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

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН. ПЕРСПЕКТИВИ ЇЇ РОЗВИТКУ

Текстова частина до курсової роботи

Керівник курсової роботи
к.е.н., ст.викладач Невмержицький Є.І.
(прізвище та ініціали)
_____
(підпис)
“____” _____ 2021 р.
Виконав студент БП ІПЗ-3
Мальков Є.В.
(прізвище та ініціали)
“____” _____ 2021 р.

Київ 2021

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

ЗАТВЕРДЖУЮ

Зав.кафедри інформатики,

доцент, к.ф.-м.н.

_____С. С. Гороховський

(підпис)

“____”_____2021 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсову роботу

студенту Малькову Єгору Вікторовичу факультету інформатики 3 курсу

ТЕМА Використання технології блокчейн. Перспективи її розвитку.

Вихідні дані: Веб-застосунок для проведення виборів, що використовує блокчейн

Зміст ТЧ до курсової роботи:

Індивідуальне завдання

Вступ

1 Технологія блокчейн: особливості, історія та розвиток.

2 Використання технології блокчейн

3 Розробка застосунку для проведення виборів

Висновки

Список літератури

Дата видачі “___” _____ 2020 р. Керівник _____

(підпис)

Завдання отримав _____

(підпис)

Тема: Використання технології блокчейн. Перспектики її розвитку.

Календарний план виконання роботи:

№ п/п	Назва етапу дипломного проекту (роботи)	Термін виконання етапу	Примітка
1.	Отримання завдання на курсову роботу.	Листопад 2020	
2.	Огляд технічної літератури за темою роботи.	Лютий 2021	
3.	Виконати аналіз алгоритмів та реалізацій	Лютий 2021	
4.	Написання першого розділу	Лютий 2021	
5.	Написання другого розділу	Березень 2021	
6.	Створення смарт-контракту	Березень 2021	
7.	Створення веб-застосунку	Квітень 2021	
8.	Завершення виконання практичної частини	Квітень 2021	
8.	Написання третього розділу	Квітень 2021	
10.	Корегування роботи	Травень 2021	
11.	Розробка презентації	Травень 2021	
12.	Захист курсової роботи	Травень 2021	

Студент Мальков Єгор Вікторович

Керівник Невмержицький Євген Іванович

“_____”_____

ЗМІСТ

АНОТАЦІЯ

У роботі розглядаються основні теоретичні відомості про технологію блокчейн, її особливості, переваги та недоліки, частину уваги було приділено розвитку та зародженню технології. Було досліджено сфери використання блокчейну, зокрема фінансову, медичну, державний сектор. У роботі аналізуються ключові особливості технології.

У практичній частині було розроблено смарт-контракт та веб-застосунок для проведення виборів, за приклад було взято президентські вибори.

ВСТУП

Інформаційні технології поступово проникають в усі сфери нашого життя. Однією з найцікавіших та найперспективніших за останній час стала технологія блокчейн. Деякі її концепції були описані ще 30 років тому, проте перше її практичне застосування відбулося у 2008 році – була створена криптовалюта Bitcoin на базі блокчейну. З кожним днем технологія стає все більш популярною, набуває ширшого спектру застосування.

Блокчейн – новий вид зберігання інформації, децентралізована база даних, представлена неперервним ланцюгом зв’язаних між собою блоків. Найбільшими перевагами даної технології є надійність, відмовостійкість та безпека. За невеликий проміжок часу її почали застосовувати для зберігання цифрових активів, ідентифікаційної інформації, захисту авторського права, голосування та інших речей.

Криптовалюти стали однією з найбільш обговорюваних та спірних тем у мережі, щохвилини їх сумарна капіталізація збільшується на величезні суми. Людство поступово втрачає довіру до банків, фіатних грошей через їх нестабільність, на фоні численних світових криз.

Все більше розвинутих країн починають використовувати блокчейн у державному секторі, збільшуючи надійність даних та зменшуючи значимість людського фактору, що знижує рівень корупції.

Мета курсової роботи: дослідити доцільність використання технології блокчейн в певних видах діяльності, оцінити подальші перспективи її розвитку, створити застосунок з її використанням.

Робота включає в себе три розділи.

1. ТЕХНОЛОГІЯ БЛОКЧЕЙН: ОСОБЛИВОСТІ, ІСТОРІЯ ТА РОЗВИТОК.

1.1 Поняття блокчейну

Blockchain – термін утворений поєднанням двох англійських слів: «block» - блок та «chain» - ланцюг. Блок – файл, який в залежності від системи має певні характеристики: частота створення, розмір, дані. Дані у блоках зашифровані з використанням криптографічних алгоритмів. Ланцюг – по'єднання блоків у логічну послідовність, кожен новостворений блок містить посилання на попередній блок. Такий спосіб зберігання інформації майже унеможливлює підробку даних. Зміна даних в будь-якому блоці призведе до зміни його посилання, таким чином буде запущена «ланцюгова реакція» і зміна буде відхилена.

Чим блокчейн відрізняється від типових баз даних? Бази даних використовують таблиці для зберігання інформації, а блокчейн – блоки, що пов'язані один з одним. Блокчейн – це децентралізована база даних (P2P), тобто уся інформація міститься на великій кількості машин, які можуть знаходитись у будь-якій точці світу, головний сервер відсутній. Ці комп'ютери називають вузлами.

Блокчейн – прозора система. Кожен може побачити інформацію про будь-який блок.

Блокчейн використовує криптографічні алгоритми для забезпечення роботи системи. Вони гарантують незмінність блоку транзакцій, керують аутентифікацією.

Хешування – криптографічна техніка, яка перетворює вхідний масив даних довільної довжини у стрічку фіксованої довжини. Хеш-функції, що використовуються у блокчейні мають задовольняти умови відсутності колізій: не можна отримати однаковий хеш з різного набору вхідних даних.

Хеші використовуються для вказівок суміжних блоків у зв’язному списку. Уся інформація у блоці хешується для створення вказівника за допомогою бінарного дерева хешів (дерево Меркла), а отже зміна будь-якого шматку інформації призведе до зміни хешу самого блоку і, відповідно, усього ланцюжку.

Також у блокчейні використовуються цифрові підписи, що базуються на криптографії з відкритим ключем. Відкритий ключ – використовується для перевірки електронного підпису, доступний усім. Закритий ключ зберігається в таємниці, потрібен для створення електронного підпису.

Відкритий ключ можливо обрахувати за допомогою закритого, проте зворотний процес має бути неможливим (тільки за допомогою брут-форсу). Ініціатор транзакції підписує дані своїм закритим ключем, шифрує повідомлення за допомогою публічного ключа одержувача, отримувач же розшифровує дані за допомогою свого закритого ключа. Таким чином єдиний хто може розшифрувати повідомлення – власник приватного ключа, якому адресована транзакція. Підпис використовується для того, щоб довести, що саме цей користувач ініціював транзакцію. Маючи повідомлення, підпис, та публічний ключ підписанта можна підтвердити його авторство.

1.2 Історія виникнення технології блокчейн

Уперше технологія схожа на блокчейн була описана у 1991 році. Двоє американських вчених, Скотт Сторнетта та Стюарт Габер, опублікували працю, в якій описали технологію, за допомогою якої можна було отримувати інформацію про час створення та модифікації електронного документа. Вирішення проблеми за допомогою використання звичайної клієнт-серверної архітектури мало багато недоліків: можливість «прослуховування» мережі, невпевненість в достатній захищеності серверу, невисока швидкість обробки даних, потреба у великому обсязі пам’яті для зберігання інформації.

Було запропоновано покращення до існуючої системи, зокрема використання сімейства криптографічно захищених хеш-функцій. Замість надсилання усього документу на сервер, надсилалося лише його хеш-значення. Таким чином необхідний обсяг пам’яті зменшується, а пропускна здатність навпаки збільшується. Другим покращенням було запровадження цифрового підпису.

Проте залишалася проблема, коли сервер міг видавати невірні часові мітки, для її вирішення було надано два способи. Перший полягав у використанні централізованого серверу, який би створював часові мітки таким чином, що значно ускладнювало процес створення недостовірних. Друге рішення пропонувало розділити процес підтвердження достовірності між іншими користувачами.

Підхід з використанням серверу вимагав від нього наступного списку дій:

1. сервер надсилав певний сертифікат у відповідь на запит користувача. Сертифікат містив у собі хеш, ідентифікаційний номер (ID) клієнта, часову мітку, порядковий номер та з’єднувальну інформацію (ЗІ), яка в свою чергу складалася з часової мітки, хешу, ID та хешу ЗІ попереднього сертифікату.
2. При обробці наступного запиту сервер надсилав клієнту ID наступного запиту.

Таким чином кожен з клієнтів мав достатньо інформації про попереднього та наступного з клієнтів. Для перевірки достовірності інформації достатньо було рухатися по вибудованій ієрархії та перевіряти збіжність інформації. Виникнення розбіжностей свідчило б про недостовірність інформації, наданої сервером. Обманути систему можна було одним чином: створити «фейковий» ланцюг такої довжини, що кількість кроків перевірки була б меншою, тобто при перевірці було обійдено лише «фейкову» частину ланцюгу.

Останнім рішенням було розділити процес підтвердження між іншими користувачами. Було зроблено припущення, що ми маємо захищену схему, згідно з якою кожен користувач може підписувати повідомлення, також в системі присутній псевдорандомний генератор, доступний усім користувачам. Якщо клієнт бажає поставити мітку часу на документ, то він використовує хеш документа як

породжуючий елемент генератору. Результатом роботи генератору є кортеж, що складається з ID інших користувачів мережі. Клієнт надсилає повідомлення кожному з членів кортежу, в якому вказує хеш документа та свій ідентифікатор, кожен з них ставить свою часову мітку та відправляє результат назад до клієнта. В результаті у клієнта формується масив часових міток, згенерованих іншими членами мережі.

Мережа без використання серверу має значно більше переваг: час отримання відповіді швидший, клієнту не мають зберігати доволі великі за обсягом сертифікати з з'єднувальною інформацією.

Таким чином, в статті було описано більшість рішень і ідей, що використовують та лягли в основу сучасних блокчейн-систем.

Другим проривним моментом у 2009 році стала розробка одною або групою осіб під псевдонімом Сатоші Накамото блокчейн системи для збереження транзакцій, у яких використовувалася криптовалюта Bitcoin. Проект став дуже успішним, з кожним днем все більше людей починають використовувати біткойн для розрахунку або зберігання коштів. До цього часу Bitcoin зберігає лідерство на ринку криптовалют.

У 2015 році світ побачила платформа Ethereum. Її ключовою особливістю стали «Smart Contracts» - розумні контракти. Розумні контракти – невеликі програми, що зберігаються у блокчейні та виконуються при досягненні певних умов. Використовуються для створення домовленостей без використання «посередницьких послуг».

1.3 Типи блокчейн-платформ

Зазвичай виділяють три типи блокчейн-платформ:

1. Публічні платформи

2. Приватні платформи
3. Гібридні (консорціум) платформи.

Публічні платформи не обмежують участь у них – будь-який користувач може доєднатися. Будь-хто може переглядати інформацію у блоках, доєднатися до їх створення та верифікації. Користувачі залишаються анонімними, адже ідентифікація особистості відсутня. Серед переваг слід зазначити такі:

1. Високий рівень довіри (не треба турбуватися про довіру до окремих вузлів завдяки алгоритмам підтвердження).
2. Захищеність. Чим більше вузлів – тим важче зловмисникам завдати шкоди системі.
3. Прозорість. Інформація про будь-який блок доступна для будь-кого.

Недоліки:

1. Низька швидкість обробки транзакцій. Через величезну кількість вузлів швидкість верифікації транзакцій є низькою. Краща безпека – нижча швидкість.
2. Надвелике споживання електроенергії. Тисячі машин залучені до створення нових блоків, підтвердження транзакцій.

Зазвичай використовуються для зберігання та обміну криптовалютами. Приклади: Bitcoin, Ethereum…

Приватні платформи обмежують участь користувачів, доєднання до мережі дозволено лише окремим особам. Зазвичай використовуються всередині організацій. Контролююча організація власноруч слідкує за безпекою, правами користувачів, доступом до мережі. За структурою схожі на публічні, проте набагато менші. Такі системи важко назвати децентралізованими, адже фактично контроль має певна організація. Ідентифікувати користувачів зазвичай досить легко, адже потреби у анонімності немає. Переваги приватних платформ:

1. Швидкість. Кількість вузлів значно менша ніж у публічної платформи, тому швидкість обробки транзакцій набагато більша.

2. Масштабування. Організації можуть легко зменшувати або збільшувати кількість вузлів за потреби.

Недоліки:

1. Побудова довіри. Анонімність у такій мережі відсутня, тому треба вибудувати механізми довіри для передачі конфіденційної інформації.
2. Низький рівень безпеки. Через невелику кількість вузлів рівень безпеки значно нижчий публічну. Існує можливість вразити систему, отримавши доступ до системи управління, оскільки повна децентралізація відсутня.
3. Централізованість. Необхідно мати систему контролю доступу та ідентифікації. Ще одна вразливість приватної системи, оскільки отримавши доступ до контролера, ми отримаємо доступ до всієї системи.

Використовуються для голосувань, цифрової ідентифікації, аудиту. Приклади: Fabric, Corda…

Гібридні платформи поєднують у собі властивості публічних і приватних. Контролюються кількома організаціями. Переглядати інформацію у блоках можуть тільки окремі користувачі. Можна обирати яку інформацію зробити загальнодоступною, а яку конфіденційною. В залежності від конкретної системи можуть наслідувати переваги та недоліки як від публічних платформ, так і від приватних. Використовуються у банківській і державній сфері. Приклади: Dragonchain, R3…

Отже, не можна сказати, який тип є кращим, усе залежить від індивідуальних потреб замовника, кожен тип має достатньо переваг і недоліків.

1.4 Типи консенсусу

Блокчейн системи є децентралізованими структурами, а отже усі її учасники мають взаємодіяти за допомогою певного набору правил.

Консенсус у блокчейні – алгоритм, описаний деяким набором правил та функцій, що дозволяє встановити певні домовленості між усіма учасниками мережі. За допомогою консенсусу вибудовується уся система надійності.

Наразі існує багато алгоритмів консенсусу, які дають різний рівень безпеки та швидкості обробки транзакцій. Найпоширенішими з них є такі: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS).

Алгоритм PoW є одним з перших і найбільш вживаних алгоритмів. У створенні блоку задіяні усі вузли у системі. Майнери змагаються у формуванні нового блоку з списку останніх транзакцій. Кожен майнер має доступ до даного списку та вирішує «пазл», має бути доведено, що усі транзакції є валідними.

Особливість алгоритму полягає у тому, що він потребує колосальних обчислювальних потужностей задля формування результату, проте його перевірка є легкою.

В результаті роботи, кожен майнер формує хеш-значення, отримане з обробки отриманих даних хеш-функцією (Наприклад SHA-256). Якщо ж хоч якась транзакція є сфальсифікованою, хеш-значення буде іншим. Обрахунок хеш-значень є легкою задачею для сучасних машин, тому щоб ускладнити цей процес алгоритм використовує обмеження значення хешу. Встановлюється певне цільове (target) значення, результат хешування не має його перевищувати. Для цього до даних кожен раз додається певне число – nonce (зазвичай довільно-згенероване), для зміни значення результуючого хешу. Щоб збільшити складність обчислення слід зменшити значення target, тоді майнерам доведеться перебирати більше nonce значень задля досягнення цілі. Коли будь-хто з майнерів отримує хеш, який задовольняє умовам пошуку, він сповіщає про це усі інші машини, які мають підтвердити правильність обрахунку.

Серед переваг даного алгоритму є надійність та простота, недоліками є надзвичайна кількість витраченої енергії, низька швидкість обробки транзакцій. Через це багато систем планують перейти на інший алгоритм – Proof of Stake.

Алгоритм PoS трактує таке правило: чим більша «ціна» майнера (Наприклад кількість криптовалюти, якою він володіє) – тим більша вага його внеску у створення наступного блоку (Більша вірогідність створення ним нового блоку). В залежності від імплементацій, за «ціну» можуть братися різні показники. Наприклад, якщо майнер має n % від загальної кількості криптовалюти, то теоретично його шанс згенерувати наступний блок є n %. Сенс даного алгоритму полягає у тому, щоб зробити атаки тяжкими не по рівню ресурсів, а по ціні. Перевагами алгоритму є надійність та невелике споживання енергії, недоліки – спонукання до утворення монополій.

DPoS утворився шляхом внесення змін до PoS. Суть полягає у тому, що користувачі обирають «свідків» - witnesses, які мають валідувати наступний блок. Кожен користувач «голосує» за певного свідка, вага голосу пропорційна його ціні. Якщо свідок має погану репутацію, то він видаляється з роботи. Перевагою у порівнянні з PoS є більша швидкість обробки транзакцій, краща масштабованість.

Існує й багато інших алгоритмів, проте вони не є широковживаними на даний момент. В залежності від потреб системи, кожна з них обирає відповідний вид алгоритму. Наразі розробники з усього світу працюють над новими алгоритмами, що будуть краще задовольняти потреби безпеки, швидкості та надійності одночасно.

2. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Напрямки застосування блокчейну

З плином часу технологія блокчейн проникає у нові сфери діяльності, висвітлюючи свої переваги на фоні з іншими. Найпоширенішим її застосуванням до цих пір є ведення обліку криптовалютних активів. Багато державних та комерційних організацій вже розпочали тестувати або запроваджувати елементи блокчейну у своїх потребах. Блокчейн завойовує нових фанатів своїми перевагами у порівнянні з іншими технологіями. Блокчейн – це децентралізоване сховище даних, а отже при великій кількості вузлів проблема втрати даних або їх пошкодження майже не має шансів на виникнення. Крім того рівень захищеності даних є високим.

2.2 Криптовалюти та фінансовий сектор

Криптовалюти стали першими розробками, де була використана технологія. На фоні багатьох криз та конфліктів людство почало шукати способи альтернативного зберігання своїх заощаджень. Зародилася недовіра до банків та фінансових установ. Поява на ринку абсолютно нового продукту одразу ж викликала зацікавленість багатьох осіб. Капіталізація криптовалют почала зростати і досягла обсягів, більших або рівних за річний ВВП розвинутих країн. Багатьох привабила відсутність керуючого органу, який би регулював обіг валют. Серед переваг використання криптовалют замість банків можна виокремити такі: доступність 24\7, фіксований розмір комісії незалежно від місцезнаходження сторін, швидка обробка транзакцій, збереження анонімності, достатньо просто мати девайс з під’єднанням до інтернету для початку використання послуг, відсутність єдиного серверу з даними користувача, відсутність можливості відхилення транзакції за різних обставин. Банк може збанкрутіти, гроші певної країни – дуже швидко знецінитись, криптовалюти ж зазвичай не прив’язані до ситуації на певній території. Проте стабільністю вони теж не можуть похизуватися, тому були

створені так звані стейблкоїни – криптовалюти, прив’язані до запасів звичаної валюти, або певних товарів (дорогоцінні метали, нафта). Їх курс коливається відповідно до активу, до якого вони прив’язані.

Фінансові установи також можуть відчути переваги використання блокчейну, інтегрувавши його у свою систему платежів.

2.3 Охорона здоров’я

Багато організацій із сфери охорони здоров’я вже використовують блокчейн для збереження даних своїх пацієнтів та записів у їх медичних книжках. Дані можуть бути зашифровані з використанням публічних та приватних ключів, таким чином тільки деякі користувачі зможуть переглядати записи про відповідного пацієнта, а за потреби ділитися своїм приватним ключем з особами, яким має бути доступна приватна інформація пацієнта. Зрозуміло, що така система зберігання інформації підійде не для всіх даних, а отже деякі доведеться зберігати у звичному вигляді. Впровадження блокчейну допоможе пацієнтам упевнюватися, що лікарі зробили всі відповідні записи, і вони не будуть видалені або перезаписані іншими. Пацієнтам буде доступний увесь ланцюжок записів всіх лікарів у хронологічній послідовності. Також це допоможе лікарям, які обслуговують одного пацієнта уникати непорозумінь. Буде зменшено шкоду від хакерських атак, оскільки інформація про хвороби пацієнта, його персональні дані є конфіденційною інформацією, знаючи яку, зловмисники можуть шантажувати або обманювати пацієнта, а збереження даних у блокчейні гарантує високий рівень безпеки. Багато таких проектів вже реалізовані, та активно використовуються.

2.4 Реєстри прав власності, договори

Дуже доцільним є використання блокчейну для фіксації прав власності особи над певним майном. По-перше питання безпеки за збереження усіх даних в цьому випадку є дуже важливим, оскільки при їх втраті особа не зможе довести своє право власності над певним об’єктом, або процес відновлення прав буде дуже

трудомістким. Також, як було зазначено раніше, блокчейн гарантує незмінність усіх записів, зроблених з початку функціювання мережі. Тому зловмисники, що захочуть шахрайськими методами заволодіти чужим майном не матимуть змоги це зробити. Також у разі атаки на один з вузлів, працездатність та вміст мережі не буде порушено.

Розумні контракти – новий вид укладання домовленостей між особами, або групами осіб. Умови договору, перевірка їх дотримання, результат прописуються в коді контракту. Головною їх перевагою є відсутність третіх осіб, що регулювали б виконання умов договору кожною із сторін. Розумні контракти вбудовуються в блокчейн, тому наслідують усі переваги використання технології. Теоретично сфера застосування смарт контрактів є безмежно широкою, їх використання значно зменшує витрати на нотаріальні послуги, послуги третіх осіб, адвокатів.

2.5 Ланцюги поставок

Ланцюги поставок допоможуть людству значно зменшити поширення деяких хвороб, збиток від них, відслідковувати походження товару та його шлях. Наразі досить складно відслідкувати партії продуктів, що поставляються невеликим підприємствами або фермерами. У випадку виявлення поганих або інфікованих продуктів одним з отримувачів майже неможливо досягти вилучення продуктів цієї партії в інших. IBM та Wallmart розробляють систему відстежування, яка допоможе їм швидко відслідковувати «погані» товари, та подавати сигнали щодо необхідності їх вилучення. Наприклад певний ресторан або магазин отримав партію товару, що викликала недуги у покупців, використовуючи блокчейн систему вони можуть швидко відслідкувати партію товару, по ній ідентифікувати дистриб’ютора та постачальника цієї продукції. Якщо товар дійсно пошкоджено, то постачальник отримає мітку, всі хто купував такі товари, або якось пов'язаний з їх реалізацією отримають повідомлення про небезпеку. Також цю систему можна використовувати для помітки продуктів, які мають мітки «органічні», «вибір року» або будь-які інші для підтвердження їх валідності.

2.6 Вибори

Питання чесних виборів є актуальним вже багато століть. Підкуп виборців, учасників виборчих комісій, підробка бюлетенів та інші протизаконні дії призводять до виникнення багатьох конфліктів та зросту недовіри до виборчої системи. Використання блокчейну для проведення виборів унеможливить будь-які види підкупів, оскільки підрахування голосів проходить автоматично.

2.7 Державний сектор

Використання блокчейну у державному секторі має багато застосувань. Як зазначалося вище переваги технології можна застосовувати для організації виборів, фінансових операцій, охорони здоров’я, критичної інфраструктури, майнових реєстрів, освіти.

Американський центр контролю захворювань планує використовувати блокчейн для збереження інформації про випадки захворювань важкими або заразними хворобами як гепатит, COVID-19 та інші. Якщо один штат фіксує спалах захворюваності, то сусідні мають бути негайно повідомлені та застосувати всі необхідні дії для захисту населення. Таким чином можна краще контролювати поширення захворювань, швидко обмежуючи дії осіб у зонах спалахів інфекцій.

Міністерство внутрішньої безпеки США загалом виділяє 16 галузей критичної інфраструктури. Серед них є енергетична, транспортна, медична, фінансова та багато інших. Кожна секунда, яку система буде у непрацездатному стані може завдати значної економічної шкоди країні, або навіть призвести до загибелі певних осіб. Тому використання блокчейну якнайкраще підходить для цих галузей та наразі широко використовується ними. У серпні 2019 року американське міністерство енергетики відзначило перспективність проекту «Енергетичний інтернет», що побудовано на базі блокчейну. Використовуючи дану платформу, власники будинків зможуть купувати електроенергію з розподілених джерел, наприклад ферм вітряків. Завдяки цій платформі має покращитись регулювання

споживання енергії. Споживач буде вибирати кращий час для використання електроенергії в залежності від її ціни, чим більше попит – тим вища ціна. Проект вже почав співпрацювати з великими постачальниками та деякими дослідницькими центрами. Усі користувачі мережі (постачальники, споживачі) зможуть в режимі реального часу відслідковувати рівень витрат енергії та доступності енергетичних ресурсів.

Цікавим є проект, підтримуваний японським міністерством охорони довкілля, що на цілений на побудову системи виміру та обміну відновлюваної енергії. Проект використовує криптовалюту для побудови системи обміну. Енергія конвертується в обмінювану валюту. Ціна будується на попиті та ціні передачі енергії.

У малайзійському місті Малакка планують відкрити блокчейн-місто майбутнього. У ньому будуть розташовані фешенебельні готелі, вілли з видом на море, шале та водні атракціони. Спочатку вони планують запустити власну криптовалюту DMI, яка буде використовуватися для оплати послуг. Також туристи зможуть обмінювати їх гроші на DMI монети та платити за допомогою телефона або комп'ютера. Планується, що інноваційне блокчейн-місто буде приймати близько трьох мільйонів туристів на рік.

Двадцять дві країни Європейського Союзу у 2018 році підписали документ про потенціал використання блокчейну в трансформації електронних сервісів у Європі. За останньою інформацією у проекти вже було інвестовано близько 350 мільйонів євро. Європейські експерти впевнені, що усі громадські сервіси мають майбутнє, пов'язане з блокчейном, адже громадяни будуть впевнені в захисті та надійності їх персональних даних.

У Естонії було створено велику платформу з онлайн доступом до ідентифікаційних даних, медицини та «держави в смартфоні». 99% їх медичних даних оцифровано і доступно з будь-якого девайсу. Усі дані зберігаються у блокчейні.

Грузія та Швеція запровадили систему для реєстрації прав власності на землю, продажу нерухомості на базі блокчейну, це дозволило зменшити корумпованість цієї сфери.

Мальта використовує блокчейн для збереження студентських дипломів, шкільних табелів та нагород. Це допомагає зберігати персональну інформацію в таємниці, мінімізує бюрократію, полегшує доступ до ресурсів.

Варто також відзначити українську платформу Дія, що використовує блокчейн для збереження критично важливих даних. У 2017 році Кабінет Міністрів уклав договір з американською компанією BitFury про переведення державних реєстрів на блокчейн, що має полегшити реєстрацію фізичних осіб та підприємств. Міністерство агарної політики презентувало оновлений земельний кадастр на блокчейні, який має полегшити роботу підприємців.

Багато інших країн уже долучилося або долучається до виористання блокчейну. Цікаво, що експериментують з використанням технології не тільки передові країни світу, а й доволі бідні держави Африки та Близького сходу. Блокчейн має багато шансів завоювати популярність та довіру у сферах, що мають стратегічне значення для держави та мають бути доступними кожну секунду зберігаючи при цьому надійність та безпеку даних.

3. РОЗРОБКА ЗАСТОСУНКУ ДЛЯ ПРОВЕДЕННЯ ВИБОРІВ

3.1 Аналіз проблеми

Майже кожні президентські вибори як в України так і в усьому світі проходять не без проблем. Численні мітинги, порушення, підкидання бюлетенів, тисячі обвинувачень. Недовіра до сучасної виборчої системи, яка потребує ручної перевірки голосів створює багато недоліків, серед яких можливість фальсифікації результатів, втрати бюлетенів та інші. Ідеальним рішенням було б виключення людського фактору з процесу перевірки та збирання голосів.

Переведення процесу виборів в електронний режим має багато переваг, особливо якщо буде використано технологію блокчейн, головною перевагою якої є незмінність даних, записаних у реєстр. По-перше перевірка буде відбуватися автоматично, а отже можливість підкупу членів виборчих комісій буде вилучено. По-друге блокчейн гарантує незмінність даних, тому ніхто не зможе змінити вибір особи. По-третє можна буде уникнути багатьох «несучасних» операцій на кшталт перевірки документів, розписів у журналі виборців, перевірки списків виборців. Ідентифікація особи буде проводитися скануванням її паспорту та відбитку пальця – для підтвердження використання саме свого паспорту. Також така схема має пришвидшити процес голосування, що допоможе уникати довгих черг.

Для реалізації системи доречним буде використання розумних контрактів – програм, що працюють на блокчейні, містять у собі функції та дані. Користувачі можуть взаємодіяти з контрактами через транзакції, що викличуть певні функції, які змінять дані.

Платформа Ethereum має гарні можливості для розробки децентралізованих застосунків на базі розумних контрактів, саме тому була обрана для реалізації завдання.

3.2 Написання смарт-контракту

Для написання контрактів використовується мова програмування Solidity, створена спеціально для розробки смарт-контрактів, що унаслідувала функції з багатьох інших мов програмування і є схожою на JavaScript.

На Рисунку 3.1 зображено смарт-контракт, що було розроблено для вирішення поставленої задачі.

На початку кожного контракту слід зазначити, яку версію компілятора слід використовувати.

```
pragma solidity >=0.4.22 <0.8.0;

contract Voting {
    struct Candidate {
        uint id;
        string name;
        string surname;
        string patronymic;
        string description;
        string dateOfBirth;
        uint votesNumber;
    }
    mapping(address => uint) public voters;
    mapping(uint => Candidate) public candidates;
    uint public candidatesNumber;

    function addCandidate(string memory _name, string memory _surname,
        string memory _patronymic, string memory _description, string memory _dateOfBirth) private{
        ++candidatesNumber;
        candidates[candidatesNumber] = Candidate(candidatesNumber, _name, _surname, _patronymic, _description, _dateOfBirth, 0);
    }

    function vote (uint _candidateId) public {
        require(voters[msg.sender]==0);
        require(_candidateId > 0 && _candidateId <= candidatesNumber);
        voters[msg.sender] = _candidateId;
        candidates[_candidateId].votesNumber++;
    }

    constructor() public {
        addCandidate("Петро","Порошенко","Олексійович","Голова партії \"Європейська Солідарність\"","1958-09-26");
        addCandidate("Володимир","Зеленський","Олександрович","Голова партії \"Слуга Народу\"","1978-01-25");
        addCandidate("Юлія","Тимошенко","Володимирівна","Голова партії \"БЮТ\"","1960-11-27");
    }
}
```

Рисунок 3.1 – смарт-контракт для виборів

Тіло контракту обгортається за допомогою ключового слова contract, за яким іде його назва. За синтаксисом схоже на оголошення класу в об’єктно-орієнтованому програмуванні.

Для опису типу кандидат було використано структуру, що містить у собі поля описових характеристик кандидату: ідентифікатор, ім’я, прізвище, по-батькові, дата народження, опис та кількість голосів.

Для збереження кандидатів та голосів виборців використано структуру mapping, яка є хеш-таблицею. Для виборців ключем є адреса їх акаунту, значенням – голос за певного кандидата. Для кандидатів ключ – унікальний ідентифікатор кандидата, значення – власне сам об’єкт. Також у Solidity відсутня можливість переглянути кількість елементів в хеш-таблиці, тому треба створити додатковий лічильник для кількості кандидатів.

Щоб додатки кандидата до хеш-таблиці було створено окрему функцію, що приймає на вході значення усіх полів та створює відповідний елемент у хеш-таблиці. Метод оголошено як приватний, тому викликати його можна тільки зсередини контракту, в нашому випадку він викликається у конструкторі – при створенні контракту.

Останньою функцією є віддання голосу. На вхід приймається ідентифікатор обраного кандидата. За допомогою ключового слова require перевіряється валідність переданого параметру. Також перевіряється, чи не проголосував виборець до цього. Якщо усі перевірки пройдено, то голос додається до загальної кількості голосів, а адреса виборця до списку тих, хто вже проголосував.

На цьому створення контракту завершується. Важливим є створення тестів та перевірка правильності його роботи, оскільки як тільки контракт буде додано до блокчейну, змінити його вже не буде можливості.

3.3 Розгортання та запуск контракту

Для тестування і розгортання контракту використовується truffle ide. Завантажити truffle можна за допомогою npm – менеджеру пакетів. Для ініціалізації проекту слід виконати команду truffle init – для створення нового проекту, або ж використати заготовку проекту, для цього треба виконати команду truffle unbox.

Після виконання команди створюється базова структура директорій (рисунок 3.2).

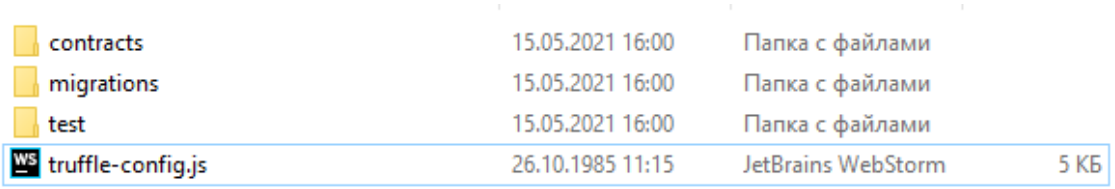

Рисунок 3.2 – результат виконання команди truffle init

В директорії contracts зберігаються усі контракти, migrations зберігає JavaScript файли, які відповідають за розгортання контрактів в мережі, зміну їх станів. Усі тести мають бути поміщені у відповідну директорію з назвою tests.

Виконавши команди truffle compile, truffle migrate ми скомпілюємо контракти та помістимо їх у блокчейн.

Truffle має консольний інтерфейс для взаємодії з контрактами, ми можемо викликати функції, переглядати змінні.

За допомогою команди truffle develop можна увійти до консолі для розробки та зібрати і перевірити проект в тестовому режимі. У цьому режимі ми можемо взаємодіяти з контрактом точно так, як і при його розгортання у справжньому блокчейні.

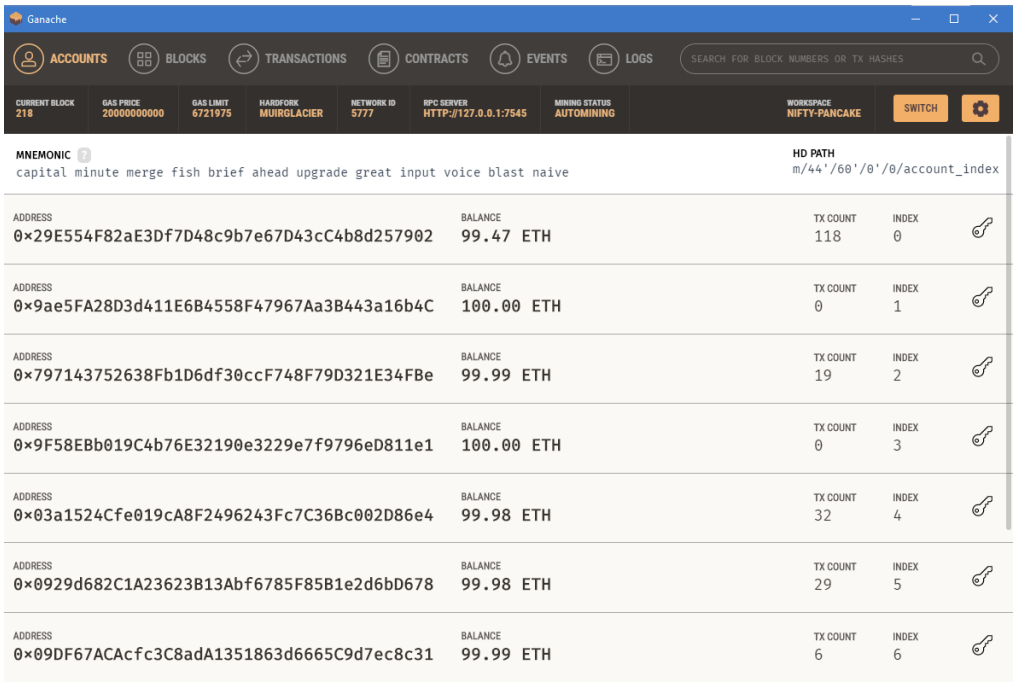

Рисунок 3.3 – додаток Ganache

У створенні блокчейну для розробки на локальній машині додаток Ganache. Він створює власну Ethereum-блокчейн мережу на нашому комп’ютері.

Після встановлення додатку ми побачимо інформацію про локальну блокчейн-систему, що була утворена: її ідентифікатор, кількість блоків, акаунти та інше (Рисунок 3.3).

Останній встановлений додатком є MetaMask, який допоможе нам підключитися до локальної мережі блокчейну із браузеру. Достатньо встановити лише додаток до браузеру Google Chrome. Застосунок має зручний інтерфейс, на якому можна побачити мережу, до якої нас під’єднано, поточний акаунт та його баланс (Рисунок 3.4).

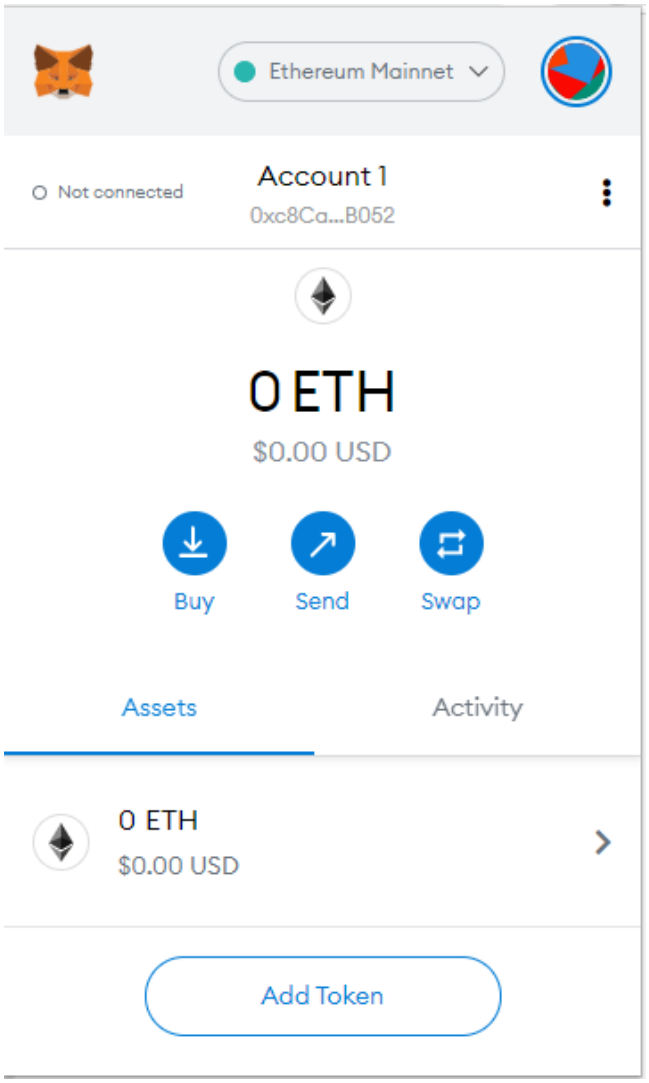

Рисунок 3.4 – додаток Metamask

Усі необхідні додатки встановлено. У результаті було створено власну Ethereum-блокчейн мережу для тестування та роботи застосунку, у ній було розгорнуто контракт, взаємодіючи з яким ми можемо брати участь у голосуванні.

3.4 Взаємодія з блокчейном через користувацький інтерфейс.

Для взаємодії користувача з нашою мережею було розроблено простий веб-застосунок. Розробка користувацького інтерфейсу не відрізнялася від процесу створення інших веб-застосунків. Формуємо звичну структуру каталогів (Рисунок 3.5)

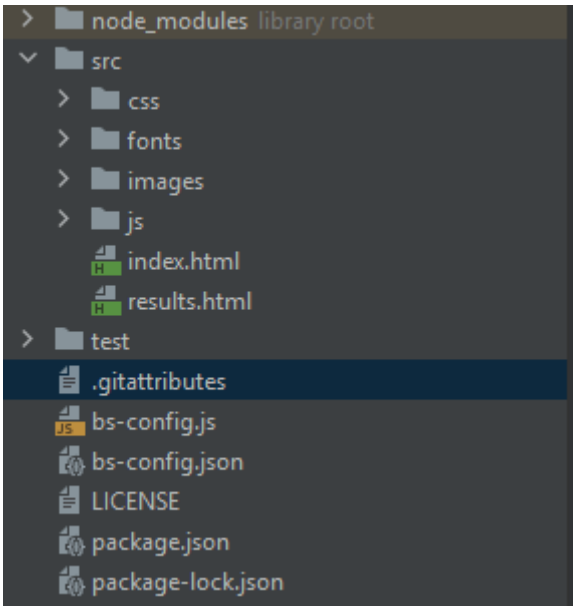

Рисунок 3.5 – структура каталогів

Створюємо html заготовки базових сторінок, додаємо та підключаємо стилі, шрифти, зображення, JavaScript-файли, конфігуруємо сервер, встановлюємо залежності.

Особливістю застосунку є частина коду, що вибудовує логіку взаємодії з блокчейном та власне нашим контрактом. Щоб працювати із блокчейном із користувацького інтерфейсу використовується бібліотека web3.js.

Підключаємо до нашої html сторінки файл, що містить об’єкт App, в якому є інформація про поточного провайдера, контракти, акаунт та голос користувача.

```
App = {
    web3Provider: null,
    contracts: {},
    account: '0x0',
    userVote: 0,

    init: function() {
        return App.initWeb3();
    },

    initWeb3: function() {
        App.web3Provider = new Web3.providers.HttpProvider('http://localhost:7545');
        web3 = new Web3(App.web3Provider);
        return App.initContract();
    },

    initContract: function() {

        $.getJSON("Voting.json", function(election) {
            App.contracts.Voting = TruffleContract(election);
            App.contracts.Voting.setProvider(App.web3Provider);
            return App.render();
        });
    },
```

Рисунок 3.6 – використання web3

При завантаженні вікна викликається функція ініціалізації об’єкту App (рисунок 3.6). Встановлюється провайдер, який містить адресу інтерфейсу локального блокчейну. Підтягується інформація та дані з відповідного контракту, та на основі цих даних будується сторінка з інтерфейсом користувача. Таким чином завдяки використанню бібліотеки web3 застосунок отримує повний доступ до даних контракту та функцій взаємодії із ним (рисунок 3.7), може ініціювати транзакції (рисунок 3.8).

```
await App.contracts.Voting.deployed().then( fn: function(instance) {
    contractInstance = instance;
    return contractInstance.candidatesNumber();
```

Рисунок 3.7 – отримання екземпляру контракту

```
App.contracts.Voting.deployed().then( fn: function(instance) {
    return instance.vote(candidateId, { from: App.account });
});
```

Рисунок 3.8 – взаємодія з контрактом

Як зазначалося вище, для взаємодії з блокчейном через браузер використовується додаток MetaMask. По замовчуванню MetaMask використовує головну мережу Ethereum, а отже треба підключитися до нашої локальної мережі. Для цього у додатку обираємо дію створення нового підключення, обираємо його назву та вводимо адресу мережі (Рисунок 3.9).

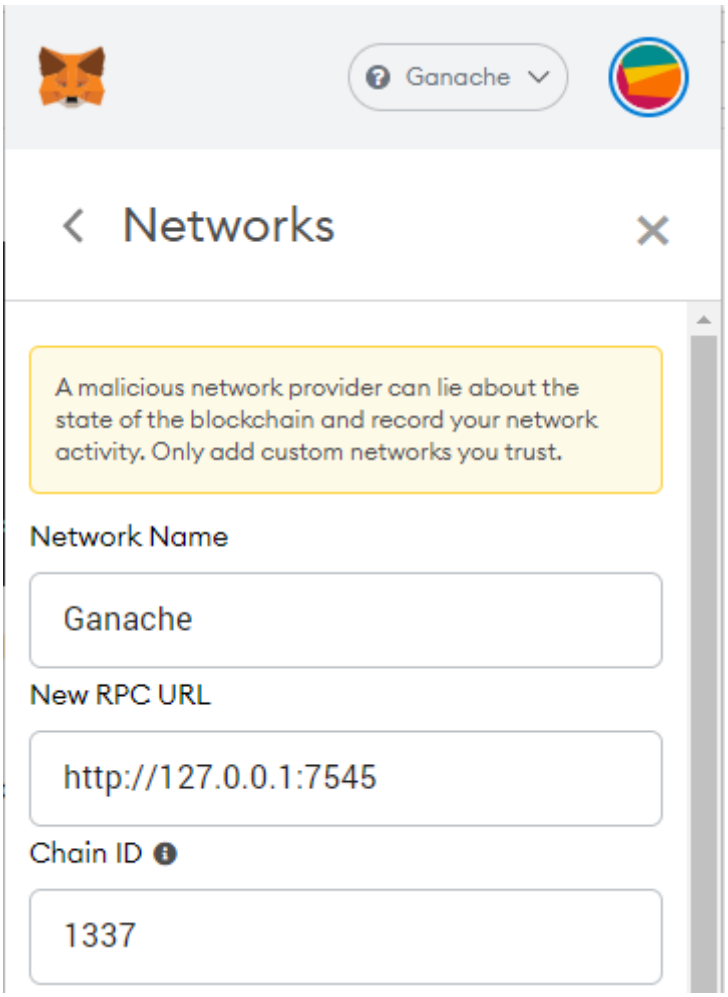

Рисунок 3.9 – підключення до локального блокчейну

Тепер ми підключені до нашої мережі та можемо обирати акаунти, що були створені в нашому блокчейні, бачити їх баланс. MetaMask впроваджує глобальні API для веб-сайтів, які відвідували користувачі, цей API дозволяє веб-сайтам отримувати інформацію про акаунти користувача, доступатися до блокчейну. Таким чином наш застосунок отримує доступ до акаунту, який обраний у додатку MetaMask (Рисунок 3.10).

```
web3.eth.getCoinbase(async function(err, account) {
    localStorage.setItem("accounts",web3.eth.accounts.length.toString());
        const accounts = await ethereum.request({ method: 'eth_requestAccounts' });
        const account = accounts[0];
        App.account = account;
        $('#content').show();
        $("#accountAddress").html("Ваш ідентифікатор: " + account);
});
```

Рисунок 3.10 – Отримання даних про акаунт користувача

На цьому розробку та налаштування застосунку завершено, локальний блокчейн запущено, у ньому розміщено контракт, налаштовано взаємодію користувача з мережею через браузер.

3.5 Інструкція та особливості використання

Для початку використання застосунку слід запустити веб-сервер та перейти на відповідну сторінку браузеру. Користувача зустрічатиме відповідне вікно, в якому треба натиснути на кнопку «Увійти», попередньо обравши акаунт у додатку MetaMask (Рисунок 3.11). Якщо користувач не увійде в акаунт, то перейти далі він не зможе. Цей процес імітує ідентифікацію та аутентифікацію користувача, у реальному житті замість додатку MetaMask використовувалися б паспортні дані та біометрія. Якщо ж користувач увійшов у додаток та обрав акаунт, він зможе перейти на наступну сторінку, натиснувши відповідну кнопку.

Наступна сторінка містить власне виборчий бюлетень, на якому розміщується опис кандидатів: ПІБ, дата народження, додаткова інформація та

місце для мітки. Користувачі, чиїх акаунтів немає у локальному блокчейні, не зможуть віддати голос за кандидата і отримають відповідне повідомлення, проте зможуть подивитися на бюлетень (Рисунок 3.12) та дізнатися результати.

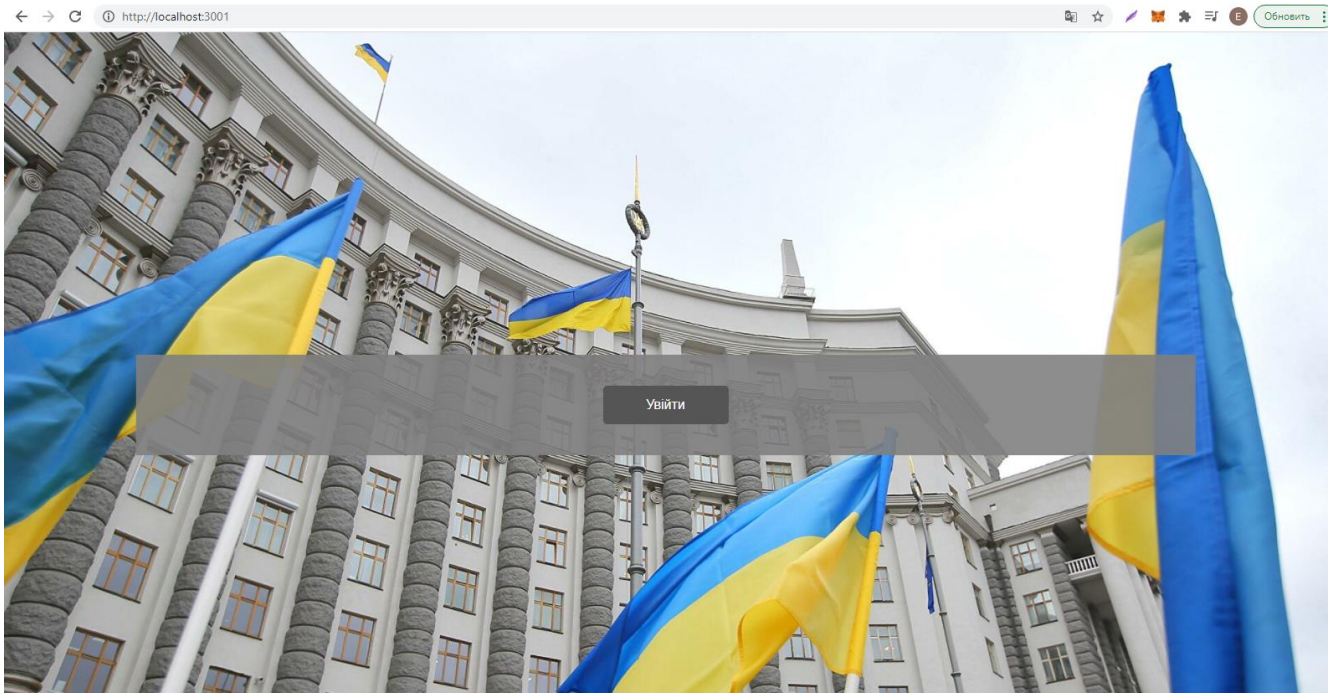

Рисунок 3.11 – Вітальна сторінка застосунку

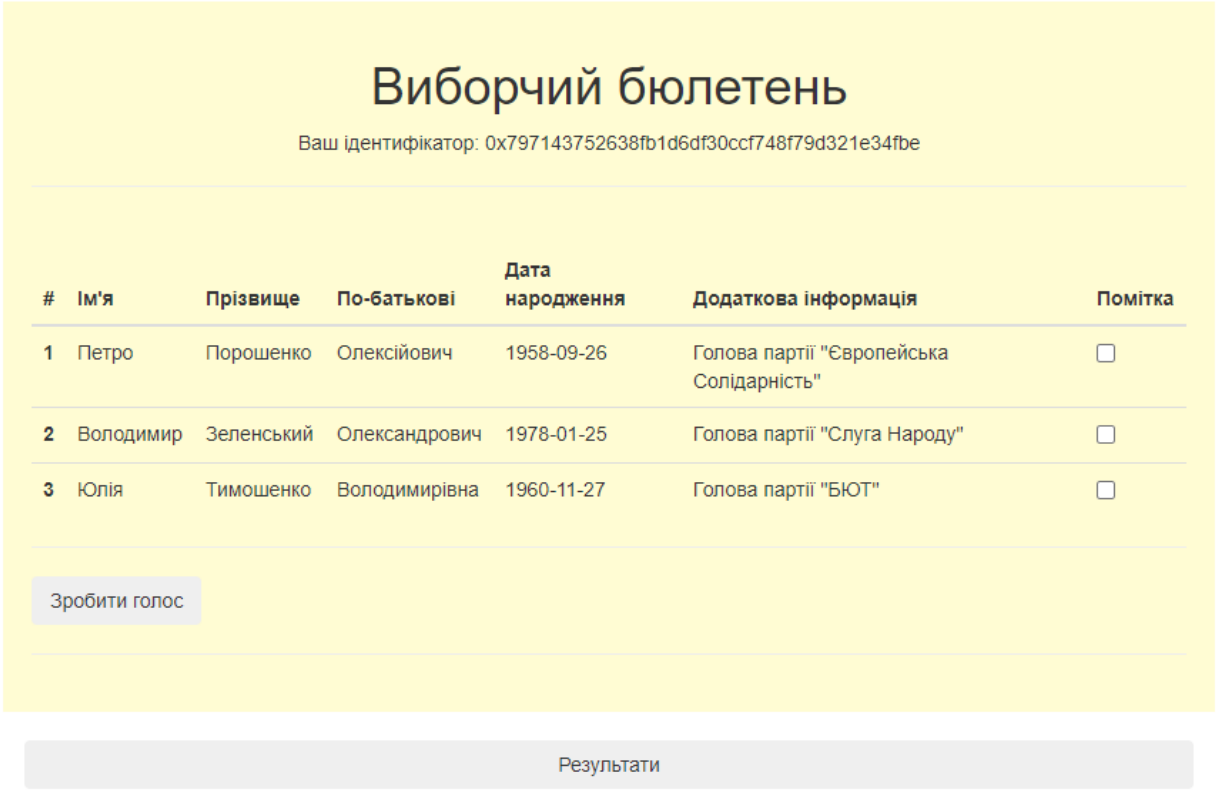

Рисунок 3.12 – Виборчий бюлетень

Усі ж інші зможуть поставити помітку навпроти вподобаного кандидата та натиснути кнопку голосування для підтвердження. Якщо користувач вже проголосував, то він отримає відповідне повідомлення та зможе побачити, за кого саме віддав свій голос (Рисунок 3.13).

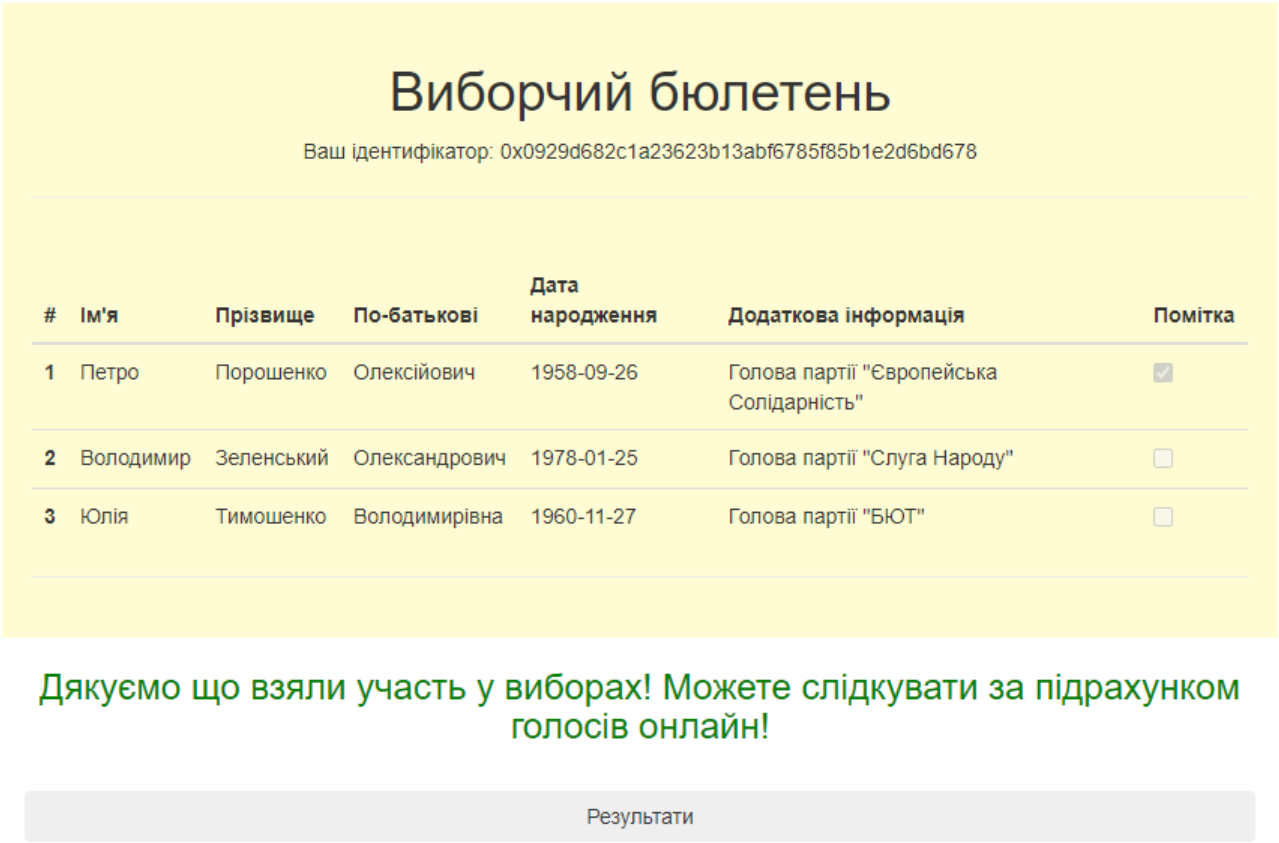

Рисунок 3.13 – Сторінка особо, що взяла участь у виборах

Натиснувши кнопку «Результати», користувач може побачити різні дані про підрахунок голосів на даний момент часу: поточна явка, що обраховується загальна як кількість відданих голосів, поділена на загальну кількість виборців, кількість голосів, що отримав кожен кандидат, діаграму з відсотком голосів, відданих за певного кандидата (Рисунок 3.13).

Загальна явка на даний момент складає 60%

Кількість голосів за кандидата

Ім'я	Прізвище	По-батькові	Кількість голосів
Петро	Порошенко	Олексійович	3
Володимир	Зеленський	Олександрович	2
Юлія	Тимошенко	Володимирівна	1

Рисунок 3.13 – Поточний результат

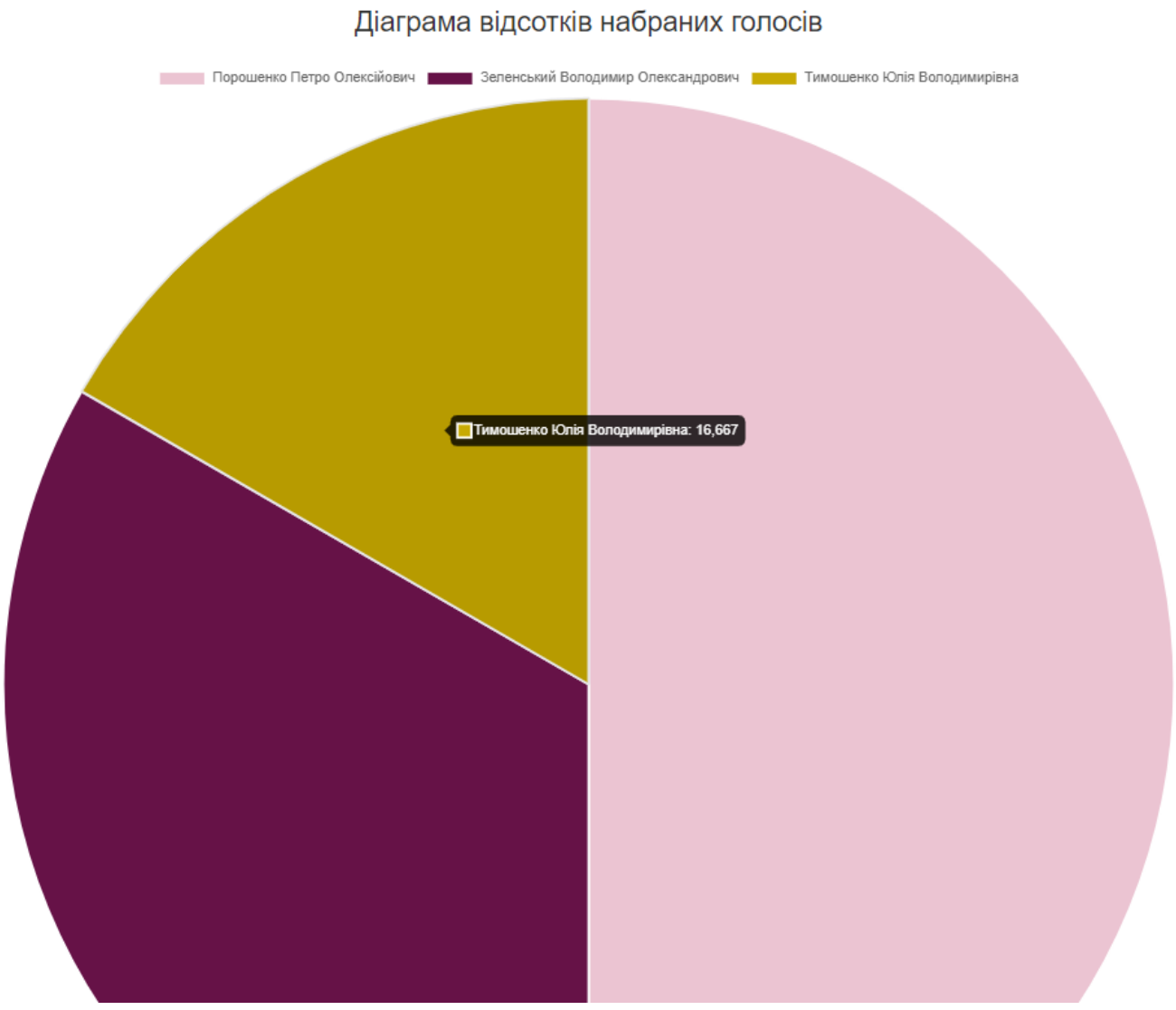

Рисунок 3.13 (продовження)

При зміні акаунту або виході з MetaMask користувач перенаправляється на сторінку з вітанням – це імітує зміну виборця за виборчим місцем.

ВИСНОВКИ

У процесі роботи були розглянуті основні теоретичні відомості про технологію блокчейн. Було досліджено історію та передумови її виникнення, ключові події. Окрему увагу присвячено типам блокчейн платформ, типам консенсусу.

У окремому розділі розглядаються особливості, переваги та недоліки технології, приклади її використання в різних сферах, цікаві проекти основані на блокчейні. Серед основних її переваг та причин популярності є відмовостійкість та захищеність даних від пошкодження та злочинних дій, саме тому технологія привертає все більше уваги у сферах, де ці параметри є критично важливими. За останні роки було створено чимало проектів для медичної, державної, енергетичної та інших сфер.

Практична частина роботи була присвячена розробці веб-застосунку для проведення виборів з використанням блокчейну для збереження голосів, що допомогло б уникнути можливості фальсифікації. У результаті було розроблено смарт-контракт, запущено тестову мережу на локальній машині, досліджено особливості взаємодії блокчейну з клієнтською частиною застосунків, розроблено веб-застосунок.

Список використаної літератури

1. What is Consensus Algorithm In Blockchain & Different Types Of Consensus Models [Електронний ресурс] // BangBit Technologies. – 2018. – Режим доступу до ресурсу: https://medium.com/@BangBitTech/what-is-consensus-algorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77.
2. Григорчук К. Обзор 9 алгоритмов блокчейн консенсуса [Електронний ресурс] / Кирилл Григорчук // DigitalForest. – 2018. – Режим доступу до ресурсу: https://digiforest.io/blog/blockchain-consensus-algorithms.
3. What Are Public Keys and Private Keys? [Електронний ресурс] // Ledger Academy. – 2019. – Режим доступу до ресурсу: https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys.
4. Haber S. How to Time-Stamp a Digital Document] / S. Haber, W. Scott Stornetta. – Morristown, 1991. – 19 c. – (Bellcore).
5. Williams S. 20 Real-World Uses for Blockchain Technology [Електронний ресурс] / Sean Williams // The Motley Fool. – 2018. – Режим доступу до ресурсу: https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx.
6. Conway L. Blockchain Explained [Електронний ресурс] / Luke Conway // Investopedia. – 2020. – Режим доступу до ресурсу: https://www.investopedia.com/terms/b/blockchain.asp#:~:text=By%20spreading%20its%20operations%20across,the%20processing%20and%20transaction%20fees..
7. Clavin J. Blockchains for Government: Use Cases and Challenges [Електронний ресурс] / J. Clavin, S. Duan, H. Zhang // DGOV. – 2020. – Режим доступу до ресурсу: https://dl.acm.org/doi/fullHtml/10.1145/3427097.
8. Solidity Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://docs.soliditylang.org/en/v0.5.3/index.html.

9. Thomas L. Blockchain Applications in Healthcare [Електронний ресурс] / Liji Thomas. – 2021. – Режим доступу до ресурсу: https://www.news-medical.net/health/Blockchain-Applications-in-Healthcare.aspx.
10. Soni N. Evolution of Blockchain [Електронний ресурс] / Neha Soni. – 2020. – Режим доступу до ресурсу: https://medium.com/@nehasoni1812/evolution-of-blockchain-f243f7509fe6#:~:text=Stefan%20Konst%20published%20his%20theory,linked%20together%20using%20cryptographic%20methods..
11. How Walmart used blockchain to increase supply chain transparency [Електронний ресурс] // The Leadership Network. – 2020. – Режим доступу до ресурсу: https://theleadershipnetwork.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency.