Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра програмної інженерії
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи

магістра
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: **Розробка складних систем з використанням blockchain**

Виконав: студент VI курсу, групи СПм-62
спеціальності (напряму підготовки) 121
Інженерія програмного забезпечення
(шифр і назва спеціальності (напряму підготовки))

	(підпис)	Когут А.О. (прізвище та ініціали)
Керівник	(підпис)	Цуприк Г.Б (прізвище та ініціали)
Нормоконтроль	(підпис)	Бойко І.В. (прізвище та ініціали)
Рецензент	(підпис)	Михайлишин М.С. (прізвище та ініціали)

м. Тернопіль – 2019

ПЕРЕЛІК СКОРОЧЕНЬ, УМНОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

Blockchain	Ланцюжок з формованих блоків транзакцій, який побудований за певними правилами.
Bitcoin	P2P платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних.
Біткоїн-адреса	Біткоїн-адреса подібна до фізичної чи електронної адреси. Це єдина інформація, яку необхідно передати тому, хто надсилатиме Вам біткоїни, важлива відмінність полягає у тому, що кожна адреса повинна використовуватись тільки для однієї транзакції.
Блок	Це частина ланцюжку блоків, що містить та підтверджує багато транзакцій, що очікують підтвердження
Криптовалюта	Цифрові рахункові одиниці, облік яких децентралізований.

Майнінг	Процес, що передбачає використанн апаратних ресурсів комп'ютера з метою виконання математичних розрахункі для підтвердження транзакцій забезпечення безпеки мережі Біткоїн Винагородою за свої послуги майнер можуть збирати комісії за підтвержден ними транзакції - новостворені біткоїни
Ланцюжок блоків	Публічний запис біткоїн - транзакцій хронологічному порядку. Ланцюжо блоків єдиний
Етеріум	Платформа для створення практично будь-яких децентралізованих онлайн-сервісів на базі блокчейна (Đapps), що працюють на базі розумних контрактів
Смарт-контракти	Комп'ютерний протокол, який спрощує, верифікує, або забезпечує дотримання переговорів, або виконання договору, перевіряє непотрібні пункти договору. Смарт-контракти, зазвичай, мають інтерфейс користувача і часто слідують логіці договірних положень.

Приватний ключ	Це секретна послідовність певних даних, що дає вам право витрачати цифрову валюту з конкретного гаманця за допомогою криптографічного підпису.
P2P	Термін peer-to-peer означає системи, що працюють як організована спільнота, надаючи можливість кожному учаснику безпосередньо взаємодіяти з іншими.

ЗМІСТ

ВСТУП

Технологія blockchain зараз на своєму піку. Вона є новою технологією, яка вже докорінно трансформувала фінансовий сектор. Біткойн та інші електронні валюти працюють на блокчейні. Blockchain значно полегшив передачу грошей третім особам та приманку грошей на їхні проекти. Як і будь-яка нова технологія, яка полегшує життя людині, вона дуже популярна.

Ще не торкнувшись життя звичайних людей, він уже показав, як може докорінно змінити бізнес-процеси. Компанії, що використовують цю технологію, стають транскордонними: вони мають можливість залучати нових клієнтів у всьому світі. В даний час блокчейн використовується в основному постачальниками віртуальних послуг.

Ця технологія вирішила давні проблеми безпеки з обмеженою ємністю зберігання і вже дала можливість передавати та зберігати набагато дешевші дані, ніж традиційні послуги.

Blockchain - це розподілена база даних. Ви можете думати про це як про мережу з кількома вузлами (скажімо, їх є кілька, але насправді більше). Ці вузли зберігають мережеві записи: коли в мережу надходить нова інформація, вона додається до всіх вузлів. Особливість мережі полягає в тому, що вона отримує лише достовірну інформацію.

За допомогою blockchain ви можете ефективно реалізувати будь-яку діяльність, пов’язану з розподілом ресурсів. Дані будуть дуже добре захищені. Якщо вони знаходяться в одній базі даних, їх все одно можна зламати або замінити. У blockchain нічого не можна замінити без сліду. Це його найбільша перевага.

На самому базовому рівні блокчейн - це буквально лише ланцюжок блоків, але не в традиційному розумінні цих слів. Коли ми говоримо слова

"блок" і "ланцюг" в цьому контексті, ми фактично говоримо про цифрову інформацію ("блок"), що зберігається в публічній базі даних ("ланцюжок").

"Блоки" на блокчейні складаються з цифрових фрагментів інформації. Зокрема, вони мають три частини:

1) Блоки зберігають інформацію про трансакції, такі як дата, час та сума долара вашої останньої покупки від Amazon. (Цей приклад Amazon призначений для ілюстративних покупок; роздрібна торгівля Amazon не працює за принципом blockchain)
2) Блоки зберігають інформацію про те, хто бере участь в операціях. Блок для вашої закупівлі в Amazon записує ваше ім’я разом з Amazon.com, Inc. Замість використання власного імені ваша покупка записується без будь-якої ідентифікаційної інформації, використовуючи унікальний "цифровий підпис", подібний до імені користувача.
3) Блоки зберігають інформацію, яка відрізняє їх від інших блоків. Так само, як ви і умене є імена, які відрізняють нас один від одного, кожен блок зберігає унікальний код під назвою "хеш", який дозволяє нам розказувати його, крім кожного іншого блоку. Скажімо, ви зробили свою покупку на Amazon, але поки вона перебуває в дорозі, ви вирішите, що просто не можете протистояти і вам потрібна друга. Незважаючи на те, що деталі вашої нової транзакції виглядатимуть майже однаково, ніж попередні покупки, ми все одно можемо розповісти про блоки через унікальні коди.

Спочатку запропонований як дослідницький проект у 1991 році, Blockchain комфортно влаштовується у двадцяті роки. Як і більшість тисячоліть свого віку, Blockchain отримав широкий розголос протягом останніх двох десятиліть, коли компанії у всьому світі спекулювали на можливостях технології та на те, як вона розвиватиметься в наступні роки.

Завдяки безлічі практичних застосувань технологій, вже впроваджених та досліджених, блокчейн нарешті відомий у віці двадцяти семи років, значною мірою через біткойн та криптовалюту. Як лайфхак про мову кожного інвестора в країні, блокчейн має на меті зробити ділові та державні операції більш точними, ефективними та безпечнішими.

Слід зазначити, що використання технології blockchain також цікавить Україну. Тому стало відомо, що Україна досягла домовленості з міжнародною технологічною компанією Bitfury Group про передачу всіх електронних державних даних у блокчейн.

Таким чином, стає зрозуміло, що технологія Blockchain певною мірою є революційною і може бути використана в різних сферах людської діяльності. Зокрема, мова йде про такі реалізації, як: криптовалюта, різні реєстри, цінність підприємства або державне значення.

1 BLOCKCHAIN

1.1 Загальні поняття

У цьому розділі ми розглядаємо поняття blockchain, його основні характеристики.

Блокчейн - це база криптовалют. Сама назва частково характеризує мету Blockchain: частина "Block" складається з блоків, а "Chain" - рядок. Виявляється, "Blockchain" - це ланцюжок блоків, в якому він підтримує сувору послідовність.

Блоки – є даними про угоди, транзакції, контракти в середині системи, представлені в криптографічній формі (забезпечує конфіденційність, цілісність, правдивість інформації).

З самого початку блокчейн був (і залишається) основою криптовалюти біткойн. Всі блоки пов'язані між собою і щоб мати можливість створити новий блок, спершу потрібно прочитати інформацію зі старих блоків (Рисунок 1.1.1).

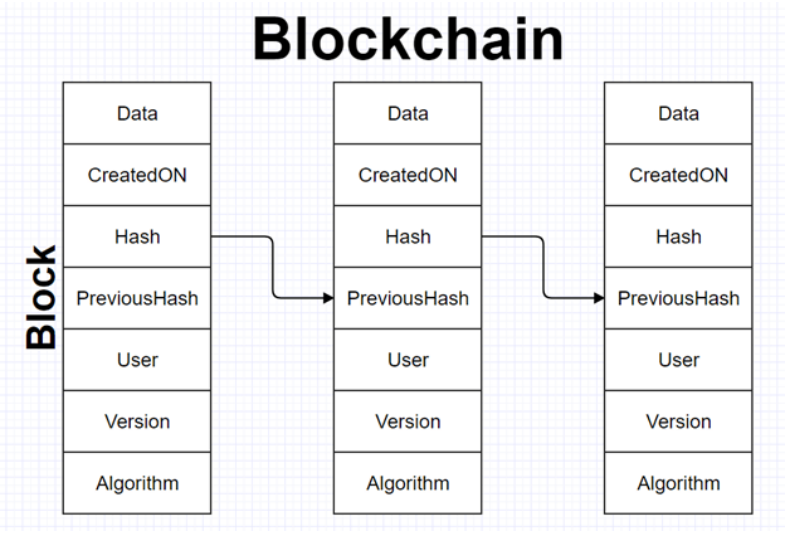

Рисунок 1.1.1 – Схема роботи blockchain

Усі дані в blockchain накопичуються і створюється єдина база даних, яка постійно оновлюється. Видалити або замінити блок цієї бази даних, який нескінченний, неможливо. Ви зможете записати нескінченну кількість транзакцій.

Операція блокової ланцюга виконується в режимі P2P (одноранговий - всі члени мережі рівні). У цьому випадку всі члени можуть спілкуватися безпосередньо між собою, на відміну від традиційної архітектури, коли лише одна категорія членів, що називається серверами, може надавати певні послуги іншим (Рисунок 1.1.2).

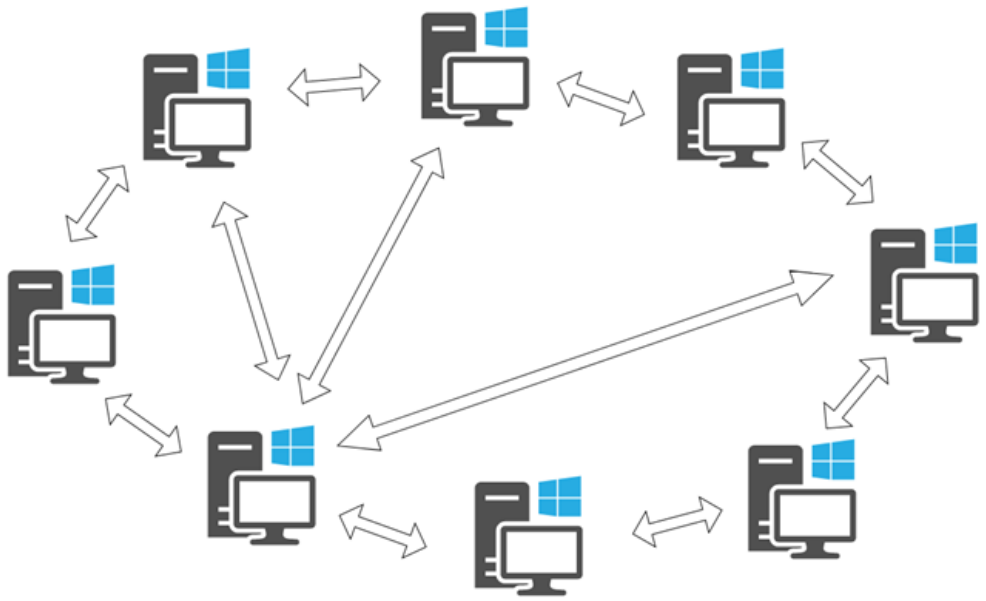

Рисунок 1.1.2 – Схема спілкування клієнтів

Ця технологія була створена з появою криптовалюти Bitcoin. Це сталося в 2009 році. Сатосі Накамото вважається громадським творцем нової віртуальної валюти та Blockchain. Однак ця людина міфіфікується у світі криптовалюти. Це прізвисько, за яким слідує один або кілька людей, які вирішили не розкривати свою особу. Очевидно, що знадобилося тисячі

годин, щоб створити блокчейн. Blockchain - це по суті розподілений реєстр, який реєструє транзакції між користувачами (Рисунок 1.1.3).

Є два види ланцюжків :

1) Public Blockchain - відкрита і сучасна база даних. Кожен учасник має право читати та записувати дані. Цей тип не підходить для організацій, що обробляють конфіденційну інформацію. Усі вузли рівні. Створюючи блоки, вони складають рядок і мають тимчасовий тег. Вони перевіряються комп'ютерами вузлів, перш ніж записуватися в блокчейн. Дані не є змінними, і всі транзакції є загальнодоступними. Цей тип Blockchain використовує криптовалюти Bitcoin та Ethereum (використовуються для створення розумних контрактів, ми обговоримо їх нижче). Однією з головних переваг публічного блокчейна є децентралізація. Наприклад, коли ми передаємо гроші з рук в руки, нам не потрібні банки чи посередники, це називається децентралізацією. Трансакція грошових переказів (в даному випадку в біткойнах) записується в мережу (блокчейн) раз і назавжди, змінити або скасувати її неможливо. Він не вимагає від посередників, які отримують гроші від клієнта і передають їх іншим, що гарантують укладення договору.

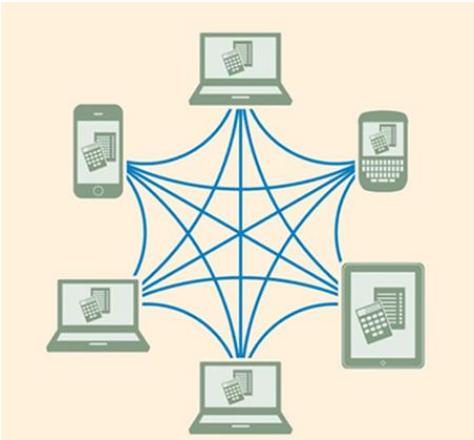

Рисунок 1.1.3 – Private Blockchain

Приватний Blockchain містить обмеження для читання/запису даних. Він використовується приватними організаціями і може співпрацювати лише за запрошенням цієї організації. Визначаються різні рівні доступу користувачів. Учасники повинні мати дозвіл читати, писати чи перевіряти сайт. Інформація шифрується з метою конфіденційності. Приватний Blockchain набагато швидше, ніж загальнодоступний Blockchain, і дозволяє визначати пріоритетні вузли. Підвид Private Blockchain - це ексклюзивний блокчейн. Цей ланцюжок створює групу людей, що займаються обробкою транзакцій. Вона називається консорціум. Консорціум - приватна мережа яко включає декілька компаній. Контрольні вузли вибираються заздалегідь. Він також визначає правила перевірки блоків у головному ланцюзі та параметри доступу до мережі (Рисунок 1.1.4).

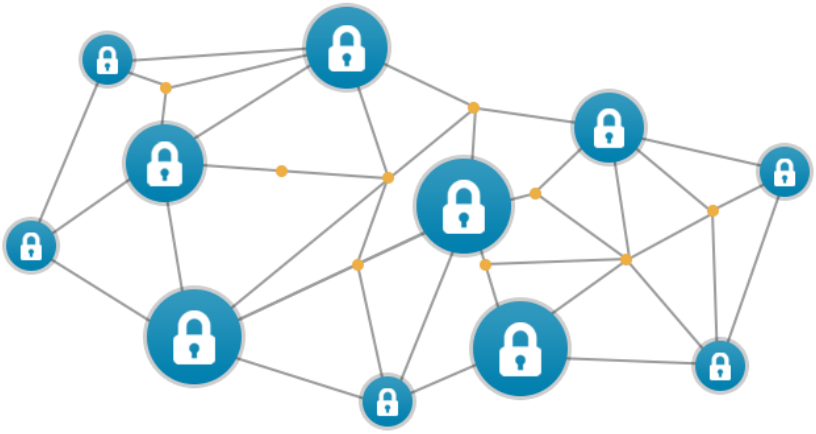

Рисунок 1.1.4 – Консорціум

1.2 Технічні деталі і нюанси роботи.

Кожен блок містить таблицю конкретних даних, і всі блоки пов'язані між собою. Тобто створення нової «таблиці» може бути виконано лише після закриття старої таблиці (Рисунок 1.2.1).

Рисунок 1.2.1 – Взаємодія блоків

Як ви бачите на зображенні вище, кожне посилання ланцюга містить певний ключ - хеш, згенерований за допомогою криптографічного алгоритму SHA256, застосованого до заголовка блоку. Він не закриється, поки не розшифрується. Як працює ця сама розшифровка? У криптовалютах за це відповідає майнінг. Майнер криптовалютних мін робить це за допомогою процесорів та відеокарт. Вони, у свою чергу, виконують обчислювальні операції, основною метою яких є пошук криптографічного підпису на блоці у вигляді хешу. Як тільки він обраний, блок закривається. І за це майнер отримує винагороду за криптовалюту.

Якщо ми подивимось на структуру блокчейна, це виглядає як структура даних. Він містить єдиний список посилань кожного вузла, з якого він має посилання на інший блок, але у випадку blockchain він має посилання на попередній блок.

Блокчейн часто візуалізується як вертикальний міст з накладеними блоками. Це відображення використовує термін "висота" для позначення відстані від першого блоку і "вершина" для позначення щойно доданого блоку.

Що до про публічного блокчейну - всі учасники рівні між собою, а сервера немає. Також, може здатися, що блокчейн не є надійним, але в цьому випадку кожен користувач blockchain є гарантом.

До Blockchain доступні спеціальні ключі - вони є для кожного користувача і являють собою набір криптографічних записів. Він абсолютно унікальний, не передбачаючи можливості його заміни або хакерських атак.

Створюючи гаманець Bitcoin, у користувача є два ключі: приватний та загальнодоступний. Публічний ключ - це певна адреса трансакції, за нею можна загальновідомо переказувати гроші або відслідковувати транзакції іншим користувачам. А приватний ключ відомий лише власнику гаманця, і саме він є гарантією безпеки коштів.

Для створення адреси гаманця, системою буде спочатку згенеровано приватний ключ і з нього, використовуючи хеш, створює відкритий ключ, який є підходе виключно одному приватному. Знання приватного ключа може легко допомогти у визначенні публічно, але зворотний процес не є можливий (Рисунок 1.2.2).

Рисунок 1.2.2 – Механізм створення адреси

Приватний ключ адреси Bitcoin - це складна криптограма, яка ідентифікує власника і дозволяє отримати доступ до грошей, що є типом підпису при виїзних транзакціях.

Приватний ключ - це 256-бітове число, яке можна записати у двійковій і шістнадцятковій формі.

У двійковій системі комбінація нулів і одиниць генерує приватний ключ біткойна. Наприклад, 0101111111000110. Але поводження з ключами

триває не дуже практично. Приватний ключ, таким чином, зменшується в байтах і записується як 32-байтне число, кожен символ вимагає двох цифр шістнадцяткової системи, тобто 64 символи від 0 до 9 і від A до F. Наприклад, C4453213301DA11B22BD67CC233AC31262. Діапазон комбінацій настільки великий, що якби вдалося зібрати мільярди комбінацій в секунду, це витратило б більше часу, ніж наша планета вже існувала.

Дійсний цифровий підпис створюється на основі секретного ключа, який підтверджує, що транзакцію перевіряє власник відкритого ключа. Цифровий підпис і відкритий ключ порівнюються, як тільки транзакція надсилається в мережу. Однак жоден з учасників аудиту не може знайти секретний ключ відправника угоди. Як тільки необхідна кількість блоків підтвердить дійсність підпису та відкритого ключа, транзакція визнається дійсною та завершеною. Таким чином забезпечується надійність внутрішніх транзакцій системи. Ще одна особливість приватного ключа - надійність зберігання криптовалюти на гаманці. Гаманець можна використовувати лише на приватному ключі.

Володіння криптовалютою підтверджується володінням приватного ключа, що зберігається у відповідному відкритому ключі. Це конфіденційна інформація, яка ніколи не передається третім особам і не реєструється системою. Приватний ключ забезпечує безпеку трансакцій та зберігання токенів у загальній системі. Цей ключ повинен надійно зберігати власник гаманця. У разі втрати неможливо відновити доступ до публічно доступних коштів.

1.3 Механізми, які забезпечують надійність блокчейну

1.3.1 Proof of Work

Використовується в криптосистемах для перевірки транзакцій та створення нових рядків у блокчейні. Майнери змагаються за право підписувати контракти так як за це отримуються нові одиниці криптовалюти.

Користувачі Інтернету можуть надсилати цифрові монети своїм друзям або роботодавцям. Децентралізований реєстр групує всі транзакції по блоках. Однак підтвердити угоду або створити нову блокам без участі користувача неможливо. Ця відповідальність покладається на плечі спеціальних вузлів, які називаються Майнерами. Сама процедура підтвердження операцій та створення нових блоків називається майнингом

Майнінг - це пазл, вирішити який можна лише за допомогою потужних обчислень.

Прикладом задачі яку він вирішує може бути наступна: які будуть вхідні параметри якщо маємо ось такий вихідний результат (функція хешу).

Функція Hashcash використовується в Bitcoin для утворення блоків. Під час майнингу потрібно підтвердити роботу, що стосується вмісту блоку, щоб блок був прийнятий системою. Складність цього завдання варіюється в залежності від того, як часто бувають блоки. Система запрограмована таким чином, що частота пошуку блоків складає в середньому 1 блок за 10 хвилин.

Оскільки процес пошуку блоку є дуже трудомістким і випадковим, неможливо з впевненістю передбачити, який биткойн-worker вирішить проблему і знайде блок. Щоб система визнала блок істинним, його хеш повинен бути меншим за поточну ціль.

Кожен блок вказує на те, що зроблено таку роботу з його пошуку:

1) Факторизація цілих чисел: Знаходження числа, отриманого в результаті добутку двох інших.
2) Guided Tour Puzzle Protocol, криптографічний протокол, призначений для захисту. Якщо сервер підозрює DDDoS атаку, ви повинні вирішити хеш-функцію для деяких вузлів встановленої послідовності.

Складність таких завдань повинна бути як високою для захисту від DDOS-атак і простою, щоб не перешкоджати створенню нових блоків. Відповідь повинна бути такою, щоб її легко перевірили інші вузли.

Майнер займається математичними проблемами, створює нові блоки та обробляє транзакції. Складність завдання залежить від кількості людей в системі, її потужності та її навантаження. Хеш кожного блоку містить хеш попереднього, що підвищує рівень безпеки та зменшує ризик зловмисника.

Якщо Майнер зможе знайти правильне рішення то буде створено новий блок. Укладені там угоди вважаються перевіреними.

1.3.2 Де можна зустріти використання Proof of work ?

У багатьох сучасних криптовалютах існують PoWs, найпопулярніші - це біткойни. І саме в Bitcoin закладені принципи такого типу транзакцій. Завдання відповідає алгоритму Hashcash. Це змінює складність залежно від ємності всієї системи. Криптовалюта на основі Bitcoin (наприклад, lightcoin) використовує ту саму систему, головна перевага полягає в тому, що вона захищає від DDoS-атак. Важливо, щоб у нього була достатня потужність комп'ютера для вирішення проблеми та створення нових блоків. Таким чином, власники портфеля з великими запасами грошей не можуть впливати на рішення, прийняті в системі.

Недоліки такого підходу:

1) Витрати. Експлуатація вимагає потужної комп'ютерної техніки, що дозволяє здійснювати складні розрахунки. Крім того, вартість такого обладнання може бути високою. Видобуток має сенс лише приєднавшись до пулів або створивши ферми. Обладнання споживає занадто багато енергії, що також збільшує виробничі витрати. Високі витрати загрожують криптографічній системі тим, що вона може бути централізованою, а управління нею зосереджено в одній руці
2) Марність розрахунків. Майнери постійно виробляють нові блоки та споживають багато енергії. Однак розрахунки, зроблені системою, більше ніде не використовуються. Вони лише забезпечують надійність мережі і не можуть бути застосовані у діловому світі, науці чи якійсь іншій галузі.

1.4 Атака 51%

Іншими словами - атака більшості, і це те, що користувач або група контролює переважну більшість виробничих потужностей. Як результат, у них достатньо «сильних сторін» для контролю над великою кількістю подій. У цьому випадку створення нових блоків монополізується. Користувач або група, яка взяла монополію, винагороджується та не надається іншим для повного участі в процесі.

Розглянемо наступну ситуацію. Припустимо, Тетяна перераховує гроші через блокчейн-мережу, і вона стала жертвою 51% нападу, а Андрій - ні. У цьому випадку угода знаходиться в блоці, але зловмисники не дозволяють вам повернути гроші Андрія. Інші зловмисники формуватимуть блоки та створюватимуть транзакції, використовуючи потужність своїх комп’ютерів, але в цьому випадку мережа буде порушена, це зменшить потік клієнтів, що

спричинить зменшення вартості валюти. В результаті нападник втратить лише свої гроші та свій час.

Загалом алгоритм перевірки завдань схожий на звітність на робочому столі. Співробітники регулярно подають аудиторські звіти, щоб підтвердити, що вони виконали конкретне завдання. В іншому випадку вони не отримають зарплату, оскільки не підтвердили виконану роботу.

PoW у blockchain робить перевірку обчислення, згенерованого при створенні нового блоку. Тут використовується наступна модель: блок розпізнається як істинний та закритий, за умови, що його хеш-значення менше, ніж підпис, до якого звертаються неповнолітні. Тобто певна криптографічна цифра вказує на справжність блоку. А вузли в цьому випадку виступають слухачами, підтверджуючи справжність блоку.

Proof of Stake

Засновник PoS також засував криптовалюту Ethereum. Він констатує, що цей алгоритм є менш застратним та дорогим, ніж PoW. Якщо головну роль в PoW відіграє потужність комп'ютерної техніки, в PDS - обєм гаманця. У цьому випадку всі учасники мережі, що володіють криптовалютою, стають інвесторами. Роль майнингу як галузі втрачає позицію, але головним недоліком такого підходу є можливість дублювання транзакцій. Найкращий варіант - комбінувати алгоритми PoS та PoW.

1.5 Застосування технології блокчейн у різних сферах життя

1.5.1 Визначення особистості

Тепер, ринкова економіка неможлива без визначення особистості, оскільки не є можливим точно визначити хто є власником матеріальних благ.

Доведення ідентичності може бути проблемою як для багатих, так і для бідних. Для багатих йдеться про боротьбу з відмиванням грошей, а ідентифікація важлива для запобігання злочинним та шахрайським діям, неправильне рішення яких збільшує юридичні та регуляторні витрати та клопоти. 90% компаній, опитаних Міжнародним опитуванням фінансів торгівлі у 2016 році Міжнародної торгової палати, заявили, що відмивання грошей є найбільшою перешкодою для торгівлі.

Рішенням цієї проблеми можуть стати спільні розподілені регістри (MDL) або блокчейн-технології. MDL - це багато організаційна база даних про аудит супер-слідів. Хоча центральна база даних може призвести до монополії, яку всі повинні використовувати тоді, факт полягає в тому, що MDL є загальними і їх важко використовувати як монополії. Ви не можете призначити свою копію реєстру, оскільки у вас її немає. Ніхто не може. Комп'ютери дотримуються загального протоколу, який дозволяє особам сворювати нові транзакції та розповсюджувати їх за допомогою тимчасової архітектури.

Технологія Blockchain забезпечує децентралізоване, надійне та послідовне виішення проблеми зберігання даних. Блокові рядки можуть забезпечити збереження цифрових даних людини в безпечному місці, яке не можна записати. Ці дані завжди містять найсвіжішу інформацію про людину.

Багато компаній усвідомили можливості нової технології та почали створювати системи управління цифровими ідентифікаціями та авторизацією на основі блокчейну. Серед перших були Bitnation, Civic, Blockchain Cambridge LLC, BlockAuth та Existence ID.

Діяльність державної платформи Bitnation спрямована на надання послуг, що надаються урядом. Тих хто користуються системою називають "громадянами" Bitnation. У липні минулого року громадський проект, який

спеціалізувався на шахрайстві та крадіжці захисту персональних даних, завершив ICO - ідентифікація особи, яка б повністю відповідала законам про конфіденційність.

Кожен проект цифрової ідентичності на основі блокчейна, що включає компанії та установи, не може бути корисним без згоди користувача. У багатьох галузях, що шукають спосіб використання рішень управління ідентифікацією користувачів на основі блокчейну, застосовуються суворі правила. У цей перелік входять банки, компанії з кредитними картками та медичні установи. Створення успішного проекту вимагає механізмів інформаційної безпеки, розподілу вузлів та децентралізації команди розробників.

Надалі кожна людина матиме цифровий клон, який надаватиме їм актуальну інформацію. Шифрування даних blockchain захистить людей від крадіжок особи. Ми зможемо вибрати, якими даними поділитися та з ким, використовуючи різні транзакційні канали торгівлі, які відповідають поставленим вимогам. Залишаються лише питання щодо платформ управління цифровою ідентичністю блокчейну, які досягнуть критичної маси та створять мережевий ефект.

1.5.2 Авторські права

Інтеграція технології допоможе спростити складний захист авторських прав. Тепер, щоб підтвердити свої авторські права, творці повинні довести свою першість, щоб реалізувати ідею на практиці та забезпечити надійний запис про дату та зміст твору.

Наприкладом може бути Mediachain. Проект що дозволяє авторам не стати здобиччю плагіату та цинічної крадіжки, зберігаючи весь новий вміст в єдиному блокчейні.

Співзасновниками служби є Джессі Уолден та Деніс Назаров, які організували стартап. Вони помітили потужність Інтернету та технології Blockchain для миттєвого зберігання даних у глобальному масштабі, що було б корисно творчим людям, оскільки захист авторських прав займає занадто багато часу та бюрократичних клопотів. У цьому випадку також буде доступний зворотний пошук, коли автора твору можна буде знайти через твір. При запуску акцент буде зроблено на образотворчому мистецтві. Використовуючи спільно з такими ресурсами, як Instagram, проект Mediachain вказує автору фактичної фотографії, коли вона буде перевидана іншими користувачами в мережі.

В довгостроковій перспективі така надійна база даних може дати можливість створювати мультимедійні платформи нового покоління, які тісно співпрацюватимуть з проектом та дозволять середньостатистичним авторам ефективно монетизувати власну творчу роботу.

Крім того, існує платформа Ascribe, яка використовує додатковий реєстр, в якому художники, музиканти та винахідники можуть зберігати авторські права, використовуючи зашифровані облікові дані.

Перша ж хвиля використання повністю змінила підхід до придбання, оцінки реклами та її доставки. NYIAX (Нью-Йоркська інтерактивна рекламна біржа) - перший в світі обмін контактами для реклами. AdShares - це децентралізований рекламний ринок особистого спілкування. MadHive - це платформа для відеореклами та обміну даними, яка дозволяє брендам та видавцям будувати стосунки для залучення аудиторії на різних платформах. Загалом, блокчейн-технології в галузі захисту інтелектуальної власності значно спрощують віднесення до певного змісту.

1.5.3 Голосування

Канада, Нідерланди, Бразилія, США та Франція вже прийняли електронне голосування. У Швейцарії нещодавно блокчейн провів свої перші вибори. Естонія - найдосконаліша. Також є вимоги секретності, але офіційне онлайн-голосування проводиться в країні вже більше десяти років.

Як так вийшло? В Естонії таємне голосування вважається правом, а в Україні таємне голосування - обов'язком. "У нас є стаття, за те що ви повідомили як проголосували, наприклад, за зображення галочки в інформаційному бюлетені, а в деяких випадках це злочинний пункт", - говорить Флонт.

У випадку Естонії все трохи інакше. Виборник може голосувати здалеку, але якщо він не впевнений, що таємне голосування захищене, він може проголосувати знову за тиждень. В останній день на виборчій дільниці він може обрати традиційний спосіб, шляхом паперового голосування, і це його голос. Цей алгоритм дає право як на пряме таємне голосування, так і на електронне голосування. Онлайн-вибори в Естонії відбуваються без технології blockchain, але реалізувати це буде простіше у такому форматі, ніж в Україні.

1.5.4 Управління і юриспруденція

Надалі юристи укладуть контракти так само, як розробники програмного забезпечення пишуть код програми. Можливо, юристи майбутнього повинні знати основи програмування, щоб мати можливість створювати смарт-контракти на основі блокчейна (ці договори вже використовуються). Більше того, юристам потрібно буде зрозуміти тонкі нюанси використання цих технологій для пояснення потенційних підводних каменів та найкращих практик використання таких систем у конкретному

бізнесі клієнта. Деякі країни, як Гондурас, вже висловили своє тверде зобов'язання замінити існуючі реєстри нерухомості технологією blockchain і, можливо, зможуть продати чи придбати житло через додаток iPhone колись.

Контрактована взаємодія окремих людей також може різко змінитися. Наприклад, застосування принципів справедливості, безумовно, докорінно зміниться. Більшість розумних контрактів самореалізуються. Коли певні умови виконуються і це підтверджено в блокчейн, криптовалюта автоматично розблокується та контролюється іншою стороною. Ця угода нічого не порушує, це очевидно для всіх, також скасувати її майже неможливо. Псевдонімність учасників цих ринків ще більше ускладнює Ситуація ще більше ускладнюється, враховуючи псевдонімність учасників таких ринків.

Що стосується більш мирських угод, сторони можуть навіть бути незнайомі. Таким чином, якщо сторона вважає, що аспект договору не був дотриманий (наприклад, контракт був неналежним чином укладений), він може не отримати компенсації збитків від нашої правової системи. Це створить серйозні проблеми для законодавців.

Оскільки блокчейн - це структура децентралізована, учасники (самі по собі), можуть залишатися анонімним, що призводить до неможливості пені або стягнення у разі порушення договору. Зрештою, проблеми компенсації не завадять розвитку блокчейн-технологій. Арбітражні механізми та навіть засоби доступу до операцій у традиційних правових системах вже обговорюються. Однак ці механізми потрібно буде включити до коду індивідуальних розумних договорів у міру їх написання, і адвокати повинні будуть пояснювати клієнтам, як це працює і навіщо це.

Замість того, щоб складати найбільш детальні контракти на основі звичних шаблонів та змінювати їх у Microsoft Word, юристи можуть

визначати договори, використовуючи кілька рядків коду. 95% вашого договору позики можна замінити найпростішим шматком коду. Перевага такого підходу полягає в тому, що з часом усі договори стануть одноманітними, що зменшить витрачання ресурсів та прискорить примирення між різними сторонами.

1.5.5 Сертифікація операцій

Більшість документів бухгалтерського обліку є у підробленому папері чи електронних книгах. Інформацію про блокчейн, яка є послідовним ланцюжком блоків даних і зберігається на комп'ютері, не можна редагувати.

Так, цифрова інформація поділяється на пов'язані блоки. Припустимо, кожен блок це конкретна країна і містить інформацію про свої міста. Весь вміст блоку перетворюється в єдиний числовий рядок фіксованої довжини під назвою "хеш", такий як "6hp613AHA02". Нехай американський блок містить міста Нью-Йорк, Лос-Анджелес та Чикаго, тоді він буде відповідати хешу "NILACH".

Кожен блок має у собі хеш попереднього блоку - це з'єднує їх один з одним. Якщо хтось спробує змінити перший блок, наприклад, додати місто Бостон, хеш блоку буде автоматично змінено на NILACHB. Але наступний блок після американського блоку, Індія вже зареєстрував попередній хеш "NILACH". Через цю різницю ланцюг руйнується. В результаті інформація блокчейн не може бути пошкоджена або видалена, і якщо хтось намагається це зробити, всі члени ланцюга негайно повідомляються про це.

1.5.6 Цифрові активи

ICO або початкова позиця койнів (подібно до початкового розміщення акцій) - це новий спосіб залучення фінансування. Інвестором може стати будь-хто у світі. У цьому випадку гарантією є не акції, а цифрові активи, які

називаються "жетонами", що зберігаються в блокчейн-портфелях. Власник може використовувати ці активи щоб оплачувати послуги бізнесу або для обміну «звичайних» грошей, коли їх вартість з часом збільшується.

Розумний контракт - це програмний алгоритм, призначений для укладання та обслуговування контрактів блокчейн. Розумні контракти не тільки містять інформацію про обов'язки сторін, але й автоматично гарантують дотримання умов цього договору. Ці договори реєструються в кодовій формі. Наприклад, орендар зобов'язаний щомісяця платити за квартиру. У цьому випадку код виглядав би так: "Якщо сьогодні тридцятий день місяця, ви повинні перерахувати N-ту суму з рахунку того хто орендує приміщення на рахунок власника".

Розумний контракт зберігається не лише на комп'ютерах обох сторін, але й записується в блокчейн, а копія його коду доступна для всіх учасників мережі. При укладанні такого типу договору 30 числа кожного місяця, опівночі, програма підключається до рахунку орендодавця і автоматично знімає необхідну суму на користь власника.

Сервіси зберігання, такі як Google Drive та Dropbox, популярні сьогодні. Однак немає гарантії, що вони не можуть отримати доступу до даних своїх користувачів. Крім того, уряд може вимагати розкриття збереженої інформації. Блокчейн - це децентралізована база даних, яка зберігається на великій кількості комп'ютерів у повністю зашифрованому вигляді, що також сприяє зниженню витрат. І кожен може орендувати вільний простір на жорсткому диску - наприклад, у Storj.

1.5.7 Енергетика

Засновники Energy Blockchain Labs стверджують, що компанія - єдина компанія у світі, діяльність якої повністю присвячена повному циклу

створення цінності в енергетичній галузі. Заснована в 2016 році трьома фахівцями в такій галузі як енергетика, фінанси та інформаційні технології, лабораторія працює над проривними рішеннями, включаючи спільні проекти з іншими компаніями з розробки ряду Інтернет-технологій в області енергії що вирішує виробничі завдання для споживання енергії, торгівлі, управління тощо.

В енергетичному секторі є й інші сфери, де талановиті підприємці знайшли спосіб впровадити децентралізовані децентралізовані регістри. Ось кілька цікавих прикладів.

Grid Singularity - це галузева, децентралізована, платформа обміну інформацією, яка надає різноманітні програми, які спрощують аналіз та тестування даних, керують розумними сітками, працюють із зеленими сертифікатами тощо.

Проект TransActive Grid від LOA Energy - це криптографічно захищена платформа з відкритим кодом для додатків. Вбудовані інструменти бізнес-логіки дозволяють вимірювати рівень виробництва та споживання електроенергії, а також інших показників у режимі реального часу. Наразі проект знаходиться в стадії розробки, і на сьогоднішній день в районі Нью-Йорка в Брукліні працює перший демонстраційний майданчик.

1.5.8 Організація приватного та державного управління

Блокчейн можна використовувати не тільки для прозорості та цілісності політсистем. Навіть існує міжнародна віртуальна нація що називає себе BITNATION. У ньому є фізичні місця, громадяни, партнери, та посли всьому світу. Кожен може приєднатися до нього без будь-яких обмежень.

Ще один цікавий приклад - Advocate, ресурс для поліпшення взаємодії громадян з урядовими посадовими особами, спрямована на підтримку

простих членів суспільства та претендентам на керівні посади в місцевих органах влади.

Компанія з управління, під назвою Borderless - платформа громадянського управління, яка позиціонується як коаліція юридичних послуг (шлюб, бізнес, нотаріат) та економічних (базовий дохід, фінансові операції) на основі смарт контрактів і Блокчейн простору.

З точки зору ефективних управлінських рішень в рамках організацій, для цього існують такі послуги, як Colony, Otonomos, BoardRoom. Друга та третя з яких автоматизують процес створення, фінансування та керування бізнесом через Blockchain. Colony дозволяє жителям усього світу створювати інтернет-бізнес.

1.5.9 Сфера інтернет речей

По-перше, те, що пов’язано з використанням блокчейна в Інтернет речах, - це цілісність даних та їх безпека. Насправді використання розподіленого реєстру в IoT набагато ширше і глибше.

Рішення Blockchain та IoT в певних областях мають на меті швидко встановити взаємодію між декількома економічними агентами. Ці зв'язки передбачають юридичні та фінансові наслідки, а часто потребують формалізації відносин шляхом укладення угоди про рівень обслуговування (SLA). Цей блокчейн-документ визначає загальні поняття, права та обов'язки обох сторін, вимоги якості та іншу відповідну інформацію. Використання розумних контрактів може дати змогу системі отримати об'єктивну інформацію про дотримання Угоди про економічну відповідальність, а також відповідні стимули або санкції для учасників бізнесу.

За словами Джона Вілмса, блокчейн може впорядкувати багато процесів і створити нову систему довіри на основі відносин, яка виключає всі

типи шахрайства. Вілмс також вважає, що стрімкий розвиток Інтернету речей створює проблеми управління, які раніше не існували.

Існує багато цікавих прикладів взаємодії цих двох дуже перспективних технологій.

Наприклад, Filament використовує blockchain та IoT для інтелектуального управління великими промисловими системами. Рішення, розроблені компанією, здатні підвищити ефективність в різних галузях промисловості, будь то видобувна промисловість або сільське господарство.

Chimera пропонує інноваційну систему для покращення догляду за людьми похилого віку або тих, що потребують допомоги. Він використовує фізичні пристрої (у вигляді браслетів та медальйонів) та додатки для віддаленого збору та аналізу життєдіяльності, а також для виявлення ситуацій, у яких підтримка цих пристроїв потребує допомоги.

Стартап blockchain Factom обговорює перспективні розробки. Абі Добал, що є віце-президентом компанії з розвитку бізнесу, зауважує, що ідентифікація пристроїв та забезпечення цілісності даних будуть основними напрямками використання блокчейна в IoT. Factom створює блокчейн-рішення, що дозволяють організаціям захищати найважливішу інформацію. Розроблені компанією блокчейн-рішення пропонують великі можливості для прозорого аудиту бізнес-процесів та фінансових послуг, реєстрації прав власності, гарантії цілісності та надійності медичних записів тощо.

Слід зазначити, що минулого року команда Factom отримала грант від уряду США на розробку рішень для цифрової ідентифікації в Інтернет-об’єктних додатках (IoT).

Массачусетський Context Labs розробляє рішення, які допомагають виявити підроблені продукти. За словами генерального директора Context Labs, Ден Харпл, компанія спеціалізується на Інтернеті всього (IoE) і прагне

використовувати технологію blockchain максимально ефективно для боротьби з піратством, підвищуючи ефективність роботи мережі закупівель, захисту брендів та розвитоку довгострокових відносин із клієнтами тощо.

Intel, який нещодавно продемонстрував роботу блокчейн-платформи для відстеження ланцюгів поставок морепродуктів, також відстає. Платформа дозволяє ефективно контролювати виробництво морепродуктів, підвищує точність та надійність їх обліку з моменту захоплення, а також сприяє дотриманню умов зберігання відповідно до вимог. На момент запуску нового продукту IT-гігант показав, як датчики IoT використовуються для відстеження даних, що зберігаються в блокчейні, що містить інформацію про власника, місцезнаходження товару, температуру зберігання тощо.

Німецький промисловий гігант Bosch плонує використовувати блокчейн-технологію для протидії шахрайству, пов'язаному зі зниженням лічильника треків. Рішення базується на розподіленому реєстрі, який надсилає дані пробігу, і за допомогою програми на смартфоні власник може в будь-який час перевірити його фактичний пробіг, порівнюючи його, наприклад, з показаннями, відображеними на екран автомобіля.

1.6 Eutherium

Ethereum (ethereum, ефір) - це як криптовалюта, так і функціональне децентралізоване середовище, що справді зробило революцію у всій комп'ютерній сфері. Творці Eutherium, серед яких виділяється Віталій Бутерин, переслідували стандартну мету творців криптовалют - покращити біткойн при запуску цієї платформи. Однак bitcoin-ом 2.0 ефір важко назвати. Вони дещо схожі, але між ними існує низка концептуальних відмінностей.

Про це сказали не багато, але бум криптовалют 2016-2017 років пов'язаний із запуском та просуванням Ethereum. Нове середовище

максимізувало потенціал блокчейна в галузі фінансових технологій і стало поштовхом до запуску нових стартапів та залучення величезних інвестиції. ETH міцно захопив статус другої за популярністю та найреволюційною криптовалютою у світі. Тоді ми поговоримо про функції Ethereum, не вдаючись до технічних деталей.

Вірно догматичній термінології, Ethereum - це платформа для створення та використання децентралізованих додатків на основі блокчейна з смарт контрактами. Внутрішня валюта платформи - ефір. Скорочення ETH. Ефіри використовуються не тільки як одиниця обліку. Вони також гарантують виконання смарт контрактів, виступаючи в якості палива.

Творцем і головним ідеологічним натхненником, що стоїть за Ethereum, є росіянин Віталій Бутерин. Він зацікавився криптовалютами в 2011 році, деякий час публікуючи журнал Bitcoin. У той же час він уважно вивчає програмування та планує створити вдосконалену блокчейн-платформу.

Про це згадує сам Бутерин: «Ідея створення Ethereum прийшла не одразу. Спочатку я намагався просувати її в проект, над яким працював. Але мені сказали, що на його реалізацію піде рік. Тож я покинув роботу.

Пам’ятаю, як ходив по Сан-Франциско, думаючи, тоді я взяв і написав білий папір, надіслав його своїм друзям. Ось як все і почалося. " 2013 рік прийшов. Вже в 2014 році розпочато збір коштів для розвитку платформи за допомогою краудфандингу. ICO Ethereum зібрав 31101 BTC (понад 18 мільйонів доларів), а також у проекті брали участь банки та фінансові установи. Сам запуск відбувся уже липні 2015 року. Однак як така вона запрацювала у березня 2016 року з випуском Homestead.

Ethereum надав нові можливості для створення децентралізованих проектів та стартапів на основі blockchain та смарт-контрактів. Одним із таких стартапів був The DAO. Це платформа дослідження інвестиційних

проектів, побудована на основі розумних контрактів. ICO DAO став одним з найуспішніших в історії. Під час краудфандингу вдалося зібрати 150 мільйонів доларів інвестицій. Однак через помилку у вихідному коді частина коштів (60 мільйонів доларів) була вкрадена.

Щоб відновити викрадені кошти, було запропоновано відкотити мережу. Це поверне блокчейн до початкового стану - ще до того, як летіти до ДАО. Повного консенсусу в мережі не було досягнуто, тому паралельно з Ethereum вийшов Ethereum Classic - версія "відкату". Незважаючи на те, що це дало можливість повернути вкрадені інвестиції, його окритикували за порушення одного з головних принципів блокчейну - незворотності операцій.

Запуск Ethereum серйозно пожвавив світ криптовалюти, показавши універсальність та його гнучкіст. Автори платформи створили середовище з практичними інструментами, в яких людина без серйозної технічної підготовки може створити стартап або децентралізовану програму. Наприклад, у криптовалюти Namecoin лише 5 рядків коду. Тому Ethereum можна назвати гнучким механізмом, в якому всі розробки базуються на смарт контрактах. Раніше концепцію смарт контракту називали однією з основ Ефіріуму. Це комп'ютерний алгоритм, який забезпечує контракти всередині блокчейна. Розумні договори будуються таким чином, що певні дії відбуваються лише за певних умов.

Роботу розумного контракту можна пояснити простим прикладом оренди квартири. Оплата є необхідною умовою користування будинком. Поки орендар платить, він може спокійно користуватися будинком. В іншому випадку може бути запрограмований теоретично діючий договір для блокування замків дверей. І людина просто не зможе увійти в квартиру, поки не сплатить оренду. Приклад умовний, але у чіткому форматі він пояснює мету та принцип розумних договорів. Це гарантує децентралізацію, оскільки

орендар і власник безпосередньо співпрацюють. Без банківських чеків, рахунків тощо. Творцем і головним ідеологічним натхненником, що стоїть за Ethereum, є росіянин Віталій Бутерин. Він зацікавився криптовалютами в 2011 році, деякий час публікуючи журнал Bitcoin. У той же час він уважно вивчає програмування та планує створити вдосконалену блокчейн-платформу. Про це згадує сам Бутерин: «Ідея створення Ethereum прийшла не одразу.

Спочатку я намагався просувати її в проект, над яким працював.Але мені сказали, що на його реалізацію піде рік. Тож я покинув роботу. Пам'ятаю, як ходив по Сан-Франциско, думаючи, тоді я взяв і написав білий папір, надіслав його своїм друзям. Ось як все і почалося. " 2013 рік прийшов. Вже в 2014 році розпочато збір коштів для розвитку платформи за допомогою краудфандингу. ICO Ethereum зібрав 31101 BTC (понад 18 мільйонів доларів), а також у проекті брали участь банки та фінансові установи.

Сам запуск відбувся уже липні 2015 року. Однак як така вона запрацювала у березня 2016 року з випуском Homestead. Ethereum надав нові можливості для створення децентралізованих проектів та стартапів на основі blockchain та смарт-контрактів. Одним із таких стартапів був The DAO. Це платформа дослідження інвестиційних проектів, побудована на основі розумних контрактів. ICO DAO став одним з найуспішніших в історії.

Під час краудфандингу вдалося зібрати 150 мільйонів доларів інвестицій. Однак через помилку у вихідному коді частина коштів (60 мільйонів доларів) була вкрадена. Щоб відновити викрадені кошти, було запропоновано відкотити мережу. Це поверне блокчейн до початкового стану - ще до того, як летіти до ДАО. Повного консенсусу в мережі не було досягнуто, тому паралельно з Ethereum вийшов Ethereum Classic - версія

"відкату". Незважаючи на те, що це дало можливість повернути вкрадені інвестиції, його окритикували за порушення одного з головних принципів блокчейну - незворотності операцій. Запуск Ethereum серйозно пожвавив світ криптовалюти, показавши універсальність та його гнучкіст. Автори платформи створили середовище з практичними інструментами, в яких людина без серйозної технічної підготовки може створити стартап або децентралізовану програму. Наприклад, у криптовалюти Namecoin лише 5 рядків коду. Тому Ethereum можна назвати гнучким механізмом, в якому всі розробки базуються на смарт контрактах.

Раніше концепцію смарт контракту називали однією з основ Ефіріуму. Це комп'ютерний алгоритм, який забезпечує контракти всередині блокчейна. Розумні договори будуються таким чином, що певні дії відбуваються лише за певних умов.

Роботу розумного контракту можна пояснити простим прикладом оренди квартири. Оплата є необхідною умовою користування будинком. Поки орендар платить, він може спокійно користуватися будинком. В іншому випадку може бути запрограмований теоретично діючий договір для блокування замків дверей. І людина просто не зможе увійти в квартиру, поки не сплатить оренду. Приклад умовний, але у чіткому форматі він пояснює мету та принцип розумних договорів. Це гарантує децентралізацію, оскільки орендар і власник безпосередньо співпрацюють. Без банківських чеків, рахунків тощо.

1.7 Smart Contracts

Смарт-контракт Ethereum - це умова письмової угоди з використанням коду, який повинен бути виконаний одержувачем та продавцем будь-якого товару чи валюти. По суті, він виступає посередником між двома сторонами.

Наприклад, розглянемо невелику транзакцію за допомогою смарт-контракту Ethereum: двоє користувачів вирішили обміняти криптовалюти за допомогою цієї технології. Один з них надсилає свої кошти програмі, де вони в безпеці. Зараз ніхто не може отримати доступ до них. А другому користувачеві потрібно виконати свої умови: перерахувати певну суму в ту саму програму. Як тільки ця умова буде виконана, торговці отримують гроші. Якщо хтось із учасників не дотримується угоди, гроші повертаються їх власникам.

Після реєстрації угоди всі дані щодо неї зберігаються у блокчейні. І ніхто не може отримати доступ до цієї інформації. Десятки тисяч примірників можна знайти на комп'ютерах різних користувачів по всій планеті. Великою перевагою створення смарт-контракту на Ethereum є його повна автоматичність. Участь третіх осіб взагалі не потрібна. Це означає, що користувачі можуть зекономити багато грошей на комісіях, які повинні платити торгові посередники.

До речі, подібні операції виконуються у сфері нерухомості: минулого року, наприклад, у Києві, користувач скористався послугою Propy, щоб придбати квартиру в місті. Однак через те, що офіційне використання криптовалюти в Україні не може, довелося розробити додатковий договір обміну. Ви також повинні зв'язатися з адвокатом для повторного видання паперів від імені іншої особи: проте оплата була здійснена за допомогою смарт-договору Ethereum.

1.7.1 Звичайний контракт vs. смарт-контракт

Перш ніж розбиратися в деталях, давайте візьмемо приклад різниці між стандартним паперовим договором та смарт-цифровим договором. Як це працювало до появи розумних контрактів? Уявіть групу людей, які хочуть

встановити правила та умови розподілу цінностей, а також механізм забезпечення цього розподілу відповідно до заданих правил та умов. Потім вони зустрілися, склали договір, на якому вони записали свої дані, умови, значення, пов'язані з цим, встановили дату та підписали. Цей договір також було надано стороні довіри, наприклад, нотаріусу. Крім того, ці особи по-різному не погодилися зі своєю паперовою копією такого договору і почали виконувати будь-які дії, які можуть не відповідати самому договору, тобто вони зробили річ, і на папері їх запевнили, що вони повинні зробити щось інше.

І як вийти з цієї ситуації? Насправді, деякі члени групи мають взяти цей документ, зібрати докази, подати його до суду та шукати відповідності між договором та фактичною дією. Часто важко отримати справедливе виконання цього договору, що має неприємні наслідки. А смарт контракти? Вони поєднують в собі як можливість написання умов договору, так і суворий механізм примусового виконання. Якщо умови були визначені та підписана відповідна трансакція або додаток, змінити умови або призначити їх під час прийняття цього запиту чи транзакції вже неможливо. Є валідатор або вся мережа, а також база даних, в якій зберігаються всі розумні контракти, виконані в суворому хронологічному порядку. Що ще важливіше, ця база даних повинна містити всі тригерні умови виконання розумного контракту. Крім того, він повинен враховувати те саме значення, що і розподіл, описане в договорі. Якщо це цифрова валюта, ця база даних повинна враховувати це.

Коротше кажучи, валідатори таких контрактів повинні мати доступ до всіх даних, що використовуються в них. Наприклад, база даних повинна використовуватися для обліку як цифрових валют, транзакцій користувачів,

так і часових позначок. Тоді в розумному договорі умовою може бути отриманя певної суми на рахунку користувача, певний час або факт угоди.

1.7.2 Визначення смарт-контракту

Взагалі сама термінологія була винайдена дослідником Ніком Сабо і вперше була застосована в 1994 році, і була задокументована в 1997 році в статті, що описує саму ідею розумних контрактів.

Розумні контракти означають, що існує деяка автоматизація розподілу вартості, яка може залежати лише від заздалегідь визначених умов. У найпростішому варіанті це звучить як договір із строго визначеними умовами, підписаними деякими сторонами.

Розумні контракти розроблені для мінімізації довіри до третіх сторін. Іноді центр рішень, від якого все залежить, повністю виключається. Крім того, ці договори простіше перевірити. Це наслідок деяких конструктивних особливостей такої системи, але частіше за все ми розуміємо розумний контракт як децентралізовану мережу і функції, які дозволяють будь-кому аналізувати базу даних і виконувати повну перевірку виконання договору.

Це забезпечує захист від зворотних змін до даних, що призведе до змін у виконанні самого контракту. Оцифрування більшості процесів під час створення та виконання розумного контракту часто спрощує технологію та витрати на їх виконання.

Можна привести такий приклад: у нас є я будь-який покупець і також інтернет-магазин. Покупець хоче придбати монітор у даному магазині. У простішому випадку покупець створює та надсилає платіж, а інтернет-магазин приймає, підтверджує та відправляє товар. Однак у цій ситуації потрібна велика впевненість - покупець повинен довіряти інтернет-магазину у розмірі загальної вартість монітора. Оскільки для покупця магазин може

мати погану репутацію то існує ризик, що з якихось причин після отримання оплати магазин відмовиться від послуги і не відправить телевізор. Тому покупець задається питанням (відповідно, і інтернет-магазин задає це питання), що можна застосувати в цьому випадку, щоб мінімізувати ці ризики та зробити ці транзакції надійнішими.

Що стосується біткойна, ви можете дозволити покупцеві та продавцеві самостійно вибрати посередника. У вирішенні суперечливих питань бере участь багато людей. А наші учасники можуть обрати із загального списку посередників, яким довірятимуть одночасно. Разом вони створюють багатосигнатурну адресу 2 з 3, де є три ключі, і два підписи потрібні двом ключам, щоб отримати кошти з адреси. Власником одного ключа є покупець, іншого - інтернет-магазин, а третій - посереднику. І за такою багатозначною адресою покупець надішле суму, необхідну для оплати монітора. Тепер, коли продавець бачить, що гроші на деякий час були заблоковані за адресою мультисигнатури, яка залежить від нього, він може впевнено відправити монітор поштою.

Потім покупець отримує пакет, оглядає товар і приймає рішення про остаточну покупку. Він може повністю погодитися зі службою і підписати транзакцію своїм ключем, де він передає шматки багатосигнатурної адреси продавцю, і може в чомусь сумнівається. У другому випадку він спілкується з посередником, щоб встановити альтернативну транзакцію, яка по-різному поширюватиме ці монети.

Скажімо, монітор трохи подряпаний і що кабель не знаходиться в коробці для підключення до комп'ютера, хоча веб-сайт інтернет-магазину сказав, що кабель повинен бути включений. Потім покупець збирає докази, необхідні для підтвердження того, що посередник був обманутий у цій ситуації: він робить знімки екрана сайту, фотографує чек поштою, робить

фотографії подряпин на моніторі та показує, що ущільнення було зламане і кабель потягнувся. Схожі дії робить і інтернет-магазин, збираючи свої докази та передає їх посереднику.

Посередник хоче задовольнити як обурення покупця, так і інтереси інтернет-магазину (ми розуміємо, чому). Це така угода, при якій монети з багатозначними адресами будуть витрачені у певній угоді між покупцем, інтернет-магазином та посередником, оскільки він отримує порцію як винагороду за свою роботу. Припустимо, що 88% від загальної суми належить продавцю, 9% - посереднику та 3% - компенсації покупцеві. Угода підписується посередником своїм ключем, але не може бути застосована, оскільки для цього потрібні два підписи а не лише один. Він відправляє цю транзакцію і покупцеві, і продавцю. Якщо хоча б одну з них влаштовує такий варіант розподілу монет, транзакція буде попередньо підписана та трансльована в мережі. Для перевірки достатньо, щоб одна із сторін угоди погодилася з варіантом посередника.

Важливо спочатку вибрати посередника, щоб обидва учасники довіряли йому. У цьому випадку він буде діяти незалежно від інтересів того чи іншого та об’єктивно оцінювати ситуацію. Якщо посередник не пропонує такий варіант розповсюдження монет, який задовольнить принаймні одного учасника, то, домовляючись разом, покупець та інтернет-магазин можуть передавати койни на нову багатосигнатурну адресу шляхом скріплення їх двох підписів. Нова адреса мультисигнатури вже буде зроблена з іншим посередником, який міг би бути більш компетентним у цій галузі та запропонувати кращий варіант.

Розглянемо більш складніший приклад, який більш чітко відображає можливості розумного контракту. Скажімо, є троє хлопців, які нещодавно переїхали до гуртожитку. Троє зацікавлені придбати холодильник у свою

кімнаті, яким вони будуть ділитися. Один з них погодився зібрати суму, необхідну для придбання холодильника та домовитися з продавцем. Однак вони нещодавно зустрілися і між ними недостатньо довіри. Очевидно, двоє з них ризикують віддавати гроші третій стороні. Більше того, вони повинні домовитись про вибір продавця.

Перша умова заключається в тому, щоб до певного періоду сказати, що протягом одного тижня три платежі певної адреси на певну суму повинні бути надіслані на відповідний контрактний рахунок. Якщо цього не відбудеться, смарт-контракт буде розірвано і всі кошти бдуе повернено учасникам. Якщо умова виконується, вказуються значення ідентифікаторів продавця та посередника, і перевіряється умова, що всі учасники погоджуються з вибором постачальника та посередника. Коли всі умови виконані, кошти перерахуютьсяі за вказаними адресами. Такий підхід може захистити учасників від шахрайства з будь-якої сторони та позбавить потреби в довірі.

В цьому прикладі проглядається принцип, що така можливість визначення покрокових параметрів для виконання кожної умови дозволяє створювати системи різної складності та глибини. Крім того, перша умова може бути встановлена спочатку в смарт-контракті, але лише після її виконання можна встановити параметри для наступної умови. Іншими словами, умова формально прописана і її параметри можуть бути визначені під час її роботи.

1.7.3 Класифікація смарт-контрактів

Ви можете вказати різні групи критеріїв класифікації. Однак на даний момент актуальні чотири з них: смарт договори можна виділити за середовищем виконання, яке може бути централізованим або

децентралізованим. У разі децентралізації ми маємо набагато більше незалежності та стійкості при виконанні розумних контрактів.

Вони також відрізняються за процесом встановлення та виконання умов: вони можуть бути запрограмовані, обмежені або попередньо записані довільно, тобто строго набрані. Якщо на платформі смарт-контрактів є лише 4 конкретні смарт-контракти, то ви можете встановлювати параметри довільно. В результаті їх визначити набагато простіше: ми обираємо контракт у списку і вкидуємо параметри.

За інціалізацією є автоматизовані розумні контракти, тобто коли виникають певні умови, вони автоматично реалізуються і є договори, в яких визначені умови, але платформа не перевіряє їх автоматичного виконання, для цього вони повинні бути запущені окремо.

Крім того, розумні контракти відрізняються з точки зору конфіденційності. Вони є повністю відкритими, частково або повністю конфіденційними. Останнє означає, що сторонні спостерігачі не бачать умов розумних контрактів. Однак тема конфіденційності дуже широка, і найкраще розглядати її окремо від поточної статті. Нижче ми розробимо перші три критерії.

У середовищі виконання розрізняються централізовані та децентралізовані платформи. При використанні централізованих цифрових контрактів послуга активується, коли існує лише один валідатор, і може бути сервісом резервного копіювання та відновлення, який також керується централізовано. Існує база даних, яка зберігає всю інформацію, необхідну для визначення умов інтелектуального контракту та розподілу значення, яке враховується в одній базі даних послуг. Такий централізований сервіс має замовника, який визначає умови та запити та використовує ці договори.

Оскільки платформа є централізованою, механізми криптовалюти можуть бути більш надійними за авторизацію.

Для прикладу візьмемо операторів мобільних послуг. Наприклад, певний оператор підтримує на своїх серверах централізований обліковий запис для обробки трафіку, який передається в різних форматах, таких як голосові дзвінки, SMS, мобільний інтернет-трафік та відповідно до різних стандартів і веде облік трафіку та балансу користувачів. Як результат, постачальник мобільних послуг може укладати договори на облік наданих послуг та їх оплату за різних умов. У цьому випадку ви можете легко встановити умови типу "надіслати SMS з таким кодом за таким момером та отримати такі умови трафіку".

Інший приклад - традиційні банки з розвиненою функціональністю інтернет-банкінгу та прості контракти, такі як регулярні платежі, автоматична конвертація платежів тощо.

Що стосується розумних контрактів з децентралізованим терміном виконання, то у нас є група валідаторів. В ідеалі будь-хто може бути валідатором. Завдяки протоколу синхронізації баз даних та пошуку консенсусу у нас є спільна база даних, яка тепер зберігатиме всі транзакції зі ретельно описаними контрактами, а не деякі умовні запити, формати яких мають тенденцію змінюватися та немає відкритої специфікації. Угоди тут міститимуть інструкції щодо виконання договору відповідно до суворих специфікацій. За умови що ця специфікація відкрита - користувачі платформи можуть самі перевіряти та затверджувати розумні контракти. Ми бачимо тут, що децентралізовані платформи випереджають централізовану незалежність та стійкість, але їхнє проектування та обслуговування врази важче.

1.7.3.1 Смарт-контракти за способом завдання і виконання умов

Давайте докладніше розглянемо, як розумні контракти можуть відрізнятися за способом визначення та виконання умов. Тут ми звертаємо увагу на розумні контракти, які довільно програмуються та завершуються за Тьюрінгом. Комплексний розумний контракт Intelligent Turing дозволяє визначити практично будь-який алгоритм як умову виконання контракту: прописати цикли, певні функції обчислення ймовірності тощо, це валідно аж до власних алгоритмів. У цьому випадку це означає дійсно довільне логічне написання.

Є також довільні розумні договори, але не завершені Тьюрінгом. Сюди входять біткойни та Lightcoin зі своїм сценарієм. Очевидно, що лише певні операції можна використовувати довільно, але користувацькі цикли та алгоритми вже не можна записувати.

Крім того, існують такі розумні контрактні платформи, які реалізують попередньо встановлені контракти. До них відносяться Бітшарес і Стеміт. Bitshares має ряд розумних контрактів на торгівлю, керування рахунками, управління самою платформою та її налаштуваннями. Steemit - це подібна платформа, але вона не фокусується на чіпах та торгівлі, як Bitshares, а на блогах, а це означає, що вона зберігає та обробляє контент децентралізовано.

1.7.3.2 Смарт-контракти за способом ініціації

Розумний договір також можна розділити щонайменше на дві групи: автоматизовані та неавтоматизовані. Зазвичай для перших для всіх відомих параметрів та умов, що відбулися, розумний договір є повністю автоматичним, а це означає, що йому не потрібно надсилати додаткові транзакції та мати додаткові витрати на кожне наступне виконання. Сама платформа нілічує всі дані для розрахунку закінчення розумного контракту.

Логіка не довільна, а заздалегідь визначена і все це можна передбачити. Іншими словами, можна заздалегідь оцінити складність виконання розумного контракту, використовувати для нього постійну комісію та зробити всі процеси більш ефективними для її виконання.

Для розумних контрактів, які можна запрограмувати у будь-якій формі, виконання не є автоматичним. Щоб виконати такий розумний контракт, кожен крок вимагає створення нової транзакції, що призведе до наступного етапу виконання або наступного методу розумного контракту, сплатити відповідну комісію та чекати, коли транзакція буде підтверджена. Виконання може пройти чи не вдастись, оскільки розумний контрактний код - це атрибут та непередбачені моменти, такі як життєвий цикл, відсутні параметри та аргументи, виняткові моменти можуть не створюватися тощо.

1.7.4 Типи акаунтів Ethereum

Подивимося, якими можуть бути акаунти платформи Ethereum. Тут є лише два типи облікових записів. Перший тип називається обліковим записом користувача, другий - контрактом. Подивимось, чому вони різні.

Обліковий запис користувача керується лише персональним ключем електронного підпису. Власник акаунту генерує власну пару ключів для алгоритму цифрового підпису еліптичної кривої (ECDSA). Лише транзакції, підписані цим ключем, можуть змінити статус цього облікового запису.

Для облікового запису розумного контракту існує окрема логіка. Керувати ним можна лише за допомогою попередньо визначеного програмного коду, який повністю визначає поведінку розумного контракту: те яким чином він розпоряджається своєю частиною за певних обставин, за ініціативою якого користувача та за яких умов додатково ці монети будуть розповсюджуватися. Якщо деякі пункти розробники не враховані у коді, то

це призводить до проблеми. Наприклад, розумний контракт може отримати умову, при якій він не дозволяє жодному з користувачів розпочати наступний запуск. У цьому випадку деталі будуть заморожені, оскільки розумний договір не передбачає вихід з цієї ситуації.

1.7.5 Структура транзакції Ethereum

У транзакції Ethereum є кілька полів. Перший з цих нунцій - це своєрідний номер транзакції для самого рахунку, який розповсюджує його і є автором. Це необхідно для розмежування дублікатів транзакцій, тобто для виключення випадку, коли наприклад транзакція приймається двічі. Використовуючи ідентифікатор, кожна володіє унікальним хеш-значенням.

Далі йде така сфера, як ціна на бензин. Він визначає ціну, за якою базову валюту Ethereum перетворюють на газ, який оплачує виконання розумного контракту та розподіл ресурсів віртуальної машини. Що це означає?

У біткойнах комісії сплачуються безпосередньо валютою - самими біткойнами. Застосовується простий механізм розрахунку: ми суворо сплачуємо кількість даних, що містяться в транзакції. У Ethereum складніша ситуація, оскільки зробити транзакцію дуже важко. Транзакція все ще може містити програмний код, який буде працювати на віртуальній машині, і кожна операція віртуалки може мати різну складність. Також існують операції, які допомагають виділити пам'ять змінним. Вони матимуть свою складність, яка залежатиме від оплати кожної транзакції.

Вартість кожної операції в газовому еквіваленті буде постійною. Він вводиться виключно для визначення постійної величини кожної операції. Залежно від навантаження на електромережу, ціна газу зміниться, тобто курс,

за яким базову валюту буде перераховано до цього допоміжного підрозділу для сплати комісії.

Є ще одна характеристика транзакцій в Ethereum: байт-код, з кодом до віртуальної машини, буде виконуватися доти, доки він не закінчиться певним результатом (pass-fail) або поки не буде виділено більше монет для сплати комісії.

Наступне поле називається адресою призначення. Сюди входить адреса одержувача частини або конкретна адреса розумного контракту, яка буде викликана. За ним слідує поле значення, яке містить кількість фрагментів, надісланих на адресу призначення.

Потім з'являється цікаве поле під назвою дані, яке адаптується до всієї структури. Це не окреме поле, а ціла структура, що визначає код віртуалки. Тут можна помістити будь-які дані - для цього є окремі правила.

Останнє поле називається підписом. Він також містить електронний підпис автора угоди та відкритий ключ, який підтвердить цей підпис. З відкритого ключа ви можете отримати ідентифікатор облікового запису відправника для цієї транзакції, що означає, що обліковий запис відправника однозначно ідентифікується в самій системі.

У біткойнах комісії сплачуються безпосередньо самим біткойном. Це можливо завдяки простому механізму розрахунку: ми суворо сплачуємо кількість даних, що містяться в транзакції. У Ethereum складніша ситуація, оскільки зробити транзакцію дуже важко. Тут транзакція все ще може містити програмний код, який буде працювати на віртуальній машині, і кожна її операція може мати іншу складність. Існують також операції для виділення пам'яті для змінних. Вони матимуть свою складність, яка залежатиме від оплати кожної транзакції.

2 ПРИКЛАДИ ВИКОРИСТАННЯ БЛОКЧЕЙН ТА SMART CONTRACTS

2.1 Створення програми купівлі - продажу нерухомості

Solidity - це об'єктно-орієнтована мова JavaScript для розробки розумних контрактів. Він є багатоплатформенним, але на практиці в основному використовується для розробки на блокчейн.

Основна проблема "Солідарності" - це її підводні камені. Вивчення синтаксису вже давно не є проблемою для когось, та на шляху може наступити вивчення інших мов, неточностей системи для того, щоб обійти їх. Складаючи смарт-контракти, ви завжди повинні думати, яка функція буде легшою у виконанні. І якщо в архітектурному коді є невелика помилка, це може спричинити втрату десятків мільйонів доларів. Таке програмування дійсно екстремальне.

Поперше, потрібно створити клас-контракт, який описуватиме всі об'єкти та працювати з ним (Рисунок 2.1.1):

```
contract Realty
{   address payable public seller;
    address public customer;
    string title;
    uint256 public price;
    string public streetAddress;
    constructor () payable public{
        //Who is seller
        seller = 0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB;
        customer =  msg.sender;
        //Street address
        streetAddress = "221B Baker Street, London";
        //Title
        title = "RealtyProgram";
 //Price
        price = 99000000000000000000; //99 ether
    }
```

Рисунок 2.1.1 – Структура класу

Тут є деякі нюанси - перший заключається в слові payable. У розумних контрактах методи, що визначають певну цінність, окупаються, та читання безкоштовне і є менш затратним у плані ресурсів. Платіжні операції відзначаються словом payable.

Можете помітити змінну price, яка вказується у wei - це деномінал ефіру. Насправді це поле визначає ціну оплати нерухомості. Тепер необхідно й сам функцію покупки (Рисунок 2.1.2).

```
function buyHouse() payable public{
        require(seller != address(0));
        require(customer != address(0));
         require(customer != seller);
         require(msg.value == price);
        customer = msg.sender;
        seller.transfer(msg.value);
    }
```

Рисунок 2.1.2 – Функція купівлі

BuyHouse – функція оплати яка визначає умови договору, після чого - договір набирає чинності і криптовалюта надходить на рахунок продавця. Перші умови потрібні для перевірки чи є продавець і покупець, і чи це не одна людина томущо торгівля з собою це не дуже правильно.

Тоді, коли ми розриваємо договір на екрані отримуємо такий результат (Рисунок 2.1.3):

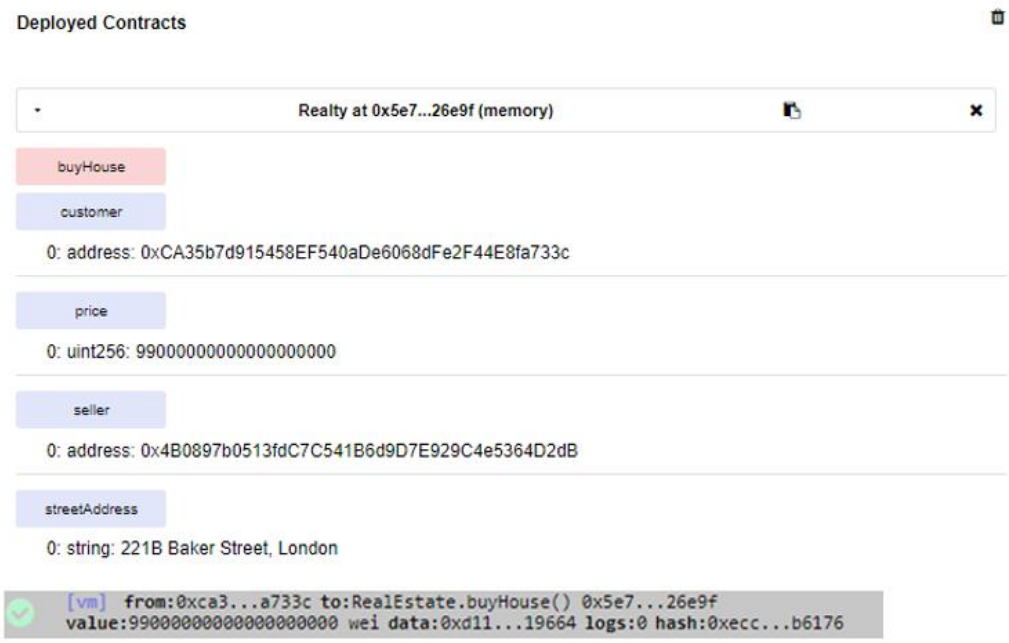

Рисунок 2.1.3 – Результат роботи програми

Якщо ми вводимо ціну будинку, вона не повинна бути вищою або нижчою, ніж зазначена (оскільки ми не хочемо платити занадто багато або менше), тоді угода буде виконана, і майно стане власністю користувача. У інших випадках одержимо помилку (Рисунок 2.1.4):

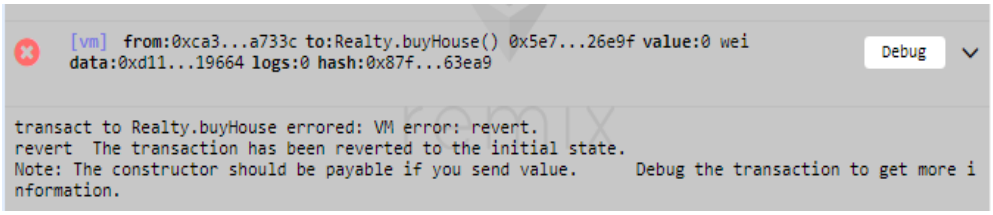

Рисунок 2.1.4 – Приклад помилки виконання

Транзакція повернулась до свого попереднього стану. Ось так ми можемо бути впевнені, що обидві сторони дотримуються всіх пунктів договору.

2.2 Система голосування на базі блокчейн

Ще один приклад використання технології blockchain - програма, яка мінімізує ризик фальсифікацій на виборах. Тому що в наш час розумні контракти довіряють людям - за винятком того, що програму розроблятиме нечесний програміст, але її можна простежити до стадії розробки. Окрім того, розумні контракти, швидше за все, не зміняться - коли вони набудуть чинності - сфальсифікувати кандидата неможливо.

Нам необхідно модель яка описує претендента, масив для зберігання адрес акаунтів які вже віддали свій голос та ще один масив для, власне, збереження самих кандидатів (Рисунок 2.2.1).

```
struct Candidate {
    uint id;
    string name;
    uint voteCount;
}

mapping(address => bool) public voters;

mapping(uint => Candidate) public candidates;
```

Рисунок 2.2.1 – Клас претиндента

Ініціалізуємо всіх кандитаків при при створенні контракту (Рисунок 2.2.2):

```
function Election () public {
        addCandidate("Candidate 1");
        addCandidate("Candidate 2");
    }
```

Рисунок 2.2.2 – Ініціалізація кандидатів

AddCandidate - приватний метод, який унеможливлює створення нових кандидатів після закінчення контракту.

Ось дві перевірки, щоб визначити, чи є такий кандидат у базі даних, за якого було подано голосування, і чи вже хтось проголосував. Також код, необхідний тоді коли контракт вступає в дію (Рисунок 2.2.3).

```
assert(!voters[msg.sender]);
assert(_candidateId > 0 && _candidateId <= candidatesCount);


voters[msg.sender] = true;
candidates[_candidateId].voteCount ++;
```

Рисунок 2.2.3 – Приклад перевірки кандидатів

2.3 Тестування

Тестування є не менш важливою частиною розробки додатку - це процес оцінки функціональності програмного забезпечення з метою визначення того, чи має розроблене програмне забезпечення вказані вимоги чи ні, та виявлення дефектів, щоб гарантувати, що продукт не має дефектів перед тим як попаде до кінцевого користувача. Визначення тестування програмного забезпечення ANSI / IEEE 1059 - Процес аналізу програмного елемента для виявлення відмінностей між існуючими та необхідними умовами (тобто дефектами) та оцінки характеристик програмного забезпечення. програмний елемент.

Існують такі рівні тестування:

1) Тести одиниць: Тести одиниць або Unit тести виконуються, щоб перевірити, чи працюють окремі модулі вихідного коду. Тобто тестування коду розробником в його середовищі для кожного блоку програми окремо. Це тест модуля або випробування компонентів

2) Тест на інтеграцію: Тест на інтеграцію - це процес випробування на з'єднання або передачу даних між двома модулями, що перевіряються. Це тестування I&T або String Testing. Він підрозділяється на низхідний, висхідний і сендвіч-підхід (поєднання зверху вниз і знизу вгору).
3) Тест на систему(енд ту енд): Це тест чорного якщоку. Тестування повністю інтегрованої програми також називається тестуванням сценарію. Для забезпечення роботи програмного забезпечення у всіх призначених цільових системах.
4) Тест на прийняття: отримати схвалення клієнта, щоб можна було доставити програмне забезпечення та отримати платежі. Типи приймальних тестів - це альфа, бета та гамма тести.

Для прикладу, код вище можна було б покрити Unit тестами. Наступний тест буде перевіряти здатність системи правильно ініціалізуватись, з заданою кількістю кандидатів, та їх параметри відповідають тим що вже є у програмі (Рисунок 2.3.1).

```
it("it initializes the candidates with the correct values", function() {
  return Election.deployed().then(function(instance) {
    electionInstance = instance;
    return electionInstance.candidates(1);
  }).then(function(candidate) {
    assert.equal(candidate[0], 1, "contains the correct id");
    assert.equal(candidate[1], "Candidate 1", "contains the correct name");
    assert.equal(candidate[2], 0, "contains the correct votes count");
    return electionInstance.candidates(2);
  }).then(function(candidate) {
    assert.equal(candidate[0], 2, "contains the correct id");
    assert.equal(candidate[1], "Candidate 2", "contains the correct name");
    assert.equal(candidate[2], 0, "contains the correct votes count");
  });
});
```

Рисунок 2.3.1 – Тестування ініціалізації системи

Крім того, щоб бути впевненим у дієздатності продукту нам потрібна функція яка допоможе перевірити чи можуть ніші кандидати брати участь у голосуванні (Рисунок 2.3.2).

```
it("allows a voter to cast a vote", function() {
 return Election.deployed().then(function(instance) {
  electionInstance = instance;
  candidateId = 1;
  return electionInstance.vote(candidateId, { from: accounts[0] });
 }).then(function(receipt) {
  assert.equal(receipt.logs.length, 1, "an event was triggered");
  assert.equal(receipt.logs[0].event, "votedEvent", "the event type is correct");
  assert.equal(receipt.logs[0].args._candidateId.toNumber(), candidateId, "the candidate id is correct");
  return electionInstance.voters(accounts[0]);
 }).then(function(voted) {
  assert(voted, "the voter was marked as voted");
  return electionInstance.candidates(candidateId);
 }).then(function(candidate) {
  var voteCount = candidate[2];
  assert.equal(voteCount, 1, "increments the candidate's vote count");
 })
});
```

Рисунок 2.3.2 – Тестування права голосувати

Також, так як у систему можуть хотіти потрапити зловмисники, нам необхідно превірити чи дані юзери є зареєстровані, або чи їх данні є валідними данними (Рисунок 2.3.3).

```
it("throws an exception for invalid candiates", function() {
 return Election.deployed().then(function(instance) {
  electionInstance = instance;
  return electionInstance.vote(99, { from: accounts[1] })
 }).then(assert.fail).catch(function(error) {
  assert(error.message.indexOf('revert') >= 0, "error message must contain revert");
  return electionInstance.candidates(1);
 }).then(function(candidate1) {
  var voteCount = candidate1[2];
  assert.equal(voteCount, 1, "candidate 1 did not receive any votes");
  return electionInstance.candidates(2);
 }).then(function(candidate2) {
  var voteCount = candidate2[2];
  assert.equal(voteCount, 0, "candidate 2 did not receive any votes");
 });
});
```

Рисунок 2.3.3 – Перевірка валідності данних користувача

Також і самі кандидати можуть вдатись до не чесної гри, необідно перевірити чи забороняє система голосування кільк разів (Рисунок 2.3.4).

```
it("throws an exception for double voting", function() {
 return Election.deployed().then(function(instance) {
  electionInstance = instance;
  candidateId = 2;
  electionInstance.vote(candidateId, { from: accounts[1] });
  return electionInstance.candidates(candidateId);
 }).then(function(candidate) {
  var voteCount = candidate[2];
  assert.equal(voteCount, 1, "accepts first vote");
  // Try to vote again
  return electionInstance.vote(candidateId, { from: accounts[1] });
 }).then(assert.fail).catch(function(error) {
  assert(error.message.indexOf('revert') >= 0, "error message must contain revert");
  return electionInstance.candidates(1);
 }).then(function(candidate1) {
  var voteCount = candidate1[2];
  assert.equal(voteCount, 1, "candidate 1 did not receive any votes");
  return electionInstance.candidates(2);
 })
});
```

Рисунок 2.3.4 – Тестування повторних голосувань

В разі завершення усіх тестів ми отримуємо відповідний меседж про їх в якому описується кількість успішно пройдених тестів, або повідомлення з помилками, в туму випадку коли якийсь тест не пройшов (Рисунок 2.3.5).

```
$ truffle test
Using network 'development'.


  Contract: Election
    √ initialize with 4 candidates


  1 passing (56ms)
```

Рисунок 2.3.5 – Приклад виведення в разі успішного завершення

2.4 Створення власної криптовалюти з технологією блокчейн

Для початку, необхідно створити клас який буде відповідати за наші блоки, тобто їх внутрішню структуру (Рисунок 2.4.1).

```
constructor (index,timestamp,userId, previousHash = ''){

    this.index = index;
    this.timestamp = timestamp;
    this.userId = userId;
    this.previousHash = previousHash;
    this.hash = this.calculateHash();
    this.count = 0;
}
```

Рисунок 2.4.1 – Конструктор блоку

У данній частині коду поле index є порядковим номером блоку, timestamp відповідає за дату створення блоку, поле userId є унікальним ідентифікатором користувача у системі та необхідні змінні для утворення ланцюжку, тобто поле для значення hash, та вказівник на попередній блок previousHash.

Крім того, не мало важливою є функція генерування хешу підчас створення класу у Blockchain (Рисунок 2.4.2).

```
    calculateHash(){
       return SHA256 (this.index + this.previousHash +this.timestamp
+JSON.stringify(this.userId)+this.count).toString();
    }
  constructor (){
           this.chain = [this.createGenesisBlock()];
           this.difficulty = 4;
       }
```

Рисунок 2.4.2 – Обчислення хеш посилання

Необхідна функція яка буде дозволяти створити наш перший блок, в нашому випадку це функція createGenesisBlock (Рисунок 2.4.3).

```
createGenesisBlock(){
      return new Block (0, "01/01/2017","163bffa5-83f2-4d82-99e9-
35f26aec2b3b","0");
    }

    addBlock(newBlock){
    newBlock.previousHash = this.getLatestBlock().hash;
    this.chain.push(newBlock);
```

Рисунок 2.4.3 – Створення стартового блоку

Також необхідна перевірка валідності уже існуючих данних та перевірка валідності системи.

```
isChainValid(){
    for( let i =1;i<this.chain.length - 1;i++){
        const currentBlock = this.chain[i];
        const previousBlock = this.chain[i-1];
        if (currentBlock.hash !==currentBlock.calculateHash()){
            return false;
        }
        if(currentBlock.previousHash !== previousBlock.hash)
        {
            return false;
        }
    }
        return true;
}
```

Рисунок 2.4.4 – Функція перевірки данних

Транзакції є невідємною частиною взаємодії у системі. Тому нам необхідний клас для їх ініціалізацій (Рисунок 2.4.5).

```
class Transaction {
  /**
   * @param {string} fromAddress
   * @param {string} toAddress
   * @param {number} amount
   */
  constructor(fromAddress, toAddress, amount) {
    this.fromAddress = fromAddress;
    this.toAddress = toAddress;
    this.amount = amount;
    this.timestamp = Date.now();
  }
```

Рисунок 2.4.5 – Клас транзакці

Після створення класу, необхідно сворити функцію яка буде сворювати нові транзакції з заданими параметрами (Рисунок 2.4.6).

```
addTransaction(transaction) {
  if (!transaction.fromAddress || !transaction.toAddress) {
    throw new Error('Transaction must include from and to address');
  }
  if (!transaction.isValid()) {
    throw new Error('Cannot add invalid transaction to chain');
  }

  this.pendingTransactions.push(transaction);
}
```

Рисунок 2.4.6 – Функція створення транзакцій

Основна операція з транзакціями – підписання її публічним ключем. Для цього створимо функцію signTransaction, яка буде приймати ключ для підпису, що дозволить нам опрацьовувати данні динамічно (Рисунок 2.4.7).

```
signTransaction (signingKey) {

    if (signingKey.getPublic ( 'hex')! == this.fromAddress) {
      throw new Error ( 'You can not sign transactions for other wallets!');
    }
    const hashTx = this.calculateHash ();
    const sig = signingKey.sign (hashTx, 'base64');

    this.signature = sig.toDER ( 'hex');
  }
```

Рисунок 2.4.7 – Функція підпису

3 ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок норм часу на виконання науково-дослідницької роботи

Головною метою розділу виступає встановлення економічної доцільності розробки програмного розширення веб браузерів із використанням кросплатформованих технологій на мові php.

На ринку програмного забезпечення представлена велика кількість продуктів, проте з часом міняються вимоги до існуючих систем. Для впровадження нових функцій, які задовільнять ці вимоги, можна дописувати уже існуюче програмне забезпечення або розробити нове.

Розробка нового програмного продукту вимагає свого управління і контролю з боку керівника. Таким чином, складання та організація економічної частини є актуальною проблемою сучасного менеджменту.

Планування потребує будь-яке підприємство, будь-яке виробництво, економіка в цілому. Спланувати – означає оцінити можливості, необхідність і обсяги випуску конкурентоспроможної продукції, визначити місткість ринку і його конкретного сегмента, оцінити попит на продукцію, що випускається підприємством, результативність його роботи на ринку.

Швидкий розвиток технологій, ускладнення і різноманіття пропонованої продукції та послуг, скорочення їх життєвого циклу, поява великої кількості конкурентоспроможних компаній, підвищення вимог з боку споживачів, збільшення обсягів і швидкості отримання інформації, нових знань – всі ці і інші зміни в світі змушують господарюючі суб'єкти шукати методи для кращої адаптації до нових умов.

Головною метою розділу є встановлення економічної доцільності розробки програмного веб-розширення розширення, розрахувати передбачені витрати та оцінити ризики непередбачуваних витрат.

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Розробку поділяють на декілька етапів, що дозволить полегшити і структуризацію виконання розробки.

Для виконання проекту може буде залучено 1 керівника, 10 розробників та 4 тестувальник. На проекти такою складності виділяється 160 робочих годин, тому в подальшому будемо орієнтуватися саме на таку часову одинцю.

Витрати часу по окремих етапах розробки програмного забезпечення відображено в таблиці 3.1.1.

Таблиця 3.1.1 – Операції процесу розробки ПЗ і часові затрати

	Місячна зарплата грн.	Денна зарплата грн	Трудомісткість, людино-дні		Основна заробітня плата, грн	
			Процедурний підхід	ООП підхід	Процедурний підхід	ООП підхід
Керівник	5000	250	1	1	250	250
Розробник	11000	550	10	13	5500	7150
Тестувальник	4000	200	4	8.5	800	1200
Всього			17.5	22.5	6550	8600

Процедурний підхід передбачає використання більшої кількості ресурсів, це пов’язано з використанням застарілих принципів та методів розробки програмного забезпечення. В даній таблиці він наведений для наглядної демонстрації та як один з можливих варіантів.

В основному під час проекту та розробки програмного продукту головний нахил робився на об’єктно – орієнтований метод розробки, через його простоту ти потребу в меншій кількості ресурсів. З використанням цього підходу можна оптимізувати вартість розробки програмного продукту на більше як 10%.

3.2 Визначення ключових витрат

Першою ключовою витратою є заробітна плата.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

$$ЗП_{осн1} = 6550 \text{ грн};\ ЗП_{осн2} = 8600 \text{ грн}$$

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

$$ЗП_{дод} = 0{,}2 \cdot ЗП_{осн} \qquad (3.2.1)$$

$$ЗП_{дод1} = 0{,}2 \cdot ЗП_{осн1} = 1310 \text{ грн.};$$

$$ЗП_{дод1} = 0{,}2 \cdot ЗП_{осн2} = 1720 \text{ грн.}$$

Таким чином загальний фонд заробітної плати, що обчислюється за формулою:

$$ФЗП = ЗП_{осн} + ЗП_{дод}. \quad (3.2.2)$$

$$ФЗП_1 = 6550 + 1310 = 7860 \text{ грн.};$$

$$ФЗП_2 = 8600 + 1720 = 10320 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок – 3,6 %;
- військовий збір – 1,5 %;
- ПДФО (прибутковий податок) – 15 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$Відр_{ЄСВ1} = 0{,}036 \cdot ФЗП = 282{,}96 \text{ грн.};$$

$$Відр_{ЄСВ2} = 0{,}036 \cdot ФЗП = 371{,}5 \text{ грн.};$$

$$Відр_{вз1} = 0{,}015 \cdot ФЗП = 154{,}8 \text{ грн.};$$

$$Відр_{вз2} = 0{,}015 \cdot ФЗП = 117.9 \text{грн.}$$

$$Відр_{ПДФО1} = 0{,}15 \cdot ФЗП = 1548 \text{ грн.};$$

$$Відр_{ПДФО2} = 0{,}15 \cdot ФЗП = 1179 \text{ грн..}$$

Нарахування на фонд оплати праці, які включають відрахування до Пенсійного фонду, фонду з тимчасової втрати працездатності, фонду з безробіття і фонду страхування від нещасних випадків на виробництві; для бюджетної організації тариф на фонд оплати праці встановлено на рівні 36,3%.

Зокрема, видання програмного забезпечення – 36,77%.

Нарахування на Фонд оплати праці (ФОП): $ФОП_{ЄСВ} = 0{,}3677 \cdot ФЗП$

$$ФОП_{ЄСВ1} = 0{,}3677 \cdot ФЗП = 2890{,}12 грн.;$$

$$ФОП_{ЄСВ2} = 0{,}3677 \cdot ФЗП = 3162{,}22 грн$$

Вього витрат:

$$В_{ЗП1} = ФЗП_1 + ФОП_{ЄСВ1} = 6550 + 2890{,}12 = 9440{,}12 грн.;$$

$$В_{ЗП2} = ФЗП_2 + ФОП_{ЄСВ2} = 8600 + 3162{,}22 = 11762{,}22 грн.;$$

Також важливою складовою витрат є матеріальні витрати. Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i , \qquad (3.2.3)$$

де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} . \qquad (3.2.4)$$

Таблиця 3.2.1 – Зведені розрахунки матеріальних витрат.

Найменування матеріальних ресурсів	Один. Виміру	Фактично витрачено матеріалів	Ціна 1-ці., грн.	Загальна сума витрат, грн
Папір формату А4	листів	150	0,5	75
Тонер для принтера	шт	2	80	160
Флеш-накопичувач	шт	4	80	320
Всього				555

Отже, загальна сума матеріальних витрат становить 555 гривень.

В багатьох випадках існує ряд додаткових витрат які пов’язані із реалізацією проекту, але в більшості випадків їхня сума не перевищує десяти відсотків від загальної собівартості реалізації проекту.

Також варто врахувати електроенергію. Затрати на електроенергію використану 1-цею обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S\,, \tag{3.2.5}$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,50 грн.

Потужність комп’ютера для створення проекту – 750 Вт, кількість годин роботи необхідних для проекту – 140 години при процедурному підході та 180 годин при об'єктно орієнтованому підході.

$$З_{е1} = 0{,}4 \cdot 140 \cdot 2{,}50 = 140$$

$$З_{е2} = 0{,}4 \cdot 180 \cdot 2{,}50 = 180$$

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{С_Б \cdot N_А \cdot T_{ФАК}}{Т_{год}} \tag{3.2.6}$$

де $С_Б$ – балансова вартість обладнання, грн;

N_A – норма амортизаційнихвідрахувань в рік, %;

$Т_{год}$ – річний робочий фонд часу, год;

$T_{ФАК}$ –фактичний час роботи обладнання по написанню програми, год.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Отже, використовуючи в роботі 1 комп'ютер балансовою вартістю 12000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A_1 = (12000 \cdot 0{,}6 \cdot 140)/2080 = 484{,}61 \text{ грн.}$$

$$A_2 = (12000 \cdot 0{,}6 \cdot 180)/2080 = 623{,}07 \text{ грн.}$$

Варто врахувати і накладні витрати, адже вони пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20-60 % від суми основної та додаткової заробітної плати працівників.

$$НВ = 0{,}5 \cdot ЗП_{осн} \qquad (3.2.7)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати:

$H_{в1} = 1310 \cdot 0{,}5 = 655$ грн. $H_{в2} = 1720 \cdot 0{,}5 = 860$грн.

3.3 Визначення періоду окупності та собівартості

Проведемо розрахунок вартості створюваного програмного продукту. Вартість продукції включає у собі собівартість і планований прибуток.

Приймемо прибуток на рівні 30%. Для нових інноваційних продуктів, що користуються високим попитом на ринку, ринкову вартість Вр можна втановити вищу.

Отже, вартість розробленого програмного забезпечення:

Вр1,2= Св1,2 + 0,3 · Св1,2 = 16000 + 0,3 · 16000 = 21500 грн..

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу. Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{П}{C_B} \qquad (3.3.1)$$

де $П$ – прибуток;

$C_в$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = В_р - C_в \qquad (3.3.2)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 21500 - 16000 = 5500 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П_{пл}}{C_в}. \qquad (3.3.3)$$

$$Е_р = 5500 / 16000 = 0,3.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$\mathrm{T_{ок}} = \frac{1}{\mathrm{E}} \qquad (3.3.4)$$

Термін окупності дорівнює:

$$\mathrm{T_{ок}} = 1 / 0{,}3 = 3{,}3 \text{ роки}$$

У нашому випадку Ток1= Ток2 =1/0,30=3,33 років, що є нормальним, оскільки допустимим вважається термін окупності до 5 років.

Даний розрахунок виконаний у розрахунку на 1 екземпляр програмного продукту без врахування його тиражування.

Загальна вартість пропонованих робіт по розробці програмного продукту становить 21500 грн. Оскільки ефективність для обидвох проектів відповідно до встановленого рівня прибутку становить 0,3, що є високим показником, то проводити дані роботи варто і вкладені кошти окупляться за 3 та три місяці. Також слід врахувати можливість не одиничного замовлення програми, відповідно її ціна в такому випадку значно понизиться, а при продажі понад план прибуток зросте.

Виходячи із експертних оцінок і складності програми, приймемо величину витрат на супровід і модернізацію програмного забезпечення, створеного за процедурним методом 60% від початкових витрат, а за об’єктно-орієнтованим – 20%.

Собівартість модернізації:

$\mathrm{С_вМ_1} = 0{,}6 \cdot \mathrm{С_{в1}} = 0{,}6 \cdot 16000 = 9600$ грн.,

$\mathrm{С_вМ_2} = 0{,}2 \cdot \mathrm{С_{в2}} = 0{,}2 \cdot 16000 = 3200$ грн.

Для споживача вартість модернізації:

$М_1 = 0{,}6 \cdot В_1 = 0{,}6 \cdot 21500 = 11700$ грн;

$М_2 = 0{,}2 \cdot В_1 = 0{,}2 \cdot 21500 = 3900.$

Таким чином, уже після першої модернізації, загальні витрати на створення і супровід ПЗ для виробника за об'єктно-орієнтованим методом менші, ніж за процедурним, навіть якщо його собівартість є дещо дорожчою.

$ЗВ_{1\,(вир)} = 16000 + 9600 = 25600$ грн.;

$ЗВ_{2\,(вир)} = 16000 + 3200 = 19200$ грн..

Як і для споживача:

$ЗВ_1 = 21500 + 11700 = 33200$ грн.;

$ЗВ_2 = 21500 + 3900 = 25400$ грн..

Річна економія витрат за всіма можливими напрямами і додатковими витратами, пов'язаними з супроводом і тільки одноразовою модернізацією (у розрахунку на одиницю продукції) при об'єктно-орієнтованому методі порівняно із процедурним:

$\Delta С_{(вир)} = ЗВ_{1\,(вир)} - ЗВ_{2\,(вир)} = 25600 - 19200 = 6400$ грн.;

$\Delta С = ЗВ_1 - ЗВ_2 = 33200 - 25400 = 7800$ грн..

Чистий приведений дохід (ЧПД) визначається як різниця між сукупними доходами (сукупний грошовий потік) і сукупними витратами (сукупними інвестиціями) взятими за весь період життя інвестицій і дисконтова ними в кожному році на фактор часу. Дисконтування являє собою визначення вартості майбутніх грошових потоків у теперішній момент часу.

Коефіцієнт дисконтування показує, яку величину грошових коштів ми отримаємо з урахуванням фактору часу та ризиків. Він дозволяє перетворити майбутню вартість у вартість на даний момент.

Для розрахунку коефіцієнта дисконтування (коефіцієнта приведення) грошових потоків за роками періоду економічного життя інвестицій використовується формула:

$$\alpha = \frac{1}{(1+i)^n} \quad ;$$

(3.3.12)

де i – ставка дисконтування або норма дисконту, i = 0,2;

n – час або кількість періодів (років), протягом якого планується отримання доходу.

$$\alpha_0 = 1, \alpha_1 = \frac{1}{1+0,2} = 0,60.$$

Вважатимемо, що обидва програмних продукта одинаково забезпечують потреби і вимоги споживача, і тому придбання першої чи другої програми однаково вплинуть на розмір його додаткових доходів на вкладений капітал. Тому приймемо цю величину за постійну, а порівняння дохідності двох проектів проведемо тільки за витратами.

$ЧПД'_1 = ГП + 0,60 \cdot ГП = 21500 - 0,60 \cdot 7090 = 16760$ грн.;

$ЧПД'_1 = ГП + 0,60 \cdot ГП = 21500 - 0,60 \cdot 3900 = 19160$ грн..

Чим менші витрати, тим більша дохідність проекту.

$ЗВ_1 = 21500 + 7090 = 28590$ грн.;

$ЗВ_2 = 21500 + 3900 = 25400$ грн..

Таблиця 3.3.1 – Техніко–економічні показники програмного продукту

Показник	Процедурний підхід	Об'єктно-орієнтований підхід
Зарплата основна, грн	6550	8600
Зарплата додаткова, грн	1310	1720

Фонд заробітньої плати, грн	7860	10320
Відрахування на ФОП, грн	2890,12	3162,22
Разом на виплату плаці, грн	9440,10	11762,35
Матеріальні витрати, грн	730	730
Електроенергія, грн	120	160
Амортизація, грн	484,61	623,07
Накладні витрати, грн	3545	4682,5
Разом на ін.витрати, грн	4080,40	5396,35
Собівартість	16000	21500
Прибуток	5500	7150
Вартість розробленого ПЗ	19200	25600
Економічна ефективність	0,34	0,34
Термін окупності, років	3,33	3,33
Собівартість модернізації	11700	3900
Супровід і модернізація	33200	25400
Загальні витрати на розробку	22411,68	18036,38
Порівняльна економія витрат (для виробника)	-	4375,30
Загальні витрати (для споживача, на придбання програмного прод.)	28590	25400
Порівняльна економія витрат для споживача)	-	3190

Дохідність проекту для споживача за витратною частиною	−4178,32	−12928,92
Економія	-	8750,6

Економія витрат у випадку придбання, супроводу і одноразової модернізації програмного продукту, створеного за об’єктно-орієнтованим підходом, становить 8750,6 грн.

Оскільки ефективність для обидвох проектів відповідно до встановленого рівня прибутку становить 0,3, що є високим показником, то проводити дані роботи варто і вкладені кошти окупляться за 3 роки та два місяці, бо нормальним терміном окупності є термін, який коливається від 1 до 3 років, в даному випадку допуск 2 місяці можна вважати допустим, тоді розробка вважається доцільною і економічно вигідною.

При використанні об’єктно-орієнтовного підходу зменшується кількість працівників, які залучаються у проект, та зменшуються витрати на реалізацію проекту, але для підтримки проекту і його подальшої модернізації.

Отже, програмний продукт може бути впроваджений та мати подальший розвиток, оскільки він є економічно вигідною за всіма основними техніко-економічними показниками.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Висока швидкодія сучасних комп’ютерів зумовлює зростання споживання електричної енергії, значна частина якої розсіюється у вигляді тепла. Основні компоненти комп’ютера – центральний процесор та графічний процесор відеокарти – вимагають масивних систем охолодження. До складу сучасного системного блоку зазвичай входить декілька вентиляторів: як мінімум один в блоці живлення, один охолоджує процесор, відеокарта комплектується своїм вентилятором. Декілька вентиляторів встановлено в корпусі комп’ютера, зустрічаються також материнські плати з активним охолодженням набору мікросхем (чіпсета).

Одним з важливих недоліків сучасних високопродуктивних домашніх і офісних комп’ютерів є настирливий, монотонний і дратівливий шум.

Зі збільшенням тактових частот процесорів і інших мікросхем материнської плати неминуче зростало і споживання енергії. Закони фізики стверджують, що потужність, яка поглинається мікросхемою, прямо пропорційна квадрату напруги і тактової частоти. Отже, якщо збільшиться продуктивність за рахунок збільшення частоти, то неминуче підвищиться і потужність, що розсіюється. В результаті, природно, збільшується і тепловиділення мікросхем. І якщо не відводити тепла з корпусу комп’ютера, то неминуче настане перегрівання — зі всіма негативними наслідками. Сучасні процесори настільних комп’ютерів виділяють більш ніж 140 Вт теплової енергії'. Але в комп'ютері джерелом тепла є не лише процесор – гріються і мости чіпсета, і модулі пам’яті, і жорсткі диски, і сам блок живлення, і, звичайно ж, відеокарта, яка на сьогодні є своєрідним «комп’ютером у комп'ютері», зі своїми графічним процесором і пам’яттю.

Тому у всіх сучасних корпусах передбачені місця для встановлення вентиляторів, призначених для відведення тепла з корпусу комп'ютера. Таких вентиляторів в одному корпусі може налічуватися до семи. Але кожен вентилятор – це джерело шуму. Власне, все, що обертається, генерує шум, причому цей шум може посилюватися самим корпусом комп'ютера.

Існують технічні рішення, які дозволяють створити повністю безшумний комп'ютер: рідинне (зазвичай водяне) чи фреонове охолодження, спеціальний алюмінієвий корпус-радіатор комп'ютера, який розсіює тепло всією своєю поверхнею, теплові трубки, використання спеціалізованих матеріалів, що поглинають шум. В тих випадках, коли сторонні шуми повинні бути відсутніми за будь-яку ціну, такі рішення є цілком виправданими. Однак ціна лише корпусу- радіатора може бути в 3-5 разів більшою, ніж ціна звичайного системного блоку, такі рішення для офісного та домашнього використання є непридатними.

В зв'язку з цим виникає проблема пошуку компромісного рішення між зменшенням рівня шуму та витраченими для цього коштами. Простим висновком є наступний: потрібно взяти радіатори більшого розміру, та забезпечити сильніший потік повітря. Проте є ще два важливі чинники: вартість системи охолодження і шум, який вона створює при роботі. Вартість систем охолодження зростає зі зростанням розміру радіаторів: підвищується металоємність і складність виробництва. Внаслідок більшої вартості мідні радіатори використовуються рідше, ніж алюмінієві.

Зменшення числа обертів є одним з найефективніших методів для зменшення рівня шуму, але доволі часто постає запитання, чи достатньо цього і як таке зменшення вплине на температурний режим загалом.

Здається, проблему дійсно важко розв'язати і при високій продуктивності вентилятора шуму не уникнути. Хоча деякі зарубіжні

компанії почали спеціалізуватися на випуску компонентів систем охолодження для безшумних комп’ютерів, а інші – на випуску власне безшумних комп’ютерів.

Оскільки розробка програмного забезпечення для тестування Інтернет ресурсу відбувалась на комп’ютері, потрібно розглянути основні нормативно-правові документи та відповідні особливості охорони праці. Перелік нормативно-правових актів, що так чи інакше регулюють дане питання, є досить широким. Обов’язки роботодавця щодо забезпечення працівникам комфортних та безпечних умов для здійснення роботи, а також права працівників на такі умови передбачено частиною 2 ст. 2 та ч. 1 ст. 21 КЗпП, а також ст. 13 Закону України «Про охорону праці». Даний закон визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних органів державної влади відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні. Більшість актів у даній сфері становлять акти підзаконного рівня, а саме, численні правила, інструкції, державні санітарні правила і норми (ДСанПІН) тощо, якими врегульовуються окремі моменти щодо власне конструкції електронно-обчислювальної техніки, особливостей облаштування приміщень для роботи з нею та низки інших подібних вимог[13].

До таких нормативних актів, наприклад, належать ДсанПіН 5.5.6.009-98, норми, що регулюють влаштування та обляднання кабінетів компютерної техніки в навчальниз закладах та режим праці учнів на персональних компютерах

4.2 Ергономічні вимоги до організації робочих місць

Робоче місце — це зона простору, що оснащена необхідним устаткуванням, де відбувається трудова діяльність одного працівника чи групи працівників.

Раціональне планування робочого місця має забезпечувати: найкраще розміщення знарядь і предметів праці, не допускати загального дискомфорту, зменшувати втомлюваність працівника, підвищувати його продуктивність праці. Площа робочого місця має бути такою, щоб працівник не робив зайвих рухів і не відчував незручності під час виконання роботи. Важливо мати також можливість змінити робочу позу, тобто положення корпуса, рук, ніг. Проте доцільно виключати або мінімізувати всі фізіологічно неприродні і незручні положення тіла.

Проведені дослідження показують, що при раціональній організації робочих місць продуктивність праці зростає знати на 15-25%.

Основні ергономічні вимоги до проектування робочого місця в системі "людина — техніка — виробниче середовище" (Рисунок 4.2.1).

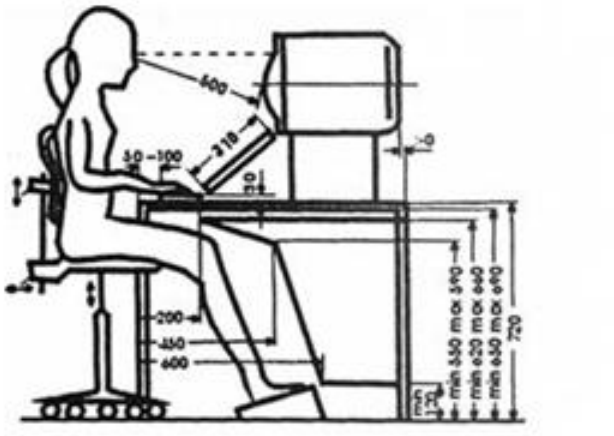

Рисунок 4.2.1 - Робочий стіл і розміщення користувача ПК

Гігієнічні вимоги визначають умови життєдіяльності і працездатності людини у процесі взаємодії з технікою і середовищем; показниками є рівень освітлення, температура, вологість, шум, вібрація, токсичність, загазованість тощо.

Антропометричні вимоги визначають відповідність конструкцій техніки антропометричним характеристикам людини (зріст, розміри тіла та окремі рухові ланки). Показниками е раціональна робоча поза, оптимальні зони досягнення, раціональні трудові рухи.

Фізіологічні та психофізіологічні вимоги визначають відповідність техніки і середовища можливостям працівника щодо сприйняття, переробки інформації, прийняття і реалізації рішень.

Організація робочого місця передбачає

1) правильне розміщення робочого місця у виробничому приміщенні;
2) вибір ергономічно обґрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;
3) раціональне компонування обладнання на робочих місцях;
4) урахування характеру та особливостей трудової діяльності.

Загальні принципи організації робочого місця:

1) на робочому місці не повинно бути нічого зайвого. Усі необхідні для роботи предмети мають бути поряд із працівником, але не заважати йому;
2) ті предмети, якими користуються частіше, розташовуються ближче, ніж ті предмети, якими користуються рідше;
3) предмети, які беруть лівою рукою, повинні бути зліва, а ті предмети, які беруть правою рукою — справа;

4) якщо використовують обидві руки, то місце розташування пристосувань вибирається з урахуванням зручності захоплювання його двома руками;
5) робоче місце не повинно бути захаращене;
6) організація робочого місця повинна забезпечувати необхідну оглядовість.

Статичні напруження працівника в процесі праці пов'язані з підтриманням у нерухомому стані предметів і знарядь праці, а також підтриманням робочої пози.

Робоча поза — це основне положення працівника у просторі: зручна робоча поза має забезпечувати стійкість положення корпуса, ніг, рук, голови працівника під час роботи, мінімальні затрати енергії та максимальну результативність праці.

Найпоширенішими у процесі праці є пози сидячи і стоячи. Проектуючи робоче місце, потрібно враховувати, що при виконанні роботи з фізичним навантаженням бажана поза стоячи, а при малих зусиллях — сидячи.

Робоча поза стоячи втомлює людину більше, ніж сидяча. Вона вимагає на 10 % більше енергії, спричиняє підвищення артеріального і венозного тиску крові, розширення вен на ногах, пошкодження ступень, викривлення хребта.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам.

Виконуючи практичні завдання щодо використання робочої пози, потрібно: зменшувати величину статичних напружень; розподіляти статичні напруження; передбачати можливість змін пози під час роботи.

ВИСНОВКИ

Досліджено багато способів застосування технології blockchain - від системи голосування до фінансових операцій із власною криптовалютою. Розумні контракти мінімізують ризик недотримання будь-якого договору. Публічний блокчейн дозволяє відкрито здійснювати фінансові операції, гарантуючи всім його учасникам прозорість та чесність будь-якої транзакції.

Розумні контракти - це чудова заміна стандартних юридичних процедур, оскільки вони дешеві і безпечні: і немає ризику, що одна сторона обдурить іншу. У розумних контрактах підприємець - це децентралізована мережа Ethereum, а не людина чи компанія, тому нам не доводиться покладатися на довіру та чесність іншої сторони.

Цілком можливо, що зараз - саме той час, коли технологія проходить обкатку наживо на вельми значущих сферах суспільного життя, і незабаром ми побачимо все більше і більше проектів і платформ, які використовують блокчейн. Вже зараз банки намагаються активно впроваджувати це у себе (в тому числі і для зниження операційних витрат), на ринку з'являються все нові і нові гравці, які прагнуть популяризувати використання технології.

Нові проекти на блокчейне будуть грунтуватися на його головнтх перевагах - відкритості, захищеності, безпеці. Тому блокчейн стане гарною підмогою для будь-яких сервісів, де користувачі могли переживати про можливе шахрайство або про збереження даних: мікроплатежі, банківські операції, логістика, юриспруденція, медицина.

Всього за кілька років блокчейн вже пройшов шлях від новинки в технологічному світі до інструменту, яким починають користуватися великі банки, корпорації та держави. Це тільки зміцнює впевненість в тому, що в майбутньому технологія розкриє свій потенціал ще сильніше.

СПИСОК ЛІТЕРАТУРИ

1) The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order [Текст] – Paul Vigna 2016. – 231с.

2) Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by [Текст] - Don Tapscott 2016. – 103с.

3) Mastering Ethereum by Gavin Wood and Andreas Antonopoulos [Текст] - O'Reilly Media, 2018 – 210с.

4) “Blockchain: Blueprint for a New Economy” [Текст] - Melanie Swan 2018. – 114с.

5) “Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations” [Текст] - Henning Diedrich 2017 - 314с.

6) “The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology” [Текст] - William Mougayar 2016 – 116с.

7) “Blockchain: The blockchain for beginners guide to blockchain technology and leveraging blockchain programming” [Текст] Josh Thompsons 2017, - 84с.

8) Blockchain [Текст] – Melanie Swan 2018, - 32с.

9) The Book of Satoshi [Текст] - Phil Champagne 2016, - 103с.

10) The Science of the Blockchain [Текст] - Roger Wattenhofer 2017, - 23с.

11) “Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations” [Текст] - Henning Diedrich 2016 – 78с.

12) “A Gentle Introduction to Blockchain” [Електронний ресурс]: режим доступу: https://medium.com/@mattmcilwham

13) В.І. Голінько, М.Ю. Іконніков, Я.Я. Лебедєв Охорона праці в галузі інформаційних технологій [Текст] – Дніпропетровськ : НГУ – 2015. – 247 с.

14) Smart Contracts: The Blockchain Technology That Will Replace Lawyers: [Електронний ресурс]: режим доступу: https://blockgeeks.com/guides/smart-contracts/

15) Smart Contracts [Електронний ресурс]: режим доступу: https://blockchainhub.net/smart-contracts/

16) What are smart contracts on Blockchain? [Електронний ресурс]: режим доступу: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/

17) Blockchain Security Solutions [Електронний ресурс]: режим доступу: https://safenet.gemalto.com/blockchain/

18) What Makes a Blockchain Secure? [Електронний ресурс]: режим доступу: https://www.binance.vision/blockchain/what-makes-a-blockchain-secure

ДОДАТКИ

Додаток А

Додаток В

УДК 004.415.5

А. Когут ст. гр. СПм-61
Тернопільський національний технічний університет імені Івана Пулюя

Використання технології blockchain для забезпечення відкритості інформації

Блокчейн, тобто ланцюжок блоків транзакцій (англ. Blockchain, Block chain від block — блок, chain — ланцюг) — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Дані захищено від підробки та спотворення. Кожен блок містить часову позначку, геш попереднього блока та дані транзакцій, подані як геш-дерево.

За допомогою Blockchain можна будувати будь-який сервіс, це свого роду несуча технологія. Щось по типу того, як виглядав інтернет у 90-х. Видно, що крута штука, зрозумілі переваги, але ще треба довго працювати над тим, щоб це стало доступно широким массам.Кожен окремий Blockchain — це завжди спільнота чи певна екосистема. Усі вони глобально діляться на два типи: публічні та приватні — public blockchain and private blockchain. Нині найбільш розповсюджена модель публічних blockchain. поняття Blockchain напряму пов'язане з найвідомішим криптовалютним проектом Bitcoin.

Bitcoin — це тільки один із проектів, їх існує сотні варіантів. Переважна більшість з них — це клони Bitcoin, тобто проекти, які не несуть нічого нового, але по-своєму забрендовані. Дуже важливо усвідомлювати, що Bitcoin — це проект та бренд, де в основі закладена технологія Blockchain. Та всі властивості, які йому приписують, насправді досягаються виключно за допомогою технічного рішення Blockchain.

Ethereum — другий за значущістю проект в екосистемі, який чітко утримує друге місце досить тривалий час. Проект позиціонується не як криптовалюта, а як платформа для різних задач, в тому числі для безупинного виконання програми. Для запуску так званих smart-contracts контракти представлені у вигляді програмного коду.

Блокчейн як спосіб зберігання даних є затребуваним у найпрогресивніших країнах світу. У США розглядають питання про застосування цієї технології під час виборів до Конгресу. Влада Канади запустила тестову версію системи, яка через блокчейн забезпечує прозорість розподілу державних грантів. Японія досліджує можливості впровадження блокчейну у системі державних закупівель, Австрія — в енергопостачанні. Європейські фінансові інститути, серед яких Національний Банк Франції, виділяють допомогу блокчейн-стартапам.

Ця технологія користується попитом, оскільки надає безпрецедентний ступінь довіри до інформації у відносинах між людиною та державними або приватними установами. Блокчейн — це децентралізована база даних з відкритим кодом, яка не потребує посередників для верифікації. Інформація, що зберігається у такий спосіб, є відкритою для всіх учасників. Її неможливо знищити або непомітно змінити.

Світовий досвід застосування блокчейну дуже корисний і для України. За допомогою блокчейну відкриваються нові можливості для усунення корупційної складової при наданні послуг. Зараз київська влада активно працює над застосуванням цієї технології для низки міських електронних сервісів. У КМДА планують розпочати перехід на блокчейн з сервісу "Онлайн-запис до дитячих садочків".

Список використаної літератури:

1.Delo.ua [Електронний ресурс]. – Режим доступу: https://delo.ua/business/blokchejn-proti-korupciji-v-ukrajini-ta-v-sviti-347026/– Назва з екрану.

2. Wikipedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Blockchain – Назва з екрану.

Додаток С