Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Світовий досвід інтеграції "смарт контрактів" в інноваційні застосунки

Виконав: студент IV курсу, групи СНзс-42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Перетятко Т.П.
(підпис) (прізвище та ініціали)

Керівник _____ Кунанець Н.Е.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Гащин Н.Б.
(підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«_10_» _червня_ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Перетятко Тарасу Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Світовий досвід інтеграції "смарт контрактів" в інноваційні застосунки

Керівник роботи Кунанець Наталія Едуардівна, д.н.с.к., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «23» березня 2021 року № 4/7-172

2. Термін подання студентом завершеної роботи 13 червня 2022р.

3. Вихідні дані до роботи Наукові публікації про "смарт контракти" та їх застосування в інноваційних застосунках

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Старт-контракти. Опис та аналіз предметної області. 1.1 Означення сутностей предметної області. 1.2 Смарт-контракти, поняття, терміни та визначення. 1.3 Класифікація смарт-контрактів. 1.4 Інформаційно-технологічні платформи для запровадження смарт-контрактів. 2. Аналіз світового досвіду запровадження смарт контрактів в інноваційні застосунки. 2.1 Розумні контракти для децентралізованих автономних організацій. 2.1.1 Використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій. 2.1.2 Організаційні переваги смарт-контрактів. 2.1.3 Застосування та варіації смарт-контрактів. 2.2 Безпека смарт-контрактів. 2.3 Практика запровадження смарт-контрактів. 2.4 Перспективи подальших досліджень. 3. Безпека життєдіяльності, основи охорони праці. Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Тема та мета дослідження. 3. Завдання дослідження. 4. Актуальність дослідження. 5. Смарт-контракт. 6. В контексті Блокчейну «розумними» контрактами є. 7. Застосування бізнес-логіки зі смарт-контрактами. 8. Опис елементів структурної схеми. 9. Смарт-контракти в публічних та приватних блокчейнах. 10. Децентралізована криптовалюта з інтегрованими смарт-контрактами. 11. Ключові етапи процесу перевірки з використанням смарт-контрактів та DLT. 12. Переваги смарт-контрактів. 13. Висновки. 14. Доповідь завершено.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик Олег Ярославович, доцент	04.04.2022	01.05.2022

7. Дата видачі завдання 24 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Підбір джерел про смарт-контракти, Блокчейн та	04.01.2022-30.01.2022	*Виконано*
	розподіленої книги.		
3.	Переклад та опрацювання джерел про смарт-	31.01.2022-06.02.2022	*Виконано*
	контракти, Блокчейн та розподіленої книги.		
4.	Виконання дослідження щодо аналізу Світового	07.02.2022-13.02.2022	*Виконано*
	досвіду інтеграції смарт контрактів в інноваційні		
	застосунки.		
5.	Оформлення розділу «Старт-контракти. Опис та	14.02.2022-06.03.2022	*Виконано*
	аналіз предметної області».		
6.	Оформлення розділу «Аналіз світового досвіду	07.03.2022-03.04.2022	*Виконано*
	запровадження смарт контрактів в інноваційні»		
	застосунки		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	04.04.2022-17.04.2022	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	18.04.2022-01.05.2022	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат	03.06.2022	*Виконано*
12.	Попередній захист кваліфікаційної роботи	07.06.2022	*Виконано*
13.	Захист кваліфікаційної роботи	13.06.2022	

Студент _____ Перетятко Т.П.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кунанець Н.Е.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Світовий досвід інтеграції "смарт контрактів" в інноваційні застосунки // Кваліфікаційна робота освітнього рівня «Бакалавр» // Перетятко Тарас Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНзс-42 // Тернопіль, 2022 // С. 45, рис. – 7, табл. – 2, кресл. – 14, бібліогр. – 53.

Ключові слова: Смарт-контракт, Блокчейн, угода, інтеграція, інформаційні технології, характеристики.

Кваліфікаційна робота присвячена аналізу світового досвіду інтеграції "смарт контрактів" в інноваційні застосунки. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є підвищення ступеня поінформованості про особливості використання та інтеграції цифровізованих угод.

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» подано означення сутностей предметної області. Наведено поняття, терміни та визначення смарт-контрактів. Подано класифікацію смарт-контрактів. Описано та охарактеризовано інформаційно-технологічні платформи для запровадження смарт-контрактів.

В другому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» проаналізовано розумні контракти для децентралізованих автономних організацій. Розглянуто використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій. Описано організаційні переваги смарт-контрактів. Подано застосування та варіації смарт-контрактів. Висвітлено питання безпеки смарт-контрактів. Проаналізовано практику запровадження смарт-контрактів. Висвітлено перспективи подальших досліджень.

ANNOTATION

World experience of "smart contracts" integration into innovative applications // Qualification work of the educational level "Bachelor" // Peretiatko Taras Petrovych // Ternopil Ivan Pulyuy National Technical University, Computer information systems and software engineering faculty, Computer science department, Group SNzs-42 // Ternopil, 2022 // P. 45, fig. - 7, tabl. - 2, chair. - 14, ref. - 53.

Keywords: Smart contract, blockchain, agreement, integration, information technology, characteristics.

The qualification work is devoted to the analysis of the world experience of integration of "smart contracts" into innovative applications. The purpose of this qualification work of the educational level "Bachelor" is to increase awareness of the peculiarities of the use and integration of digitized transactions.

In the first section of the qualification work of the educational level "Bachelor" the definition of the essences of the subject area is given. The concepts, terms and definitions of smart contracts are given. The classification of smart contracts is given. Information and technology platforms for the implementation of smart contracts are described and characterized.

In the second section of the qualification work of the educational level "Bachelor" reasonable contracts for decentralized autonomous organizations are analyzed. The use of smart contracts for the formation of information technology platforms of enterprises and organizations is considered. The organizational advantages of smart contracts are described. Applications and variations of smart contracts are presented. The issue of security of smart contracts is covered. The practice of introducing smart contracts is analyzed. Prospects for further research are highlighted.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

ВЕФ – Всесвітні економічні форуми.

FI (англ. Finansial Institution) – фінансова установа.

DApps (англ. Decentralized Applications) – децентралізовані застосунки.

DDAO (англ. Digital Decentralized Autonomous Organization) – цифровая децентралізована автономна організація.

DLT (англ. Distributed Ledger Technology) – технологія розподіленої книги.

PCA (англ. Principal Component Analysis) – метод головних компонент.

KYC (англ. Know Your Customer) – «знай свого клієнта».

ISDA (англ. International Swaps and Derivatives Association) – Міжнародна асоціація свопів і деривативів.

ЗМІСТ

ВСТУП

Актуальність теми. Контракти – це угоди, які передбачають переміщення активів або вартості від одного власника до іншого на основі набору умов між людьми або речами. Враховуючи той факт, що установи та організації зазвичай є основоположними довіреними органами урядування, частина їх центральних операцій може бути переведена в розумні контракти, які контролюються децентралізованою згодою на основі Блокчейн.

Розумні контракти усувають потребу двох сторін залежати від центрального органу, оскільки вони можуть «домовлятися» між собою, визначати умови та наслідки угоди програмно та умовно, з автоматичним вивільненням активів під час виконання послуг у послідовному порядку або нести штрафні санкції. якщо не виконано. Тому актуальним напрямом досліджень є аналіз світового досвіду інтеграції смарт контрактів в інноваційні інформаційно-технологічні застосунки. Доцільно проаналізувати, як установи та організації можуть використовувати інформаційну технологію смарт-контрактів шляхом інтеграції програмно-алгоритмічних кодів смарт-контрактів та основі Блокчейну для нагляду за угодами та процесами їх виконання.

Мета і задачі роботи. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є підвищення ступеня поінформованості про особливості використання та інтеграції цифровізованих угод. Для досягнення поставленої мети потрібно:

– Проаналізувати стан досліджень в галузі смарт-контрактів.

– Сформувати класифікація смарт-контрактів.

– Проаналізувати характеристики інформаційно-технологічних платформ для запровадження смарт-контрактів.

– Описати використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій.

– Проаналізувати організаційні переваги смарт-контрактів.

Практичне значення одержаних результатів. На основі проведеного аналізу наукових літературних джерел сформовано структурну схему застосування бізнес-логіки зі смарт-контрактами. Сформовано класифікацію смарт-контрактів. Подано інтегральну характеристику смарт-контрактів в публічних та приватних блокчейнах. Розроблено перелік ключових етапів процесу перевірки з використанням смарт-контрактів та DLT. Подано характеристичний опис переваги смарт-контрактів.

РОЗДІЛ 1. СТАРТ-КОНТРАКТИ. ОПИС ТА АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Означення сутностей предметної області

Договір надає сторонам набір прав та обов’язків, які використовуються серед іншого для формалізації довгострокових відносин [1]. Це дуже корисно в середовищі, де відносини процвітають на основі довіри. Водночас, ліцензії використовуються для надання сторонам дозволу на здійснення діяльності з продуктами або майном, які в іншому випадку були б незаконними. Ліцензія може бути надана стороною («ліцензіаром») іншій стороні («ліцензіатом») як форма угоди між цими сторонами [2]. Ліцензіар може дати дозвіл ліцензіату на копіювання та розповсюдження захищених авторським правом творів, наприклад:

– програмного забезпечення;
– даних;
– алгоритмів;
– видобутих знань;
– творів цифрового мистецтва тощо.

Серед різноманітних визначень [3] договір – це добровільна, навмисна та юридично обов’язкова або дійсна угода між двома сторонами. Закон вважатиме договір дійсним, якщо він містить усі наступні елементи:

– пропозиція та акцепт;
– намір між сторонами створити зобов'язальні відносини;
– комісія, яка буде сплачена за дану обіцянку;
– дієздатність сторін;
– справжня згода сторін;
– законність угоди.

Угода, в якій відсутній один або декілька зазначених елементів, не є дійсним договором [3]. Контракти, як правило, підлягають виконанню

незалежно від того, в письмовій формі чи ні, хоча письмовий договір захищає всі його сторони. Деякі договори, наприклад, купівля-продаж нерухомості, оренда, розстрочка фінансування автомобілів або поліси страхування житла, мають бути укладені у письмовій формі, щоб бути юридично невідкличними та підлягати виконанню [4]. Якщо є порушення договору, наприклад, невиконання, неякісне виконання або часткове виконання, незадоволена сторона або сторони в більшості випадків покладаються на суд або третю сторону для забезпечення виконання контракту. Одна з останніх інновацій в галузі інформаційних технологій – Блокчейн, означив, що деякі юридичні контракти тепер можуть стати «розумними» [5].

Ідея смарт-контрактів була висунута в 1994 році, коли Сабо [6], криптограф, який повідомляв про створення основи Біткоїна та вперше сформулював термін «розумний контракт» [7]. Ці автоматизовані контракти в основному працюють, як і оператори «if-then» будь-якої іншої комп’ютерної програми.

1.2 Смарт-контракти, поняття, терміни та визначення

На даний час існують різні визначення того, що таке смарт-контракт. Розглянемо деякі з них. За даними Ідельберґер [8], смарт-контракт – це комп’ютерна програма, яка підтримує умови контрактної угоди, а також реалізує угоду, забезпечуючи довіру, прозорість та порозуміння між сторонами. Смарт-контракт можна вважати лише декларативною назвою для комп’ютерного коду, який працює на основі Блокчейн та взаємодіє з його станом [9]. Тому в контексті Блокчейну «розумними» контрактами є [10]:

– Попередньо написана та самостійно виконана комп’ютерна програма.

– Збережена та відображена на спільній платформі сховища, тобто в Блокчейні, інформація.

– Виконані мережею комп’ютерів, зазвичай тих, що працюють у Блокчейн-мережі, операції.

– Зарахування транзакцій блокчейну.

– Інтерпретація та запис даних в базу даних Блокчейнів та оновлення книги, наприклад, перекази криптовалюти.

Подані визначення означають, що смарт-контракти – це комп'ютерні коди, які знаходяться в Блокчейні та при потребі реалізуються, запускається і підтверджується множиною комп'ютерів для забезпечення достовірності. Водночас немає потреби в посередниках чи проміжних компаніях [11] з використанням вбудованого в Блокчейн комп'ютерного коду для формулювання, перевірки та виконання угод між довіреними сторонами. Деякі автори називають це «розумним юридичним договором» [12]. Інші наголошують, що програми можуть замінити юристів та банки для обробки певних повторюваних фінансових операцій у перспективі [7]. Якщо Блокчейни дають розподілене надійне сховище даних, то розумні контракти дають розподілені надійні судження [10]. Автори [8] подають приклади практичного використання розумних контрактів:

– Ліцензування та банківські функції – «Automated Escrow», «Savings».

– Децентралізовані ринки – «OpenBazaar», www.openbazaar.org.

– Ринки прогнозування – «Augur», www.augur.net.

– Розподіл гонорарів за музику – «Ujo», www.ujomusic.com.

– Кодування віртуальної власності – «Ascribe», www.ascribe.io.

Блокчейни можуть запускати код. Перший тип блокчейнів був створений для здійснення транзакцій з цифровою валютою – токенами, схожими на валюту. Потім з'явилися методи, які дозволили блокчейну виконувати складні завдання, визначені повноцінними мовами програмування [13].

Оскільки зазначені програми працюють на Блокчейні, це робить їх несхожими на інші типи програмного забезпечення. По-перше, сама програма реєструється в блокчейні, отже, має унікальну підтримку Блокчейну [13]. Блокчейни можуть автоматизувати повідомлення, додаючи фрагменти коду. Ці фрагменти коду називаються «розумними контрактами», в них. використовується логіка «якщо-це-то-то». Виконання смарт-контрактів жодним

чином не передбачає використання будь-якої людини. Смарт-контракти децентралізовані і вони, як правило, працюють без будь-якого регулювання посередників або третьої сторони. Вони використовують розподілену базу даних, щоб учасники могли перевірити, чи відбулася цифрова подія, не вимагаючи посередників або третьої сторони. Смарт-контракти не написані юридичними мовами – це комп'ютерні програми, які мають здатність визначати суворіші правила [14].

Програмне забезпечення може самостійно керувати активами блокчейну. Воно може фактично зберігати та розподіляти частини криптовалюти. Програма запускається блокчейном, тобто вона завжди працюватиме так, як задумано, і ніхто не може перешкодити чи змінити її роботу [13].

Для більшості розробників програмного забезпечення термін «розумні контракти» доволі часто використовується для позначення коду інтегрованого до Блокчейну. Це є сприйняттєвою проблемою, оскільки практично кожен громадянин може прочитати паперовий контракт, але не кожен зможе прочитати та повністю зрозуміти смарт-контракт [13], оскільки не кожен громадянин є розробником програмного забезпечення.

Смарт-контракти можна кодувати, щоб відображати керовану даними бізнес-логіку. Вона може, наприклад, включати:

– визначення пріоритетності структурованого погашення;
– забезпечення кредиту;
– голосування за повідомлення на форумі [14].

Початкові теорії Сабо про те, як можуть працювати розумні контракти, на даний час залишилися нереалізованими, оскільки ще не розроблено інформаційної технології для підтримки програмованих угод і транзакцій між сторонами. Існували дві основні проблеми, які потрібно було вирішити, перш ніж розумні контракти можна було використовувати в реальному світі. По-перше, контроль фізичних активів за допомогою смарт-контрактів, щоб мати можливість забезпечити виконання угод. По-друге, відсутність надійних

комп’ютерів, які є надійними та довіреними для виконання контракту між двома або більше сторонами [12].

На рисунку 1.1 показана структурна схема застосування бізнес-логіки за допомогою смарт-контрактів.

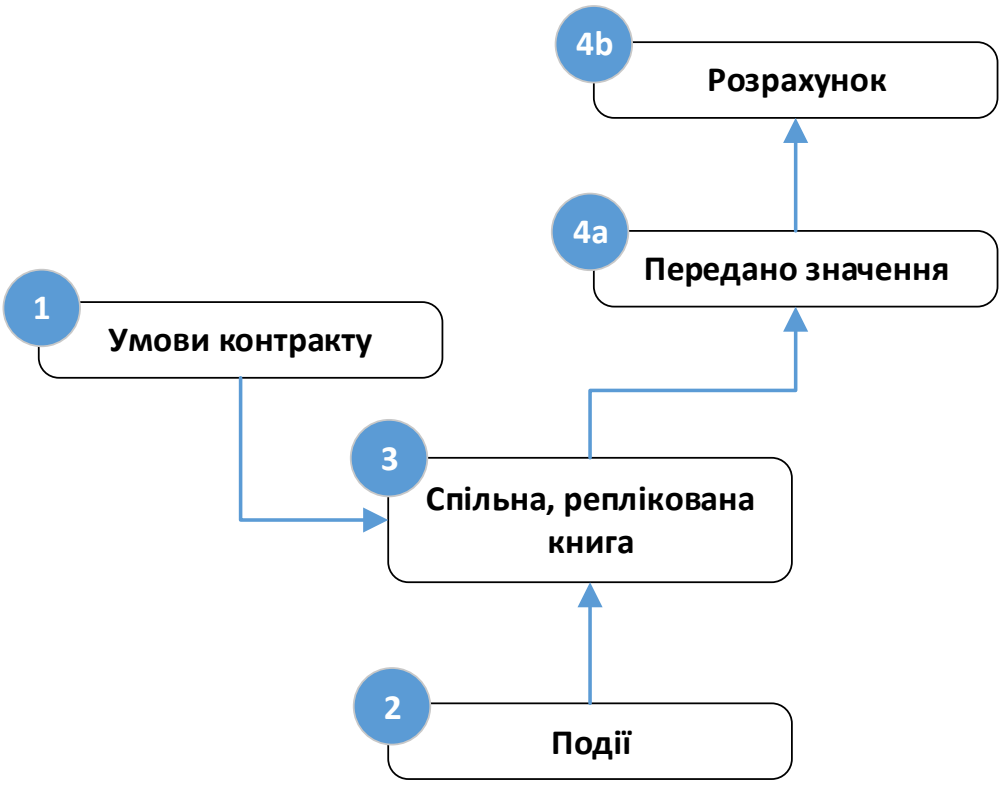

Рисунок 1.1 – Структурна схема застосування бізнес-логіки зі смарт-контрактами [15]

Подані на рис. 1.1 позначення елементів прокоментовано таблиці 1.1. Зокрема, блок 1 – «Умови контракту». При цьому контрагенти встановлюють зобов’язання та розраховують інструкції, активи передаються під опіку смарт-контракту та вказуються умови виконання.

Блок 2, позначає подію. Події можуть посилатися на ініційовані транзакції або отриману інформацію та ініціювати виконання контракту.

Блок 3, позначає сутність «бізнес-логіка», яка визначає як рух вартості диктується умовами контракту.

Таблиця 1.1 – Опис елементів структурної схеми. Адаптовано з [15]

Номер	**Назва події**	**Опис**
1	Умови договору	Контрагенти встановлюють зобов'язання та розрахункові інструкції. Активи, передані під охорону смарт-контракту. Умови виконання («Якщо… то…»).
2	Події	Подія ініціює виконання контракту. Подія може стосуватися ініційованої транзакції або отриманої інформації.
3	Бізнес-логіка	Бізнес-логіка (Умови контракту) визначає рух вартості на основі виконаних умов.
4a	Передано значення	Вартість передана передбачуваному одержувачу відповідно до умов контракту. Для цифрових активів у ланцюжку. Біткоїн-рахунки розраховуються автоматично.
4b	Розрахунок	Для активів, представлених поза ланцюгом (наприклад, цінні папери), рахунки поза мережею відповідають інструкціям щодо розрахунків. Зміни в рахунках будуть відображені в книзі.

Елемент 4a – «Передано значення», визначає як вартість передається передбачуваному одержувачу відповідно до умов контракту. Водночас, блок 4b – «Розрахунок», визначає активи, представлені поза ланцюжком, наприклад, цінні папери. Містить інструкції щодо розрахунків за межами мережі.

Сфери актуальності смарт-контрактів для фінансового сектора:

– кредитування;
– ринок капіталу;
– бронювання торгівлі;

– контроль гаманців криптовалюти.

Зростання смарт-контрактів було експоненційно швидким, і дотепер створення смарт-контрактів здійснювалося в основному для регулярного здійснення свопів і деривативів. Декілька проектів із відкритим кодом, зокрема «Counterparty» [16] та «Ethereum» [17], досягли суттєвого інформаційно-технологічного прогресу достатнього, щоб створити мови програмування для обслуговування найсучасніших смарт-контрактів.

Потенціал технології Блокчейн і смарт-контрактів виходить за рамки фізичної передачі грошей від однієї сторони до іншої. Підключивши смарт-контракти до Інтернету речей (IoT), їх можна використовувати для виконання дій з фізичними речами, наприклад, щоб розблокувати двері автомобіля.

Традиційний юридичний контракт визначає правила щодо угоди між декількома людьми або сторонами. Розумні контракти фактично забезпечують дотримання цих правил, контролюючи передачу валюти або активів за певних умов [18]. Розумні контракти та ліцензії децентралізують модель довіреної сторони або особи. Однак є проблеми, пов’язані зі смарт-контрактами, зокрема:

– Гнучкість – оскільки розумні контракти вважають, що все, що стосується переговорів на початку переговорів, можуть вирішувати учасники – це іноді буває неточним.

– Відповідальність – внаслідок відсутності посередників регулятори можуть зіткнутися з певним рівнем труднощів.

– Забезпечення – наразі буде досить складно, якщо взагалі можливо, структурувати всі умови транзакції за допомогою повної опори на розумні контракти) [14].

Одним із перших ринків, на якому очікується, що розумні контракти будуть функціонувати, є синдиковані позики, оскільки цей ринок з капіталізацією понад чотири трильйони доларів, працює на факсах, електронній пошті та електронних Excel-таблицях [19]. «Розумна» власність вимагає контролю власності на фізичне майно та нефізичну власність, наприклад, акції компанії [20].

1.3 Класифікація смарт-контрактів

Блокчейн-мережі «Ethereum» та «Bitcoin» мають обмеження на введення та виведення через вимоги безпеки. Зокрема обмежено доступ до зовнішніх даних, наприклад, ціни, погоди, місцезнаходження тощо. Ці дані необхідні для виконання контракту та форм оплати сторонам, які беруть участь в контракті. Для виконання деяких розумних контрактів потрібні надійні посилання на зовнішні джерела даних. Тому, смарт-контракти можна розділити на детерміновані та недетерміновані смарт-контракти.

Детерміновані смарт-контракти не залежать від зовнішньої інформації, крім інформації про блокчейн, у якому вони існують, запускаються та ефективно працюють. Мережа Блокчейн, яка сприяє смарт-контракту, має достатньо інформації для прийняття рішень. Наприклад, однорангова лотерея – кошти зберігаються в Блокчейн-мережі, а випадкові числа ґенеруються кодом смарт-контракту. Після закінчення лотереї кошти перераховуються на рахунок переможця через його адресу в Блокчейн-мережі [21].

У недетермінованих смарт-контрактах мережа, яка сприяє коду смарт-контракту, не має достатньої інформації для прийняття рішень. Необхідна третя сторона, яку зазвичай називають «оракл». Наприклад, рішення щодо потоку цінностей на основі поведінки людини, подій або прогнозів. Проте дослідження показали, що використання зовнішнього стану не завжди викликає потребу довіряти додатковій стороні [22]. Наприклад, у сценарії оновлення водійських прав уряд все одно є довіреною стороною, тому використовується уряд як «оракул» перевірки, який додає зовнішній стан в Блокчейн [22].

«Оракли» в інформатиці здатні надавати інформацію ззовні системи, яку сама система не може отримати. При застосуванні до мереж смарт-контрактів «оракули» діють як програмовані агенти, які надають смарт-контракту необхідні дані – вхідні «оракули» і діють від його імені, виконуючи платіж або повідомляючи зовнішнім системам, що смарт-контракт укладено – вихідні «оракли» [23]. «Оракли» зберігають та передають в смарт-контракт лише

важливі та релевантні дані. Це забезпечує безпеку та високу конфіденційність мережі, підвищує ефективність.

Зазвичай бажані застосунки смарт-контрактів містять певний ступінь недетермінізму. У будь-якому випадку, якщо «оракли» є федеративними, то смарт-контракт все одно знижує ризик шахрайства. Приклад джерела надійних інформаційних каналів – термінал Bloomberg. Тому недетерміновані смарт-контракти добре відображаються в застарілих системах.

Канонічний приклад недетермінованого смарт-контракту – сценарій ставок на спорт, коли система не може точно знати, яка команда виграла гру. Учасники повинні домовитися про довірену третю сторону – «оракл» для надання результату. Безпека системи зводиться до надійності джерела [23]. Оскільки смарт-контракти є комп'ютерними програмами, не потрібно було б додавати складніші елементи ставок – коефіцієнти та диференціали результатів [7]. Однак можна визначати правило, шанси та умови передачі вартості. Ми можемо використовувати ретельно продумані процеси для небажаної поведінки, наприклад, об'єднання «оракла» або арбітражного процесу [21]. Компанії «Augur» і «TruthCoin» аналізують шляхи покращення моделі довіри для «ораклів» за допомогою аналізу основних компонентів (PCA).

1.4 Інформаційно-технологічні платформи для запровадження смарт-контрактів

Для створення децентралізованих застосунків (DApps) з'явилися платформи «Eris», «Ripple», «Ethereum», «Nxt» тощо [22] та мови програмування «Solidity» і «Serpent» [24]. Однак не всі Блокчейн-платформи забезпечують достатню гнучкість для розробки смарт-контрактів [10]. У таблиці 1.2 подано порівняльну характеристику Блокчейн-платформ.

Платформа Біткоїн підходить для обробки транзакцій з криптовалютою, але має низькі обчислювальні можливості. У Біткоїн існує обмежена можливість додавати або реалізовувати будь-яку розширену логіку [25].

Таблиця 6.1 – Смарт-контракти в публічних та приватних блокчейнах [10]

Блокчейни без смарт-контрактів	**Блокчейни зі смарт-контрактами**	**Блокчейни з розумними контрактами Тьюринга**
Послуга		
Дисперсне сховище	Дисперсні обчислення– має здатність обчислювати попередньо визначену логіку	Дисперсні обчислення – має здатність обчислювати будь-яку логіку
Інформаційно-технологічні платформи		
«Bitcoin» – публічний «Litecoin» – публічний «Multichain» – приватний	«NXT» – загально-доступний	«Ethereum» – публічний «Eris» – приватний «Clearmatics» – приватний

Наприклад, у «Біткоїн» можна додати логіку, яка вимагає кількох підписантів до транзакції перед оплатою. Але, при цьому, потрібно буде внести зміни до функцій майнінгу та схем стимулювання майнінгу, щоб задіяти розумні контракти на Блокчейні біткоїнів. «Sidechains» – підключені до «Bictoins blockahin» Блокчейни, можуть забезпечити розумні контракти з можливістю передачі вартості з основного Блокчейну в бічний. Бак [26] стверджує, що «сайдчейн» дозволяє передавати біткоїни та інші активи книги між декількома Блокчейнами.

«NxT» – це публічна Блокчейн-платформа, яка містить інтегровані та діючі смарт-контракти. Однак вона не «завершена Тьюрингом» тому, що не дозволяє розробляти налаштовані смарт-контракти. Зараз потрібно використовувати існуючі шаблони.

«Ethereum» – це публічна Блокчейн-платформа, яка наразі є найдосконалішою системою кодування «за Тьюрингом». «Ethereum» містить функціональні можливості реалізації смарт-контрактів [27]. Індивідуальні

смарт-контракти можна розробляти та розгортати у всій Блокчейн-мережі. Льюїс [10] стверджує, що існують механізми запобігання зловживанням. Тому користувачі повинні платити за обчислювальну потужність в «Ethereum», передаючи токени «ether», як оплату для майнерів що запускають код. «American Express», «Deloitte», «Goldman Sachs», «MasterCard» і Нью-Йоркська фондова біржа інвестували мільйони доларів у блокчейн-компанії, зокрема в «Ethereum» [27].

У рівноправній фінансовій книзі для кожної операції необхідно підтримувати абсолютну суму коштів, інакше суб'єкти матимуть можливість вільно розподіляти стільки грошей, скільки вони захочуть. На даний момент часу існують дві провідні парадигми, сформовані Біткоїн та «Ethereum» [9].

Перша парадигма – метод Bitcoin перевіряє кожну транзакцію на основі:

– записів бази даних, видалених транзакцією;

– зґенерованих записів.

У фінансовій книзі правило стверджує, що загальна частка коштів у видалених записах має дорівнювати загальній кількості тих, що були створені.

Друга парадигма, сформована «Ethereum» – це розумні контракти. Програмний код смарт-контрактів повинен виконувати всі зміни в даних контракту. У традиційних базах даних це можна визначити як примусову збережену процедуру.

Дані смарт-контрактів змінюються запитами користувачів, надісланими до їх коду. Потребу і як виконувати ці запити, вирішується кодом смарт-контрактів (див. рисунок 1.2). Код смарт-контракту для фінансової книги виконує ті самі три операції, що контролер централізованої бази даних:

– перевірка наявності задовільних коштів

– зняття коштів з одного рахунку

– додавання на баланс іншого рахунку.

Зазначені парадигми є адекватними. Висока розпаралеленість та продуктивність забезпечуються обмеженнями Біткоїн-транзакцій, а висока гнучкість та адаптивність забезпечується смарт-контрактами «Ethereum» [9].

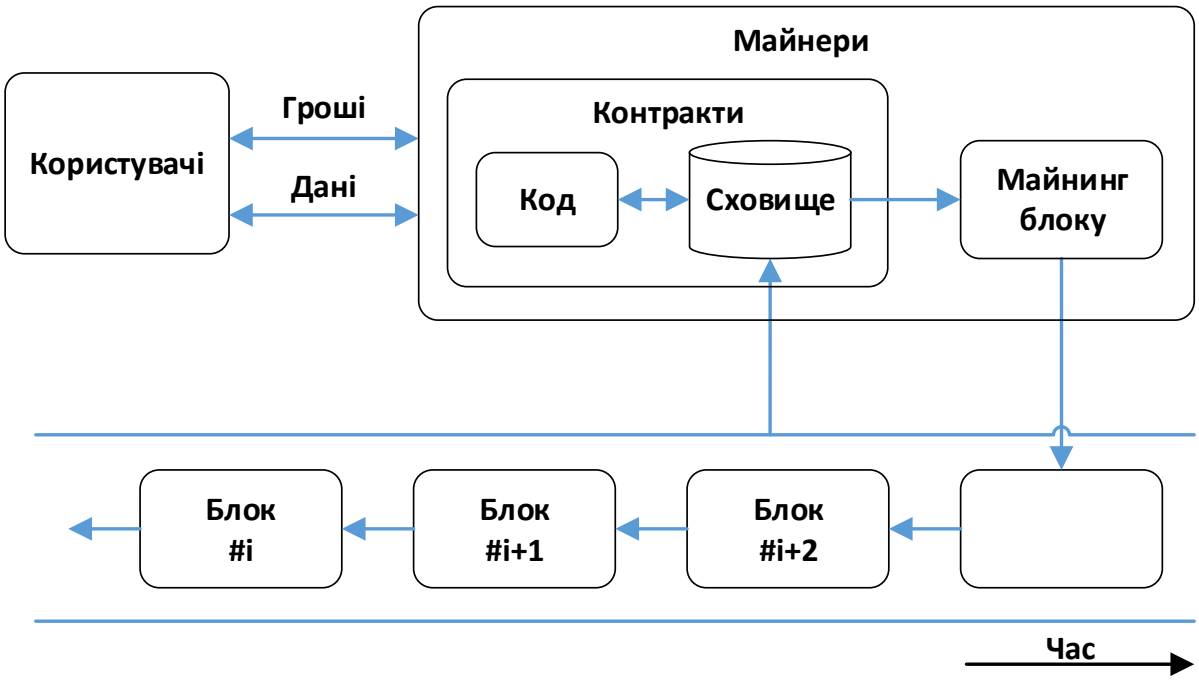

Рисунок 1.2 – Децентралізована криптовалюта з інтегрованими смарт-контрактами [28]

Коулу [29] наводить приклад недетермінованого смарт-контракту між двома сторонами, розробленого з використанням мови програмування «Solidity» та розгорнутого в Блокчейн-мережі «Ethereum». Поданий приклад демонструє, що простий договір між двома сторонами можна перевести в рядки коду – «код смарт-контракту».

1.5 Висновок до першого розділу

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» подано означення сутностей предметної області. Наведено поняття, терміни та визначення смарт-контрактів. Подано класифікацію смарт-контрактів. Описано та охарактеризовано інформаційно-технологічні платформи для запровадження смарт-контрактів.

РОЗДІЛ 2. АНАЛІЗ СВІТОВОГО ДОСВІДУ ЗАПРОВАДЖЕННЯ СМАРТ КОНТРАКТІВ В ІННОВАЦІЙНІ ЗАСТОСУНКИ

2.1 Розумні контракти для децентралізованих автономних організацій

За даними Метта Левіна з «Bloomberg» [11], найкращі можливості для смарт-контрактів закладені в бізнес-організаціях. Здатність Блокчейну усунути виключні вимоги щодо довіри дозволить громадянам перестати працювати в старих організаціях, натомість кожна особа буде суб'єктом у комерційній системі, що працює на Блокчейні. Функції керівників і правління компанії можна звести до смарт-контрактів, реалізованих у комп'ютерних програмах. Інвестори можуть приймати рішення щодо електронного голосування. Така децентралізована організація буде звільнена від зовнішнього впливу, оскільки вона працюватиме саме так, як було запрограмовано.

Старий спосіб досягнення угод передбачає, що група людей збиралася разом, щоб створити організацію з комерційною метою, інша група вклала інвестиції, щоб керувати нею, інші керували бізнесом, а ще інші працювали на нього та вирішували, як розподілити вигоди або прибуток на підприємстві [11].

Новий спосіб полягає в тому, що група людей вкладає свої гроші в компанію, організовану за допомогою смарт-контрактів, без будь-яких складних рішень, які потрібно приймати в майбутньому, крім того, як отримати свої гроші, якщо хакери їх викрадуть. Дослідження [11] показали, що люди погоджуються з передумовою, що підхід смарт-контрактів кращий за попередній підхід, який вимагає діяльності людини.

Найбільшою проблемою, з якою стикаються перпективи смарт-контрактів в організаціях, це людський фактор [30]. Людям подобається свобода. Блокчейн повинен знайти спосіб відокремити їх від організаційної ієрархії та, натомість, не підкоряти їх новому лідеру – Блокчейну. Однак смарт-контракти не слід недооцінювати. Деякі ідеї щодо використання смарт-контрактів дивовижні.

Фінансові служби «Toyota» експериментують з ідеєю підключити смарт-контракти на основі Блокчейну до автомобілів, щоб люди не пропускали платежі по фінансуванню автомобіля. Сформовано модель, якщо було пропущено регламентне обслуговування авто, то автомобіль не ввімкнеться, і право власності на автомобіль може бути передано новому власнику. Але люди воліють використовувати цей варіант для фінансування свого автомобіля, тому що вони отримають кращу угоду за дешевшою ціною без необхідності звертання до банку або інвестора, який виступає посередником [31], вони будуть платити безпосередньо «Toyota», і це зменшить стороннє фінансування.

Смарт-контракти діють в режимі реального часу і зменшують ймовірність людських помилок та процесів, схильних до шахрайства, підвищують конфіденційність та надійність. Це, безсумнівно, особливості смарт-контрактів, які можна додати до існуючих бізнес-процесів для підвищення ефективності. Компанія «SmartContract» [23], що базується в Сан-Франциско, розробила інформаційну технологію, здатну підключати смарт-контракти до зовнішніх каналів даних, внутрішньої інфраструктури та зовнішніх платежів.

Смарт-контракти можна використовувати для побудови внутрішніх та зовнішніх організаційних відносин, одночасно дотримуючись бізнес-правил, покращуючи ефективність та внутрішню продуктивність між відділами і зовнішніми організаціями, наприклад, між постачальниками та акціонерами.

2.1.1 Використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій

Для бізнесу важливо підтримувати добрі відносини між підприємствами, постачальниками та інвесторами, які надають кредитні особливості, необхідні для управління організацією. Саме тут допоможуть розумні контракти. Організації можуть підключити інфраструктуру до смарт-контрактів та продовжувати використовувати існуючі IT-системи для позаланцюжкових даних і звітів, але підключати ці системи за допомогою смарт-контрактів [23] та

дозволяючи їм виконувати дії в життєвому циклі смарт-контракту. Різні застосунки в системі корпоративного програмного забезпечення, наприклад, «SAGE», «SAP ERP» тощо, можуть бути пов’язані з розумним контрактом, що зменшує навантаження на персонал. Це дозволить персоналу зосередитися на клієнтах, а не виконувати повторювані завдання, які знижують мотивацію та обмежують персонал. Слід звернути увагу на запуск систем і перевірку записів вручну, оскільки вони передбачають можливість шахрайства. Корпоративні системи зможуть автоматично перевіряти запаси на основі збережених даних, отриманих з «Oracle», та закуповувати необхідне в постачальників при потребі.

При взаємодії з контрактом можна сформувати запити про конкретного постачальника [31], наприклад:

– Чи завершив постачальник доставку в належний час та відповідно до бюджету?

– Як постачальник працював у минулому?

Такі прототипи тепер можуть бути реалізовані практично, оскільки будівельні блоки існують у блокчейнах із підтримкою смарт-контрактів.

Смарт-контракти можуть автоматично здійснювати прямі платежі постачальникам без необхідності чекати часу обробки банками, коли доставка товарів була перевірена, залежно від бізнес-правил організації, запрограмованих у коді смарт-контракту.

Всесвітній економічний форум стверджує [32], що оскільки блокчейн дозволяє безвідкличним транзакціям здійснюватися в режимі реального часу, то ризик контрагента може бути усунений, а витрати на транзакції можуть бути значно знижені. Постачальники зможуть отримувати оплату в режимі реального часу, а закупівлі стануть швидшими для бізнес-організацій. Смарт-контракти можуть використовуватися для розробки «розумних цінних паперів»:

– смарт-облігацій;

– акцій;

– інших фінансових інструментів.

Вони можуть обслуговувати себе протягом усього життєвого циклу, наприклад, виплачуючи власні купони та дивіденди та бути власними зберігачами. Це може дати змогу співробітникам організації стати її акціонерами, мотивувати досягнення успіху та реалізувати свій потенціал – «децентралізована та ефективна організація» [32].

Смарт-контракти високофективні в галузях, де точний моніторинг та виконання контрактів з високою вартістю є критичними. Через надзвичайно низьку вартість обслуговування повністю автоматизованого смарт-контракту в перспективі значний прибуток отримають:

– страхування [33];
– похідні фінансові інструменти [34]
– фінансування торгівлі [35].

Відповідно до заснованого в Сан-Франциско «SmartContract», замість того, щоб декілька людей з різних відділів викликали джерело даних або перевіряли веб-ресурси на наявність інформації щодо ціни, геолокації та метеофакторів для підтвердження виконання, сам контракт може автоматично перевіряти наявність підтвердження виконання [23].

На смарт-контракти можуть посилатися декілька приватних систем у різних компаніях, які є учасниками контракту. Це що робить смарт-контракт єдиною точкою «істини», захищеною від несанкціонованого доступу, і на яку можна покладатися, щоб ініціювати події платежів, обліку та відповідності внутрішнім системам [23]. Асоціація семи банків, включно з «CIBC» і «Santander», стала одною з перших фінансових установ у світі, які перевели реальні гроші за кордон за допомогою Блокчейну [36].

Банки конвертують гроші в цифрову валюту «Ripple» і здійснюють транзакції в режимі реального часу. Слід враховувати, що глобальна фінансова система складається з великої кількості комп’ютерів, які вказують, скільки грошей у кожного, а транскордонний платіж просто оновлює стан комп’ютерів, щоб вказати, що в одному банку більше грошей, а в іншому – менше. Звичайний фінансовий процес повинен тривати п’ять днів – це займає багато

часу, дозволяє легко зрозуміти, чому люди так захоплюються блокчейном, незважаючи на всі хаки [36].

Дослідники підкреслюють переваги створення та використання розумних контрактів в організаціях. Зокрема, в дослідженні корпоративного управління [37] автор стверджує, що розумні контракти на блокчейні допоможуть знизити витрати на торгівлю та забезпечити чіткіші записи щодо прав власності акціонерів, дозволяючи при цьому чітку та прозору передачу акцій у режимі реального часу від одного власника до іншого.

Менеджерська власність могла б стати набагато прозорішою, оскільки інсайдерські купівлі та продажі будуть виявлятися на ринку програмними засобами в режимі реального часу, а різнотипові махінації на кшталт виплат компенсації акцій заднім числом, стануть набагато складнішими, якщо взагалі неможливими. Корпоративне голосування може бути точнішим, а порожнє голосування було б важче проводити таємно. Будь-які зміни такого роду можуть різко вплинути на баланс між директорами, менеджерами та акціонерами [37]. Наприклад, організація вимагає позику від фінансової установи. Передача кредиту з фінансової установи до організації займає багато часу та паперової роботи [38]. У доповіді про майбутнє фінансової інфраструктури [39] ВЕФ описують ключові етапи процесу (див. рисунок 2.1):

– Фірма подає заявку (1) на отримання позики від фінансової установи (FI) –головного організатора (2).

– Користуючись перевагами цифрової ідентифікації Компанії, FI оперативно виконує KYC-верифікацію (2a) за допомогою Блокчейн-компонента обліку розподілених реєстрів (2b), який надає регуляторам кришталево чітке уявлення про діяльність.

– Фінансові записи та толерантність інвестора до ризику зберігаються на DLT (3) та автоматизують процес відбору. Водночас мінімізують час, необхідний для створення асоціації.

– Використання фінансової інформації про фірму та даних плану проекту, доступних через DLT, механізація заходів ретельної перевірки здійснюється за допомогою смарт-контракту (2c).

– Важливі функції (4a) процесу андеррайтингу додаються до його шаблону (4). Ключові атрибути процесу андеррайтингу (4b) заповнюються в його шаблон, консолідуючи процес та мінімізуючи час завдяки DLT-передачі цінності.

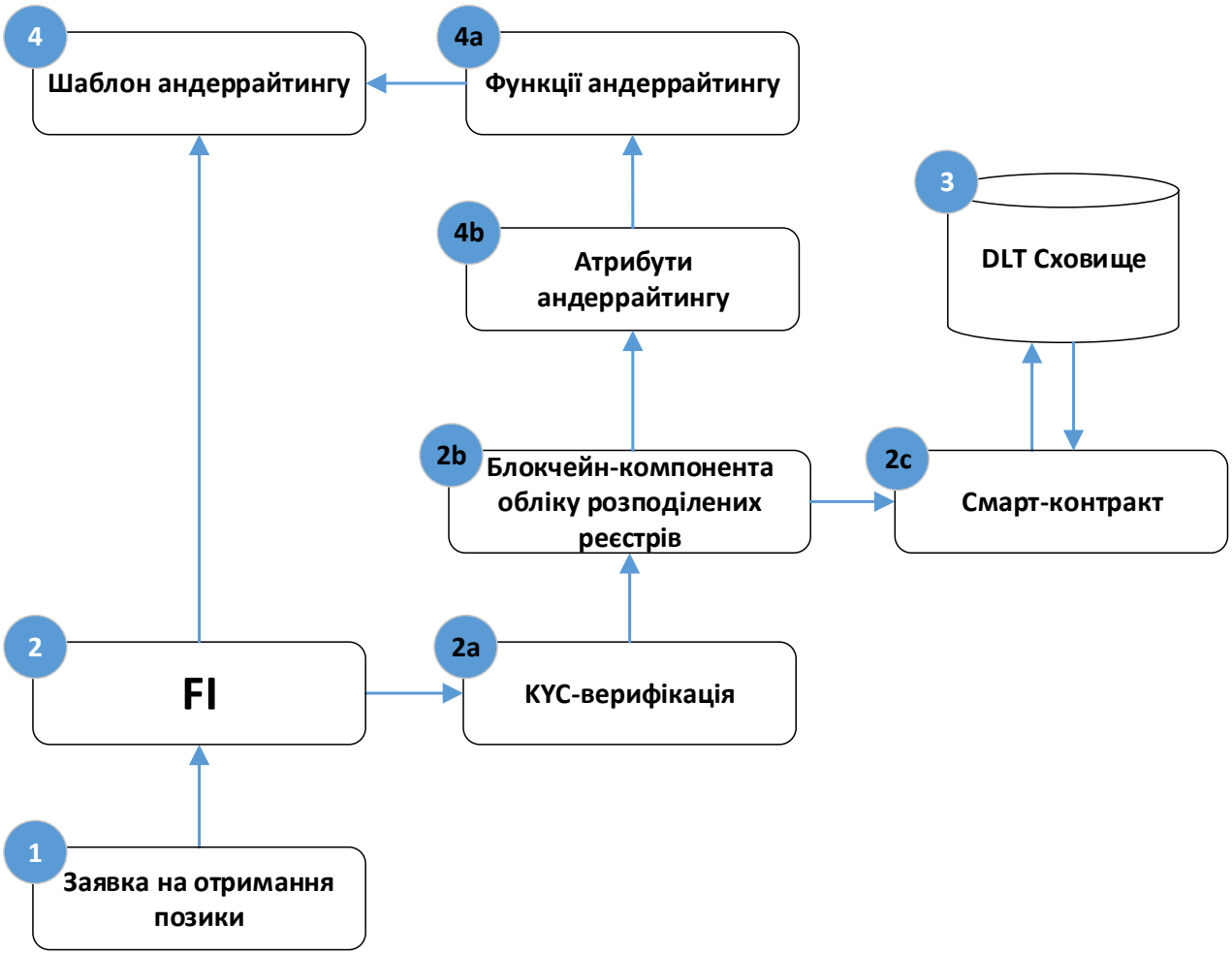

Рисунок 2.1 – Ключові етапи процесу перевірки з використанням смарт-контрактів та DLT

Смарт-контракти усувають потребу третьої сторони для фінансування позики, розподілу коштів та полегшення процесу обслуговування кредиту.

Розглянутий регламент полегшує перегляд фінансових деталей для забезпечення належного дотримання процедур.

Бачення ВЕФ щодо заявки та переказу позик зменшує конфіденційність організацій, оскільки їхні дані будуть у всьому доступні для інвесторів та фінансових установ. Однак це дозволить досягти головної мети – своєчасної доступності коштів для ведення організацій та безперебійної роботи бізнесу при зниженні процентних ставок та витрат на обслуговування та оформлення кредитів, які зараз беруть банки – посередники.

2.1.2 Організаційні переваги смарт-контрактів

У попередніх розділах були виділені переваги смарт-контрактів [5]:

– конфіденційність;
– заборона посередництва;
– самовиконання;
– довіра.

Смарт-контракти децентралізують централізовану або федеративну службу, щоб підвищити прозорість, зменшити потребу в довірі та іноді отримати економічну ефективність, оскільки не доведеться платити центральному арбітру за виконання певного завдання. Наявність центральної сторони, яка регулює контракти, створює багато ризиків [40], зокрема:

– конфіденційність даних;
– надійність;
– довіра;
– монополія;
– роадмап;
– конфіденційність;
– автентичність.

Підсумовуючи, розумні контракти (див. рисунок 2.2) гарантують:

– Анонімність: учасники можуть бути повністю анонімними, але передача цінності від однієї сторони до іншої гарантується. У сценарії комерції, оскільки система гарантує, що сторона-покупець має спроможність платити, продавцю не потрібно знати особу особи, яка купує. Смарт-контракт гарантує, що кошти надходять на рахунок продавця після виконання попередньо узгодженої умови. Це гарантує, що інформація про кредитні картки людей захищена і не може бути вкрадена або використана для шахрайства [41]. Цінність можна витрачати або передавати лише так, як задумали сторони. Жодному центральному суб'єкту не потрібно платити, оскільки система децентралізована [18]. Модель довіри зрозуміла до того, як цінність перетікає від однієї сторони до іншої.

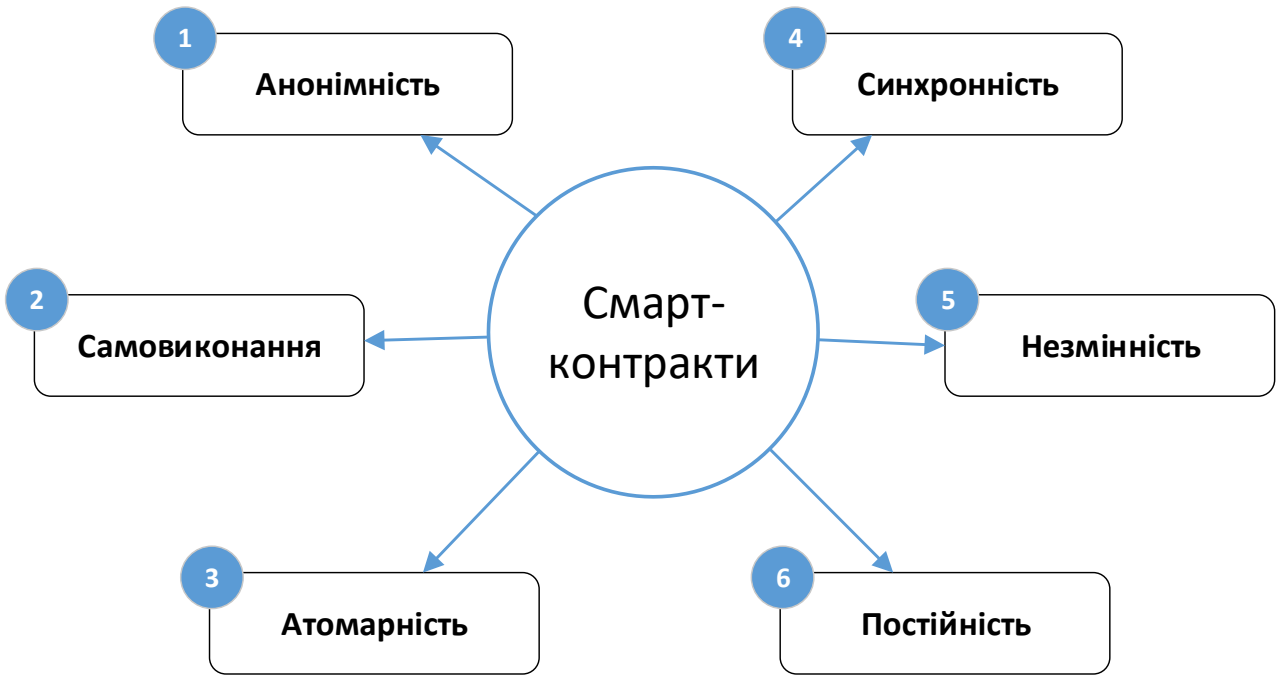

Рисунок 2.2 – Переваги смарт-контрактів

– Самовиконання. Розумні контракти можуть автоматично виконувати контракт, наприклад, розподіляти ресурси автономно, незалежно від довіри між сторонами. Немає необхідності довіряти третім сторонам, таким як послуги депонування або компанії, що займаються кредитними картками [29]. Вартість зміни правил надзвичайно низька. Комп’ютерний код можна «легко»

переписати залежно від досвіду програмістів. Мережа, в якій розміщено смарт-контракт, завжди може взяти на себе ризик зберігання, а не третій сторонній. Жодна анонімність комунікацій або транзакцій, розроблена для платформ блокчейн, не повинна бути жертвою використання смарт-контрактів. Наприклад, система анонімного голосування або система лотереї.

– Атомарність – через концепцію майнінгу блокчейну, коли кожен вузол мережі винагороджується за виконання транзакції, виконується ціла операція або нічого не робиться [21].

– Синхронність – дві операції не можуть заважати одна одній.

– Безсмертя – за словами Хоскінсона, об’єкти ніколи не можуть бути видалені, якщо вони не вчиняють «добровільне самогубство» [21].

– Незмінність – об'єкти не можуть бути змінені [42].

– Постійність – об'єкти є постійними і зберігаються на блокчейні (історія трансакцій, які можна зв'язувати та відстежувати) [4].

2.1.3 Застосування та варіації смарт-контрактів

Для програмного коду смарт-контракту ключовою вимогою є те, що код має виконуватися успішно та точно до завершення протягом розумного періоду часу. Якщо платформа виконання повністю контролює всі дії, які бажає виконати код смарт-контракту, тоді ці дії слід сумлінно виконувати з розумною продуктивністю. Сценарії, які можуть виконуватись не так і, отже, вимагають «забезпечення виконання», можуть бути технічними проблемами всередині або за межами платформи платформи виконання.

В системі із застосуванням консенсусу мережі із захистом від несанкціонованого доступу не буде положень «перевизначення виконання». На даний час угоди, які колись були розгорнуті як код смарт-контракту, не можуть бути змінені. Але досить часто положення угоди динамічно змінюються. Наприклад, дозволити постійному клієнту відкласти виплату відсотків на декілька днів або дозволити оплачувану відпустку для високоефективних

співробітників організації. Якщо всі можливі передбачувані варіації не закодовані заздалегідь – це не буде можливо в системі захисту від несанкціонованого доступу. Смарт-контракти зосереджені лише на заздалегідь запрограмованому виконанні [43].

Очевидним прикладом того, що може піти не так за межами платформи виконання, можуть бути процеси фізичної доставки товарів [43]. Наприклад, користувач не любить ходити по магазинах фізично, а натомість любить робити покупки в Інтернеті. Він купує товар онлайн у продавця та обирає дату доставки. Потім гроші знімаються з його рахунку і зберігаються в системі з підтримкою смарт-контракту, яка була запрограмована на оплату продавцю, якщо замовник отримає товар відповідно до узгодженої дати доставки, або повернути гроші замовнику, якщо він не отримає товар відповідно до узгодженої дати. Однак кур'єрська компанія, яку продавець використовує для відправлення товару замовнику, не доставить товар вчасно, а натомість доставляє товар через день після обраної дати. Однак смарт-контракт на основі закладеної конструкції вирішує, що продавець не доставив товар, і повертає гроші на рахунок замовника. Але товар прибуває наступного дня на адресу замовника. У смарт-контракті немає способу ідентифікувати, що це не було наміром або провиною продавця, а виною кур'єрської компанії.

У реальних ситуаціях початкова угода зазвичай не є останньою. Угоди іноді узгоджуються, якщо це можливо, і змінюються для врахування непередбачених обставин, які було важко передбачити на початку. Характеристика самовиконання попередньо написаної логіки розумних контрактів означає, що поточні смарт-контракти, що розповсюджуються, не є гнучкими до динамічних змін реального світу.

2.2 Безпека смарт-контрактів

Обмеження використання смарт-контрактів були продемонстровані атакою на розподілену автономну організацію (DDAO) [29], яка витратила

п’ятдесят три мільйони доларів до того, як було внесено зміни до комп’ютерного коду для відновлення коштів. DDAO – це набір смарт-контрактів, новий інвестиційний фонд на ранній стадії без менеджера. Замість того, щоб задіяти менеджера, інвестори голосують за те, які проекти слід профінансувати, а програмне забезпечення робить усе інше. DAO рекламував себе як розумний контракт, який ґрунтується на незмінному, незупинному та неспростовному програмному забезпеченні, яким повністю керують його члени. DAO мав бути схожим на цифрову валюту Біткоїн, оскільки він працюватиме без будь-якого централізованого втручання.

Зроблені передачі не порушували смарт-контракт, але використовували недоліки комп’ютерного коду. Якщо кодекс розглядається як закон, як стверджують деякі прихильники розумних контрактів, те, що сталося з DAO, було в межах закону. Наприкінці липня 2016 року організації, які використовують програмне забезпечення, проголосували за повернення коштів початковим інвесторам [44]. Код DAO був неповним, оскільки він не передбачав можливості того, що помилки програмного забезпечення можуть призвести до несподіваного передачі матеріальних цінностей від одних учасників іншим. Однак не можна стверджувати, що ця прогалина в коді виникла через подію, яку неможливо було передбачити. Незважаючи на те, що злому та переміщення коштів не передбачалося, Гідеон Грінспен, засновник і генеральний директор «Coin Sciences» – компанії, яка обслуговує інформаційно-технологічну платформу «MultiChain» для приватних Блокчейнів, стверджує, що будь-який великий фрагмент комп’ютерного коду зазвичай містить помилки, які нелегко виявити під час. тестування [9].

2.3 Практика запровадження смарт-контрактів

Розглянемо реальні приклади впровадження смарт-контрактів у різних галузях. «Barclays Bank» нещодавно протестував спосіб торгівлі деривативами

за допомогою смарт-контрактів та схожої на Блокчейн інформаційної технології, яка розробляється консорціумом провідних банків світу [13].

Похідний фінансовий інструмент є торговим контрактом між двома або більше сторонами, який може приймати різні форми та сформований на базовому активі [45]. Наразі контракти складаються з трьох основних частин з організацією «Міжнародна асоціація свопів і деривативів» (ISDA), яка створює стандарти для торгівлі деривативами у всьому фінансовому світі. Але цей процес є важким, оскільки поточні паперові контракти у вигляді комп'ютерних документів ще видаються [13]. Цей приклад показує, як розумні контракти були прийняті у фінансовому секторі, щоб зменшити надмірність даних, забезпечуючи при цьому транзакції в режимі реального часу.

Смарт-контракт може автоматично виконувати умови контракту, коли виконуються певні умови, що потенційно позбавляє людей участі у виконанні угоди. Використовуючи смарт-контракти на блокчейні, всі банки матимуть однаковий документ, який не буде незначно відрізнятися від банку до банку, і щось, що може спричинити затримки та непотрібне втручання людини. Наразі кожна сторона має свою версію правових документів. Завдяки централізованому сховищу документації всі сторони зможуть розраховувати угоди швидше та дешевше.

Страхові компанії зможуть здійснювати страхування тимчасової відповідальності. Наприклад, використовуючи розумні контракти, страхова компанія може стягувати ставки по-різному залежно від того, де та за яких умов клієнти керують своїми транспортними засобами. Наприклад, автомобіль, який їздив у ясний день, збираючи інформацію про погодні умови від метеослужби, в районі, де відремонтовані всі дороги, перевіривши інформацію про ремонт доріг, яку надає Департамент транспортних засобів. При цьому буде стягуватися нижча ставка в порівнянні з автомобілем, який експлуатується в погану погоду та, можливо, на дорогах із вибоїнами [18].

Німецький страховий гігант «Allianz» успішно використовував розумні контракти на основі блокчейну для обробки катастрофічних обмінів і облігацій.

Вони повідомили, що ця технологія може підвищити ринковість фінансових інструментів [33].

«Кот-своп» та облігації – це інструменти, які захищають страховиків від величезних потенційних збитків після великих катастроф, фактично активованих за заздалегідь визначеними параметрами. «Кот-свопи» та облігації дозволяють передавати ризики від одного страховика до іншого [46].

Розумні контракти можуть зробити страхові тарифи гнучкими. Це може збільшити прибуток страхових фірм, оскільки клієнти, ймовірно, будуть зацікавлені у гнучкому страхуванні, а не в страхуванні з фіксованими цінами. Розумні контракти можна використовувати, щоб зменшити кількість шахрайських претензій, які відбуваються в страховій галузі та запобіганню подвійним вимогам клієнтів від двох різних страховиків.

2.4 Перспективи подальших досліджень

Програмні коди смарт-контрактів є самовиконуваними, і з цієї причини багато хто віддає перевагу терміну «розумний агент», що відповідає більш загальному поняттю програмного агента. Рано чи пізно використання цього терміну зникне в міру розвитку інформаційних технології Блокчейн. Розробники стараються посилатися на мову програмування, наприклад Solidity, а не на загальну термінологію, яка описує складну операцію, що працює на Блокчейні – «розумні контракти» [13].

Часткова невизначеність навколо «розумних контрактів» є результатом зв’язку між юридичною концепцією контракту та елементом «розумного» – тобто того факту, що договір може бути сформований і визначений програмним забезпеченням [29]. Незважаючи на непередбачені підводні камені, перспективність смарт-контрактів зрозуміла [47].

Беззаперечний факт – інформаційна технологія має тенденцію розвиватися швидше, ніж може відреагувати юридично-правова система.

Інформаційно-технологічні інновації та застосунки не чекають, поки правова система наздожене прогрес [29].

Довгострокове дослідження може призвести від існуючого розрізненого комп’ютерного коду та поданих природною мовою юридичних документів до вихідних мов, які можуть бути автоматично перекладені у виконуваний код або юридичні документи. Причому в перспективі обидва документи будуть прийнятними в судах. Довгострокові дослідження можуть привести до формальних мов, які самі по собі будуть прийнятними в суді [43]. Наближається поява легального програмування [29] – ця інформаційна технологія може змінити розуміння договірного права, вирішення спорів, забезпечення виконання та сформувати розрив між державним і приватним використанням влади.

Контракти, що використовуються сьогодні, є статичними файлами, якими керують окремі особи. В сучасному світі, де літаки та автомобілі їздять самі, безумовно, настав час для контрактів, якими керують і виконуються самі [31]. Розумні контракти можуть означати, що найближчим часом нам, ймовірно, не знадобляться люди для управління контрактами, оскільки контракти зможуть бути самовиконаними.

2.5 Висновок до другого розділу

В другому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» проаналізовано розумні контракти для децентралізованих автономних організацій. Розглянуто використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій. Описано організаційні переваги смарт-контрактів. Подано застосування та варіації смарт-контрактів. Висвітлено питання безпеки смарт-контрактів. Проаналізовано практику запровадження смарт-контрактів. Висвітлено перспективи подальших досліджень.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1 Таксонометрія небезпек

Кваліфікаційна робота освітнього рівня «Бакалавр» присв'ячена аналізу світового досвіду інтеграції «смарт контрактів» в інноваційні застосунки. Оскільки зазначені застосунки використовуються для обширного переліку галузей людської діяльності, то доцільно висвітлити питанні таксономії небезпек. *Таксономія небезпек* – класифікація та систематизація явищ, процесів, інформації, об'єктів, які здатні завдати шкоди [48] (див. рисунок 3.1).

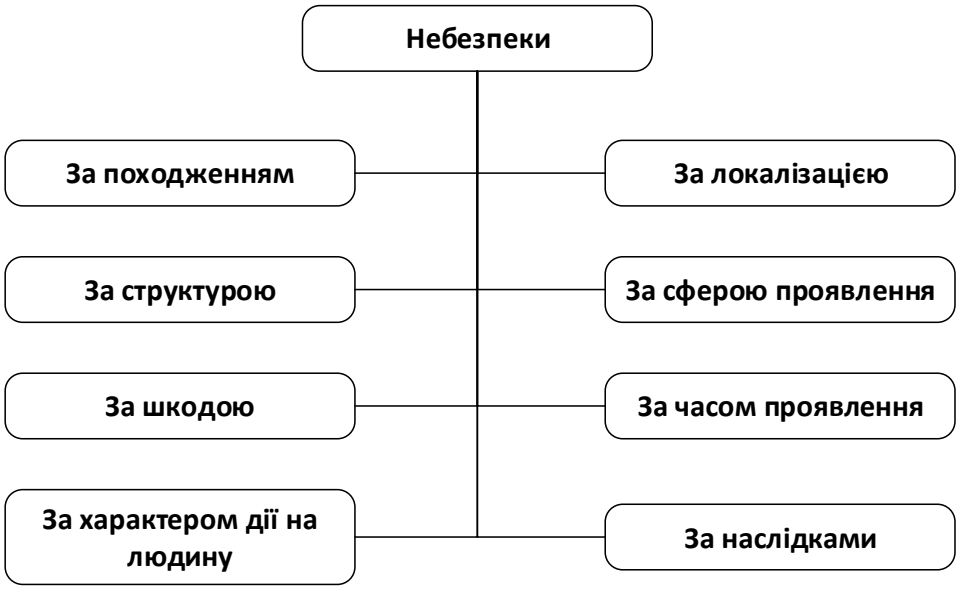

Рисунок 3.1 – Таксономія небезпек

Ідентифікація небезпек– це знаходження типу небезпеки та встановлення її характеристик, необхідних для розробки заходів щодо її усунення чи ліквідації наслідків.

Номенклатура небезпек – це перелік назв, термінів, систематизованих за окремими ознаками.

Квантифікація небезпек– введення кількісних характеристик для оцінки ступеня (рівня) небезпеки.

Найпоширенішою кількісною оцінкою небезпеки є ступінь ризику.

Небезпека, як вище було зазначено – це негативна властивість матерії, яка проявляється у здатності її завдавати шкоди певним елементам Всесвіту, потенційне джерело шкоди [49]. Якщо мова йде про небезпеку для людини, то це явища, процеси, об'єкти, властивості, здатні за певних умов завдавати шкоди здоров'ю чи життю людини або системам, що забезпечують життєдіяльність людей. При ідентифікації небезпек необхідно виходити з принципу «все впливає на все», тобто джерелом небезпеки може бути все живе і неживе, а підлягати небезпеці також може все живе і неживе. Класифікація джерел небезпек [50] подана на рисунку 3.2.

Рисунок 3.2 – Класифікація джерел небезпек

Згідно з цією класифікацією всі небезпеки поділяються на:

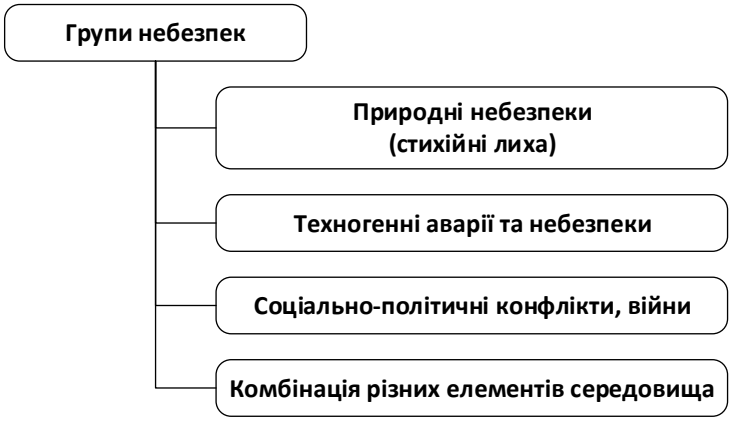

Рисунок 3.3 – Групи небезпек

Хоча поділ вражаючих факторів на небезпечні та шкідливі досить умовний, бо інколи неможливо віднести який-небудь фактор до тієї чи іншої групи, він ефективно використовується в охороні праці для організації розслідування та обліку нещасних випадків та професійних захворювань.

Небезпечні та шкідливі фактори дуже часто бувають прихованими, неявними або ж такими, які важко виявити чи розпізнати. Це стосується будь-яких небезпечних та шкідливих факторів, так само як і джерел небезпеки, які породжують їх [51].

Сонячне випромінювання, яке необхідне для існування майже всіх живих організмів на Землі, в тому числі людини, може бути причиною захворювань шкіри. Приваблива дитяча іграшка може виділяти шкідливі речовини, а пасажир, який мирно куняє в кріслі салону літака, може виявитися терористом.

3.2 Суть та зміст управління охороною праці

Комплексне управління охороною праці як із боку держави, так і з боку роботодавців і працівників у найбільш оптимальній формі відображено у Фонді соціального страхування від нещасних випадків на виробництві та професійних захворювань (ФССНВ – недержавна організація з однаковим представництвом усіх трьох вищезгаданих сторін в органах управління). Саме з цієї причини ФССНВ є однією з найбільш ефективних складових УОП [52].

Управління охороною праці (УОП) умовно має три основних центри, які саме і здійснюють комплексне управління охороною праці, це:

– держава (Кабінет Міністрів України; галузеві Міністерства; державні наглядові органи; органи виконавчої влади та самоврядування);

– роботодавці (власники підприємств чи уповноважені ними особи; керівники структурних підрозділів та служби охорони праці підприємств);

– працівники (трудові колектив підприємств; профспілки; уповноважені трудових колективів; комісії з охорони праці підприємств).

Комплексне управління охороною праці зображене на рисунку 3.4.

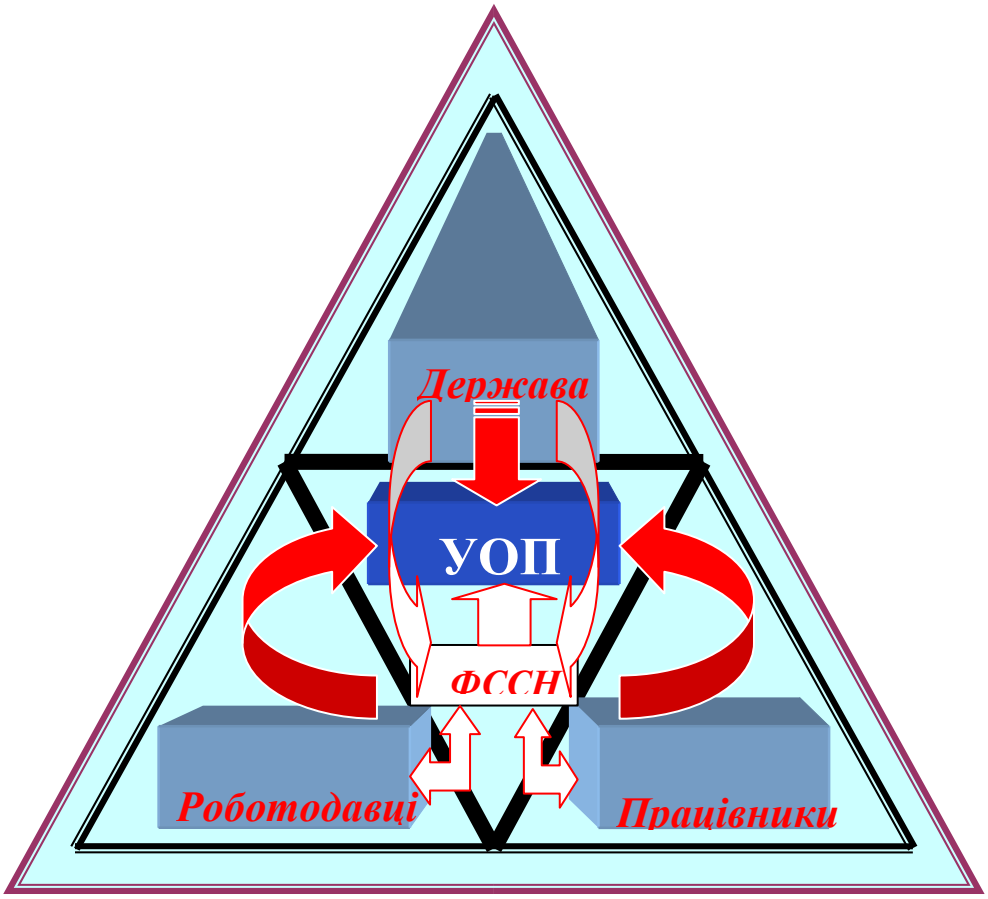

Рисунок 3.4 – Комплексне управління охороною праці

В усіх трьох центрах – держава, роботодавці та працівники– управління охороною праці може здійснюватися на декількох рівнях [53], а саме:

– загальнодержавному (національному) рівні;

– регіональному рівні;

– галузевому рівні;

– виробничому рівні (рівень підприємства).

На загальнодержавному рівні управління охороною праці здійснює:

– Кабінет Міністрів України;

– спеціально уповноважений центральний орган виконавчої влади з нагляду за охороною праці (до 09.12.2010 р. – Держгірпромнагляд, функції якого Указом Президента України від 09.12.2010 покладено на Державну службу гірничого нагляду та промислової безпеки України та Державну інспекцію техногенної безпеки України);

– Генеральна Прокуратура;

– ФССНВ;

– Спілка промисловців та підприємців України;

– Центральні всеукраїнські органи об’єднань профспілок тощо.

На регіональному рівні:

– Рада міністрів Автономної республіки Крим; місцеві державні адміністрації та органи місцевого самоврядування;

– територіальні підрозділи спеціально уповноваженого центрального органу виконавчої влади з нагляду за охороною праці;

– регіональні органи об’єднань профспілок;

– регіональні органи об’єднань роботодавців (промисловців і підприємців) тощо.

На галузевому рівні:

– галузеві міністерства;

– Державна архітектурно-будівельна інспекція України;

– Центральні органи об’єднань профспілок у галузі;

– Центральні органи об’єднань роботодавців (промисловців і підприємців) у галузі;

– Центральні органи виконавчої влади тощо. На виробничому рівні:

– роботодавець чи уповноважена ним особа;

– служба охорони праці підприємства;

– керівники відповідних структурних підрозділів і служб підприємства тощо.

3.3 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи висвітлено таксонометрію небезпек. Описано суть та зміст управління охороною праці.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр»:

– Подано означення сутностей предметної області.

– Наведено поняття, терміни та визначення смарт-контрактів.

– Подано класифікацію смарт-контрактів.

– Описано та охарактеризовано інформаційно-технологічні платформи для запровадження смарт-контрактів.

В другому розділі кваліфікаційної роботи:

– Проаналізовано розумні контракти для децентралізованих автономних організацій.

– Розглянуто використання смарт-контрактів для формування інформаційно-технологічних платформ підприємств та організацій.

– Описано організаційні переваги смарт-контрактів.

– Подано застосування та варіації смарт-контрактів.

– Висвітлено питання безпеки смарт-контрактів.

– Проаналізовано практику запровадження смарт-контрактів.

– Висвітлено перспективи подальших досліджень.

У розділі «Безпека життєдіяльності, основи хорони праці» висвітлено таксонометрію небезпек. Описано суть та зміст управління охороною праці.

ПЕРЕЛІК ДЖЕРЕЛ

1 Hart O, Moore J (2002) Contracts as reference points. Q J Econ CXVII:1 – 48.

2 Taylor R (1984) Licensing in theory and practice: licensor-licensee relationships. Antitrust Law J 53:561. 1.

3 The Law Handbook: What is a contract? Available online at: http://www.lawhandbook.org. au/07_01_01_what_is_a_contract/.

4 BusinessDictionary: Contract. Available online at: http://www.businessdictionary.com/ definition/contract.html.

5 Lim C, Saw T, Sargeant C, Smart contracts: bridging the gap between expectation and reality. Available online at: https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smartcontracts-bridging-gap-between-expectation-and-reality.

6 Szabo N (1997) Formalizing and securing relationships on public networks. First Monday 2(9).

7 Cassano J, What are smart contracts? Cryptocurrency's Killer App. Available online at: http:// www.fastcompany.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencyskiller-app.

8 Idelberger F, Governatori G, Riveret R, Sartor G (2015) Evaluation of logic-based smart contracts for blockchain systems. In: Alferes JJ, Bertossi L, Governatori G, Fodor P, Dumitru R (eds) Rule technologies. research, tools, and applications 10th international symposium, RuleML 2016, Stony Brook, NY, USA, July 6 – 9, 2016. Volume 9718 of the series lecture notes in computer science, pp 167 – 183, Springer, Switzerland.

9 Greenspan G, Why many smart contract use cases are simply impossible. Available online at: http://www.coindesk.com/three-smart-contract-misconceptions/.

10 Lewis A, A gentle introduction to smart contracts. Available online at: https://bitsonblocks. net/2016/02/01/a-gentle-introduction-to-smart-contracts/.

11 Levine M, Herbalife deals and blockchain dreams. Available online at: https://www.bloomberg.com/view/articles/2016-08-26/herbalife-deals-and-blockchain-dreams.

12 Stark J, How close are smart contracts to impacting real-world law? Available online at: http:// www.coindesk.com/blockchain-smarts-contracts-real-world-law/.

13 Stark J, Making sense of blockchain smart contracts. Available online at: http://www. coindesk.com/making-sense-smart-contracts/.

14 Tuesta D, Alonso J, Cámara N et al (2015) Smart contracts: the ultimate automation of trust? Digital Economy Outlook-October 2015, BBVA Research.

15 Skinner C (2016) Applying Blockchain to trade finance. In: Chris Ski. blog. http://thefinanser. com/2016/08/applying-blockchain-trade-finance.html/.

16 Counterparty Counterparty. In: Counterparty. http://counterparty.io/.

17 Ethereum (2016) Ethereum. In: Ethereum found. https://www.ethereum.org/.

18 Troy S What is a smart contract and what's it good for? Available online at: http://searchcio.techtarget.com/feature/What-is-a-smart-contract-and-whats-it-good-for.

19 Euromoney (2016) Getting to grips with Blockchain. In: Euromoney Institutional Invest. PLC. http://www.euromoney.com/Article/3501936/Getting-to-grips-with-blockchain.html.

20 Crosby M, Nachiappan N, Pattanayak P et al (2016) Blockchain technology: beyond bitcoin. Applied Innovation. 2:6–10.

21 Hoskinson C, A brief introduction to smart contracts. Available online at: https://www. youtube.com/watch?v=3bY66Zgr8Cs.

22 Xu X, Pautasso C, Zhu L et al (2016) The blockchain as a software connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA 2016), Venice, 2016, pp. 182 – 191.

23 SmartContract: Smart contract oracles. Available online at: http://about.smartcontract.com.

24 Delmolino K, Arnett M, Kosba A et al (2015) A Programmer's guide to ethereum and serpent acquiring the virtual machine, Available at https://www.cs.umd.edu/*elaine/smartcontract/guide.pdf.

25 Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. 9. www.Bitcoin.Org.

26 Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, Poelstra A, Timón J, Wuille P (2014) Enabling blockchain innovations with pegged sidechains, pp 1 – 25.

27 Brown C, How companies are using ethereum as an advanced version of bitcoin. Available online at: https://due.com/blog/ethereum-advanced-version-bitcoin/.

28 Delmolino K, Arnett M, Kosba AE, Miller A, Shi E (2015) Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. IACR Cryptol ePrint Arch 460.

29 Koulu R (2016) Blockchains and online dispute resolution : smart contracts as an alternative to enforcement. Scripted A J Law Technol Soc 13.

30 Coy P, Kharif O, This is your company on blockchain. Available online at: http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain.

31 Chesebro R (2015) A contract that manages itself: the time has arrived, Defense AT&L: January – February 2015.

32 Lehmann A, Why banks shouldn't fear blockchain. Available online at: https://www. weforum.org/agenda/2016/06/why-banks-shouldn-t-fear-blockchain/.

33 Allianz Press Release: Blockchain technology successfully piloted by Allianz Risk Transfer and Nephila for catastrophe swap. Available online at: http://www.agcs.allianz.com/about-us/ news/blockchain-technology-successfully-piloted-by-allianz-risk-transfer-and-nephila-forcatastrophe-swap-/.

34 Kharpal A, Barclays used blockchain tech to trade derivatives. Available online at: http:// www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html.

35 Palmer D, Allianz tests blockchain to boost catastrophe bond trades. Available online at: http://www.coindesk.com/allianz-blockchain-smart-contracts-boost-catastrophe-bond-trading/.

36 Levine M, Conflicted deals and stress tests. Available online at: https://www.bloomberg.com/ view/articles/2016-06-23/conflicted-deals-and-stress-tests.

37 Yermack D (2015) Corporate governance and blockchains. NBER Working Paper Series December. Available at http://www.nber.org/papers/w21802.

38 Levine M, Kitten hugs and the blockchain heart. Available online at: https://www.bloomberg. com/view/articles/2016-08-12/kitten-hugs-and-the-blockchain-heart.

39 McWaters J (2016) The future of financial infrastructure – an ambitious look at how blockchain can reshape financial services, An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte, World Economic Forum. Available at http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

40 Wood G, DEVCON1: ethereum. Available online at: https://www.youtube.com/watch?v=U_ LK0t_qaPo.

41 Fairfield J (2014) Smart contracts, bitcoin bots, and consumer protection. Wash Lee Law Rev Online 71:35 – 50.

42 Cuomo J, How businesses and governments can capitalize on blockchain. Available online at: https://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-cancapitalize-on-blockchain/.

43 Clack CD, Bakshi VA, Braine L (2016) Smart contract templates: foundations, design landscape and research directions, pp 1 – 15.

44 Wall L, “Smart contracts” in a complex world. Available online at: https://www.frbatlanta. org/cenfis/publications/notesfromthevault/1607.

45 Parsons JE (2013) Hit or Miss: regulating derivative markets to reduce hedging costs at non-financial companies, MIT Center for Energy and Environmental Policy Research, CEEPR WP 2013-002, January 2013.

46 Teh T-L (2015) Counterfactuals for the appraisal of disaster risk financing and insurance strategies. Br Actuar J 20:241 – 256.

47 Schneider N, Meet Vitalik Buterin, the 20-year-old who is decentralizing everything. Available online at: http://www.shareable.net/blog/meet-vitalik-buterin-the-20-year-old-whois-decentralizing-everything.

48 Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. – 336 с.

49 Модель життєдіяльності людини. Безпека життєдіяльності. Доступно онлайн: https://www.shevchenkove.org.ua/person_syte/Lusak/%D0%91%D0%96%D0%94%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA/GOLOVNA.htm.

50 Небезпеки та їхня класифікація. Доступно онлайн: https://web.posibnyky.vntu.edu.ua/fmbt/berezyuk_bezpeka_zhittyediyalnosti/12.htm.

51 Класифікація небезпечних і шкідливих виробничих факторів. Доступно онлайн: http://vn.dsp.gov.ua/novini-upravlinnya/klasifikatsiya-nebezpechnih/.

52 Система управління охороною праці в організації. Доступно онлайн: http://opcb.kpi.ua/wp-content/uploads/2014/09/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F_2.pdf.

53 Комплексне управління охороною праці. Доступно онлайн: https://pidru4niki.com/15060913/bzhd/kompleksne_upravlinnya_ohoronoyu_pratsi.