління складними і важкокерованими. Отже, необхідні стратегії керівництва і управління відрізняються від тих, які використовуються у більше класичних підходах» [87, с. 305].

Усі вищезгадані визначення управління дотримуються різних парадигм державного управління. Порівнюючи різні визначення управління, визначення 3 і 4 обоє фокусуються на тому, що управління – це концепція, яка проявляється в мережах. Сучасна концепція управління перетворилася на слово, що означає перехід від традиційних організацій з вертикальною ієрархією до управління мережевого типу [87, с. 305], оскільки воно розглядає співпрацю держави і громадянського суспільства як необхідну умову функціонування уряду. Таким чином, здатність управляти – це не лише управління ресурсами державного сектора, але і використання ресурсів інших секторів. Бюрократична структура – це не щось ізольоване, а швидше центральний механізм, який забезпечує рух економіки і громадянського суспільства. Аналог «механізму» доречний, оскільки він має на увазі, що якщо одна з частин працює неефективно, це впливає на інші частини, пов'язані з механізмом. Для того, щоб механізм суспільства працював стабільно, потрібні «рамки» для досягнення гармонії.

У 2008 році світ пережив фінансову кризу, приблизно в той же час програміст під псевдонімом Сатоші Накамото випустив технічний документ про криптовалюту. У документі була представлена концепція цифрової готівки в технічних деталях, що обіцяла проведення цифрових транзакцій з низькою оплатою без довірених посередників [82, с. 1]. Хоча цифрові гроші і криптографічно захищений ланцюжок блоків не були новими ідеями, було запропоновано вирішення візантійської проблеми генералів шляхом впровадження протоколу консенсусу Proof-of-Work. Бачення Накамото полягало не в скиданні уряду і початку фінансової революції, а в наданні послуг тим, хто нині не обслуговується [103], особливо країнам третього світу, де багато установ працюють повільно, а уряди корумповані. Ця нова технологія

надала громадянам надійну систему, яка знаходиться за межами нинішньої сфери діяльності урядів.

Блокчейн розподілений між вузлами (учасниками блокчейну), і всякий раз, коли новий блок підтверджується, він негайно додається в усі вузли. За своєю суттю, мета блокчейну – розв’язати проблему довіри під час транзакцій між сторонами. Коли традиційно існує третя сторона, довірена організація, будь то уряд або банк, блокчейн усуває необхідність в посереднику за допомогою однорангової мережі. Декілька транзакцій об’єднуються в новий блок, який додається у блокчейн. Коли новий учасник входить в мережу блокчейн, він обирає найдовший ланцюжок, який вважається найбільш достовірним [75, с. 3]. Таким чином, не існує єдиної точки відмови, тобто жоден вузол не може переписати блокчейн або підтвердити шахрайські транзакції, а якщо один вузол буде знищений, мережа все одно функціонуватиме. Попри те, що Bitcoin і блокчейн довгі роки залишалися непоміченими, останнім часом багато чинників сприяють їх популярності. Перший додаток заснований на блокчейні – Bitcoin – має безліч переваг перед традиційними неблокчейновими аналогами, що є однією з причин популярності цієї технології. Додаткова причина, по якій публічні блокчейни, такі як Bitcoin, викликають громадський резонанс, пов’язана з фактом підвищеної недовіри до існуючих форм уряду і інститутів. Технологія блокчейн обіцяє нову форму управління і кидає виклик традиційним ієрархічним моделям управління за допомогою бездовірної децентралізації.

На концептуальному рівні блокчейн дозволяє двом сторонам здійснювати законні угоди один з одним без участі третьої сторони. Традиційно для законної угоди потрібен посередник, який керує транзакцією, стежачи за тим, щоб обидві сторони виконували свою частину транзакції. Уряд традиційно передає цю роль посередника на аутсорсинг, наприклад, банкам або юридичним фірмам, які несуть відповідальність у разі неправомірних дій. Використання управління блокчейном піднімає важливе питання про управління мережею: хто несе відповідальність в повністю децентралізованій мережі без

центрального органу влади. Анонімність і децентралізація роблять блокчейн і інтернет досить схожими. Блокчейн часто порівнюють з інтернетом в контексті технологічних інновацій [61], але у них є ключова істотна відмінність. Інтернет – це фундаментально технологічна інновація, тоді як блокчейн, можна стверджувати, є фундаментально інституціональною інновацією. Блокчейн не примушує електрони рухатися швидше, проте він знижує транзакційні витрати, усуваючи опортунізм за допомогою криптографічних механізмів [32, с. 15]. З цієї точки зору блокчейн є засадничою технологією для нових форм управління. Іншими словами, блокчейн конкурує на ринках з організаціями як інституціональна альтернатива для координації економічних дій людей [32, с. 3]. У рамках реформ виникає питання, чи приносить блокчейн найбільшу користь, будучи реалізованим просто як технологічне рішення або прийнятим більш глибоко як окрема форма управління.

Концептуально існує мало меж для використання блокчейну, оскільки він може принести користь у будь-якій сфері, яка спирається на бухгалтерський облік або бази даних, які мають бути змінені або до яких мають доступ безліч учасників. Основна концепція блокчейну, можливо, проста, але особливості мережі блокчейн визначають її використання на ринках або в державному секторі. Дві основні характеристики технології блокчейн – це розподіл вузлів і незмінність блокчейну. Криптовалюта стала першим широко поширеним прикладом використання технології блокчейн, тому багато хто не розуміє, що у своїй основі блокчейн (і Bitcoin) – це децентралізація довіри. У традиційному суспільстві довіра централізована в уряді через закони і правоохоронні органи. Наявність централізованої організації означає, що дані, знання або ресурси належать одному підрозділу. Централізована система або організація створює ризик того, що якщо функціонування центрального органу не буде оптимальним, то це негативно позначиться на функціонуванні усєї системи – це також відомо як «єдина точка відмови» [16, с. 4]. Додатки на основі блокчейну вирішують цю проблему, розподіляючи те, що є «центральною».

Завдяки тому, що головний реєстр блокчейну розподілен між усіма учасниками мережі, змінити минулі блоки у блокчейні практично неможливо, і чим довше росте ланцюжок, тим більше ресурсоємним і менш реальним стає злом системи і зміна усіх минулих блоків – як тільки щось надруковане у блокчейні, воно залишається там назавжди. Кожен блок у блокчейні має хеш, який складається з вмісту блоку, і на цей хеш посилається наступний блок. Це забезпечує ще один рівень безпеки і прозорості, дозволяє учасникам мережі блокчейн перевірити та підтвердити транзакції. У разі публічних блокчейнів минулі транзакції можуть бути перевірені без проблем, оскільки кожна транзакція має хеш транзакції, який діє як ідентифікатор. Хоча деякі характеристики блокчейну (наприклад, публічний або приватний доступ) можуть розрізнятися, незмінність – це основний принцип, який робить блокчейн унікальним. Хоча блокчейн концептуально незмінний, основні протоколи консенсусу, такі як Proof-of-Work і Proof-of-Stake, мають теоретичний ризик до атаки 51% – 51% учасників мережі блокчейн об'єднуються проти інших 49%, обчислювальною потужністю або підрахунком голосів маючи можливість вибирати, які блоки дійсні, і таким чином генерувати нелегітимні транзакції. Проте за сучасними обчислювальними вимогами блокчейн забезпечує високу міру безпеки, якій погрожують тільки квантові комп'ютери.

Відмінність між публічною і приватною блокчейн-мережею має вирішальне значення для розуміння наслідків її використання в державному секторі. У дискусіях про блокчейн часто не робиться відмінностей між типами доступу, і хоча обидва типи все одно є блокчейном, тип доступу визначає варіант використання. Хоча обидва типи розділяють основні характеристики блокчейну, приватні блокчейни важливі в першу чергу через зниження транзакційних витрат, тоді як публічні блокчейни мають додатковий аспект децентралізованого управління. Приватні блокчейни більше схожі на розширені таблиці даних, тоді як публічні блокчейни дозволяють здійснювати децентралізоване управління.

Приватний блокчейн вимагає запрошення для участі в мережі блокчейн, і це запрошення має бути підтверджене адміністратором [63]. Існуючі користувачі приватних блокчейнів контролюють, хто може приєднатися до приватних, і, крім того, контролюють, хто бере участь у процесі консенсусу блокчейну. Приватний блокчейн в цьому сенсі є альтернативним методом управління базами даних, що має як сильні, так і слабкі сторони в порівнянні з централізованим управлінням базами даних [54]. Більше того, приватні блокчейни часто не мають токенів, на відміну від блокчейнів без дозволу. Публічні блокчейни знаходяться в центрі обговорення блокчейнів у ЗМІ. Публічний блокчейн – це блокчейн, де учасники можуть входити в блокчейн і брати участь у ньому без отримання дозволу від наявних користувачів. Будь-хто, хто має підключення до інтернету, може брати участь у блокчейні Bitcoin або Ethereum, здійснювати транзакції, а також брати участь у процесі консенсусу. Публічні блокчейни створюють проблему управління – як досягається консенсус в системі з сотень тисяч учасників. Хоча в приватних блокчейнах також виникає питання про те, як досягається консенсус, вони можуть покладатися на моделі довіри, засновані на авторитеті довірених партнерів [74, с. 6].

2.3. Впровадження blockchain технології до системи державного управління як фактор розвитку інформаційного суспільства в сучасній Україні

Впровадження інформаційно-комунікаційних технологій та Web 3.0 сприяє розвитку сектору електронного урядування, трансформуючи те, як державні адміністрації надають передові та інноваційні послуги для взаємодії з громадянами. Підривні технології блокчейну і штучного інтелекту змінюють те, як ми живемо, працюємо та взаємодіємо з державними секторами та галузями.

Розглянемо деякі приклади зарубіжного досвіду використання блокчейну в різних сферах державного управління.

Державні (комунальні) служби. З 1 грудня 2015 року в Естонії діє програма надання нотаріальних послуг онлайн-резидентам Естонії на блокчейн-платформі BitNation Public Notary. Проект здійснюється за підтримки державної програми «E-Residency». Вже в 2017 році керівництво програми E-Residency Естонії запропонувало провести перше в світі державне ICO, що дозволяє тим, хто має статус онлайн-резидента, інвестувати в Bitcoin [17].

Забезпечення виборчого процесу. У 2018 році в Західній Вірджинії, США, відбулися перші муніципальні вибори на основі блокчейну. Можна було проголосувати з будь-якого місця без бюлетенів і не потрібно було йти в посольство чи виборчу дільницю, щоб віддати свій голос за обраного кандидата [18].

Реєстрація права власності. Одним з найпоширеніших застосувань блокчейну є ведення земельних реєстрів. Наприклад, шведський уряд тестує систему реєстрації прав на землю на основі блокчейну з 2016 року. Шведський кадастровий орган об'єднався з блокчейн-стартапом ChromaWay, консалтинговою компанією Kairos Future і телекомунікаційною компанією Telia, щоб запустити блокчейн-платформу Chroma Way для оцифрування записів власності на нерухомість. Робота над впровадженням систем реєстрації прав власності на землю та майно на основі блокчейну ведеться в Японії, Руанді, Андхра-Прадеші в Індії, на Бермудських островах [104]. Державні органи впроваджують цю технологію для покращення процесів реєстрації прав власності, скорочення часу на укладення та реєстрації правочинів щодо права власності на земельні ділянки та неможливості вчинення шахрайських дій та помилок під час процедури реєстрації відповідних прав.

З 2017 року в ОАЕ працює блокчейн-система для реєстрації прав власності на нерухомість. Уряд ОАЕ оголосив, що країна має стати світовим лідером із впровадження блокчейну. Крім того, держава має намір фінансувати курси та семінари з впровадження блокчейну в органи державної влади [53].

Підсумовуючи міжнародний досвід, слід зазначити, що географія впровадження блокчейну дуже різна. Блокчейн використовують як

високорозвинені країни (США, Нідерланди, Швеція), що пов'язано з високим розвитком науково-технічного прогресу в цих країнах, так і країни з низьким рівнем розвитку. Тому можна констатувати той факт, що використання блокчейну – це популярне і нове явище, інновація нового покоління.

Можливість використання технології блокчейн в державному управлінні в Україні вперше обговорювалася у вересні 2015 року. Bitcoin Foundation Ukraine та керівництво програми електронного урядування підписали меморандум 29 вересня 2015 року в Києві. Інші країни також виявляють інтерес до використання розподілених реєстрів у державному секторі. У 2017 році Державне агентство з питань електронного урядування України та BitFury підписали меморандум про співпрацю у сфері технології блокчейн. Цей проект передбачав впровадження державних даних, що зберігаються в електронному вигляді на платформі блокчейн. Завдяки цій програмі планується запровадити державні реєстри операцій з державними активами, особливо в процесі приватизації майна. У 2017 році в Одеській області були організовані електронні аукціони з оренди та продажу державного майна за технологією блокчейн.

Основна мета системи – забезпечення прозорості та рівних можливостей для учасників ринку з оренди та продажу державного майна, усунення корупційної складової у процесі розпорядження державними активами. Також система використовуватиме технологію смарт-контрактів. Розроблена система являє собою приватний блокчейн з комплексним алгоритмом аутентифікації учасників. Основне завдання розробників на даний момент – максимально ускладнити або взагалі зробити неможливим доступ фіктивних або недобросовісних учасників.

Оскільки інтерес державних установ до використання блокчейнів зростає, зростає інтерес до використання приватних блокчейнів. Розглянемо вісім проектів за цією технологією, які були запущені та працюють в Україні (див. табл. 2.2).

Таблиця 2.2

8 проектів з використанням технологій блокчейн для комерційних цілей в Україні запущених більше 4 років назад

№ з/п	Проект	Дата випуску	Сфера діяльності
1	Rentberry	2015	Прозора платформа для оренди житла. Власники будинків можуть знайти орендарів
2	D-Market	2017	Глобальна платформа, що дозволяє продавати ігровий контент
3	Remme	2017	Служба безпеки, що використовується для криптопростору
4	Hacken	2017	Служба безпеки, яка захищає розробників веб-сайтів від атак
5	Karbo	2016	Електронна валюта України
6	Земельний кадастр	2018	Проект електронної торгівлі землею
7	Ambisafe	2015	Компанія надає допомогу у створенні власної криптовалюти
8	Distributed Lab	2014	Сервіс обміну валют, в тому числі криптовалют

Як видно з таблиці 2.2, Державний земельний кадастр є пілотним проектом використання захисту даних блокчейн в державному управлінні в Україні. Технологія блокчейн також використовується для державного реєстру прав на нерухоме майно, системи електронної торгівлі арештованим майном СЕТАМ. 27 травня 2017 року Кабінет Міністрів України схвалив пропозицію Міністерства юстиції та Державного агентства з питань електронного урядування щодо впровадження заходів, спрямованих на впровадження системи зберігання даних блокчейн у Державному реєстрі речових прав на нерухоме майно та СЕТАМ. У цьому ж році було підписано меморандум про співпрацю між Міністерством юстиції України, Міністерством аграрної політики та продовольства України, Державним агентством з питань електронного урядування, Transparency International Україна та Bitfury Holding щодо створення та обслуговування земельного кадастру і інших державних

реєстрів на основі блокчейна. Оновлений Державний земельний кадастр містить інформацію про кожну операцію, яка відбулася в кадастрі. Ця інформація надходить у ланцюжок блоків за заданим алгоритмом. Це означає, що кожен документ, що засвідчує право власності на землю, супроводжується QR-кодом, тому всі дані про місце розташування, розміри ділянки та її власника зашифровані. За допомогою QR можна визначити справжність документа або просто перевірити інформацію в реєстрі. Вносити зміни до кадастру можуть лише уповноважені спеціалісти. Для ідентифікації осіб, які можуть змінити інформацію про ділянку, необхідно використовувати електронний підпис або банківський ідентифікатор.

Вивчаючи досвід створення Державного земельного кадастру в частині блокчейн-технологій в державному управлінні, ми стикаємося з однією важливою проблемою, яку наразі неможливо вирішити технологічно. Справа в тому, що на початковому етапі використання технології у сфері реєстрації земельних договорів виникли певні проблеми з первинною ідентифікацією власників землі, оскільки дані, які вносяться в реєстр блокчейн, можуть бути неточними. У свою чергу, блокчейн гарантував незмінність даних, але не їх достовірність. Ця система може використовувати власні ресурси для перевірки даних або отримання витягів, але не для перевірки точності даних. Тому дуже важливо розробити законний та контрольований порядок передачі паперових даних до державних реєстрів із гарантією чесності та прозорості. Ефективне функціонування блокчейн-технологій в Україні залежить від точності заповнення реєстрів громадян, нерухомості, компаній тощо. Ні збереження цілісності даних у разі випадкових збоїв, ні запобігання маніпуляції з уже введеними даними не є серйозними проблемами для державного управління. Справжньою небезпекою є практика внесення в реєстри явно неточних даних, і в цьому випадку технологія блокчейн безсила.

Таким чином, головна мета впровадження блокчейн-технологій в державне управління – створення такої інфраструктури, яка допоможе запобігти корупції та бюрократії в системі блокчейн. Але для цього потрібно

розробити закони про статус блокчейну, досягти прозорості даних і вихідних кодів, запровадити автономну виконавчу адміністрацію, сформувати систему управління на основі прямої демократії та створити розподілений державний реєстр [81].

Загалом, вся справа в наявності відповідної державної політики [84] і, звісно, політичної волі впроваджувати таку політику та будувати стосунки з іншими зацікавленими сторонами на основі принципово іншої інформаційної культури. Тому, моделюючи майбутні системи державного управління з точки зору впровадження технології блокчейн, необхідно в першу чергу звернути увагу на зміну інформаційної культури в цій системі.

У загальному значенні інформаційна культура – це сукупність принципів і механізмів освоєння, зберігання, передачі та використання інформації, встановлених у конкретній соціальній спільноті. Для системи державного управління в цьому контексті найбільш принциповими є питання володіння інформацією, використання інформації для забезпечення процесу управління та захисту інформації. Блокчейн формує відповідні технології для управління діяльністю суб'єктів, які його використовують, таким чином змінюючи традиційні уявлення про владу та управління. Нова технологія дозволяє людям безпрецедентно взаємодіяти, однак обмежуючи їхню взаємодію в конкретних рамках, дозволених технологією. Це означає, що його можна вважати примусовою силою, яка обмежує людську діяльність. У зв'язку з цим може виникнути нове алгоритмічне суспільство, тобто суспільство, в якому примусова сила алгоритмів буде узагальнена в суспільстві в цілому. Програмне забезпечення, що реалізує алгоритм, можна розглядати як набір особливих умов, що обмежують поведінку та взаємодію індивідів у межах цих технологій.

Отже, ідея розподіленого реєстру втілена в цілій низці програмних платформ відкритого, закритого та комбінованого типу, більшість з яких задумані як універсальні, але деякі мають свою спеціалізацію. Платформи дозволяють розробляти прикладні програми для багатьох сфер ділових відносин. Найбільшу вигоду впровадження додатків на основі платформ

розподіленого реєстру приносить у тих областях, де бізнес-процеси включають значну кількість фізичних і юридичних осіб, розділених державними та відомчими бар'єрами.

Блокчейн в контексті державного управління є частиною електронного уряду, який є інструментом для сучасних рамок державного управління. Можна стверджувати, що системи управління мають певну форму передбачуваності залежно від того, в якому контексті вони використовуються. Таку ж логіку можна застосувати до наслідків блокчейну у рамках системи управління, оскільки результати можуть бути отримані для конкретного випадку. Електронне управління визначає, як блокчейн може використовуватися в контексті державного управління (голосування, відкриті дані, уряд, співпраця), а рамки реформ додають контекст того, чому блокчейн використовується або може бути використаний (підвищення ефективності державного сектора або підвищення легітимності).

Впровадження блокчейн-систем органами державної влади неможливе без реінжинірингу процесу прийняття управлінських рішень, активного розвитку цифровізації як державного управління, так і суспільства в цілому. Подальші наукові дослідження мають бути спрямовані на вивчення механізмів впровадження блокчейну в державне управління та місцеве самоврядування для прискорення переходу на новий еволюційний рівень соціально-владних відносин – широке використання цифрового управління.

Використання блокчейну дозволить перетворити систему державних послуг на нову, якісну систему, яка допоможе надавати послуги набагато швидше та якісніше. Це значно знизить експлуатаційні витрати, а головне – забезпечить прозорість усіх операцій.

Нині державне управління в Україні стикається з численними проблемами розвитку інформаційного середовища. Основна проблема полягає в тому, що більшість операцій, пов'язаних з документообігом, не завжди здійснюються в електронному вигляді. Навіть якщо реалізовані системи адміністрування цифрових документів і баз даних, вони часто забезпечують

обмежені функції. Це створює проблеми на шляху доступу та обміну інформацією на всіх рівнях державного управління. У свою чергу, недосконале інформаційне середовище впливає на суспільство, яке стикається з бюрократією і, як наслідок, корупцією.

В Україні доцільно розвивати спільну інформаційну підтримку в усіх сферах державного управління. Наразі лише в документації у сфері земельних відносин спостерігаються спроби використання технології блокчейн для побудови інформаційної системи. Можна зробити висновок, що ця система далека від досконалості. Зокрема, він не використовує всі переваги блокчейну, дозволяючи виконувати тільки завдання архівації. Необхідно розвивати цю систему і поширювати її на всі інші сфери управління. Головне завдання розробників на даний момент – зробити доступ до інформації якомога ускладненим або взагалі неможливим. Нечесні учасники, які можуть ввести неправдиві дані в процесі оцифрування документів, не повинні мати навіть найменшого шансу змінити дані в системі. Крім того, необхідно вирішити певні нормативні питання щодо створення та функціонування таких інформаційних платформ, а також створити наглядові ради для нагляду за процесом цифровізації даних.

РОЗДІЛ 3

ПРАКТИЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ BLOCKCHAIN ТЕХНОЛОГІЇ ДО СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ

3.1. Управлінські рішення для систем на основі blockchain в державному секторі

Проаналізуємо управлінські рішення, необхідні для використання технології блокчейн у державному секторі. Аналіз літератури з управління блокчейном, зроблений у підрозділі 1.3 показує, що рішення щодоуправління блокчейном в державному секторі можна аналізувати на мікро-, мезо- та макрорівнях. Управлінські рішення на одному рівні не є самостійними, а є взаємопов'язаними рівнями управління блокчейном. Стратегії управління на мікро-, мезо- та макрорівнях тісно пов'язані в державномууправлінні, і неможливо вивчати один рівень управління без усвідомлення інших рівнів.

Управління на мікрорівні пов'язане з вибором розробників систем щодо інфраструктури системи на основі блокчейну. Під цю категорію підпадають рішення щодо інфраструктурної архітектури блокчейну, модульних додатків смарт-контрактів і децентралізованих додатків, а також взаємодії системи на основі блокчейну з існуючою ІТ-інфраструктурою.

Управління на мезорівні стосується взаємодії між мережевою спільнотою, на якій базується система на основі блокчейну. Система на основі блокчейну покладається на взаємодію між різними типами користувачів, такими як майнери, верифікатори (або оператори вузлів), основні розробники, власники маркерів, виробники контенту та користувачі мережі. Управлінські рішення на мезорівні встановлюють, як керується прийняття рішень між цими користувачами, який тип механізмів стимулювання підтримує систему та як механізми консенсусу впливають на роль користувачів в управлінні блокчейном.

Управління на макрорівні зосереджується на тому, як правила та норми, що впливають із конституційних, культурних, історичних та правових основ цієї установи, впливають на організацію, підзвітність та контроль системи на основі блокчейну під час реалізації цілей та функцій політики. Управління на макрорівні слугує «вбудованим рисам», які діють як параметри прийняття як індивідуальних, так і організаційних рішень [112]. Точніше, те, як права на прийняття рішень розподіляються між суб'єктами мережі, які механізми підзвітності діють, а також хто контролює та наглядає за процесами впровадження, що підпадають під сферу рішень управління на макрорівні.

В таблиці 3.1 наведено три рівні управління та дев'ять типів управлінських рішень, необхідних для використання систем на основі блокчейну в державному секторі.

Таблиця 3.1

Трирівневий аналіз для управління блокчейном

Рівень управління	Види рішень	Проблеми
Мікрорівень	Архітектура інфраструктури	З/без дозволу, публічні/приватні блокчейни
	Архітектура програми	Смарт-контракти та DApps
	Інтероперабельність	Сумісність з існуючою системною інфраструктурою
Мезорівень	Механізм прийняття рішень	Рішення на ланцюжку або поза ланцюжком
	Механізм стимулювання	Види (де)стимулювання
	Механізм консенсусу	PoW, PoS, DPoS, PoA тощо
Макрорівень	Організація управління	Розподіл ролей в управлінні
	Підзвітність управління	Регулювання та виконання правил
	Контроль управління	Керовані людиною чи автоматизовані агенти

На додаток до цих управлінських рішень, деякі дослідження зосереджуються на цілях політики в управлінні блокчейном (наприклад, суспільні інтереси, висвітлення в ЗМІ), а також на обмінах на макрорівні між політичними, соціально-культурними, законодавчими та ринковими установами в управлінні систем на основі блокчейну [60; 77; 89]. У нашій структурі ми не включаємо ці елементи як окрему категорію, але припускаємо їх повсюдний вплив як контекстуальні фактори на кожному рівні управління. Наприклад, у державному секторі кожне рішення щодо управління блокчейном має бути узгоджено з цілями політики, суспільними цінностями, інституційною структурою та суспільними очікуваннями.

Архітектура інфраструктури. Блокчейни можуть бути публічні і приватні, з дозволом і без. Різниця між публічними та приватними блокчейнами полягає в тому, кому належить інфраструктура даних. Різниця між системами без дозволу і з дозволами полягає в обмеженнях, накладених на учасників мережі щодо функцій читання, запису та аудиту/фіксації. У першому випадку будь-хто може брати участь у мережі та підтверджувати транзакції, що відбуваються на платформі, а в другому – лише вибрані особи уповноважені перевіряти транзакції. Ці класифікації не є винятковими один для одного, і можна мати публічний і приватний блокчейн з різними ступенями моделей дозволів. Наприклад, дві найбільш відомі блокчейн-платформи, Bitcoin і Ethereum, є загальнодоступними блокчейнами без дозволів. Hyperledger Fabric, R3Corda і Quorum є деякими прикладами розробників технологій, які надають вбудовані інструменти для систем із дозволом, застосованих до публічних і приватних блокчейнів. Переваги різних типів блокчейнів відрізняються технічно щодо децентралізації, безпеки, масштабованості, швидкості, пропускну здатності, конфіденційності, довіри та вимірів остаточності. З одного боку, загальнодоступні блокчейни без дозволів сприяють підвищенню довіри та безпеки для інфраструктури даних, але відчувають недостатню масштабованість та проблеми з продуктивністю. З іншого боку, приватні блокчейни з дозволом значною мірою розробляються і воліють приватними

підприємствами (наприклад, IBM, Microsoft), оскільки вони дозволяють певною мірою контролювати конфіденційність даних і управління системою.

У державному секторі вибір блокчейну вимагає розгляду кількох компромісних умов щодо пріоритетів політики (наприклад, конфіденційність, пропускна здатність, безпека тощо) та впливу на інші рівні управління (наприклад, прийняття рішень між суб'єктами мережі, організацією управління). Ці умови компромісу залежать від контексту і не обов'язково мають однакове значення для всіх типів організацій державного сектору. Наприклад, конфіденційність транзакцій і безпека інфраструктури даних можуть бути найважливішими факторами для деяких організацій державного сектору (наприклад, служби безпеки та розвідки), тоді як для інших прозорість і незмінність публічних блокчейнів можуть бути основною мотивацією. Аналогічно, вища пропускна здатність і масштабованість є життєво важливими для підприємств, але в державному секторі часто обсяг транзакцій і кількість користувачів прив'язані до юрисдикції та адміністративної сфери послуг. Ця передбачуваність мережі може дозволити заздалегідь визначити потреби в масштабованості та пропускній здатності.

Крім того, дослідники [68] визначають 23 ендогенні умови компромісу серед 7 властивостей DLT (придатність до використання, продуктивність, гнучкість, безпека, прозорість, закони і регулювання та спільнота), які змінюються залежно від вибору дизайну архітектури інфраструктури. Наприклад, якщо метою системи на основі блокчейну є підвищення довіри серед користувачів, архітектура системи має надавати пріоритет прозорості, яка може зашкодити іншим властивостям (наприклад, зручність використання, продуктивність, гнучкість). Хоча останні визначають управління як підфункцію закону та функції регулювання та зосереджуються лише на компромісах між управлінськими рішеннями та безпекою системи, важко відокремити інші умови компромісу від управлінських рішень. Таким чином, будь-який вибір архітектури інфраструктури за своєю суттю є політичним актом і передбачає

оптимізацію умов компромісу між різними властивостями DLT та системами з дозволом і без дозволів.

Архітектура програми. Як було сказано раніше, блокчейн-інфраструктури схильні до певних функцій в управлінні блокчейном. Однак ці функції можна змінити за допомогою децентралізованих додатків (DApps) і смарт-контрактів.

Кожен DApp має певні переваги та недоліки (наприклад, кінцевість, швидкість, масштабованість, енергоспоживання тощо) на основі їх консенсусу та механізмів стимулювання, що робить вибір DApp за своєю суттю управлінським рішенням. За допомогою модульних DApps також можна прив'язувати значення в системі без блокчейну або приватному блокчейні до загальнодоступного блокчейну. Наприклад, у випадку використання земельного кадастру можливо використовувати двошаровий підхід блокчейну, коли підсумок хешів із приватного блокчейну зберігається в блокчейні Bitcoin чи іншому. Таким чином, можна обійти певні компроміси між властивостями DLT (наприклад, продуктивність та безпека) за допомогою DApps.

Смарт-контракти – це механізми, які містять цифрові активи двох або більше залучених сторін, де активи розподіляються автоматично відповідно до попередньо визначених дій, коли виконуються умови активації. DApps отримує доступ до мережі блокчейн за допомогою смарт-контрактів, які забезпечують виконання умов угоди між двома сторонами. Завдяки комбінації смарт-контрактів і DApps можна створити DAO, де правила роботи закодовані в блокчейні у вигляді смарт-контрактів, а DAO можуть працювати автономно або напівавтономно без централізованого контролю або втручання третіх осіб. Ці нові форми організацій можуть перевизначити механізми контролю та координації в державному управлінні. Наприклад, підрозділи, що спеціалізуються на оптимізації, регулюванні та управлінні мережею, можуть бути замінені DAO. Крім того, нові форми управлінських домовленостей з неурядовими організаціями можуть бути створені як DAO, щоб замінити традиційні форми державно-приватного партнерства та механізми спільного управління.

Інтероперабельність. Європейська структура взаємодії (EIF) стверджує, що управління інтероперабельністю в державному секторі вимагає інтегрованого підходу до управління в рамках правової, технічної та семантичної інтероперабельності. Під функціональною сумісністю блокчейнів мається на увазі здатність останніх обмінюватися, переглядати та отримувати доступ до інформації через існуючі системи управління даними у публічному та приватному домені без необхідності посередника для обміну. У цьому сенсі важливим рішенням щодо інтероперабельності є оцінка того, наскільки управління блокчейном відповідає існуючим механізмам, технологіям, правилам і стандартам у сфері цифрового управління. Існує три типи проблем, які можна визначити щодо взаємодії блокчейну. По-перше, відсутність стандартизації від технічних протоколів до смарт-контрактів, які з'єднують допоміжні технології, такі як штучний інтелект, і автоматизовані агенти на блокчейн-платформах. Більше того, на даний момент інформація, що зберігається на блокчейнах, не обов'язково відповідає ринковим стандартам і практикам, таким як ISDA (Міжнародна асоціація свопів і деривативів), FPL (протокол обміну фінансовою інформацією) або ISO (Міжнародна організація зі стандартизації). По-друге, блокчейни за своєю конструкцією не взаємодіють один з одним. Можна запропонувати кілька рішень для полегшення міжланцюгових транзакцій, таких як полегшення обміну повідомленнями через ланцюжок управління, використання крос-ланцюгової криптовалюти для передачі атомних активів або прямий зв'язок через апаратні з'єднання за допомогою TLS або смарт-контрактів, кожне зі своїм унікальним набором проблем для вирішення. По-третє, проблеми інтероперабельності можуть виникати через специфічні потреби у сфері державних послуг. Наприклад, проблеми сумісності в секторах, які стосуються можливості розвитку, гнучкості, обсягу та безперервності обміну даними між різними постачальниками даних.

Проблеми інтероперабельності можуть вплинути на вибір управління блокчейном двома можливими способами. По-перше, вони можуть

перешкоджати масштабованості рішень на основі блокчейну і таким чином обмежити використання блокчейну лише певними функціями (наприклад, перевірка даних за допомогою перевірених облікових даних). Відсутність масштабованості може ще більше підірвати застосовність децентралізованих систем без дозволів. По-друге, технологічний вибір зацікавлених організацій в екосистемі блокчейну може підняти одну інфраструктуру блокчейну та пов'язані з нею варіанти управління над іншими і встановити її де-факто як вибір архітектури системи в державному секторі. Зокрема, національні та міжнародні політичні ініціативи можуть бути законодавцем мод у цьому відношенні. Наприклад, Естонія прагне вирішити проблеми сумісності шляхом створення однієї стандартизованої системи державних послуг на основі інфраструктури підпису без ключа (KSI). KSI не покладається на спільні дії користувачів для перевірки даних і, на відміну від механізмів консенсусу підтвердження роботи (PoW) або підтвердження участі (PoS), використовує мітки часу для перевірки цілісності даних [72]. Іншим прикладом є Європейська Інфраструктура послуг блокчейн (EBSI) [24], яка має на меті надавати транскордонні державні послуги в ЄС за допомогою використання блокчейн. Очікується, що в рамках EBSI країни-члени створять необхідну інфраструктуру для переходу та призначать вузли (тобто довірені та дієздатні організації в кожній державі-члені) для підтримки механізму консенсусу підтвердження повноважень (PoA). У випадку, якщо існує загальнонаціональна платформа для обміну даними (наприклад, цифрові рішення в уряді Естонії) або якщо буде прийнято блокчейн-платформу європейського або глобального рівня (наприклад, EBSI), вимоги до сумісності можуть обмежувати доступні варіанти управління на мікрорівні. Іншим аспектом взаємодії є те, наскільки блокчейн може включати в себе великі дані та рішення інтернету речей. Цифрова трансформація в державному секторі запровадила кілька технологій, і блокчейн як технологія загального призначення має вищі шанси на успіх, якщо він доповнює існуючі технології, а не замінює їх.

Механізм прийняття рішень. Механізм прийняття рішень різниться між процесами управління в ланцюжку та поза ланцюжком. У ланцюжковому управлінні зацікавлені сторони беруть участь в обговореннях і прийнятті рішень за допомогою самого протоколу, і коли рішення приймається за допомогою процедури голосування або перевищує порогове число користувачів, протокол автоматично адаптує рішення. У ланцюжковому управлінні спосіб взаємодії та прийняття рішень закодований безпосередньо в базовій інфраструктурі. Наприклад, під час впровадження протоколів активації софт-форк для Bitcoin (тобто BIP 8 або BIP 9), майнери використовували засоби в мережі, щоб повідомити про свою підтримку запропонованого оновлення. Коли 95% блоків сигналізують про підтримку оновлення, зміни застосовуються автоматично через короткий проміжок часу. Сильна сторона ланцюжкового управління полягає в його механізмі виконання, коли рішення узгоджується, воно реалізується відповідно до правил, закладених у кодекс. Однак недоліком цього механізму є те, що він автоматизує правило «переможець отримує все». Переможна більшість визначає функціонування всієї системи, і, таким чином, вона ризикує відштовхнути політичних дисидентів від процесу. У політичних науках це називається мажоритарною демократією, яку часто критикують як недемократичну або як меншу форму демократії.

Керування поза ланцюжком – це ендогенні та екзогенні правила та процеси обговорення протоколу, які сприяють роботі та розвитку систем на основі блокчейну. Наприклад, розробники Bitcoin діляться своїми пропозиціями щодо покращення через список розсилки, а Ethereum збирає пропозиції щодо покращення на Github. Майнери можуть вирішити, чи застосовувати пропозиції щодо покращення на практиці. Хоча управління поза ланцюжком представляє більш демократичну альтернативу і дозволяє поступово адаптуватися, воно зберігає невід’ємний ризик безпеки в системах без дозволу. Майнери системи – це шукачі ренти, і вони не обов’язково мають технічні знання для оцінки пропозиції. Таким чином, безпечна, на перший

погляд, модифікація програмного забезпечення, ініційована зловмисником, може створити ризики безпеки в майбутньому.

Обидва процеси управління виводять на компроміс розробників систем і політиків. Управління в ланцюжку забезпечує компроміс між ефективним ухваленням рішень і перехідними процесами та ризиком дестабілізації через політичний дисонанс. Управління поза ланцюжком забезпечує компроміс між посиленням політичного консенсусу в процесі прийняття рішень і процесів переходу, але при цьому безпека системи стає уразливою для майнерів, що прагнуть рентної плати. Також можна розробити гібридні системи, де одні рішення можуть прийматися за допомогою внутрішньоланцюжкових процесів, тоді як інші можуть прийматися за допомогою позаланцюжкових процесів.

Крім того, залежно від протоколу блокчейну, деякі учасники можуть мати право вето на певні рішення, або деякі рішення можуть бути відкритими лише для певних учасників для голосування. Тут інституційна структура, сфера застосування та конкретні умови країни можуть диктувати різним учасникам більш помітну роль у процесах внутрішнього та позаланцюжкового управління. Оскільки основна додаткова цінність блокчейну полягає в тому, щоб створити впевненість у процесах, де її бракує, механізм прийняття рішень може знадобитися надавати пріоритет залученню відповідних суб'єктів та підвищити рівень прозорості в розробці та роботі додатків блокчейну. Для цього в управлінні блокчейном можна ввести соціальний рівень, де основні розробники, зацікавлені сторони та громадські учасники обговорюють політичні та функціональні наслідки вибору дизайну системи. Обговорення, які відбуваються на соціальному рівні, можуть сприяти процесам у мережі для створення політично легітимного процесу і можуть служити динамічною конституцією системи на основі блокчейну. Проблема полягає у створенні інклюзивного механізму прийняття рішень, який створює легітимність в управлінні блокчейном не заводячи систему у безвихідне положення (наприклад, дебати щодо розміру блоку Bitcoin). Для встановлення правил і

ролей перевіряючих, розробників і користувачів системи може знадобитися демократична конституція управління блокчейном.

Механізм стимулювання. У офіційній документації про Bitcoin Накамото ввів механізм стимулювання для забезпечення постійного залучення користувачів Bitcoin до обслуговування мережі. Як у блокчейнах Bitcoin, так і у Ethereum цей механізм покладається на грошову винагороду у вигляді криптовалюти блокчейну, яка узгоджує індивідуальне прагнення до отримання ренти, із загальною вигодою платформи. Для організацій державного сектору використання грошових стимулів для залучення користувачів може створити етичні та політичні проблеми, однак не всі механізми стимулювання мають використовувати грошову вартість криптовалют. Наприклад, розподіл токенів і оцінок репутації, які надають користувачам розширений доступ до функцій платформи та зважені права голосу в процесах прийняття рішень, можуть бути деякими немонетизованими винагородами.

Не тільки методи стимулювання, але й спосіб, яким протоколи консенсусу стимулюють майнерів і верифікаторів, можуть мати вирішальні наслідки для загального управління блокчейном. Наприклад, механізм PoW Bitcoin разом із механізмом грошового стимулювання проклав шлях до консолідації майнінгу. Внаслідок цього по всьому світу з'явилися великі пули для майнінгу, а спеціалізоване обладнання серед майнерів набуло широкого поширення. Наразі, за оцінками, чотири великі пули майнінгу в мережі Bitcoin і два пули майнінгу в мережі Ethereum контролюють понад 50% транзакцій. Така консолідація влади підриває розподілені та децентралізовані функції блокчейн-мереж – навіть для таких великих, як Bitcoin та Ethereum, і ставить під загрозу легітимністю і довірою, вкладені в механізми управління блокчейном.

Інше відповідне управлінське рішення стосується дестимулюючої дії комісій за транзакції. Комісія за транзакції – це вартість дій у певному блокчейні, таких як транзакції або виконання смарт-контрактів (наприклад, «газ» в Ethereum). Дестимулюючий ефект комісій за транзакції та стимулюючий ефект винагород для майнерів створюють умови компромісів і

розрахунків раціонального вибору для користувачів і майнерів для взаємодії з блокчейном. У випадку, якщо вартість переважає очікувані вигоди від взаємодії, деякі блокчейн-додатки можуть втратити свою привабливість або майнери можуть знайти меншу цінність для підтримки блокчейну взагалі, що негативно вплине на безпеку блокчейну.

Механізм консенсусу. Механізм консенсусу лежить в основі систем на основі блокчейну для координації децентралізованих дій користувачів при вирішенні, яку інформацію можна додати до блокчейну. Існують різні механізми консенсусу, але більшість блокчейнів або покладаються на консенсус Накамото (PoW), який пов'язує можливості майнінгу з обчислювальною потужністю, або візантійський консенсус, який використовує стейкінг для призначення майнерів (PoS, DPoS). Існують також системи підтвердження повноважень (PoA), де менша кількість вузлів або головних вузлів виконує роль валідаторів транзакцій. Кожен із цих механізмів консенсусу має свої переваги та недоліки порівняно з іншими, і вони по-різному відносяться до децентралізованих та централізованих структур управління.

PoW здебільшого використовується в публічних блокчейнах без дозволу, таких як Bitcoin та Ethereum, де користувачі перевіряють транзакції, розв'язуючи складні математичні головоломки за допомогою обчислювальної потужності обладнання. Перевагою системи PoW є її стабільність для стримування кібератак (наприклад, атак відмови в обслуговуванні), зберігаючи при цьому розподілене управління системою. Однак його вразливість до атаки 51%, висока вартість енергії, посилення централізації майнінгових операцій і низька пропускна здатність транзакцій є одними з значних проблем для систем на основі PoW. Зокрема, підвищене навантаження на навколишнє середовище, викликане високим попитом на енергію систем на основі PoW, зменшує ймовірність того, що їм буде віддана перевага в проектах державного сектору.

У PoS потужність майнінгу приписується вузлам у пропорції токенів (або монет), які утримуються вузлами, а не їх обчислювальної потужності. Оператори вузлів блокують ставку для права брати участь у створенні блоку, а вузли з більшими ставками мають більші шанси бути обраними для перевірки транзакцій. Комісія за транзакцію сплачується оператору вузла в обмін на перевірку транзакції. У разі шахрайських транзакцій або будь-якої неправильної поведінки вузол втрачає право брати участь у стейкінгу. Відмінність DPoS полягає в тому, що власники маркерів вибирають невелику кількість вузлів як делегатів, розставляючи токени з різними кандидатами. Якщо делегат обирається для створення блоку, частина винагороди розподіляється тим, хто проголосував за делегата. У деяких системах повноваження щодо прийняття рішень пов'язані з делегуванням токенів, де делегати можуть мати можливість контролювати та змінювати параметри мережі, такі як комісія, розмір блоку, винагорода за блок та тривалість циклу транзакції. Перевага PoS полягає в тому, що він менш сприйнятливий до атаки 51% і більш масштабований з більшою пропускнуою здатністю транзакцій, але вважається менш безпечним, ніж повністю децентралізовані системи PoW.

У системах PoA, на відміну від систем PoS і PoW, особа валідатора відома, і передбачається, що репутація валідатора відіграє роль ставки. Перевага систем PoA полягає в тому, що вони можуть досягти значно більшої пропускнуої здатності в результаті меншої кількості валідаторів, і вони підходять як для приватних мереж, так і для загальнодоступних мереж. Однак недоліком є те, що PoA не наповнений відчуттям безпеки, що впливає з децентралізованих механізмів консенсусу, і, отже, вузли повинні залишатися безкомпромісними. Отже, алгоритмічна довіра, типова для Bitcoin або Ethereum, не присутня в блокчейні на основі PoA, а для вибору вузлів потрібна попередня довіра. Для блокчейну на основі PoA, вузли потрібно вибирати з ключових державних або приватних установ.

Відмінності між механізмами консенсусу також впливають на роль користувачів в управлінні блокчейном і загальному державному управлінні. Наприклад, PoW або PoS як механізм розширює роль користувачів і майнерів як демонстраторів і робить їх незамінними для безперервності, безпеки та актуальності системи. В обох цих механізмах користувачі є співвиробниками управління блокчейном. У PoA користувачі є бенефіціарами системи, тоді як деякі організації виконують роль державного агентства з виробництва державних послуг. У літературі про державне управління це розрізнення пов'язано з роллю громадян-бенефіціарів або клієнтів у традиційному державному управлінні та нових режимах державного управління, а також роллю громадян-співвиробників у нових системах державного управління.

Організація управління. Вибір організації стосується розподілу ролей у прийнятті управлінських рішень у мережі блокчейн. Можливо виділити чотири різні підходи, а саме централізовану, напівцентралізовану (або гібридну), поліцентричну та децентралізовану форми управління. Централізоване управління відноситься до тих, де конкретна група людей або організацій приймає управлінські рішення, а процеси прийняття рішень можуть бути організовані за допомогою ланцюжкових або позаланцюжкових процесів. Напівцентралізоване або гібридне управління – це коли деякі управлінські рішення (наприклад, вирішення конфліктів) приймаються лише централізованою радою директорів, а деякі інші управлінські рішення (наприклад, стосовно мережі користувачів або функцій платформи) можуть прийматися з додатковою процедурою голосування користувачів платформи в ланцюжку. Тут вплив голосів користувачів може відрізнятися на реальне виконання рішень. Наприклад, може знадобитися абсолютна або кваліфікована більшість у групі користувачів, або можуть бути використані різні параметри зважування для результатів процесів голосування, щоб доповнити рішення, прийняті радою директорів.

У поліцентричному управлінні різні кластери учасників (наприклад, майнери, розробники, вузли) виконують різні ролі та обов'язки в управлінні блокчейном, і управління вимагає обліку того, що роблять інші. У децентралізованій структурі в процесах управління не домінує один суб'єкт або група суб'єктів, швидше рішення приймаються більшістю користувачів, працюючих в мережі блокчейн, або через процеси голосування на ланцюжку, або через скоординовані дії майнерів. Тут архітектура вибору процесів голосування та відкритість пропозицій для громадськості можуть вплинути на децентралізований характер структури управління. Крім того, у децентралізованих системах з відкритим кодом пропозиції щодо вдосконалення та DApps можуть бути внесені безпосередньо користувачами мережі без втручання посередника (наприклад, розробників).

Важливо підкреслити, що певні організаційні структури можуть мати різну спорідненість з конкретними виборами управління на мікро- або мезорівнях. Наприклад, в той час як централізоване управління може бути більш придатним для систем на основі блокчейну з дозволом, поліцентричне або децентралізоване управління може бути більш придатним для систем без дозволу. Або, якщо PoA може бути більш придатним для напівцентралізованих систем, PoS і PoW можуть бути більше підходити для поліцентричних або децентралізованих систем. Також можливо, що владні відносини учасників можуть змінити структуру управління, що спочатку виглядала інакше, на іншу. Наприклад, якщо в ланцюжкових процесах управління в системах на основі PoW або PoS домінують кілька великих операторів, які контролюють більшість ресурсів майнінгу та/або токенів, початкова децентралізована структура управління може діяти як напівцентралізована або поліцентрична структура управління. Або, якщо в позаланцюжкових процесах управління домінують кілька спеціалізованих впливових гравців, централізована структура управління може діяти як напівцентралізована або поліцентрична структура.

Підзвітність управління. Підзвітність – це те, як правила управління (наприклад, вирішення спорів, управління змінами) регулюються та

дотримуються. Виділимо чотири форми механізмів підзвітності в управлінні блокчейном: примус, добровільність, адресність та рамкове регулювання. Ці чотири типи розрізняються за двома вимірами: типом застосовуваних інструментів (юридично обов'язкове законодавство або м'яке право) та підходом до виконання (гнучким чи жорстким).

Примус характеризується обов'язковими нормативними актами, які передбачають детальні і фіксовані стандарти в реалізації. У контексті блокчейну примус можна охопити концепцією «*lex cryptographica*» (ідея, що найкращим регулятором у технологічній інфраструктурі є код самої інфраструктури; використання технології може бути сформовано таким чином, щоб заборонити технічно небажане використання технології, таким чином зменшуючи потребу людського регулювання [45], це означає, що правила обміну є вбудованими кодами, і як такий код стає законом в управлінні блокчейном. Завдяки використанню смарт-контрактів винагороди та санкції виконуються автоматично, створюючи детерміновану систему управління. Проблема транспонування закону в код полягає в тому, що коди написані суворою і формалізованою мовою, і, отже, правила, засновані на коді, повинні бути передбачуваними і не залишати місця для інтерпретації. Це за своєю суттю обмежує застосовність правил, заснованих на коді, у сферах, де непередбачувані обставини та умови не можуть бути визначені априорі.

Добровільність ґрунтується на юридично необов'язкових інструментах і визначає широкі цілі реалізації. У контексті блокчейну цей режим управління відбитий у софт-форках. Софт-форк не змінює структуру блокчейну, але змінює функції блокчейну. Реалізація софт-форку покладається на координаційні дії більшості користувачів для впровадження запропонованих змін. Зміни набувають чинності лише в тому випадку, якщо більшість майнінгових потужностей мережі їх прийме. В іншому випадку софт-форк не активується, і старий блокчейн залишається незмінним. У разі політичного дисонансу між різними групами користувачів у мережі блокчейн, софт-форк представляє гнучкий інструмент для модифікації системи. Наприклад, коли

серед спільноти блокчейн не було досягнуто політичного консенсусу щодо зміни розміру блоку Bitcoin (тобто правило 1 мегабайт), використовувався «SegWit» (процес, за допомогою якого обмеження розміру блоку в блокчейні збільшується шляхом видалення даних підпису з транзакцій, які включені в кожен блок [49]) через активований користувачем софт-форк. Враховуючи, що правила консенсусу Bitcoin контролюються економічною більшістю, економічна більшість змогла активувати «SegWit» самостійно, минаючи блокуючих майнерів.

Адресність використовує необов'язкові рекомендації, але на відміну від добровільності, вона спирається на детальний опис правил. У контексті блокчейну метод адресності часто використовується для введення пропозицій щодо покращення та DApps у мережі блокчейн. За допомогою пропозицій щодо покращення будь-хто може запропонувати зміни програмного забезпечення, які згодом оцінюються та обговорюються мережевою спільнотою. Якщо пропозиція досягає консенсусу громади, вона вважається остаточною. Під час реалізації пропозицій щодо покращення користувачі мають право вирішувати, встановлювати нове програмне забезпечення чи ні.

Рамкове регулювання створює обов'язкові правила для користувачів, але на відміну від примусу, користувачі мають свободу вибору, приймати варіанти політики чи ні. Цей механізм підзвітності в контексті блокчейну найкраще охоплювати хард форками. Хард форк відбувається, коли зміна правил прийнята в протоколі блокчейну, і вузли новітньої версії блокчейну більше не приймають стару версію блокчейну. У випадку хард форка всі вузли повинні працювати за новими правилами для оновлення свого програмного забезпечення. В іншому випадку відбувається постійне відокремлення від попередньої версії блокчейну і створюються два різних блокчейна.

Контроль управління. Контроль управління полягає в тому, який тип механізмів контролю закладено в реалізацію управлінських рішень і наскільки вони автоматизовані. Механізми управління можуть стосуватися системних змін (хард і софт форки), правил роботи або системних функцій (DApps).

Зокрема, автоматизація управлінських рішень і процесів в управлінні блокчейном є важливою проблемою в державному секторі. Визначимо три можливі форми автоматизації в управлінні блокчейном: обмежене управління, напівавтономне управління та автоматизоване управління.

При обмеженому управлінні суб'єкти управління володіють усіма правами на прийняття рішень, а рішення впроваджуються за згодою та спільними діями учасників. Наразі більшість платформ блокчейн працюють на основі обмеженого управління, де операції (наприклад, перевірка, порядок транзакцій, голосування тощо) контролюються людьми, будь то централізовано чи децентралізовано.

У напівавтономному управлінні ми очікуємо, що автоматизовані агенти забезпечуватимуть певні функції управління. Тут доступ до позаланцюжкових даних через оракули і зближення функцій платформи з іншими цифровими технологіями, такими як штучний інтелект та інтернет речей, можуть доповнити роль автоматизованих агентів. Наприклад, за допомогою впровадження технологій штучного інтелекту в мережі блокчейн можна покращити можливості управління смарт-контрактами та запровадити більш ефективні процеси майнінгу для зниження споживання енергії. Показовим прикладом є блокчейн QTUM, де у випадку проблемних цін на газ для певних операцій (наприклад, вищі ціни на обробку блоків, ніж на їх створення), смарт-контракти можуть тимчасово підвищити ціни на газ для проблемних операцій, щоб пом'якшити зловмисні атаки на мережу. Ці так звані протоколи децентралізованого керування (DGP) забезпечують альтернативу хард та софт форкам для виправлень, не порушуючи взаємодію з користувачами.

В автоматизованому управлінні нові цифрові технології та передові методи аналізу даних, доповнені зовнішніми джерелами даних, можуть створити складні автоматизовані механізми управління. Тут ми очікуємо, що суб'єкти управління будуть в більш вигідному положенні, у той час як мережі машин і складні алгоритми регулюють транзакції відповідно до мінливих умов навколишнього середовища. Наприклад, проект terra0 в Нідерландах

спрямований на створення самоврядних екосистем для управління природними ресурсами, що перебувають у державній власності, такими як ліси, за допомогою дистанційного зондування, штучного інтелекту, токенів і технології блокчейн [91]. Проект передбачає DAO, де супутникові знімки за допомогою смарт-контрактів позначають дерева, які можна вирубити, перш ніж вони завдадуть занадто велику шкоду лісу, і які автоматично торгують ліцензіями на вирубку дерев. Отриманий дохід використовується для купівлі доль землі у реальних землевласників у формі токенів, створюючи власність, що не належить людині, здатну використовувати власну економічну одиницю.

Рішення про усунення людського чинника тісно пов'язане з укоріненими громадськими цінностями в організаціях державного сектора і галузевою сферою застосування. Прихильність принципам ефективності і рентабельності може спонукати до заміни певних функцій і організацій в державних службах на DAO або автоматизовані агенти, не керовані людиною. Знову ж таки, заміна великої кількості організацій державного сектору та адміністративних посад автоматизованими агентами може бути політично нездійсненною. Одним з недоліків DAO, є те, що поняття відповідальності може бути розмитим у державному управлінні. Тут культурні і поведінкові обмовки можуть припускати, що певні ролі і рішення, які можуть бути автоматизовані, мають бути залишені в руках реальних людей. Крім того, адаптація автоматизованих рішень має відповідати існуючим можливостям і практикам на рівні суспільства щодо цифрового управління. Ключовим моментом тут є оцінка того, в якому ступені люди можуть управляти своїми цифровими ідентифікаційними даними і активами і чи потрібні їм організації-зберігачі в державному управлінні.

3.2. Використання blockchain для покращення управління даними у державному секторі

Державні установи можуть використовувати технологію блокчейн для захисту довірених записів та спрощення взаємодії з громадянами.

Важливою функцією уряду є підтримання достовірної інформації про осіб, організації, активи та діяльність. Місцеві, регіональні та національні агенції зобов'язані вести записи, що включають, наприклад, дати народження і смерті або інформацію про сімейне становище, ліцензування бізнесу, передачу власності або злочинну діяльність. Управління та використання цих даних може бути складним навіть для розвинених урядів. Деякі записи існують лише у паперовому вигляді, і якщо необхідно внести зміни до офіційних реєстрів, громадянам часто доводиться особисто являтися для цього. Окремі відомства зазвичай створюють свої власні сховища даних і протоколи управління інформацією, що не дозволяє іншим частинам уряду використовувати їх. І, звичайно, ці дані мають бути захищені від несанкціонованого доступу чи маніпуляцій без права на помилку.

Технологія блокчейн може спростити управління довіреною інформацією, полегшуючи державним установам доступ до найважливіших даних державного сектора і їх використання при збереженні безпеки цієї інформації.

Досі банки, постачальники платіжних послуг і страхові компанії виявляли найбільшу зацікавленість і інвестиції у блокчейн. Але, вважаємо, що державні установи можуть отримати не меншу вигоду від експериментів з цією технологією і її стратегічного впровадження у рамках пілотних проектів. З часом блокчейн може допомогти відомствам оцифрувати існуючі записи і управляти ними у рамках безпечної інфраструктури, що дозволить відомствам зробити деякі з цих записів «розумними». Наприклад, ІТ-відділи державних установ зможуть створювати правила і алгоритми, які дозволять автоматично передавати дані у блокчейні третім сторонам при виконанні заздалегідь заданих певних умов. У довгостроковій перспективі технологія може навіть дозволити

приватним особам і організаціям отримати прямий контроль над усією інформацією, яку уряд зберігає про них. Такий рівень прозорості, у свою чергу, може полегшити відомствам завдання отримання підтримки при створенні мережевих державних послуг.

Існує ряд інструментів і технологій блокчейн, які державні установи можуть впровадити вже сьогодні для захисту критично важливих даних і поліпшення управління записами, пов'язаними з володінням власністю і реєстрацією. У довгостроковій перспективі, у міру розвитку блокчейну, уряд може також використати його для створення мережевих державних послуг.

Кожен, хто користується державними послугами, справедливо побоюється, що, незважаючи на усі зусилля відомств із захисту своїх систем, злочинці можуть отримати доступ до державних баз даних і вкрати або підробити записи. Методи шифрування ніколи не можуть бути на 100% безпечними, але технологія блокчейн може значно ускладнити процеси злому. Наприклад, технологія KSI для захисту усіх даних державного сектора. KSI створює хеш-значення, які однозначно представляють великі об'єми даних у вигляді набагато менших числових значень. Хеш-значення можуть бути використані для ідентифікації записів, але не можуть бути використані для відновлення інформації в самому файлі. Хеш-значення зберігаються у блокчейні і поширюються по приватній мережі урядових комп'ютерів. При зміні базового файлу в ланцюжок додається нове хеш-значення, і ця інформація більше не може бути змінена. Історія кожного запису повністю прозора, і несанкціоноване втручання зсередини або ззовні системи може бути виявлено і відхилено. KSI дозволяє державним службовцям відстежувати зміни в різних базах даних – хто змінює запис, які зміни внесені і коли вони зроблені. За допомогою технології KSI можливе управління електронними медичними картами громадян.

Процес володіння і передачі активів – будь то фізична власність або фінансові інструменти – зазвичай включає безліч взаємодій і довгий паперовий слід. Державні органи могли б істотно скоротити і те, і інше, оцифрувавши інформацію про володіння активами і зберігши її у блокчейн-реєстрах.

Створення мережевих державних служб. Уряди зазвичай багато знають про людей та організації завдяки всім даним, які вони збирають. Однак через те, що ця інформація існує у розрізних відомствах та департаментах, вона часто використовується не повною мірою.

Установи, що надають соціальні послуги, зазвичай не мають прямого доступу до інформації про взаємодію клієнта з іншими державними органами. А збір такої інформації може бути копіткою роботою, що вимагає багато часу та зусиль.

З технічної точки зору, немає жодних вагомих причин для зберігання даних у державних сховищах. За певних зусиль можуть бути створені центральні сховища або корпоративні системи для обміну інформацією між відомствами. Однак найважливішим каменем спотикання є безпека: як і їхні колеги у приватному секторі, державні установи за жодних обставин не можуть робити конфіденційні дані доступними без розбору. Необхідне середовище, в якому дані можуть легко обмінюватися між системами, але в якому окремі особи та організації можуть повернути право власності на свої дані та контролювати потік особистої інформації – хто її бачить, що бачить і коли.

Технологія блокчейн може підтримати такий сценарій (див. рис. 3.1). Кожна людина або організація матиме всі необхідні дані про них (наприклад, основна особиста інформація або записи про попередні взаємодії з державними органами), що зберігаються в спеціальному журналі в зашифрованій базі даних блокчейну. Приватні особи або компанії можуть отримати доступ до цих даних через інтернет. Кінцеві користувачі – надати державним установам повноваження на читання або зміну певних елементів їхніх

індивідуальних даних за допомогою криптографії з відкритим та закритим ключем. Можливо використовувати відкриті ключі для вибіркового обміну інформацією щодо конкретної транзакції послуг з установами. Або видавати закриті ключі агентствам для одноразового доступу «на запис» до їх даних.



Рис. 3.1 Сценарій взаємодії у технології блокчейн

У певних ситуаціях смарт-контракти можуть передавати деяку інформацію призначеним агентствам за умови дотримання певних умов. Наприклад, якщо одержувачі допомоги з безробіття перебувають у в'язниці, ця інформація може бути передана в агентство з праці, щоб виплати були припинені на час відбування покарання. Агентства зможуть використовувати

певну частину інформації для конкретних цілей, але не матимуть необмеженого доступу до всіх даних кінцевого користувача.

Використання блокчейн-реєстраторів знизить ризик несанкціонованого доступу (завдяки надійному шифруванню) та маніпулювання даними (завдяки надійним аудиторським слідам). Державні послуги можуть стати посправжньому мережевими без надмірного обмеження прав на приватне життя. Приватним особам та компаніям більше не доведеться витратити багато часу на заповнення форм з інформацією, яку вони вже надали уряду. Агентства зможуть адаптувати свої послуги до потреб людей, а не застосовувати універсальний підхід.

Урядові ІТ-департаменти, які хочуть впровадити рішення на основі блокчейну, будуть мати справу з галуззю, що швидко розвивається. Швидке зростання створює проблеми для осіб, які ухвалюють рішення у сфері ІТ в уряді. По-перше, немає загальноприйнятих стандартів для технологій блокчейн чи мереж, що їх використовують. Тому урядовим ІТ-організаціям, як і решті, може бути важко оцінити якість наявних рішень і визначити, як найкраще інтегрувати їх у існуючі ІТ-ландшафти. По-друге, оскільки багато постачальників блокчейну є невеликими стартапами, ІТ-відділам та відділам закупівель може бути складно знайти партнерів із стійкою репутацією, тобто компанії, які можуть запропонувати передові продукти, але при цьому досить стабільні, щоб довести проекти до кінця.

Водночас ризики конфіденційності вимагатимуть постійної уваги. Навіть якщо уряд зможе впровадити блокчейн для обміну даними через публічні мережі (як у сценарії «мережових послуг», описаному раніше), їм все одно доведеться переконатися, що існуючі та майбутні методи шифрування є достатньо сильними для забезпечення конфіденційності користувачів. Керівникам державних установ необхідно зрозуміти правові та нормативні наслідки блокчейну, серед яких:

- в якій мірі смарт-контракти будуть обов'язковими для виконання;
- чи можна використовувати журнали блокчейну як докази в суді;

– чи має бути використання блокчейну обов’язковим у певних областях.

Як уряди можуть скористатися перевагами швидких темпів інновацій в екосистемі блокчейн, одночасно справляючись із цими ризиками та проблемами. Один із способів – використовувати інкубаторний підхід до змін. Тобто вони можуть створити невелику групу, яка проаналізує та визначить пріоритетність можливостей для пілотних проектів у галузі блокчейну, а потім підбере відповідних партнерів для впровадження. Ця група може перебувати в центральному урядовому офісі з оцифрування або в окремих органах влади, які можуть отримати найбільшу вигоду від впровадження блокчейну.

Наприклад, команда інкубатору може запросити десятки блокчейн-стартапів представити свої пропозиції та можливості; кілька з них будуть відібрані для пілотного тестування. Уроки пілотних проектів можуть допомогти державним органам у вирішенні питань стандартизації, безпеки та регулювання. Алгоритм інкубаторного підходу у такому випадку матиме наступний вигляд:

– сканування. Команда інкубатора розпочинає з аналізу ідей щодо використання технології блокчейн у державному управлінні. Сканування команди зосереджено на процесах, поліпшення яких може призвести до покращення досвіду громадян – наприклад, упорядкування взаємодії, що включає надто багато ручних завдань, коштує надто дорого чи займає надто багато часу;

– визначання пріоритетів. Команда інкубатора вивчає додаткові переваги, які може дати використання технології блокчейн у кожній потенційній галузі застосування. Наприклад, використання блокчейну для обліку голосів на виборах може бути більш захищеним від злону, ніж існуючі цифрові та традиційні методи голосування. Тим не менш, додаткова вигода від переходу не завжди може бути великою. Команда зосереджується на додатках, які можуть дати негайні, значущі результати, що може сприяти активнішому впровадженню блокчейну;

– партнерство. Після визначення пріоритетів команда інкубатора вивчає можливості партнерства із постачальниками блокчейну для створення пілотних програм. Завдяки таким відносинам технологічні компанії отримують можливість продемонструвати та протестувати продукти, а державні установи прискорюють вивчення блокчейну без необхідності значного збільшення внутрішніх ресурсів.

Після створення пілотних програм уряду слід подумати, як їх розвивати. Наприклад, національна «дорожня карта» може стати чітким керівництвом для державних установ та постачальників технологій блокчейн щодо технічних стандартів та норм сумісності. Вона може включати кращі практики з нарощування потенціалу державних установ та фінансування розгортання додатків блокчейн, які показали свій потенціал на пілотних етапах. Уряд може розширити ці обговорення, включивши в них міжнародних партнерів – створити форум, подібний до консорціуму R3 фінансової індустрії, для обміну досвідом пілотних досліджень, обміну технічними шаблонами або просування глобальних технічних стандартів.

Отже, є кілька ключових висновків для розробників систем і тих, хто приймає рішення, зацікавлених у застосуванні рішень на основі блокчейну в державному управлінні.

По-перше, розробники політики та розробники систем повинні подумати про взаємозв'язки між рівнями управління та оцінити наслідки вибору на одному рівні для інших рівнів управління. Наприклад, можлива політична мета, спрямована на зміцнення довіри до формування політики, може вимагати більш децентралізованої форми управління, яка в свою чергу може впливати на вибір на мікро- та мезорівнях управління. Запропонована модель невизначає ієрархію важливості між різними рівнями управління і не визначає пріоритетність управлінських рішень над іншими. Крім того, модель не передбачає певної послідовності в оцінці наслідків управлінських рішень для формування політики, вона надає систематичний інструмент для цілісної оцінки впливу вибору політики та уподобань осіб, які приймають рішення, для управління.

Важливість та необхідність певних управлінських рішень буде відрізнятися залежно від контексту та галузевої сфери застосування.

По-друге, законодавчі, ринкові, політико-адміністративні та соціально-технологічні умови в окремих галузях можуть підкреслити певний вибір в управлінні блокчейном. Неоінституціоналістичні теорії припускають, що розрахунки витрат і вигод (фінансові витрати, витрати на транзакцію, політичні витрати тощо), норми та цінності (легітимність суб'єктів, збереження автономії, прозорості та підзвітності тощо) та залежність від шляху розвитку технологічної інфраструктури (перехресні бази даних, KSI тощо) – ось деякі способи, за допомогою яких інституційні фактори можуть відігравати визначальну роль у виборі управління. Наявність або відсутність нормативно-правової бази щодо конфіденційності даних, технології токенів, смарт-контрактів, DAO та штучного інтелекту – це інші ключові інституційні фактори, які можуть вплинути на рішення по управлінню.

По-третє, управління блокчейном від природи не є агностичним і не аполітичним. Вибір дизайну, зроблений розробниками систем на мікрорівні, або динаміка потужності в мережі блокчейну роблять акцент на певних варіантах управління над іншими. Крім того, використання технології блокчейн у державному секторі, ймовірно, вимагає від уряду та організацій державного сектору відмовитися від певних прерогатив у державному управлінні. Наскільки уряд повинен відмовитися від своїх прерогатив за допомогою технології блокчейн, пов'язано з рівнем довіри до організацій державного сектору та суспільства. Загальнодоступні блокчейни без дозволу будуть бажаними в сферах громадського обслуговування, де існує низький рівень довіри серед користувачів. Однак література про довіру свідчить про те, що коли існує низький рівень довіри до суспільства чи інших зацікавлених сторін, особи, які приймають рішення, більш схильні утримувати контроль за допомогою прямих або непрямих засобів.

Технологія блокчейн відкриває перспективи для тих державних органів, які шукають найкращі способи управління та захисту довіреної інформації.

Вона пропонує привабливий шлях до більш ефективних операцій, більш оперативного обслуговування та підвищеної безпеки даних. Однак, як можуть підтвердити перші послідовники у сфері фінансових послуг, потрібен час, щоб технологія повністю дозріла. Нині саме час для експериментів. Включивши блокчейн до своїх інноваційних програм і зробивши його найважливішим компонентом архітектури підприємства, уряд дізнається, що працює на практиці і як розкрити весь потенціал послуг, заснованих на блокчейні.

ВИСНОВКИ

Блокчейн – це інноваційна технологія загального призначення, що пропонує нові способи організації в багатьох областях для запису транзакцій, подій, сертифікатів та власності. Його характеристики, такі як незмінність, простежуваність даних, безпека та децентралізований характер, були основними рушійними факторами для забезпечення його успіху. Цінність блокчейну полягає у можливості здійснювати угоди без посередників, що ефективно знижує транзакційні витрати. Хоча першим прикладом використання блокчейну був Bitcoin, дедалі більше урядів впроваджують чи експериментують із блокчейном у державному секторі. Сучасна наукова література присвячена застосуванню блокчейну в різних галузях, і лише в кількох дослідженнях обговорюється вплив блокчейну на державне управління.

Блокчейн у державному управлінні був підтверджений як цінний інструмент, що виводить електронне управління та електронний уряд на новий рівень. У контексті електронного управління як інструменти блокчейну нового покоління були названі спеціалізовані державні послуги, смарт-контракти та уряд відкритих даних на основі блокчейну. Щодо рамок реформ було встановлено, що обговорення блокчейна повинно включати загальний опис блокчейну, що розглядається (централізований або децентралізований; приватний або публічний), оскільки результати управління блокчейном залежать від його початкового дизайну.

Розглянуто концептуалізацію управління блокчейном в різних дисциплінах і розроблено нову концептуальну основу для аналізу управління блокчейном в державному секторі. Запропонована категоризація управління блокчейном була заснована на систематичному огляді літератури, було використано концепції та теорії державного управління для з'ясування вибору управління при розробці систем на основі блокчейну. Структура передбачає, що управління блокчейном в державному секторі передбачає прийняття рішень щодо архітектури інфраструктури, архітектури додатків, інтеперабельності,

механізму прийняття рішень, механізму стимулювання, механізму консенсусу, організації, підзвітності та контролю управління.

Враховуючи організаційну потребу в машинному навчанні та можливості смарт-контрактів блокчейну, спеціалізовані державні послуги можуть виявитися вигідним рішенням як для держави, так і для громадян. Смарт-контракти можуть стати безпечним способом автоматизації організаційних процедур, у той час як машинне навчання фільтрує дані, щоб вони були найбільш актуальними для громадян. Таким чином, знижуються адміністративні та бюрократичні витрати, а громадяни отримують послуги, адаптовані до їх конкретних потреб. Уряд відкритих даних – ще один інструмент, який можна впровадити за допомогою блокчейну. Уряд відкритих даних має на увазі, що громадяни можуть отримати доступ до урядових даних, а блокчейн гарантує анонімність, безпеку та доступ до цих даних.

Технологію блокчейн називають однією з найбільш трансформуючих технологій сучасності, що є одним із найбільш очевидних випадків використання криптовалют. Це та ж сама технологія, на якій базуються криптовалюти, але вона має багато інших застосувань.

Замість того, щоб зберігати дані на серверах, як це було раніше, через хмарне сховище, блокчейн зосереджується на використанні мережі комп'ютерів, які зберігають і перевіряють дані. Комп'ютери в певній мережі можуть бути поширені по всьому світу, і мережа не контролюється централізовано. Уряди зазвичай критикують за те, що вони не знають, як ефективно управляти більшістю своїх процесів, але нові технології, такі як блокчейн, мають потенціал, щоб змінити ситуацію через блокчейн-рішення для всього уряду. Урядовий блокчейн може стати реальністю в найближчі роки, коли уряди почнуть приймати цю технологію.

Технологія блокчейн може підвищити доступ та прозорість інформації, контроль публічних даних, контроль проти корупції та шахрайства, а також інформаційну безпеку, дозволяючи надавати більш ефективні державні послуги шляхом покращення бізнес-процесів для державних структур у будь-який

рівень влади; і дозволити створити швидкі, дешеві та особливо безпечні публічні записи. Блокчейн може бути дуже корисним для державних установ, роблячи їх більш прозорими, близькими до громадян та безпечними. Однак адміністраціям також доводиться змінювати позицію в цьому новому сценарії, оскільки йдеться не лише про його користь, а й про зобов'язання просувати цю технологію, яка матиме вплив на всю економіку.

Можливо, доведеться переосмислити природу публічних баз даних й подивитися у бік нового покоління смарт-контрактів та децентралізованих додатків. Остані можуть використовувати набагато більше функцій, ніж хешування блокчейну, яке є примітивним і не розкриває весь потенціал блокчейну. Вони також можуть допомогти зменшити породжені людиною помилки, бюрократію та витрати державного управління. Тим не менш, смарт-контракти та децентралізовані додатки однаково вимагатимуть не лише послідовної нормативної бази, а й ширших організаційних змін у державному управлінні та адмініструванні. Наслідки для уряду необхідно досліджувати за допомогою міждисциплінарних досліджень, які виходять за рамки теперішнього загальноприйнятого підходу до застосування блокчейну, орієнтованого на технології.

СПИСОК ЛІТЕРАТУРИ

1. Важинський С. Е., Щербак Т. І. Методика та організація наукових досліджень : навч. посіб. Суми :СумДПУ, 2016. 260 с.
2. Державне управління: підручник: у 2 т. / Нац. акад. держ. упр. при Президентові України; ред. кол.: Ю. В. Ковбасюк, К. О. Ващенко, Ю. П. Сурмін та ін. Київ ; Дніпропетровськ : НАДУ, 2012. Т. 1. 564 с.
3. Енциклопедичний словник з державного управління / уклад.: Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін.; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. Київ : НАДУ, 2010. 820 с.
4. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України; наук. ред. колегія: Ю. В. Ковбасюк та ін. Київ : НАДУ, 2011. Т. 4: Галузеве управління / Наук.ред. колегія: М. М. Іжа, В. Г. Бодров та ін. 2011. 648 с.
5. Матюнин И. И. Сравнительные и экспериментальные исследования. Методологические и методические аспекты сравнительных социологических исследований. Москва : РАН , Институт социологии. 1984. С. 12-42.
6. Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22.07.1998 р. № 810/1998. *Офіційний вісник України*. 1999. № 21. С. 32.
7. Філософський енциклопедичний словник / редкол.: В. І. Шинкарук. Київ , Абрис : НАН України ; Ін-т філософії ім. Г.С. Сковороди, 2002. 742 с.
8. Шаталович И. В. Понятие детерминации: к проблеме определения и классификации. *Культурологічний вісник Нижньої Наддніпряниці*. 2014. № 7. С. 189-195.
9. Ajiboye T. Seoul Advances Plans on Smart City Adding Cryptocurrency for Citizens. 2019. URL: <https://www.coinspeaker.com/seoul-crypto-citizens/>.
10. Alketbi A., Nasir Q., Abu Talib M. Novel blockchain reference model for government services: Dubai government case study. *International Journal of Systems Assurance Engineering and Management*. 2020. No 11 (6). P. 1170-1191.

11. Allen D W E., Berg, C. Blockchain governance: What we can learn from the economics of corporate governance. *SSRN Electronic Journal*. 2020.
12. Allen D W E., Berg C., Lane A. M., Potts J. Cryptodemocracy and its institutional possibilities. *The Review of Austrian Economics*. 2020. No 33 (3). P. 363-374.
13. Alessie D., Janssen M., Ubacht J., Cunningham S., van der Harst G. The consequences of blockchain architectures for the governance of public services: A case study of the movement of excise goods under duty exemptions. *Information Polity*. 2019. No 24 (4). P. 487-499.
14. Angarita R., Dejous A., Blake P. From centralized to decentralized blockchain-based product registration systems: The use case of lighting and appliances. *INFOCOM*. 2019. P. 650-655.
15. Arisi M., Guarda P. Blockchain and eHealth: Seeking compliance with the general data protection regulation BioLaw journal – Rivista di BioDiritto. *BioLaw Journal – Rivista Di BioDiritto*. 2017. No 21 (2). P. 477-496.
16. Atzori M. Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*. 2017. No 6 (1). P. 45-62.
17. Atzori M. Blockchain governance and the role of trust service providers: the Trusted Chain network. *The Journal of the British Blockchain Association*. 2018. No 1 (1). P. 1-17.
18. Ayed A. B. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*. 2017. No 9 (3). P. 1-9.
19. Bagloee S. A., Heshmati, M., Dia H., Ghaderi H., Pettit C., Asadi M. Blockchain: The operating system of smart cities. *Cities*, 2021. 112 p.
20. Beck R., Müller-Bloch C., King J. L. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*. 2018. No 19 (10). P. 1020-1034.

21. Bekkers V., Dijkstra G, Edwards A, Fenger M (2007), Governance and the democratic deficit; assessing the democratic legitimacy of governance practices. Aldershot : Ashgate, 2007. 340 p.
22. Benedict G. Challenges of DLT-enabled Scalable Governance and the role of standards. *Journal of ICT Standardization*. 2019. No 7 (3). P. 195-208.
23. Bertolami O., Francisco F. A digital contract for restoration of the earth system mediated by a planetary boundary exchange unit. *Anthropocene Review*. 2021. DOI: <https://doi.org/10.1177/2053019620987270>.
24. Blockchain Strategy. European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>.
25. Brinkmann M., Heine M. Can blockchain leverage for new public governance? A conceptual analysis on process level. In ACM international conference proceeding series. 2019. part F148155. P. 338-341.
26. Cachin C., Kursawe K., Petzold F., Shoup V. Secure and efficient asynchronous broadcast protocols *Advances in Cryptology. CRYPTO*. 2001. P. 524-541.
27. Carvalho A., Merhout J. W., Kadiyala Y., Bentley J. When good blocks go bad: Managing unwanted blockchain data. *International Journal of Information Management*. 2021. No 57.
28. Chen Y., Pereira I., Patel P. C. Decentralized governance of digital platforms. *Journal of Management*. 2021. No 47 (5). P. 1305-1337.
29. Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*. 2016. Vol. 4. P. 2292-2303.
30. Daluwathumullagamage D. J., Sims A. Blockchain-enabled corporate governance and regulation. *International Journal of Financial Studies*. 2020. No 8 (2). P. 1-41.
31. Daniel F., Guida L. A Service-Oriented Perspective on Blockchain Smart Contracts. *IEEE Internet Computing*. 2019. Vol. 23. No 1. P. 46-53.
32. Davidson S., Filippi P. D., Potts J. Disrupting governance: The new institutional economics of distributed ledger technology. 2016. 27 p.

33. Dilger W. Decentralized autonomous organization of the intelligent home according to the principle of the immune system. *IEEE International Conference*. 1997. Vol. 1. P. 351-356.
34. Dimitropoulos G. The law of blockchain. *Washington Law Review*. 2020. No 95 (3). P. 1117-1192.
35. Diniz E. H., Cernev A. K., Rodrigues D. A., Daneluzzi F. Solidarity cryptocurrencies as digital community platforms. *Information Technology for Development*. 2020. No 27 (1). P. 1-5.
36. Dirose S., Mansouri M. Comparison and analysis of governance mechanisms employed by blockchain-based distributed autonomous organizations. In 2018 13th system of systems engineering conference, SoSE. 2018. P. 195-202.
37. Dobler M., Ballandies M., Holzwarth V. On the extension of digital ecosystems for SCM and customs with distributed ledger technologies: Requirements Analysis, innovation assessment, and prototype Design for the Lake Constance Region. In Proceedings : 2019 IEEE international conference on engineering, technology and innovation. ICE/ITMC, 2019.
38. Drechsler W. Governance, good governance, and government: the case for Estonian administrative capacity. *Estonian Academy Publishers*. 2004. Vol. 8.
39. Dursun T., Üstündag B. B. A novel framework for policy based on-chain governance of blockchain networks. *Information Processing and Management*. 2021. No 58 (4).
40. Erbguth J., Morin J H. Towards governance and dispute resolution for DLT and smart contracts. In Proceedings of the IEEE international conference on software engineering and service sciences, ICSESS, 2018. 2019. P. 46-55.
41. Ertz M., Boily E. The rise of the digital economy: Thoughts on blockchain technology and cryptocurrencies for the collaborative economy. *International Journal of Innovation Studies*. 2019. No 3 (4). P. 84-93.
42. Estonian eID scheme: Digi-ID. Republic of Estonia. 2018.
43. Filippi P., Loveluck B. The invisible politics of bitcoin: Governance crisis of a decentralised infrastructure. *Internet Policy Review*. 2016. No 5 (3).

44. Filippi P., Mannan M., Reijers W. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*. 2020. No 62.
45. Filippi P., Wright A. Blockchain and the law: The rule of code. Harvard University Press Cambridge Massachusetts. 2018. P. 32, 49, 193.
46. Flood J., McCullagh A. Blockchain's future: Can the decentralized blockchain community succeed in creating standards? *Knowledge Engineering Review*. 2020. No 35.
47. Franke L., Schletz M., Salomo S. Designing a Blockchain model for the Paris Agreement's carbon market mechanism. *MDPI, Open Access Journal*. 2020. No 12 (3). P. 1-20.
48. Frankenfield J. Hard Fork. URL: <http://www.investopedia.com/terms/h/hard-fork.asp>.
49. Frankenfield J. SegWit. URL: <http://www.investopedia.com/terms/s/segwit-segregated-witness.asp>.
50. Frankenfield J. Soft Fork. URL: <http://www.investopedia.com/terms/s/soft-fork.asp>.
51. Franks P. C. Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal*. 2020. No 30 (3). P. 287-299.
52. Governatori G., Idelberger F., Milosevic Z., Riveret R., Sartor G., Xu X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*. 2018. No 26 (4). P. 377-409.
53. Graglia J. M., Mellon C. Blockchain and Property in 2018: at the end of the beginning. *Innovations: Technology, Governance, Globalization*. 2018. No 12 (1-2). P. 90-116.
54. Greenspan G. Private Blockchains are more than «just» shared databases. Multichain. Private Blockchains. 2015.
55. Gruin J. The epistemic evolution of market authority: Big data, blockchain and China's neostatist challenge to neoliberalism. *Competition and Change*. 2020.

56. Guarda D. How Governments Are Adopting Blockchain and AI In Advanced Economies Part 2. URL: <https://www.intelligenthq.com/how-governments-are-adopting-blockchain-and-ai-in-advanced-economies-part-2/>.

57. Gusenbauer M., Haddaway N. R. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google scholar, PubMed, and 26 other resources. *Research Synthesis Methods*. 2020. No 11 (2). P. 181-217.

58. Halaburda H., Mueller-Bloch C. Toward a multidimensional conceptualization of decentralization in Blockchain governance: Commentary on «two sides of the same coin? Decentralized versus proprietary Blockchains and the performance of digital currencies» by Cennamo, Marchesi, and Meyer. *Academy of Management Discoveries*. 2020. No 6 (4). P. 712-714.

59. Hermstrüwer Y. Democratic Blockchain design. *Journal of Institutional and Theoretical Economics*. 2019. No 175 (1). P. 163-177.

60. Hsieh Y.-Y., Vergne J.-P., Wang S. (2018). The internal and external governance of blockchain-based organizations. In *Bitcoin and beyond*. Routledge. 2018. P. 48-68.

61. Iansiti M., Lakhani K. R. The Truth About Blockchain. *Harvard Business Review*. Technology. 2017.

62. Janssen M., Weerakkody V., Ismagilova E., Sivarajah U., Irani Z. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*. 2020. No 50. P. 302-309.

63. Jayachandran P. The difference between public and private blockchain. *Blockchain Unleashed: IBM Blockchain Blog*. 2017.

64. Jentzsch C. Decentralized autonomous organization to automate governance. 2016.

65. Jia K., Zhang F. Between liberalization and prohibition. In *Bitcoin and beyond*. Routledge. 2018. P. 88-108.

66. John T., Pam M. Complex adaptive blockchain governance. MATEC Web of Conferences. 2018. No 223.

67. Kaal W. A. Decentralized corporate governance via blockchain technology. In Foundations and trends in accounting. Now Publishers Inc. 2020. Vol. 5, issue 2. P. 101-147.

68. Kannengießer N., Lins S., Dehling T., Sunyaev A. Mind the gap: Trade-offs between distributed ledger technology characteristics. 2019.

69. Katina P. F., Keating C. B., Sisti, J. A., Gheorghe A. V. Blockchain governance. *International Journal of Critical Infrastructures*. 2019. No 15 (2). P. 121-135.

70. Kavanagh D., Ennis P. J. Cryptocurrencies and the emergence of blockocracy. *The Information Society*. 2020. No 36 (5). P. 290-300.

71. Kim S. K., Huh J. H. Blockchain of carbon trading for UN sustainable development goals. *Sustainability*. 2020. No 12 (10).

72. KSI Blockchain. Republic of Estonia. URL: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>.

73. Lacity M. Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive*. 2018. No 17 (3).

74. Martinovic I., Kello L., Sluganovic I. Blockchains for Governmental Services: Design Principles, Applications, and Case Studies. *Working Paper Series. Centre For Technology & Global Affairs*. 2017. No 7.

75. Mazonka O. What is Blockchain: a Gentle Introduction. Defence Science and Technology Group (DST). 2016.

76. McLellan C. Blockchain and business: Looking beyond the hype. URL: <https://www.zdnet.com/article/blockchain-and-business-looking-beyond-the-hype/>.

77. Meijer D., Ubacht J. The governance of blockchain systems from an institutional perspective, a matter of trust or control? ACM International Conference Proceeding Series. 2018.

78. Meunier S. Chapter 3 – Blockchain 101: What is Blockchain and how does this revolutionary technology work? In A. Marke (Ed.), *Transforming climate finance and green investment with Blockchains*. Academic Press. 2018. P. 23-34.

79. Miscione G., Goerke T., Klein S., Schwabe G., Ziolkowski R. Hanseatic governance: Understanding Blockchain as organizational technology. In 40th international conference on information systems. 2019.

80. Miyachi K., Mackey T. K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing and Management*. 2021. No 58 (3).

81. Myung S. J. Blockchain government – a next form of infrastructure for the twenty- first century. *Journal of Open Innovation: Technology, Market, and Complexity*. 2018. Vol. 4, issue 4.

82. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

83. Nicolae-Bogdan-Cristian T., Luca S. A., Pungila C. Towards efficient governance in distributed ledger systems using high-performance computational nodes. In Proceedings. SYNASC 2020. 2020. P. 294-301.

84. Novak M. Crypto-friendliness: Understanding blockchain public policy. 2018.

85. Ølnes S., Ubacht J., Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *In Government information quarterly*. 2017. Vol. 34, issue 3. P. 355-364.

86. Osborne D., Gaebler T. *Reinventing Government: How the Entrepreneurial Spirit Is Transforming the Public Sector*. 1992.

87. Osborne S. P. *The New Public Governance?* 2010.

88. Ozdemir A. I., Ar I. M., Erol I. Assessment of blockchain applications in travel and tourism industry. *Quality and Quantity*. 2020. No 54 (5-6). P. 1549-1563.

89. Paech P. The governance of blockchain financial networks. *In Modern law review*. 2017. Vol. 80, issue 6. P. 1073–1110.

90. Parkin J. The senatorial governance of bitcoin: Making (de)centralized money. *Economy and Society*. 2019. No 48 (4). P. 463-487.

91. Paul S. URL: <https://terra0.org/>.
92. Pimentel E., Boulianne E. Blockchain in accounting research and practice: Current trends and Future opportunities*. *Accounting Perspectives*. 2020. No 19 (4). P. 325-361.
93. Razzaq A., Khan M. M., Talib R., Butt A., Hanif N., Afzal S., Razeen M. Use of Blockchain in governance: A systematic literature review. *International Journal of Advanced Computer Science and Applications*. 2019. No 10.
94. Reyes C. L. (Un)Corporate Crypto-Governance. Actual Problems of *Economics and Law*. 2021. No 15 (1).
95. Rikken O., Janssen M., Kwee Z. Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity*. 2019. No 24 (4). P. 397-417.
96. Rodrigues D., Meirelles F., Cunha M. A. Benefícios do Blockchain para moedas sociais digitais. 2018.
97. Schaffers H. The relevance of Blockchain for collaborative networked organizations. *IFIP Advances in Information and Communication Technology*. 2018. No 534. P. 3-17.
98. Shah S., Jansen S. A framework for designing self-sustaining ecosystems with Blockchain. *Lecture Notes in Business Information Processing*. 2021 No 407. P 184-192.
99. Shermin V. Disrupting governance with blockchains and smart contracts. *Strategic Change*. 2017. No 26 (5). P. 499-509.
100. Singh J., Michels J. D. Blockchain as a service (BaaS): Providers and trust. 3rd IEEE European symposium on security and privacy workshops. EURO S and PW 2018. 2018. P. 67-74.
101. Strauss A., Corbin J. Basics of qualitative research: Techniques and procedures for developing grounded theory (2nd ed.). Thousand Oaks, CA: Sage. 1998.
102. Swan M. Blockchain thinking: The brain as a dac (decentralized autonomous organization). Texas Bitcoin Conference. 2015. P. 27-29.

103. Tapscott D., Tapscott A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. 2016.
104. Themistocleous M. Blockchain technology and land registry. *The Cyprus review*. 2018. No 30 (2). P. 195-202.
105. Tozzi C. Decentralizing democracy: Approaches to consensus within blockchain communities. *Teknokultura*. 2019. No 16 (2). P. 181-195.
106. Trbovich A. S. In pursuit of good governance for the energy industry blockchain. *Journal of Energy Markets*. 2019. No 12 (2). P. 1-17.
107. Trump B. D., Florin M. V., Matthews H. S., Sicker D., Linkov I. Governing the use of Blockchain and distributed ledger technologies: Not one-size-fits-all. *IEEE Engineering Management Review*. 2018. No 46 (3). P. 56-62.
108. Van Pelt R., Jansen S., Baars D., Overbeek S. Defining Blockchain governance: A framework for analysis and comparison. *Information Systems Management*. 2021. No 38 (1). P. 21-41.
109. Wang Y. Designing a blockchain enabled supply chain. *IFAC-PapersOnLine*. 2019. No 52 (13). P. 6-11.
110. Werbach K. *The blockchain and the new architecture of trust*. Cambridge, Massachusetts: The MIT Press. 2018.
111. Werbach K. The Siren song: algorithmic governance by blockchain. In K. Werbach (Ed.), *After the digital tornado: Networks, algorithms, humanity*. Cambridge University Press. 2020. P. 215-240.
112. Williamson O. E. Calculativeness, trust, and economic organization. *Journal of Law, Economics, and Organization*. 1993. No 36 (1). P. 453-486.
113. Woods J. *Blockchain: Public Sector Use Cases*. 2018. URL: <https://medium.com/crypto-oracle/blockchain-public-sector-use-cases-49a2d74ad946>.
114. Yeung K., Galindo D. Why do public blockchains need formal and effective internal governance mechanisms? *SSRN Electronic Journal*. 2019. 17 p.

115. Zachariadis M., Hileman G., Scott SV. Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*. 2019. No 29 (2). P. 105-117.

116. Zhai S., Yang Y., Li J., Qiu C., Zhao J. Research on the Application of Cryptography on the Blockchain. *Journal of Physics Conference Series*. 2019. No 1168.

117. Zhu Y., Gan G. H., Deng D. Security Research in Key Technologies of Blockchain. *Information Security Research*. 2016. No 12. P 1090-1097.

118. Ziolkowski R., Miscione G., Schwabe G. Decision problems in Blockchain governance: Old wine in new bottles or walking in someone Else's shoes? *Journal of Management Information Systems*. 2020. No 37 (2). P 316-348.

Схема кодування

Категорія	коди	підкоди	література
Мікрорівень	Архітектура інфраструктури	публічний/приватний, без/з дозволом, протокол блокчейн, архітектура блокчейн, інтерфейс, розробка системи, безпека, децентралізація, незмінність, відстежуваність	[10], [14], [27], [30], [35], [37], [41], [46], [47], [58], [66], [78], [79], [80], [88], [93], [95], [97], [100]
	Архітектура програми	смарт-контракт, DAO, додаток, Dapps, оракули, автономна організація	
	Інтероперабельність	стандарти, стандартизація, інтероперабельність, заходи	
Мезорівень	Механізм прийняття рішень	управління громадою, голосування, відкрите управління, модель, ланцюгове управління, демократія, управління, демократичне управління, прийняття рішень; участь у прийнятті рішень	[11], [20], [22], [23], [25], [34], [36], [37], [39], [40], [44], [59], [60], [66], [67], [70], [71], [83], [90], [92], [94], [98], [105], [106], [108], [109], [110], [111], [115], [118]
	Механізм стимулювання	заохочення, структура стимулювання, характер заохочень, інтенсивність стимулювання	
	Механізм консенсусу	механізм консенсусу, моделі консенсусу, консенсус, процес досягнення консенсусу	
Макрорівень	Організація управління	(де)централізований, розподілений, ієрархія, рівні децентралізації, ролі, членство, формування, спільний, напівцентралізований	
	Підзвітність управління	підзвітність, правила в управлінні, гарантія якості, вирішення спорів/конфліктів, алгоритмічні правила, протокол в мережі, розробка поза мережею, структура контрактів, механізм координації, нормативна база, політика, процедури, правила розпізнавання, правила змін, порушення первинних правил, колективна сфера застосування, захист даних, добре врядування, прозоре управління, залучення громадян	[10], [11], [12], [13], [15], [19], [20], [22], [25], [28], [30], [34], [35], [36], [40], [51], [55], [60], [65], [66], [67], [69], [73], [77], [79], [83], [85], [89], [95], [96], [97], [98], [99], [106], [107], [108], [114], [115], [118]
	Контроль управління	права прийняття рішень, механізми контролю, контроль блокчейну/інфраструктури, контроль через блокчейн, системи контролю, напрям, нагляд	

Додаток Б

Таблиця 1.1

Порівняння технології блокчейн з іншими видами DLT

Категорія	Blockchain	Hashgraph	DAG	Holochain
Майнінг	учасники мають можливість карбувати нові токени через різні консенсусні механізми	ноди створюють консенсус через віртуальне голосування	попередня транзакція перевіряє подальшу, щоб досягти консенсусу	ноди функціонують на індивідуальних ланцюжках отже майнери не потрібні, щоб перевірити транзакції
Кількість транзакцій у секунду	дуже обмежені в плані масштабованості та TPS	унікальні консенсусні механізми зменшують обчислювальне навантаження в плані високої масштабованості і високої TPS	унікальна структура даних забезпечує високу масштабованість і TPS	кожен нод створює свій власний реєстр звідси необмежена масштабованість і TPS
Структура даних	дані структуруються в блоках в порядку транзакцій, які перевіряються майнерами в екосистемі	віртуальне голосування забезпечує, щоб транзакції перевірялися більшістю	структура даних впливає з механізму спрямованого ациклічного графа, де кожна транзакція незалежна	дані розподіляються між різними вузлами на платформі, тому немає проблем з перевантаженням мережі
Перевірка транзакцій	майнер мають право відкласти транзакцію або скасувати її повністю	підтвердження транзакцій згідно консенсусу	успіх поточної транзакції залежить від її здатності перевіряти дві попередні транзакції	ноди опрацьовують свої власні реєстри, отже, майнери не потрібні
Час запуску	став надбанням громадськості в 2008	доступно для громадського користування з 24 серпня 2018 року	NXT – перша платформа, яка використовує DAG, і вона вийшла 9 листопада 2015 року	Alpha1 випущено 26 травня 2018 року
Мережі, працюючі на платформі	Bitcoin і Ethereum – найпопулярніші мережі, побудовані на блокчейні	Swirlds і NOIA єдині мережі на Хешграфі	NXT, Tangle і ByteBall найпопулярніші мережі, що використовують основу DAG	мережа Holochain найвідоміша мережа на цій платформі

Додаток В

Таблиця 1.1

Найбільш розповсюджені механізми консенсусу

№ з/п	Найменування	Опис
1	Proof of work (PoW) доказ виконаної роботи	Численні ноди підтверджують транзакції відповідно до алгоритму консенсусу. Щоб додати новий блок, учасник повинен довести, що він виконав певну роботу, він вирішує дуже складне завдання по знаходженню хеша (hash), який відповідає певним правилам. Перший, кому пощастило знайти правильну комбінацію, отримує можливість додати блок в ланцюжок. В результаті участь в PoW має на увазі витрати обчислювальних ресурсів, але перевагою є те, що він може бути реалізований в середовищі, де учасники абсолютно не довіряють один одному. Будь-який бажаючий може приєднатися до мережі, так як вона є блокчейном, що не вимагає дозволів. І хоча масштабованість тимчасових мереж висока, швидкість транзакцій залишається низькою. Ще одна проблема полягає в мотивації учасників мережі – вони, як правило, приєднуються, щоб розбагатіти, а не для підтримки справедливості.
2	Proof of Stake (PoS) доказ частки володіння	Технічна особливість консенсусу – відсутність складних і непотрібних обчислень. Замість того, щоб конкурувати з іншими, учасники мережі дають в заставу свої криптоактиви, і чекають, щоб їх вибрали для створення нового блоку. Учасники зацікавлені в безпеці, так як самі володіють монетами системи. Алгоритм вибирає одного валідатора, грунтуючись на долі, що йому належить. Тому якщо учасник володіє часткою в 5%, то і перевіряти буде 5% транзакцій. Ідея полягає в тому, що чим вище частка валідатора, що лежить в основі криптовалюти, тим менше у нього інтерес до маніпуляцій процесом валідації.
3	Delegated Proof of Stake (DPoS) делегований доказ частки володіння	Дозволяє створювати блоки на високій швидкості і обробляти більшу кількість транзакцій в секунду, в порівнянні з іншими алгоритмами консенсусу, за рахунок зменшення кількості валідаторів. Під час голосування власники монет вибирають валідаторів транзакцій, які будуть формувати блоки. Вага кожного голосування визначається сумою активів голосуючого. Тримачі монет можуть проголосувати за кандидатів в будь-який час. Це визначає високу стійкість мережі: якщо більшість виконавців зазнають невдачі, спільнота відразу ж проголосує за їх заміну.
4	Leased Proof of Stake (LPoS) орендований доказ частки володіння	Консенсус щодо підтвердження частки, що дозволяє власникам токенив «здавати» свої токени в повні вузли і отримувати відсоток від виплати як винагороду. На звичайній платформі, що підтверджує частку, кожен вузол може додати новий блок до блокчейну. Користувачі можуть вибирати між запуском повного вузла або орендою своєї частки до повного вузла з отриманням винагороди.
5	Proof-of-Activity (PoA) доказ активності	Протокол об'єднує протоколи PoW і PoS, що означає, що учасники можуть як майнити, так і закладати частку для валідації блоків. Отже, протокол PoA забезпечує баланс між майнерами і звичайними учасниками мережі.
6	Proof-of-Location (PoL) доказ розташування	Протокол дозволяє користувачам закріпити за собою конкретну GPS-локацію і таким чином аутентифікувати себе у мережі. Протокол опирається на BFT маячки, які записують геолокацію і маркери часу в блокчейні, що запобігає збоєм мережі і шахрайству у системі.

Продовження таблиці 1.1 Додатка В

7	Proof-of-Importance (PoI) доказ важливості	<p>Протокол діє майже як PoS, але включає в себе три компоненти:</p> <ul style="list-style-type: none"> – кількість токенів на рахунку; – активність операцій рахунку; – час, проведений власником рахунку в мережі. <p>Хоча перший параметр відіграє важливу роль в рейтингу для перевірки транзакцій, другий і третій параметри досить слабкі, але все ж допомагають встановити «важливість» облікового запису. Чим менше сума токенів, тим сильніше вплив інших параметрів. Слідчо, обліковий запис, який закладає сотні тисяч токенів, може збільшити коефіцієнт значущості майже в 3 рази через його активність і постійну присутності в мережі. З іншого боку, це не має ніякого значення для тих, хто володіє сотнями мільйонів токенів в своєму акаунті.</p>
8	Proof-of-Elapsed-Time (PoET) доказ минулого часу	<p>Ця система схожа на PoW, але споживає набагато менше електроенергії. Замість того, щоб учасники вирішували криптографічний головоломку, алгоритм працює в середовищі надійного виконання (Trusted Execution Environment, TEE), такий, як Intel Software Guard Extensions (SGX). Протокол PoET також гарантує, що блоки створюються випадково, але без будь-якої необхідної роботи. В якості вирішення пропонується гарантований час очікування згідно TEE.</p>
9	Proof of Capacity /Proof-of-space (PoC / PoSpace) доказ ресурсів	<p>Під час перевірки працездатності вузол отримує гроші на просторі жорсткого диска. Чим більше місця на жорсткому диску у вузла, тим більше шансів видобути наступний блок і заробити винагороду за блок. У системі перевірки працездатності до майнінгу алгоритм генерує великі набори даних, відомі як «графіки», які вузол зберігає на своєму жорсткому диску. Чим більше графіків у вузла, тим більше шансів знайти наступний блок у ланцюжку.</p>
10	Proof of Burn (PoB) доказ спалювання	<p>Алгоритм працює за принципом, що дозволяє майнерам «спалювати» токени віртуальної валюти. Майнери посилають монети на деяку спеціальну адресу, яка їх «спалює» – їх не можливо звідти повернути або витратити, – ця транзакція записується в блокчейні, будучи доказом спалювання монет, після чого користувач винагороджується.</p>
11	Proof of Authority (PoA) доказ авторитету	<p>Метод консенсусу, що полягає у перевірці та затвердженні блоків лише «авторитетними» користувачами. «Авторитет» визначається за допомогою вбудованої системи репутації, що є різними для різних систем. Коло користувачів з правом затвердження блоків обирається заздалегідь згідно з визначеними стандартами.</p>
12	Delegated Byzantine Fault Tolerance (DBFT) делегований протокол завдання візантійських генералів	<p>Цей алгоритм відноситься до старої задачі візантійських генералів, заснованої на реальній історичній події. Використовуючи аналогію, протоколу все одно, якщо «генерал» захворів або саботував. Система буде працювати, навіть коли нода переходить в режим офлайн. Але з огляду на тисячі валідаторів, консенсус все одно буде боротися за вирішення проблеми швидкості. Саме тому розробники запропонували делеговану модель BFT – DBFT.</p> <p>Зумовлені валідатори в цьому протоколі консенсусу дозволяють значно випередити інші протоколи. Зручно мати кілька відомих дійових осіб, які перевіряють транзакції перед випуском для інших нод. У разі, якщо валідатор «зливається», учасники можуть делегувати нову ноду. Варто зазначити, що хоч цей протокол розрахований на публічне оточення, він є більш централізованим.</p>

Продовження таблиці 1.1 Додатка В

13	Practical Byzantine Fault Tolerance (PBFT) практичний протокол завдання візантійських генералів	Протокол PBFT дуже схожий на DBFT, особливо щодо його більш централізованого характеру. Єдина відмінність полягає в тому, що перший має більш просту реалізацію, і часто працює в приватному середовищі з відомими учасниками. Коли валідатор отримує повідомлення, він повинен прийняти рішення – вірити йому чи ні. Для цього він виконує свої перевірки і після опитує всі інші ноди по черзі, чи дійсна транзакція на їхню думку. Якщо 2/3 учасників за цю транзакцію, нода її приймає і передає своє рішення в мережу для інших валідаторів. Таким чином, консенсус досягається на основі підтвердження, яке буде представлено всіма валідаторами. PBFT ефективний в системах з низькою затримкою, але дуже чутливий до кількості валідаторів і пропускну здатності, так як одне повідомлення генерує безліч інших запитів і перевірок. Він добре підходить для приватного середовища, де не потрібне велике навантаження, але є потреба у великій кількості транзакцій. PBFT гарантує остаточність рішень про транзакції в мережі, так як воно було прийнято абсолютною більшістю в кожен момент часу.
14	Federated Byzantine Agreement (FBA) Федеративна візантійська угода	Протокол не вимагає дозволу або заздалегідь відомого набору учасників, на відміну від PBFT і інших варіацій BFT. FBA дозволяє будь-кому приєднатися до мережі. Транзакції в цьому протоколі валідуються фіксованою кількістю учасників, які вибираються з тих, хто в той момент знаходяться в мережі. За правилами FBA існують Gateways (шлюзи) і Market-Makers (мейкери), які забезпечують чесність і ліквідність мережі. Перші виступають в ролі традиційних банків, які володіють фінансовими засобами і створюють їх еквівалент в віртуальних токенах. Другі – ведуть облікові записи з численними шлюзами і відразу в декількох валютах.
15	Round Robin Consensus Model Кругова модель консенсусу	Модель використовується деякими ексклюзивними блокчейн мережами. Кожен вузол (група вузлів) в заданому часовому вікні може створювати тільки кінцеве число блоків, створюючи циклічний перебор, де тільки дозволені учасники можуть створювати блоки по черзі.

Вразливості технології блокчейн

Вразливі компоненти	Можливі вразливості	Приклади атак
Криптографічні алгоритми	Bitcoin і Ethereum використовують криптографічний алгоритм Elliptic Curve Digital Signature Algorithm (ECDSA). У разі некоректної реалізації генератора випадкових чисел, який використовується для підпису, при спостереженні за публічно доступними транзакціями може бути відновлений секретний ключ для підписання транзакції. Некоректною реалізацією може бути, наприклад, використання константи в якості випадкового числа або повторне використання одного і того ж випадкового числа.	У 2018 р зловмисники викрали понад \$ 4 млн з гаманців користувачів ІОТА. Всі постраждали користувалися послугами зловмисного сайту для генерації секретних фраз.
Ключі (гаманці)	У разі втрати ключа користувачеві неможливо надати доступ до свого облікового запису. При компрометації ключа неможливо перезаписати ланцюжок блоків. Можлива атака за словником на закритий ключ (повний перебір паролів).	Поширена практика генерації закритого ключа з будь-якого тексту шляхом отримання значення хеш-функції від даного тексту. В цьому випадку, атака може бути здійснена шляхом аналізу ланцюжка транзакції блокчейна і пошуку таких адрес, закриті ключі яких збігаються з отриманими за заздалегідь підготовленим списком фраз.
Алгоритми консенсусу	Proof of work (PoW) схильний атаці 51%. Якщо в руках зловмисника знаходиться більше половини всіх обчислювальних потужностей в мережі, то він отримує контроль над її ресурсами, включаючи переписування історії, проведення транзакцій з подвійним витрачанням, блокування чужих транзакцій, підтвердження своїх блоків і т.п. Консенсус Proof of Stake (PoS) схильний атаці Long Range, в ході якої зловмисник з незначною мінорною кількістю коштів може створити велику альтернативну кількість блоків, які по довжині перевершать основний блокчейн. Основний блокчейн може бути після цього підмінений. У разі використання алгоритму консенсусу Byzantine Fault Tolerance (BFT) атака можлива, якщо скомпрометована одна третина обчислювальних ресурсів мережі.	Реорганізація блокчейна і подвійне витрачання токенів Ethereum Classic на суму \$ 460 тис. (2019 р.).

Продовження таблиці 1.1 Додатка Г

Смарт-контракти	Смарт-контракт по суті є комп'ютерною програмою, яка може містити помилки і уразливості. Особливістю є складність внесення виправлень після поширення смарт-контракту в мережі. Джерелами вразливостей є: невідповідність стандарту ERC20 (токен Ethereum), некоректна генерація випадкових чисел, невірне визначення області видимості, некоректна верифікація відправника транзакції, цілочисельне переповнення (integer overflow), помилки в бізнес-логіці, використання вразливих зовнішніх бібліотек.	Інцидент з проектом DAO в 2016 р, в результаті якого була викрадена криптовалюта на суму \$ 50 млн.
Ноди (вузли) мережі	Помилки, допущені під час налаштування інфраструктури, розгортання блокчейн платформи, віддаленому виклику процедур, налаштування політики безпеки можуть призвести до експлуатації відомих зловмисникові вразливостей з подальшим несанкціонованим додаванням транзакцій в блокчейн	Можливість проведення атаки DNS rebinding.
Компоненти інтерфейсу користувача і додатків	Блокчейн реалізується в веб середовищі і схильний до всіх вразливостей, притаманних десктопних, мобільним і веб додаткам. При проведенні Initial Coin Offering (ICO) можливі додаткові вразливості, що дозволяють провести атаку на організаторів ICO і вразливості, що дозволяють провести атаку на інвесторів	Зловмисниками практикується виконання дій від імені користувача, крадіжка облікових даних, підміна інформації про ціни, підбір PIN-коду програми, проведення фішингових атак. При виконанні операцій на трейдингових платформах можливо виконання операцій від імені користувача, крадіжка облікових даних для авторизації в додатку, введення користувача в оману шляхом підміни відображуваних цін

**Декларація
академічної доброчесності
здобувача ступеня вищої освіти ЗНУ**

Я, Заріпов Дмитро Вадимович, магістрант 2 курсу магістратури, форма навчання заочна, факультет соціології та управління, спеціальність «публічне управління та адміністрування» освітньо-професійна програма «публічне управління та адміністрування», адреса електронної пошти z.vadimovich@gmail.com,

– підтверджую, що написана мною кваліфікаційна робота на тему «Впровадження Blockchain технології до системи державного управління» відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст. 42 Закону України «Про освіту», зі змістом яких ознайомлений;

– заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;

– згоден на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, у тому числі за допомогою інтернет-системи, а також на архівування моєї роботи в базі даних цієї системи.

Дата _____ Підпис _____ ПІБ (студент) Заріпов Д.В.

Дата _____ Підпис _____ ПІБ (науковий керівник) Чайка І.Ю.