

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
Кафедра інформатики факультету інформатики

ВИДИ СМАРТКОНТРАКТІВ І НАПРЯМКИ ЇХ ЗАСТОСУВАННЯ
Текстова частина до курсової роботи

Галузь знань: 12 «Інформаційні технології»
Спеціальність: 122 «Комп'ютерні науки»

Керівник
курсної роботи
к-т економічних наук, ст. викладач
Невмержицький Є.І.

(підпис)

“___” _____ 2021 р.

Виконав студент КН МП-1
Єщенко М.С.

“___” _____ 2021 р.

Київ 2021

Тема: Види смартконтрактів і напрямки їх застосування.

Календарний план виконання роботи:

№	Назва етапу	Термін виконання	Примітка
1.	Отримання теми курсової роботи	15.10.2020	
2.	Пошук тематичної літератури	19.10.2020	
3.	Ознайомлення з літературою	05.11.2020	
4.	Вивчення поняття смартконтракту	12.11.2020	
5.	Огляд технологій для побудови смартконтракту з веб-інтерфейсом	22.12.2021	
6.	Вивчення технологій для побудови смартконтракту з веб-інтерфейсом	09.01.2021	
7.	Написання умов до програмної частини проекту	01.02.2021	
8.	Створення інфраструктури проекту	13.03.2021	
9.	Написання першої частини курсової роботи	26.03.2021	
10.	Перегляд змісту роботи з керівником	28.03.2021	
11.	Написання другої частини курсової роботи	12.04.2021	
12.	Перегляд змісту роботи з керівником	19.04.2021	
13.	Написання висновків курсової роботи	21.04.2021	
14.	Перегляд змісту роботи з керівником	28.04.2021	
15.	Внесення змін до курсової роботи відповідно до зауважень наукового керівника	30.04.2021	
16.	Створення презентації	10.05.2021	
17.	Захист роботи	17.05.2021	

Студент Єщенко М.С.

Керівник Невмержицький Є.І.

“ ”

Зміст

Анотація	3
Вступ	4
Розділ 1: Основні властивості технології блокчейн	6
1.1 Поняття блокчейн	6
1.2 Операції на основі блокчейн.....	8
1.3 Використання блокчейну	9
Розділ 2: Поняття і порівняльна характеристика смартконтрактів.....	10
2.1 Поняття смартконтракт	10
2.2 Ключові риси смартконтрактів; порівняння можливостей різних платформ для створення смартконтрактів.....	11
2.3 Смартконтракти з юридичної точки зору.....	13
Розділ 3: Напрямки застосування смартконтрактів в Україні і світі.....	15
3.1 Юридичне ставлення урядів до смартконтрактів	15
3.2 Смартконтракти в Україні	15
3.3 Застосування: сьогодні.....	16
3.4 Застосування: в майбутньому.....	20
Розділ 4: Практична частина, створення прототипу позикової платформи «SmartLoan» на основі смартконтрактів	22
4.1 Огляд використаних технологій.....	22
4.2 Опис проекту «SmartLoan»	23
Висновки	27
Список використаної літератури	28

Анотація

Метою даної роботи є дослідження поняття смартконтрактів і розкриття технологічних основ їх створення, зберігання та обігу (перерахування і захисту інформації).

У даній роботі розглядається поняття смартконтракту, його різновиди, значення у сучасній економіці та технологічне підґрунтя.

Вступ

Смартконтракти є виникшим відносно нещодавно видом формалізації угод, які дозволяють двом не довіряючим одна одній сторонам укласти надійний договір, не запобігаючи при цьому до допомоги третьої сторони, якій довіряли б обидві попередньо згадані. Більш того, смартконтракти дозволяють автоматизувати дотримання заздалегідь узгоджених правил угоди, а також зберегти історію дотриманих зобов'язань у розподіленому реєстрі, що унеможливорює її подальшу несанкціоновану модифікацію зі злочинною метою. Революційність рішення призвела до його стрімкого розвитку та широкого використання у різних галузях, і дана робота пропонує дізнатися більше про теоретичне підґрунтя поняття смартконтрактів та їх практичне застосування, в тому числі у сфері позик, на прикладі веб-застосунку.

Робота складається з чотирьох розділів.

Перший розділ докладно описує поняття блокчейну та його можливості.

Другий розділ досліджує поняття смартконтракту, його різновиди та правочинність.

Третій розділ має на меті докладно пояснити місце смартконтрактів у світі, та Україні зокрема, на сьогодні.

Четвертий розділ, практичний, присвячено моделюванню програмного продукту, позикової платформи на смартконтрактах.

Постановка задачі.

1. Пояснити роль блокчейну у смартконтрактах, надати необхідні знання для розуміння усіх переваг останніх.
2. Виконати аналіз поточного стану розповсюдженості смартконтрактів, а також їх чинності та користи у світі та, зокрема, в Україні.

3. Розробити прототип програмного продукту платформи для позик, що використовує смартконтракти.

Розділ 1: Основні властивості технології блокчейн

1.1 Поняття блокчейн

Блокчейн - це зростаючий список записів, які називаються блоками, пов'язаних за допомогою криптографії. Кожен блок містить криптографічний хеш попереднього блоку, позначку часу та дані транзакцій (зазвичай представлені у вигляді дерева Меркла). За задумом блокчейн стійкий до модифікації своїх даних. Це пояснюється тим, що після запису дані в будь-якому даному блоці не можуть бути змінені заднім числом без зміни всіх наступних блоків.

Для використання як розподіленого grosбуху, блокчейн зазвичай управляється одноранговою мережею, яка спільно дотримується протоколу для міжвузлового зв'язку та перевірки нових блоків. Незважаючи на те, що записи блокчейнів не є незмінними, блокчейни можуть вважатися захищеними за дизайном та ілюструють розподілену обчислювальну систему з високою стійкістю до відмов (згідно постановки криптографічної задачі візантійських генералів). Блокчейн був описаний як "відкритий grosбух, який може ефективно, надійно та постійно перевіряти запис транзакцій між двома сторонами".

Блокчейн був винайдений людиною (або групою людей), використовуючи ім'я Сатоші Накамото в 2008 році, щоб служити grosбухом публічних транзакцій криптовалюти біткойн. Особа Сатоші Накамото на сьогодні залишається невідомою. Винахід блокчейну для біткойнів став першою цифровою валютою для вирішення проблеми подвійних витрат без необхідності довіреного органу влади або центрального сервера. Дизайн біткойнів надихнув інші додатки та блокчейни, які є доступними для читання та широко використовуються криптовалютами. Блокчейн вважається різновидом платежів. Ексклюзивні блокчейни (приватні; фактично такі, що належать певній компанії) були запропоновані для комерційного використання, але «Computerworld» назвав маркетинг таких приватизованих блокчейнів без відповідної моделі безпеки

"змійною олією" [2]. Однак інші стверджують, що ексклюзивні блокчейни, якщо їх ретельно розробити, можуть бути більш децентралізованими, а отже, більш безпечними на практиці, ніж ті, що не є приватними [3].

Наразі існує чотири види блокчейнів:

1. Відкритий (публічний) блокчейн - абсолютно не обмежує доступ. Кожен, хто має підключення до Інтернету, може надсилати йому транзакції, а також стати валідатором (тобто брати участь у виконанні консенсусного протоколу). Зазвичай такі мережі пропонують економічні стимули для тих, хто захищає їх і використовують якийсь тип алгоритму Proof of Stake або Proof of Work. Одними з найбільших, найвідоміших публічних блокчейнів є блокчейн біткойнів та блокчейн Ethereum.
2. Закритий (приватний) блокчейн – базується на наявності прав доступу. До нього не можна приєднатися тільки за запрошенням адміністраторів мережі. Доступ учасників та валідаторів обмежений. Термін розподілений grosбух (DLT) зазвичай використовується для приватних блокчейнів.
3. Гібридний блокчейн - має поєднання централізованих та децентралізованих функцій. Конкретна робота мережі залежить від реалізації.
4. Бічний ланцюг – мережа блокчейну, яка працює паралельно з первинним блокчейном. Записи з первинного блокчейну (де ці записи зазвичай представляють цифрові активи) можуть бути пов'язані з бічним ланцюгом; це дозволяє бічному ланцюгу працювати незалежно від первинного блокчейну (наприклад, за допомогою альтернативних засобів ведення записів, альтернативного алгоритму консенсусу тощо).

1.2 Операції на основі блокчейн

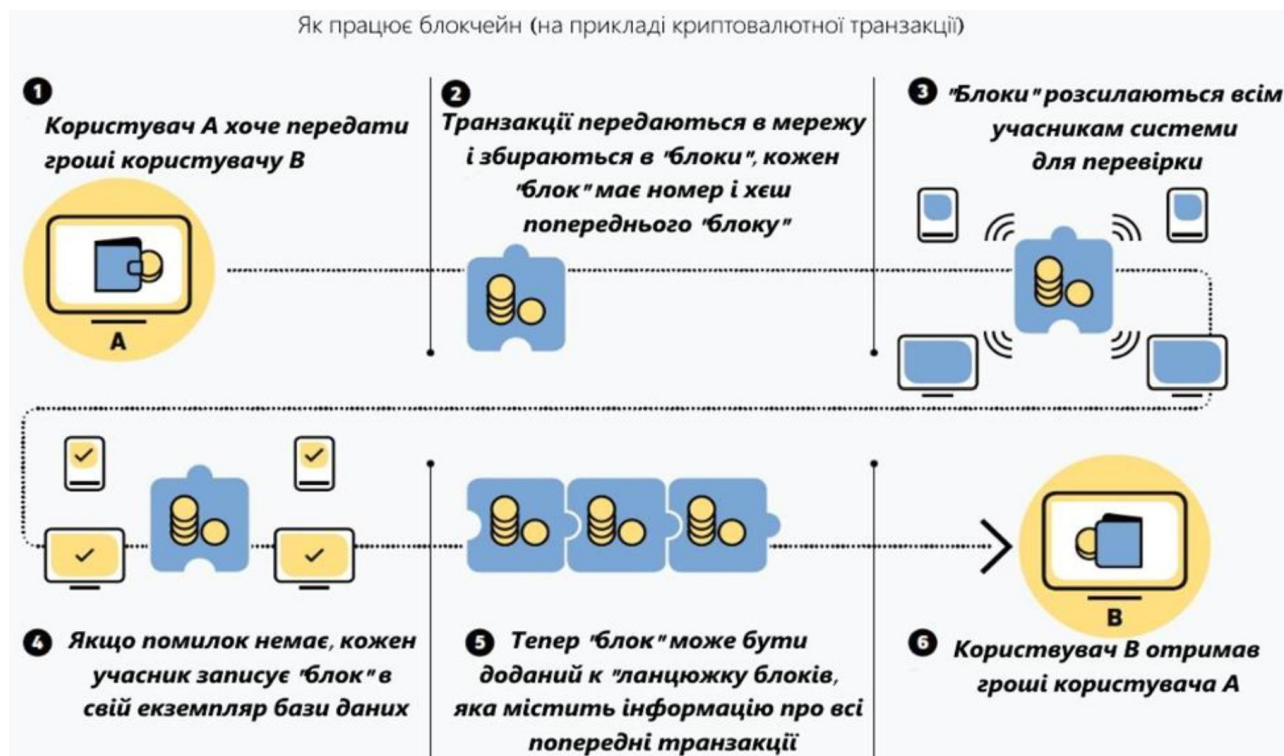


Рисунок 1 Схема транзакцій за участі технології блокчейн [4]

Блокчейн можна умовно розбити на такі шари:

- інфраструктура (апаратне забезпечення);
- мережа (виявлення вузлів, поширення та перевірка інформації) ;
- консенсус (Proof of Stake / Proof of Work) ;
- дані (блоки, транзакції) ;
- додаток (смартконтракти / dApps).

Блоки містять партії дійсних транзакцій, які хешуються та кодуються в дерево Merkle. Кожен блок включає криптографічний хеш попереднього блоку в блокчейні, що пов'язує обидва. Пов'язані блоки утворюють ланцюжок. Цей ітераційний процес підтверджує цілісність попереднього блоку, аж до початкового блоку, який відомий як блок генезису.

Іноді окремі блоки можна виробляти одночасно, створюючи тимчасову вилку. На додаток до захищеної історії на основі хешу, будь-який блокчейн має

визначений алгоритм підрахунку різних версій історії, так що той, що має більший бал, може бути обраний серед інших. Блоки, не вибрані для включення в ланцюжок, називаються блоками-сиротами. Колеги за мережею, що підтримують базу даних, час від часу мають різні версії історії. Вони зберігають лише найпершу за рейтингом версію бази даних, яка їм відома. Кожного разу, коли колега одержує версію з більшим балом (як правило, стару версію з додаванням одного нового блоку), вони розширюють або перезаписують власну базу даних і повторно передають вдосконалення своїм колегам. Ніколи немає абсолютної гарантії того, що будь-який конкретний запис назавжди залишиться в найкращій версії історії. Блокчейни, як правило, будуються для додавання оцінки нових блоків до старих блоків і отримують стимули для розширення за допомогою нових блоків, а не перезаписування старих блоків. Отже, ймовірність заміщення запису зменшується експоненційно, зі зростанням кількості блоків. Наприклад, біткойн використовує «proof-of-work», де мережа з найбільшим кумулятивним значенням вважається дійсною у всій мережею.

1.3 Використання блокчейну

Блокчейн знайшов використання у багатьох сферах. Серед них: криптовалюти, смартконтракти, фінансові послуги (банківські та не тільки), торгівля енергією, боротьба з підробками, управління ланцюгами поставок, охорона здоров'я.

Розглянемо ті з них, які найбільше покладаються на блокчейн і використовують його найбільш широко.

Криптовалюти - більшість криптовалют використовують технологію блокчейну для запису транзакцій. Наприклад, мережа біткойнів та мережа Ethereum засновані на блокчейні. Уряди мають змішану політику щодо законності своїх громадян або банків, що володіють криптовалютами.

Фінансові послуги – згідно з «Reason», багато банків виявили зацікавленість у розподілених grosбухах для використання у банківській діяльності та співпраці з компаніями, що створюють приватні блокчейни, [5], а згідно з дослідженням IBM від вересня 2016 року, це відбувається швидше, ніж очікувалося [6].

Боротьба з підробками - блокчейн може бути використаний для виявлення підробок, пов'язуючи унікальні ідентифікатори з продуктами, документами та відправленнями та зберігаючи записи, пов'язані з транзакціями, які неможливо підробити чи змінити. При цьому технологію блокчейну потрібно доповнювати технологіями, що забезпечують міцне зв'язування між фізичними об'єктами та системами блокчейнів. EUIPO заснував «Anti-Counterfeiting Blockathon Forum», з метою «визначення, пілотування та впровадження» інфраструктури боротьби з підробкою на європейському рівні [7]. Нідерландська організація стандартизації NEN використовує блокчейн разом із QR-кодами для автентифікації сертифікатів [8].

Смартконтракти - однією з головних цілей смартконтракту є автоматичний ескроу. Ключовою особливістю смартконтрактів є те, що їм не потрібна довірена третя сторона (наприклад, довірена особа), яка виступає посередником між замовниками - мережа блокчейн виконує контракт самостійно. Це може зменшити тертя між суб'єктами при передачі вартості і згодом може відкрити двері для вищого рівня автоматизації транзакцій. В ході обговорення співробітниками МВФ повідомлялося, що смартконтракти, засновані на технології блокчейн, можуть зменшити моральну небезпеку та оптимізувати використання контрактів загалом [9].

Розділ 2: Поняття і порівняльна характеристика смартконтрактів

2.1 Поняття смартконтракт

Смартконтракт - комп'ютерна програма або протокол транзакції, призначений для автоматичного виконання, контролю або документування

юридично важливих подій та дій відповідно до умов контракту чи угоди. [10] Цілями смартконтрактів є зменшення потреби у довірених посередниках, арбітражних та виконавчих витратах, збитки від шахрайства, а також зменшення зловмисних та випадкових винятків.

Торгові автомати згадуються як найстаріша технологія, еквівалентна впровадженню смартконтрактів. [11] У доповіді 2014 року про криптовалюту Ethereum [12] протокол Біткойн описується як слабка версія концепції смартконтракту, визначена комп'ютерним вченим, юристом та криптографом Ніком Сабо. Починаючи з Ethereum, різні криптовалюти підтримують мови сценаріїв, які дозволяють укласти більш просунуті смартконтракти між ненадійними сторонами. Смартконтракти слід відрізняти від юридичних смартконтрактів. Останнє стосується традиційної природною мовою юридично зобов'язуючої угоди, яка має певні умови, виражені та реалізовані в машиночитаному коді.

2.2 Ключові риси смартконтрактів; порівняння можливостей різних платформ для створення смартконтрактів

Подібно до передачі вартості на блокчейні, розгортання смартконтракту на блокчейні відбувається шляхом надсилання транзакції з гаманця для блокчейну. Транзакція включає скомпільований код смартконтракту, а також спеціальну адресу одержувача. Потім ця транзакція повинна бути включена в блок, який додається до блокчейну, після чого код смартконтракту буде виконаний для встановлення початкового стану смартконтракту. Візантійські відмовостійкі алгоритми захищають смартконтракт децентралізовано від спроб несанкціоновано змінити його. Після розгортання смартконтракту його неможливо оновити. Смартконтракти на блокчейні можуть зберігати довільний стан і виконувати довільні обчислення. Кінцеві клієнти взаємодіють зі смартконтрактом за допомогою транзакцій. Такі транзакції зі смартконтрактом можуть викликати інші смартконтракти. Ці транзакції можуть призвести до зміни стану та пересилання

монет з одного смартконтракту на інший або з одного рахунку на інший. Найпопулярнішим блокчейном для запуску смартконтрактів є Ethereum. На Ethereum смартконтракти, як правило, пишуться повною мовою програмування Тьюрінга, що називається Solidity, і компілюються в низькорівневий байт-код для виконання віртуальною машиною Ethereum. Через проблему зупинки та інші проблеми безпеки, повнота Тьюрінга вважається ризиком і її навмисно уникають такі мови, як Vyper. Існують і деякі інші мови програмування смартконтрактів, у яких відсутня повнота Тьюрінга, - Simplicity, Scilla, Ivy та Bitcoin Script. Однак вимірювання за допомогою регулярних виразів показали, що лише 35,3% із 53 757 смартконтрактів Ethereum включали рекурсії та цикли - конструкції, пов'язані з проблемою зупинки [14]. Кілька мов розроблені для формальної перевірки: Bamboo, IELE, Simplicity, Michelson (можна перевірити за допомогою Coq), Liquidity (компілюється до Michelson), Scilla, DAML та Pact.

Bitcoin	Надає неповну мову скриптів Тьюрінга, що дозволяє створювати власні смартконтракти поверх біткойна, такі як рахунки з різними підписами, платіжні канали, ескроу, часові замки, атомарну міжланцюгова торгівля, оракули або багатосторонні лотереї без оператора
Cardano	Блокчейн-платформа для смартконтрактів з використанням алгоритму «proof of stake»
Ethereum	Впроваджує повну мову Тьюрінга на своєму блокчейні; є видатною системою смартконтрактів
EOS.IO	Відносно молода блокчейн-платформа із підтримкою смартконтрактів; основою блокчейну є криптовалюта EOS
Tezos	Блокчейн-платформа, що модифікує власний набір правил з мінімальним порушенням роботи мережі через вбудовану модель управління

Рисунок 2 Порівняння блокчейн-платформ, які підтримують смартконтракти [таблиця]

Процеси на блокчейні, як правило, детерміновані для забезпечення візантійської відмовостійкості. Тим не менше, реальне застосування смартконтрактів, таких як лотереї та казино, вимагає надійної випадковості. Насправді технологія блокчейну зменшує витрати на проведення лотереї і, отже, вигідна для учасників. Випадковість на блокчейні може бути реалізована за допомогою хеш-блоків або міток часу, оракулів, схем зобов'язань, спеціальних смартконтрактів, таких як RANDAO та Quanta, а також послідовностей із змішаних стратегій рівноваги Неша [13].

2.3 Смартконтракти з юридичної точки зору

Смартконтракт не обов'язково є чинною юридично обов'язковою угодою. Деякі науковці стверджують, що смартконтракти - це не юридичні угоди, а скоріше засоби виконання зобов'язань, що впливають з інших угод [15], таких як технологічні засоби для автоматизації платіжних зобов'язань або зобов'язання, що полягають у передачі токенів або криптовалют. Крім того, інші вчені стверджують, що імперативний або декларативний характер мов програмування може вплинути на юридичну обґрунтованість смартконтрактів. [16] З моменту запуску блокчейну Ethereum у 2015 році термін "смартконтракт" став більш конкретно застосовуватися до поняття загальних обчислень, що здійснюються на блокчейні. Національний інститут стандартів і технологій США описує смартконтракт як "колекцію коду та даних (іноді їх називають функціями та станом), які розгортаються з використанням криптографічно підписаних транзакцій у мережі блокчейн". [17] У цій інтерпретації, що використовується, наприклад, Ethereum Foundation, смартконтракт не обов'язково пов'язаний з класичною концепцією контракту, але може бути будь-якою комп'ютерною програмою. Смартконтракт також можна розглядати як захищену збережену процедуру, оскільки його виконання та кодифіковані ефекти, такі як передача

деякої вартості між сторонами, суворо виконуються і не піддаються маніпуляціям, після того як транзакція з конкретними даними контракту зберігається у блокчейні. Це тому, що фактичне виконання контрактів контролюється та перевіряється платформою, а не будь-якими довільними програмами на стороні сервера, що підключаються до платформи.

Розділ 3: Напрямки застосування смартконтрактів в Україні і світі

3.1 Юридичне ставлення урядів до смартконтрактів

У 2017 році, реалізуючи Декрет про розвиток цифрової економіки, Білорусь стала першою країною, яка легалізувала смартконтракти. Білоруський адвокат Денис Алейніков вважається автором юридичної концепції смартконтракту, запровадженої указом [18]. У 2018 р. У звіті Сенату США сказано: "Хоча смартконтракти можуть звучати по-новому, ця концепція вкорінена в основному договірному законодавстві. Зазвичай судова система вирішує договірні суперечки та забезпечує виконання умов, але також загальноприйнятим є інший метод арбітражу, особливо для міжнародних транзакцій. За допомогою смартконтрактів програма застосовує контракт, вбудований у код". [19] Ряд штатів США прийняли законодавство про використання смартконтрактів, наприклад, Арізона, Невада, Теннессі, та Вайомінг. А в квітні 2020 року Палата представників Айови прийняла законопроект, що юридично визнає смартконтракти в штаті. [20] У квітні 2021 року британська цільова група з питань юрисдикції (UKJT) опублікувала Правила вирішення цифрових суперечок (Правила цифрових розмов), щоб допомогти швидкому вирішенню суперечок щодо блокчейн-судів та криптовалют у Великобританії [21].

3.2 Смартконтракти в Україні

Державний реєстр речових прав на нерухоме майно та Державний реєстр іпотек не використовують технологію блокчейн, що унеможливорює реєстрацію права власності та обтяження у вигляді іпотеки за допомогою використання смартконтракту.

Нормою ст. 44 Закону України «Про забезпечення вимог кредиторів та реєстрацію обтяжень» встановлено порядок припинення іпотеки, а саме шляхом подання відповідної заяви, яка подається в паперовому вигляді, що технічно обмежує використання смартконтракту.

Отже, особливістю смартконтракту є його автоматичне виконання, але наразі його повсякденне використання не отримало значного поширення через правову невизначеність на території України [22].

3.3 Застосування: сьогодні

Торговельне врегулювання - ефективності операцій сьогодні заважають дорогі та ризиковані процеси розрахунків. Якщо говорити дуже просто, сторона, що закуповує, завжди стикається з ризиком шахрайства, оскільки вона ніколи не може бути впевнена, що сторона, що продає, виконає свої зобов'язання.

В даний час існує низка неефективних та трудомістких послідовних практик, які включають робочі процеси затвердження торгівлі. Наприклад, термін розрахунків за позиками за кредитним кредитом може становити 20 днів. Сам цей фактор робить ринок позикових позик дуже непривабливим через проблеми, пов'язані з ліквідністю. Крім того, сторони часто використовують різні ІТ-системи, що спричиняє диспропорції та ще більше подовжує час врегулювання.

У контексті торгового фінансування технологія інтелектуального контракту відсутня: транзакція не буде виконана доти, доки не будуть дотримані заздалегідь визначені умови розрахунків, що значно зменшить пов'язані з цим ризики.

За допомогою смартконтрактів більшість процесів, пов'язаних з оформленням документів, KYC та AML, може здійснюватися автономно. Це значно зменшує широкий спектр операційних витрат, скорочує час розрахунків та робить певні ринки більш ліквідними. Усі сторони можуть бачити, чи є якісь оновлення умов смартконтракту, і будь-які такі зміни незмінно реєструються на блокчейні, надаючи надійний історичний запис.

Іпотека - подібно до клірингу торгівлі, іпотечне кредитування все ще спирається на переважно застарілі рамки. Дозвіл позики включає банківські службовці та сторонні сторони, які переглядають лавину фінансових документів, а

потім вручну передають їх по електронній пошті. Кожен документ потрібно підписати, щоб відстежувати, що робить цей процес надзвичайно трудомістким і вразливим до помилок, пов'язаних з людиною. За допомогою смартконтрактів весь процес можна оцифрувати та в основному автоматизувати. Усі залучені сторони матимуть доступ до оцифрованих версій документів, а виплати будуть здійснюватися автоматично після збору електронних підписів.

Будівництво - використання контрактів міцно закріплено в будівельній галузі. Усе, від доставки матеріалів до переказу платежів до вимірювання результатів, як правило, здійснюється за допомогою встановлених процедур підряду. У міру того, як галузь стає все швидшою, успадковані недоліки традиційного підряду все більш очевидні. За своєю суттю ці контракти завжди можна трактувати по-різному і, як правило, займає надзвичайно багато часу йде на управління, що перешкоджає продуктивності та збільшує ймовірність суперечок.

У поєднанні з аналітикою даних IoT, смартконтракти можуть допомогти будівельній галузі впорядкувати продуктивність та пришвидшити обробку платежів. Наприклад, за допомогою комп'ютерних камер із підтримкою зору система може виявити, коли постачальник доставляє матеріали, і автоматично перерахувати кошти цьому постачальнику. Це ефективно усуває посередників і звільняє працівників від ручної роботи.

Смартконтракти також можуть впорядкувати обробку рахунків-фактур. Одним з найбільш важливих викликів будівельних компаній є перевірка суми субпідрядника, що підлягає сплаті. Завищення націнки, податків та профспілок на цей момент стало галузевим продуктом. Це призводить до того, що проектні команди страждають від каскадів ручної роботи, переглядаючи тисячі невизначених контрактних зобов'язань і тим самим затримуючи платежі.

Хоча смартконтракти не можуть повністю автоматизувати процес перевірки рахунків-фактур, вони можуть зробити його значно ефективнішим, безпечнішим та прозорішим. Цього можна досягти, узгодивши рахунок-фактуру з обсягом роботи та списком виконаних завдань, записаних на блокчейні. У цьому випадку менеджер підрядника перевіряє виконання завдань, а смартконтракти автоматично гарантують, що завдання було виконано в межах параметрів, зазначених у рахунку-фактурі.

Застосовуючись для великих будівельних проектів, такі ініціативи стають проривом. Таким чином забезпечуються відповідні витрати, оптимізується робота, і всі підрядники можуть перевіряти прогрес у реальному часі.

Земельний реєстр - у даний час запис прав власності на землю часто є ризикованим, фрагментованим та громіздким. Процес включає агенти з нерухомості, які вивчають купу документів щодо підтвердження іпотеки, даних про будівництво та угод між покупцем і продавцем. Ці ручні процеси часто є причиною зміни документа і, як наслідок, шахрайства.

Спеціальний токен блокчейну може містити всю відповідну інформацію про конкретне майно, включаючи ідентифікатори власника та покупця, юридичний опис, відгуки третіх сторін тощо. Щоб перевірити ідентифікатори, продавець просто перепрофілює цифровий файл, і покупець легко його перевіряє за допомогою свого відкритого ключа. За самою природою блокчейну такий процес передачі майна робить шахрайство майже неможливим, оскільки порушникам потрібен доступ до відкритих ключів, крім того, що вони одночасно вводять шкідливе програмне забезпечення у кожную цифрову копію на розподіленому гросбусі.

Наприклад, Грузія успішно пілотувала земельний реєстр на основі блокчейну для понад 1,5 мільйона земельних прав. Весь процес тепер можна

виконати за десять хвилин, а експлуатаційні витрати можна зменшити на 90%. Однак слід зазначити, що при таких масштабних блокчейнових проектах споживання енергії може стати проблемою. У Грузії розповсюдження блокчейну значною мірою зумовлене низькими цінами на енергію [23].

Однак, що стосується нерухомості, вигідні переваги, спричинені смартконтрактами, все ще можуть зникати, не зважаючи на законодавчі норми. Як приклад, незважаючи на переконливий доказ концепції, шведський консорціум заборонив токенизацію власності навіть у прототипі. Що стосується інтеграції блокчейнів на рівні уряду, перетворення прав власності на землю в оцифровані активи може бути важкою ініціативою для здійснення.

Страхування - подібно до вищезазначених випадків використання, основні завдання страхової галузі пов'язані з довірою, повільною обробкою претензій та високими операційними витратами.

Смартконтракти можна використовувати для часткової автоматизації та прискорення транзакцій. Щоб це сталося, сторони все ще можуть використовувати письмову угоду, але розміщувати вказані тригери, які ініціюють переказ коштів на блокчейні. Ці тригери потрібно підключити до реального світу, щоб підтвердити, що сталася конкретна подія. Це можна зробити за допомогою dApps та різних пристроїв IoT.

Наприклад, розумні датчики можна розміщувати в будинках та транспортних засобах для передачі даних про аварії в реальному часі, таких як витоки газу, і запускати автоматизовану обробку претензій. «Beam Dental», постачальник стоматологічних послуг, ще більше вдосконалює підключення на основі IoT і знижує страхові тарифи за допомогою алгоритмічного андеррайтингу. Клієнти «Beam» отримують підключену зубну щітку, яка обмінюється даними з додатком, який потім використовується для регулювання ставок сплат. У двох

словах: чим більше ви дбаєте про гігієну зубів, тим менше ви сплатите за лікування у клініці.

В іншому прикладі, якщо рейс затримується на більш ніж певний період, додаток, заснований на блокчейні, може отримати цю інформацію з системи авіакомпанії та автоматично передати повернення коштів пасажирам.

Ці ініціативи щодо смартконтрактів вже виявились корисними в простих сценаріях страхування, але мало хто може масштабуватися в довгостроковій перспективі. Наприклад, у 2017 році «АХА» запустила «Fizzy», платформу смартконтрактів із затримкою рейсу, яка забезпечувала автоматичну компенсацію клієнтам, рейси яких були затримані. На жаль, продукт був припинений у 2019 році. Найголовніше, що «АХА» називає незацікавленість та недостатній попит як головні причини відмови від проекту [23].

Цікаво, що у 2020 році Лоран Бенічу, керівник блокчейну в «АХА», написав у своєму блозі «Medium»: «Об'єднання страхування та блокчейну на сьогоднішній день було найскладнішим завданням за всю мою кар'єру». Хоча блокчейн, здається, добре підходить для страхування, Бенічу зазначає, що ці дві концепції принципово різняться у тому, як вони підходять до ризиків, довіри, правил та дотримання. Більше того, проблема взаємодії блокчейну все ще переважає, оскільки застарілі рамки, що використовуються страховими компаніями, часто важко злити з блокчейном.

Підсумовуючи, можна сказати що навіть на сьогоднішній день смартконтракти цілком вдало використовуються у багатьох галузях. Тим не менш, для продовження вдалих практик та подальшого зростання зацікавленості у технології, необхідно продовжувати дослідження у широкому спектрі напрямків.

3.4 Застосування: в майбутньому

Штучний інтелект (ШІ) - це найновіша технологія для досягнення закону, але його вплив, хоча й досі непередбачуваний, здається надзвичайним. ШІ та

блокчейн - це взаємодоповнюючі та синергетичні технології в цифровому бізнесі. Хоча ШІ допомагає нам оцінювати, розуміти, розпізнавати та приймати рішення, Блокчейн допомагає нам перевіряти, виконувати та реєструвати. Хоча методи машинного навчання (МН), що є однією з найбільш розвинених галузей ШІ сьогодні, допомагають нам знаходити можливості та вдосконалювати процес прийняття рішень, передбачаючи та обробляючи великі масиви даних, інтелектуальні контракти, побудовані за технологією Blockchain, можуть автоматизувати перевірку транзакційних частин процесу, забезпечуючи незмінність, безпеку та децентралізований доступ до даних.

Але також ШІ може бути правильним інструментом для подолання проблем, виявлених на сьогодні щодо смартконтрактів, таких як визнання вад у формуванні контрактів або існування незаконної практики. Окрім МН, ще однією галуззю ШІ, над якою ведеться активніша робота, є так звана обробка природних мов (НЛП). Розвиток НЛП має важливе значення для того, щоб МН реалізував свій потенціал, проаналізувавши не лише смартконтракти, а й «традиційні» контракти, чинне законодавство та судові рішення, а також просунувшись далі в аналізі намірів сторін.

Як каже Кевін Вербах, провідний фахівець у галузі технології блокчейн, «побудова комп'ютеризованої системи, здатної інтерпретувати смартконтракти так, як це може зробити людина, є вагомим завданням для штучного інтелекту». Таким чином, хоча отримання смартконтрактів для включення методів штучного інтелекту, здається, є способом зробити їх справді «розумними», ми не повинні втрачати з виду той факт, що, як нещодавно заявив Світовий економічний форум, «побудова довіри споживачів є ключем до розблокування справжнього потенціалу ШІ, і на даний момент ще лишається пройти довгий шлях» [24].

Розділ 4: Практична частина, створення прототипу позикової платформи «SmartLoan» на основі смартконтрактів

4.1 Огляд використаних технологій

Фронт-енд: фреймворк/бібліотека React (також відомий як React.js або ReactJS) - це бібліотека JavaScript із відкритим кодом для створення інтерфейсів користувача або компонентів інтерфейсу. Він підтримується «Facebook» та спільнотою окремих розробників та компаній. React можна використовувати як основу при розробці односторінкових або мобільних додатків. Однак React займається лише управлінням станом і наданням цього стану в DOM, тому для створення програм React зазвичай потрібно використовувати додаткові бібліотеки для маршрутизації, а також певну функціональність на стороні клієнта (зазвичай вони беруться з безкоштовних доступних для вільного завантаження «node modules»).

Truffle (частина Truffle Suite) - середовище для розробки, тестова структура та конвеєр активів для Ethereum, метою якого є полегшення життя розробника на платформі Ethereum.

Ganache (частина Truffle Suite) – персональний блокчейн для швидкої розробки розподілених програм на Ethereum та Corda. Можна використовувати Ganache протягом усього циклу розробки, що дозволяє розробляти, розгортати та тестувати dApps у безпечному та детермінованому середовищі.

Metamask - програмний гаманець для криптовалют, який використовується для взаємодії з блокчейном Ethereum. Це дозволяє користувачам отримати доступ до власного гаманця Ethereum через розширення браузера або мобільний додаток, який потім можна використовувати для взаємодії з децентралізованими програмами.

Ngrok – крос-платформенний застосунок для надання безпечних інтроспективних тунелів як інструменту розробки веб-хука localhost та інструменту відлагодження.

Бек-енд: Express – фреймворк для Node.js, випущений як безкоштовне програмне забезпечення з відкритим кодом за ліцензією MIT. Він призначений для створення веб-додатків та API.

4.2 Опис проекту «SmartLoan»

Проект «SmartLoan» покликаний надати можливість користувачам утворювати угоди на основі смартконтрактів для надання та отримання позик у криптовалюті Ethereum. Створений за допомогою сучасних технологій прототип відповідає нормам безпеки з використання платформи. Для перевірки коректності роботи розробка використовувала Truffle Suite. Це уможливило використання розподіленого збереження у локальній умові. Виконаний на «React» фронт-енд хоча і є лаконічним, але дозволяє продемонструвати можливості смартконтрактів та усю революційність створеної платформи для надання позик. Наведені нижче скріншоти застосунку показують наявний функціонал.

SmartLoan Account Help Filter Contracts Create Contracts Search Search

SmartLoan: Revolutionary Smartcontracts-based Loan Platform

Please input below your Pre-Check credentials in order to be presented loan categories best suited for you.

What is your Credit Score?

Approximate Annual Salary:

☐ I'm Not a Robot

Submit

Рисунок 3 Екран логіну

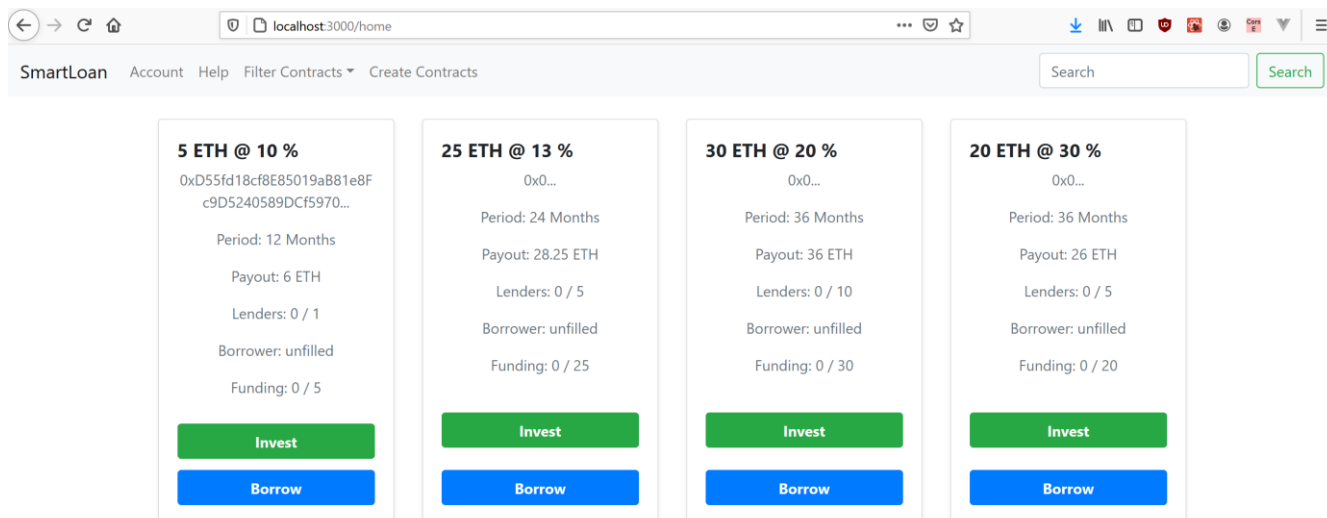


Рисунок 4 Головне меню

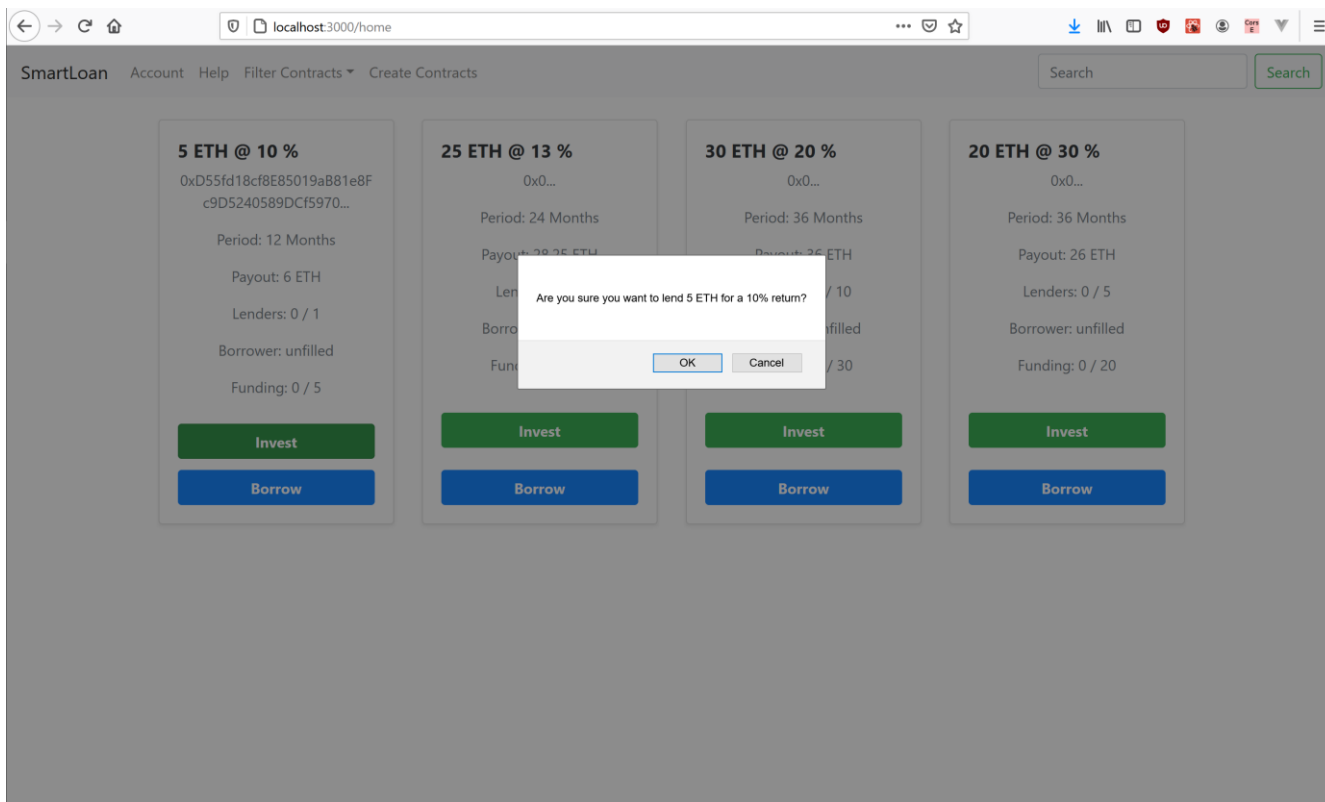


Рисунок 5 Інвестування коштів у активний контракт

The screenshot shows the SmartLoan web application interface for borrowing. The browser address bar displays 'localhost:3000/borrow'. The application header is the same as in the previous image. The main content area has a green background with the following text:

Contract 1: Borrow 5 ETH @ 10% for 12 months
Required to fulfill 0.5000 ETH to this contract on the 1st of every month
 Please input below your credentials to be checked and verified in order for your loan to be approved. In the event you are rejected, you will not be entered into the contract and will owe nothing.

The form contains the following fields:

- First Name**: TestFirstName
- Last Name**: TestLastName
- Phone Number**: +3800000000
- Annual Gross Income**: 100
- Date of Birth**: mm / dd / yyyy
- Email**: my_email@mail.com
- Social Security Number**: Enter 9 Digit Social

Below the form is a checkbox: ☐ I agree to fulfill the terms of the loan requirements if approved. A blue 'Submit' button is located at the bottom left. The browser address bar at the bottom shows 'localhost:3000/borrow#'

Рисунок 6 Оформлення отримання позики

Висновки

Отже, усвідомлюючи усю інформацію про смартконтракти, викладену в рамках роботи, можна сказати, що, не зважаючи на молодість технології та певну невизначеність її місця з юридичної точки зору, вона вже встигла зайняти важливе місце на ринку у багатьох сферах життя – від торговельних врегулювань до охорони здоров'я. Подальший розвиток та впровадження залежить тільки від кількості сміливих проектів, які здатні реформувати існуючі системи, такі як земельні реєстри; ця ідея була повністю підтримана під час створення платформи для позик на базі смартконтрактів. Досліджений експериментальний продукт показав на практичному прикладі перспективність використання смартконтрактів галузі кредитування.

Можна впевнено сказати, що вже зараз смартконтракти приносять справжню користь людству, і, за умови впровадження на державному рівні, їх переваги будуть відчутні кожному громадянину України – достатньо навести локалізований вищезгаданий приклад із Державним земельним кадастром.

Список використаної літератури

1. Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". *Harvard Business Review*.
<https://web.archive.org/web/20170118052537/https://hbr.org/2017/01/the-truth-about-blockchain>
2. Hampton, Nikolai (5 September 2016). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". *Computerworld*.
<https://www2.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/>
3. Bakos, Yannis; Halaburda, Hanna; Mueller-Bloch, Christoph (February 2021). "When Permissioned Blockchains Deliver More Decentralization Than Permissionless". *Communications of the ACM*. 64 (2): 20–22.
<https://dl.acm.org/doi/10.1145/3442371>
4. Костюк П.П. «Використання технології блокчейн для забезпечення інформаційної безпеки». *Сучасний захист інформації* №3(43), 2020
5. Epstein, Jim (6 May 2016). "Is Blockchain Technology a Trojan Horse Behind Wall Street's Walled Garden?"
<https://web.archive.org/web/20160708170429/http://reason.com/reasontv/2016/05/06/bitcoin-consensus-blockchain-wall-street>
6. Kelly, Jemima (28 September 2016). "Banks adopting blockchain 'dramatically faster' than expected: IBM". *Reuters*.
<https://web.archive.org/web/20160928163048/http://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D>
7. Brett, Charles (18 April 2018). "EUIPO Blockathon Challenge 2018 -". *Enterprise Times*.
<https://www.enterprisetimes.co.uk/2018/04/18/euipo-blockathon-challenge-2018/>

8. "PT Industrieel Management". *PT Industrieel Management*
https://www.ptindustrieelmanagement.nl/hse/nieuws/2020/06/nen-innoveert-certificatencheck-en-blockchain-1013171?_ga=2.11339894.336094574.1598975931-710406553.1598975931
9. «Virtual Currencies and Beyond: Initial Considerations». *IMF Discussion Note. International Monetary Fund*. 2016.
<https://web.archive.org/web/20180414210721/https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>
10. Röscheisen, Martin; Baldonado, Michelle; Chang, Kevin; Gravano, Luis; Ketchpel, Steven; Paepcke, Andreas (1998). "The Stanford InfoBus and its service layers: Augmenting the internet with higher-level information management protocols". *Digital Libraries in Computer Science: The MeDoc Approach. Lecture Notes in Computer Science*. Springer. 1392: 213–230.
<https://doi.org/10.1007%2Fbfb0052526>
11. Savelyev, Alexander (14 December 2016). "Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law". *Social Science Research Network*.
<https://ssrn.com/abstract=2885241>
12. *Ethereum White Paper*
<https://ethereum.org/en/whitepaper/>
13. Chatterjee, Krishnendu; Goharshady, Amir Kafshdar; Pourdamghani, Arash (21 February 2019). "Probabilistic Smart Contracts: Secure Randomness on the Blockchain".
<https://arxiv.org/abs/1902.07986>
14. Jansen, Marc; Hdhili, Farouk; Gouiaa, Ramy; Qasem, Ziyaad (2020). "Do Smart Contract Languages Need to Be Turing Complete?". *Blockchain and Applications. Advances in Intelligent Systems and Computing*. Springer

International Publishing.

https://doi.org/10.1007%2F978-3-030-23813-1_3

15. Mik, Eliza, Smart Contracts: A Requiem (December 7, 2019). *Journal of Contract Law* (2019) Volume 36 Part 1, p 72
16. Governatori, Guido; Idelberger, Florian; Milosevic, Zoran; Riveret, Regis; Sartor, Giovanni; Xu, Xiwei (2018). "On legal contracts, imperative and declarative smart contracts, and blockchain systems". *Artificial Intelligence and Law*.
<https://doi.org/10.1007%2Fs10506-018-9223-3>
17. D J Yaga et al, Blockchain Technology Overview, National Institute of Standards and Technology Internal/Interagency Report 8202, 2018, p 54, cited in Mik, Eliza, Smart Contracts: A Requiem (December 7, 2019). *Journal of Contract Law* (2019) Volume 36 Part 1, p 71
18. Makhovsky, Andrei (December 22, 2017). "Belarus adopts crypto-currency law to woo foreign investors".
<https://www.reuters.com/article/us-belarus-cryptocurrency-idUSKBN1EG0XO>
19. «Chapter 9: Building a Secure Future, One blockchain at a time», US Senate Joint Economic Committee, March 2018.
https://www.jec.senate.gov/public/_cache/files/aaac3a69-e9fb-45b6-be9f-b1fd96dd738b/chapter-9-building-a-secure-future-one-blockchain-at-a-time.pdf
20. Huckle, Steve; Bhattacharya, Rituparna; White, Martin; Beloff, Natalia (2016). "Internet of Things, Blockchain and Shared Economy Applications". *Procedia Computer Science*.
<https://doi.org/10.1016%2Fj.procs.2016.09.074>
21. Soloro, Kevin; Kanna, Randall; Hoover, David (December 2019). *Hands-On Smart Contract Development With Solidity and Ethereum: From*

Fundamentals to Deployment. California, U.S.A.: O'Reilly. p. 73

https://www.google.com/books/edition/Hands_On_Smart_Contract_Development_with/thbADwAAQBAJ?hl=en&gbpv=1&kptab=getbook

22. Ростислав Теряєв (2018). «Смартконтракти: що, як, коли?»

<https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/smartkontrakti-shcho-yak-koli.html>

23. Ivan Kot (2021). «Smart contract applications, limitations and future outlook».

<https://www.itransition.com/blog/smart-contract-applications>

24. Maria Luisa, Mena Duran (2020). «Does the future of smart contracts depend on artificial intelligence?» PG Researcher King's College London.

<https://www.thetechnolawgist.com/2020/12/07/does-the-future-of-smart-contracts-depend-on-artificial-intelligence/>

25. Truffle Suite documentation

<https://www.trufflesuite.com/docs>