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

Гібридні системи консенсусу в блокчейн

Текстова частина
магістерської роботи
за спеціальністю „Інженерія програмного забезпечення” 121

Керівник магістерської роботи
к. е. н., ст. викл.
Невмержицький Є.І.

_____

“____” _____ 2020 р.

Виконала студентка ФІ-6
Бейрак М.М.

“____” _____ 2020 р.

Київ 2020

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

ЗАТВЕРДЖУЮ
Зав. кафедри інформатики,
к.ф-м.н.
_____ С. С. Гороховський
(підпис)
7 листопада 2019 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ
на дипломну роботу

студенту 2 року ІПЗ факультету інформатики
Бейрак Марії Михайлівні
Дослідити Гібридні системи консенсусу в блокчейн

Зміст ТЧ до магістерської роботи:

Зміст
Анотація
Вступ
1. Що таке блокчейн
   1.1. Огляд технології блокчейн
   1.2. Приклади використання
2. Види консенсусу в блокчейн
   2.1. Що таке консенсус
   2.2. Proof-of-Work (PoW)
   2.3. Proof-of-Stake (PoS)
   2.4. Delegated-Proof-of-Stake (DPoS)
   2.5. Proof-of-Authority (PoA)
   2.6. Proof-of-Importance (PoI)
3. Опис гібридних систем консенсусу та напрями застосування
   3.1. Decred
   3.2. Enucuum
4. Розробка EIP
   4.1. Огляд Ethereum та стандарту ERC-20
   4.2. Ідея та реалізація нового EIP

5. Опис програмного продукту

Дата видачі „25” жовтня 2019 р. Керівник _____
(підпис)
Завдання отримав _____
(підпис)

Календарний план виконання магістерської роботи

Тема: Гібридні системи консенсусу в блокчейн

Календарний план виконання роботи:

№ п/п	Назва етапу дипломного проекту (роботи)	Термін виконання етапу	Примітка
1.	Отримання завдання на дипломну роботу	7.11.2019	
2.	Підбір матеріалів за темою	4.12.2019	
3.	Остаточне рішення щодо практичної частини	14.01.2020	
4.	Огляд інструментів для практичної частини	24.01.2019	
5.	Написання SDD	19.02.2020	
6.	Початок розробки практичної частини	25.02.2020	
7.	Початок написання теоретичної частини	2.03.2020	
8.	Проміжний аналіз та корегування	15.05.2020	
9.	Завершення написання теоретичної та розробки практичної частини	6.06.2020	
10.	Фінальне корегування роботи	11.06.2020	

Студенту Бейрак М.М.

Керівник Невмержицький Є. І.

“_____”_____

Зміст

Анотація

У роботі розглянуто сутність технолонії і різні види консенсусу блокчейна, особлива увага приділяється гібридній системі. Також розглянуті приклади використання гібридної системи консенсусу у реальному житті.

У процесі виконання дипломної роботи був розроблений новий EIP, що дозволить будь-яким токенам криптовалюти Ethereum використовувати гібридну систему консенсусу.

Вступ

Останні роки у звіті з’явилася нова технологія, яка підкорила світ. Блокчейн – система, де усі дані відкриті та кожен, за бажанням, може подивитися на них.

Це розподілена база даних, у яку кожен може записати власну інформацію, але лише якщо інші учасники мережі дійдуть згоди до того, що записувати. Є різні способи врегулювання цього «конфлікту» - це системи консенсусу. Кожна з них має свої переваги та недоліки.

У цій роботі детальніше буде розглянуто гібридну систему консенсусу. Вона намагається поєднати у собі переваги PoW (Proof-of-work) та PoS (Proof-of-stake) систем консенсусів, але разом з тим має свої недоліки.

Ethereum – блокчейн, в основі якого лежить консенсус Proof-of-work. Цей блокчейн надає можливість створювати власні токени, які можуть мати цінність та використовуватися з різними цілями. Найпопулярнішим стандартом токенів у мережі Ethereum є стандарт ERC-20.

Головна мета дипломної роботи – створити новий EIP, який реалізує концепції Proof-of-stake, що дозволить будь-яким токенам у мережі Ethereum використовувати гібридну систему консенсусу. Новий EIP буде розширювати вже існуючий стандарт ERC-20, тому нові токени зможуть виконувати усі функції цього стандарту (надсилання токенів з однієї адреси на іншу). Реалізовано EIP буде мовою для написання смартконтрактів у мережі Ethereum – Solidity.

Як приклад актуального використання нового стандарту, буде розроблена система для голосування акціонерів на базі Ethereum. Акції будуть виражатися у вигляді токенів розробленого стандарту, що дозволить їм (токенам) не тільки вільно переміщатися між акціонерами, а й у більш доступній формі бути формою волевиявлення акціонера.

Буде розроблено мобільний додаток на операційну систему Android, що дозволить акціонерам завжди мати доступ до свого аккаунту.

Додаток надасть можливість проголосувати у певному опитуванні, переглянути результати уже здійснених голосувань, а також можливість переслати свої токени іншим користувачам.

1. Що таке блокчейн?

1.1. Огляд технології блокчейн

Блокчейн – у перекладі з англійської «ланцюг блоків». Така назва не просто так – інформація у блокчейні зберігається у вигляді послідовних блоків. Ця послідовність не є випадковою, адже вона будується за певними правилами. Ці правила і утворюють консенсус.

Концепція блоків була запропонована Сатоші Накамото (Satoshi Nakamoto) у 2008 році, а вперше була реалізована у 2009 році у вигляді цифрової криптовалюти – біткоіна (Bitcoin) [1].

Завдяки блокчейну біткоін став першою криптовалютою у світі. Блокчейн не належить жодній країні. Також, він вирішив проблему подвійних витрат, адже на відміну від готівкових грошей, така електронна валюта може дублюватися кілька разів.

Але блокчейн це не тільки криптовалюти, хоча здебільшого він пов’язаний саме з ними. У блокчейн можна записувати будь-які дані, не обов’язково це будуть дані про транзакції з пересилання цифрових активів. Адже блокчейн – це база даних, яка діє за трохи іншим принципом, ніж звичайні сховища даних.

В основі блокчейну лежить ідея децентралізації. У звичних нам системах є один сервер, який завжди має єдину правдиву інформацію. Але у випадку з блокчейном це не так, адже кожен учасник мережі має свою версію стану цієї системи, яка повинна узгоджуватися з іншими. Також, таку систему називають peer-to-peer системою. Графічно різницю можна побачити на рисунках 1 та 2.

У такій децентралізованій системі замість довіри використовується система, заснована на доказі за допомогою криптографії. Це дозволяє будь-яким двом сторонам безпосередньо створювати транзакцію між собою без необхідності довіреної третьої сторони [2].

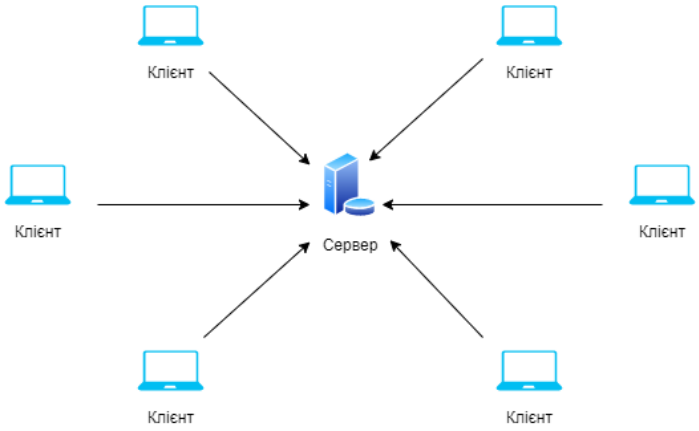


Рисунок 1. Централізована система

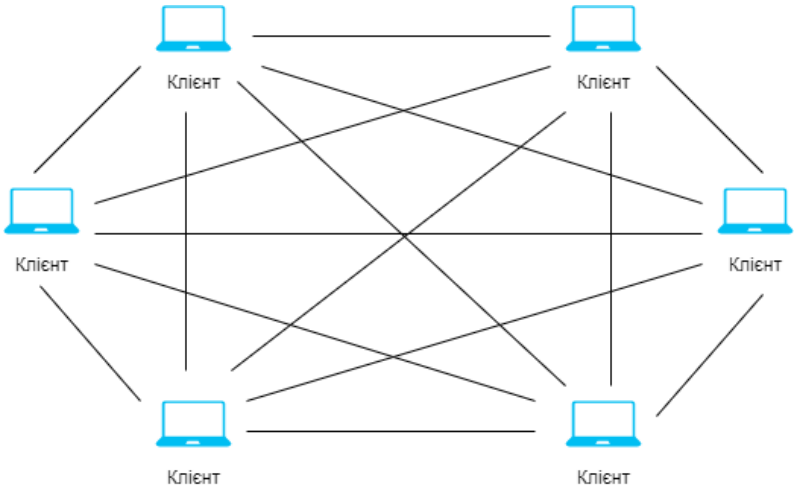


Рисунок 2. Децентралізована (peer-to-peer) система

Інформація, що зберігається у блокчейні, є повністю відкритою. Це ще один з принципів блокчейну.

Таким чином, підробити дані у такій децентралізованій та відкритій системі вкрай важко. Кожен новий запис має хеш (hash) попередньої транзакції. Хеш – закодована інформація про блок транзакцій. Хеш формується на основі усіх транзакцій, що входять до цього блоку, а також на основі хеша попередньої транзакції.

Отже для того, щоб підробити якусь транзакцію, необхідно змінити інформацію про неї. Якщо змінюється хоча б один символ оригінальної транзакції,

змінюється й хеш усього блоку. Але наступна транзакція в своєму тілі посилається на хеш, що був утворений попереднім набором транзакцій. Тому доведеться змінювати інформацію й цього блоку. Якщо так продовжувати, треба буде переписати інформацію усіх наступних блоків, які можуть з'являтися швидше аніж ми будемо переписувати усі попередні транзакцій.

Також варто враховувати, що ми не єдині учасники мережі, і кожне записування даних у блокчейн відбувається коли більшість учасників мережі визнає цей варіант валідним. Отже нам доведеться знайти таку кількість комп'ютерів, яка дозволить перевищити кількість учасників, що вже є.

Беручи до уваги всі ці факти, наразі немає жодного способу переписати дані, що уже записані до блокчейну.

На рисунку 3 можна побачити схему блоків транзакцій.

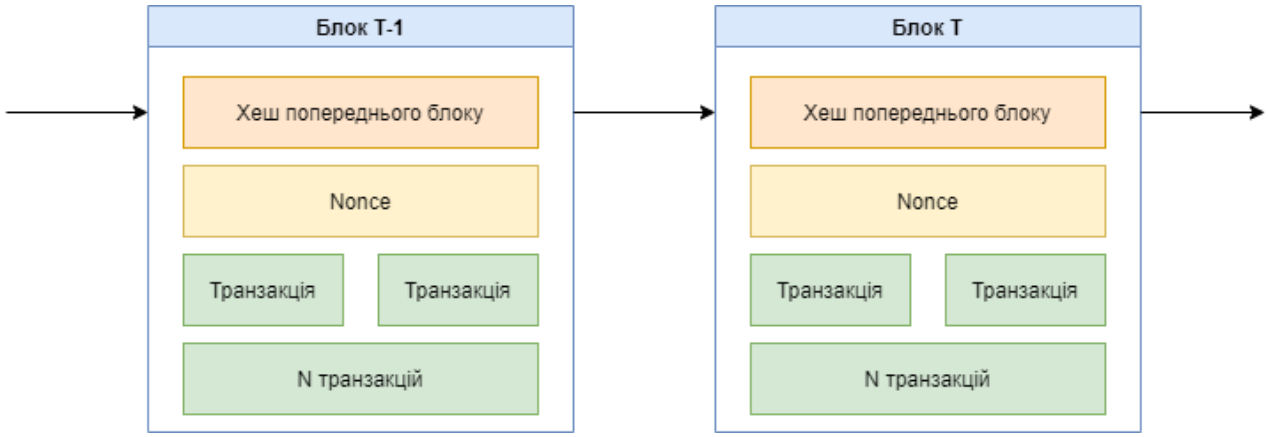


Рисунок 3. Блоки транзакцій у блокчейні

Завдяки своїй прозорості, ми завжди можемо побачити з якої адреси пересилалися які кошти за допомогою так званих блок експлорерів (від англ. explore – досліджувати, розвідувати). Можна також переглядати дані певної транзакції, знаючи її хеш.

Для того щоб стати учасником мережі, достатньо згенерувати собі публічний та приватний ключі. Приватний ключ повинен знати тільки власник аккаунту, адже саме за допомогою приватного ключа робиться підпис транзакцій (тобто

підтвердження що ви – це ви, а не хтось інший). З іншої сторони, публічний ключ може бачити будь-хто в мережі, адже це ваш унікальний «нікнейм» у блокчейні. Деякі блокчейни надають можливість ідентифікувати себе не тільки за публічним ключем, а й за якимось ім'ям. Одним з найпопулярніших прикладів є блокчейн EOS, у якому можна створювати імена до 13 символів.

Для кодування інформації використовується Elliptic Curve Cryptography, що заснована на використанні еліптичних кривих над кінцевими полями.

1.2. Приклади використання

Блокчейн – дуже перспективна концепція.

Найбільшої популярності набуло використання блокчейна як основи для криптозрахунків.

Біткоін, який був першою криптовалютою, наразі є й і її найвідомішим представником, про якого знають люди, що дуже далекі від цього ринку – на одному з найвідоміших сайтів CoinMarketCap [3], Біткоін лідирує дванадцятий рік. На другому місці Ethereum, який багато у чому покращив досвід Біткоіна, але поки все ж не зміг його випередити. Для розробників Ethereum відрізняється власною мовою програмування смартконтрактів – Solidity, що робить розробку саме під цей блокчейн цікавим для програмістів.

Криптозрахунки важко переоцінити, адже вже зараз криптовалюти активно входять у наше життя. У деяких магазинах можна розраховуватися різними криптовалютами. А державні органи країн активно працюють над проектами щодо створення власних криптогрошей – як приклади Японія [4], Китай [5] та США [6].

Але потенціал блокчейну набагато більший, адже до розподіленої бази даних можна записувати будь-яку інформацію.

Наприклад, використання блокчейну в урядових організаціях. Агенція прогресивних дослідницьких проектів в галузі оборони (DARPA) створила платформу на основі блокчейна для передачі захищених повідомлень та обробки

транзакцій, які можна простежити через численні канали. Додаток буде використовуватися по-різному - для полегшення зв'язку між підрозділами та штабами та для передачі інформації між офіцерами розвідки та Пентагоном [7].

Інший напрямок використання блокчейну – голосування. Адже там дуже важлива актуальна та правдива інформація. Проект, що був втілений у життя – голосування у Неаполі відбулося за допомогою технології блокчейн [8].

Загалом, блокчейн можна використовувати у будь-якій сфері, якій необхідне підтвердження та цілісність даних.

На сьогодні популярності набирають також приватні блокчейни – до таких систем доступ видається кожному учаснику окремо, тому тут ти не завжди можеш бачити всі дані, що є у мережі.

2. Види консенсусу в блокчейн

2.1. Що таке консенсус

Дані у блокчейні повинні бути цілісні та добре захищені від зловмисників. Алгоритми консенсусу якраз виконують такі функції, тому вони є чи не найважливішим елементом технології блокчейн.

Оскільки дані у блокчейні розподілені і немає якогось одного серверу, розподілені учасники системи повинні якось узгоджувати валідацію транзакцій, що надходять до мережі.

Важливо відрізняти алгоритм консенсусу від поняття протоколу [9] .

Протокол описує правила, за якими працює система – як повинні взаємодіяти учасники мережі, які дані вони можуть передавати, які вимоги до успішної валідації блоків.

У той же час, алгоритм виконує роль механізму, який перевіряє, що правила встановлені протоколом, виконуються – він валідує баланси та підписи, що підтверджують транзакції, а також фактично виконує перевірку блоків.

Тобто, Bitcoin та Ethereum – це протоколи, а Proof-of-Work – це алгоритм.

2.2. Proof-of-Work (PoW)

Один з найпопулярніших консенсусів, адже почав використовуватися ще у Біткоіні.

Насправді, концепція Proof-of-Work була описана ще у 1993 році в роботі «Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology» авторства Синтії Дворк та Моні Наор. Хоча термін тоді ще не був введений, автори запропонували ідею того, що для того аби отримати доступ до загального ресурсу, користувач повинен обчислити достатньою складну, але обчислювальну задачу, аби запобігти зловживанням ресурсів [10].

Сам же термін з’явився у 1999 році в статті «Proofs of Work and Bread Pudding Protocols» авторства Маркуса Якобссона та Арі Джуелс [11].

Тобто суть концепції така, що усім майнерам дається задача, яку вони повинні порахувати за певний проміжок часу (у мережі Bitcoin цей час становить

приблизно 10 хвилин). Задача - «Знайти таке значення x, щоб хеш SHA (x) містив N старших нульових біт».

У мережі Bitcoin час вирішення задачі більш менш сталий, тому що кількість біт яку треба вирахувати динамічна і залежить від кількості учасників. Функція, що вираховується – SHA-256.

Коли один учасник мережі (майнер) знайде правильну відповідь, усі інші звіряються з ним. І коли більшість завалідує знайдення відповіді – консенсусу досятнуто, блок записано.

Майнери мають свій інтерес у цьому, адже за кожну записану і підтверджену транзакцію вони отримують fee – плату. І якщо людина хоче щоб її транзакція швидше потрапила до мережі, можна запропонувати майнерам більшу плату – тоді час очікування валідації транзакції зменшиться.

Але у такого алгоритму є й мінус – він вимагає багато енерговитрат та потужного апаратного забезпечення.

2.3. Proof-of-Stake (PoS)

Другий за популярністю алгоритм консенсусу, що вперше був реалізований у валюті PeerCoin у 2012 році.

Нода, яка має найбільшу кількість токенів має більше шансів згенерувати наступний блок. Тобто чим більший баланс (stake), тим у більш вигідному становищі знаходиться нода. У цьому підході майнерам теж доводиться хешувати дані, але тут складність знову ж таки залежить від балансу.

У порівнянні з Proof-of-Work, цей алгоритм не потребує великих енерговитрат. Також до переваг можна віднести те, що задля проведення атаки на таку мережу, зловмиснику необхібно отримати більше токенів і тоді йому стане просто невигідно знецінювати власний токен.

Але тут теж є недоліки – може з’явитися група осіб, що спробує тримати токени тільки у своїх руках. У такому разі під сумнів може ставитися сама ідея децентралізації мережі [10].

2.4. Delegated-Proof-of-Stake (DPoS)

Delegated-Proof-of-Stake – ще одна альтернатива Proof-of-Work та разом з тим вдосконалення Proof-of-Stake.

Алгоритм був запропонований у 2014 році Деніелом Ларимером та використовується у таких криптовалютах як Bitshares, Steem, Ark та Lisk [12].

Суть алгоритму полягає у тому, що учасник може передати свою «роботу» іншим. Можна делегувати свій голос іншому учаснику мережі, і той буде підтримувати роботу мережі від імені іншого. Оскільки це удосконалий PoS, то чим більше баланс токенів, тим більшу вагу має голос учасника. У такій системі, як правило, винагорода за записаний блок ділиться між учасниками, що пролосували за того, хто власне записав блок.

Перевага у порівнянні з класичним Proof-of-Stake – учасники мотивовані працювати чесно, адже у будь-який момент за вас можуть перестати голосувати. До того ж, він працює швидше, ніж класичний варіант.

2.5. Proof-of-Authority (PoA)

Термін Proof-of-Authority був запропонований у 2017 році одним із засновників мережі Ethereum Гевіном Вуду [13].

Блоки записують перевірені валідатори, що завчасно обираються та по факту є модераторами системи. Тут мають цінність не кількість токенів, а репутація. Таким чином блокчейн за певним алгоритмом обирає валідатора, який запише наступний блок.

Важливо зазначити, що просто так стати валідатором важко, адже треба вкласти певну кількість грошей, а також заробити довіру інших учасників мережі, аби ті голосували за нього. Але такий процес гарантує, що валідатором стане не пересічна людина.

2.6. Proof-of-Importance (PoI)

Proof-of-Importance наразі активно використовується у криптовалюті NEM. Цей алгоритм надає перевагу користувачам, які заслужили хорошу репутацію у мережі – «спочатку ви працюєте на репутацію, потім вона на вас».

Репутація зростає з активним життям у екосистемі блокчейну та взаємодії з іншими учасниками. Чим краща репутація – тим більший шанс на створення наступного блоку [14].

Proof-of-Importance вирішує проблему Proof-of-Stake коли один учасник або група людей мали можливість контролювати мережу, отримавши більше токенів. Тут же кількість токенів на балансі не збільшують шанси на створення блоку. До того ж, коштами треба активно користуватися, адже торгувати ними вигідніше, аніж просто тримати на балансі.

3. Опис гібридних системи консенсусу та приклади застосування

3.1. Decred

Насправді, існує багато протоколів консенсусів – було розглянуто лише найпопулярніші. Усі вони створюються з єдиною метою – зробити неможливим атаку хакерів на мережу та зробити процес вибору того, хто отримує право записувати блок, більш справедливим.

Не дивно, що на базі двох найвідоміших консенсусів - Proof-of-Work та Proof-of-Stake – почали з’являтися й інші консенсуси. Їх ще називають гібридними.

Гібридні системи консенсусу мають на меті отримати переваги вже відомих консенсусів, а недоліки компенсувати одним.

Найяскравішим поєднанням гібридного консенсусу є криптовалюта Decred. Проект був запущений 7 лютого 2016 року, а вже 25 квітня 2017 року була представлена перша версія.

Одна з основних переваг цієї криптовалюти – усі люди, що володіють цією криптовалютою мають можливість не просто пересилати токени, а й брати участь у вирішення питань щодо майбутнього проекту.

Зазвичай учасників мережі можна поділити на 3 групи – розробники, інвестори та власники токенів або монет. Іноді інтереси цих 3 груп різні і їм важко знайти спільну мову. Наприклад, інвестори можуть підтримувати проект фінансово, але вони можуть бути не дуже зацікавлені в серйозних змінах проекта (адже це потребує коштів), тому ця група осіб може дещо стримувати розвиток.

Decred якраз вирішує цю проблему – адже в його екосистемі усі учасники впливають на розвиток проекту.

Серед головних особливостей Decred можна виділити наступні [15]:

- Повна децентралізація
- Самофінансування
- Створені гармонійні умови для співжиття майнерів та інвесторів.

Для голосування у мережі використовується система голосування Politea [16], що діє поза межами блокчейну (рисунок 4).

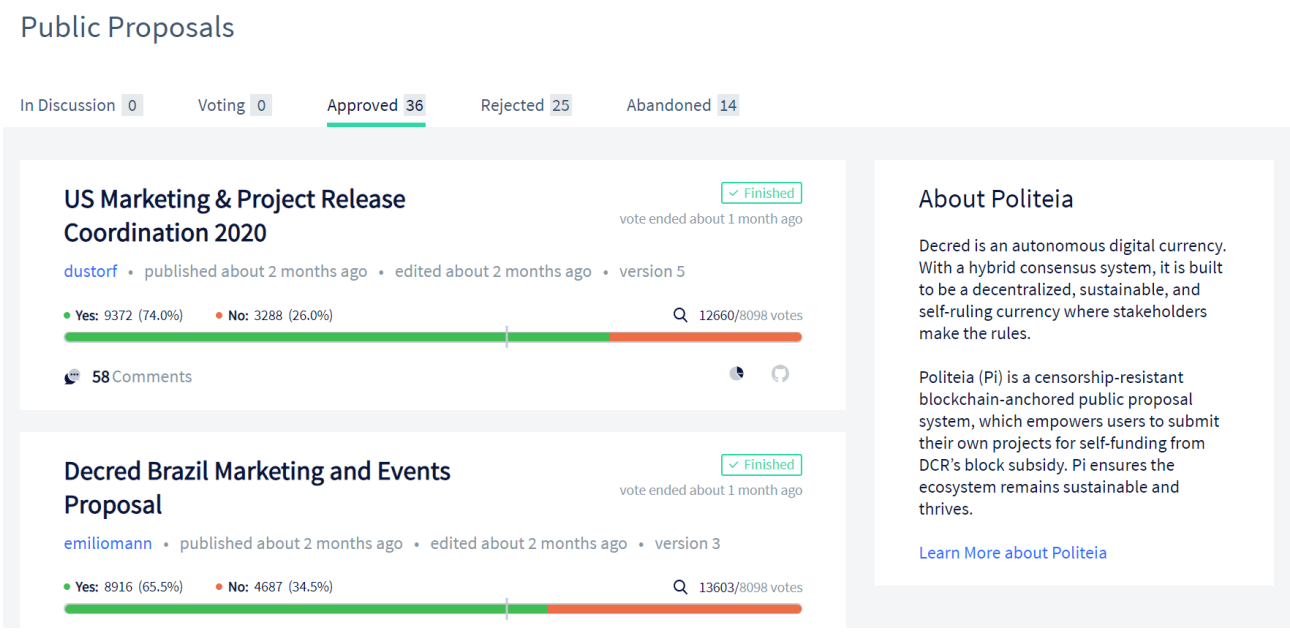


Рисунок 4. Головна сторінка порталу Politea

Для того щоб проголосувати у цій системі, необхідно отримати білет. Для того щоб його отримати, необхідно «заморозити» на своєму аккаунт суму рівну 5 DCR. Білети дають можливість не тільки голосувати, а й висувати свої пропозиції щодо покращення проекту.

Але за кожну внесену пропозицію необхідно заплатити 0.1 DCR – це зроблено для того, щоб уберегтися від спаму та зловмисників, що таким чином могли б зіпсувати чи заблокувати усю систему голосування.

Також у системі є такі поняття як «відкрита цензура» та «референдум».

Відкрита цензура – кожна пропозиція буде розглянута. Адміністрація має право не розглядати пропозицію якщо це спам – тоді аккаунт, що зробив цю пропозицію, заблокують за підтримки спільноти. Також пропозиція може не бути розглянута, якщо адміністрація має вагомі аргументи проти цієї пропозиції. В іншому разі пропозиція виноситься на загальне голосування.

Референдум – всезагальне голосування. Воно починається через 2016 блоків після внесення нової пропозиції та закінчується через 256 нових блоків після початку.

Результати рахуються, якщо у голосуванні прийняло участь не менше 20 відсотків учасників мережі. А прийнятою пропозиція буде рахуватися якщо не менше 75 відсотків учасників, що голосували висловилися за цю пропозицію.

Таким чином алгоритм консенсуса Decred захищений від атаки 51 відсотка. Адже зловмиснику необхідно буде заволодіти не тільки більшою частиною хешрейту мережі, а й взяти під контроль процес голосування. Враховуючи, що це коштує грошей, це стає просто невигідним.

Варто враховувати й інші особливості системи. Вона має досить високу пропускну здатність завдяки використанню протокола Lightning Network.

Lightning Network – «надбудова» над основною мережею, що дозволяє знизити навантаження на неї, а також збільшити пропускну здатність для запису транзакцій.

На рисунку 5 можна побачити як розподіляється криптовалюта, що видобувається у процесі майнингу.

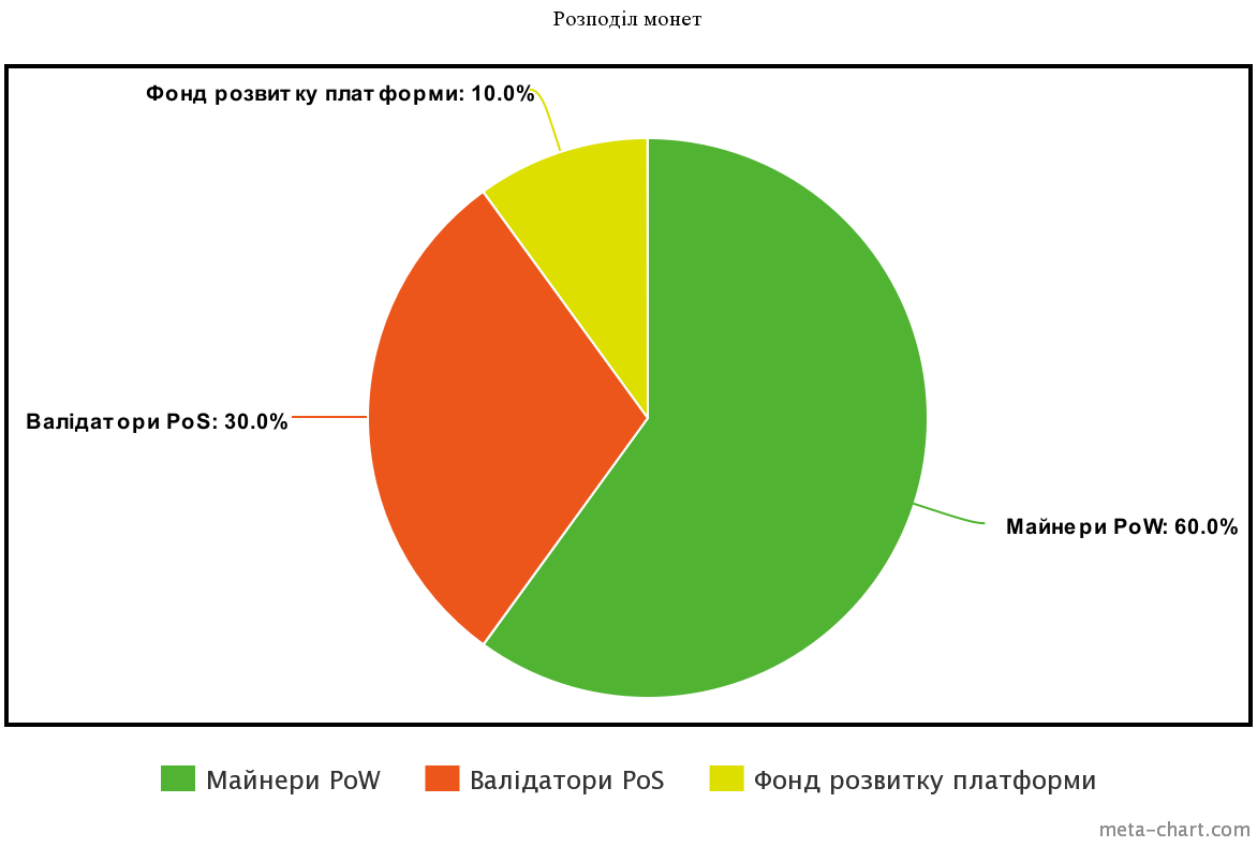


Рисунок 5. Розподіл здобутих монет у проекті Decred

У біткоіні винагорода за блок знижується у процесі халвінгу. Тут же це здійснюється не так радикально – на 1 відсоток через кожні 6144 знайдених блоки.

Алгоритм майнінгу криптовалюти Decred виглядає наступним чином [15]:

1) Як було сказано раніше, учасник мережі може купити білет. Цей білет розміщується у так званому «лотерейному пулі», звідки PoW-майнери можуть додати його до блоку. В одному блоці розміщується 20 білетів. Як і у Біткоіні, це займає час, але його можна зменшити просто збільшивши плату майнерам.
2) Після підписання блоку, білет стає «недозрілим». Його виключають з лотерейного пулу, доки не будуть створені 256 нових блоків.
3) Потім білет знову додається до пулу і чекає доки його оберуть для підтвердження блоку. Максимальний строк дії білета – 4 місяці.

До мінусів цього криптопроекту можна віднести досить маленьку вартість, а також недостатню популярність у криптосвіті.

3.2. Enecuum

Ще одним проектом, вартим уваги, є проект Enecuum, що заснований на протоколі Trinity.

Він вартий уваги завдяки тому, що у підтримці мережі Enecuum можуть приймати участь мобільні телефони та планшети. Адже, як вважають засновники проекту, ринок криптовалют розвивається дуже швидко і ним почали користуватися мільйони людей. Тому з’явилася пробелема масштабованості таких систем – постійна велика кількість людей призводить до того, що транзакціям необхідно більше часу для завершення або ж необхідно платити більше комісій.

Гібридний протокол консенсусу Trinity побудований на взаємодії відразу трьох методів консенсусу: Proof-of-Work, Proof-of-Stake і мобільного Proof-of-Activity. Його завдання полягає в забезпеченні роботи блокчейна з високою пропускною здатністю при одночасному збереженні децентралізації мережі [17].

Enecuum перший проект що звернув увагу на нереалізований потенціал мобільних телефонів. Адже прийнято думати, що мобільні пристрої занадто слабкі для того, аби приймати участь у майнінгу.

Також використання мобільних телефонів збільшить популяризацію блокчейну та криптовалют у світі, адже не у всіх є доступ до дорогого обладнання, аби стати одним із майнерів.

У розробленому проекті всі 3 види консенсусу працюють одночасно [17]. Схематичне зображення можна побачити на рисунку 6.

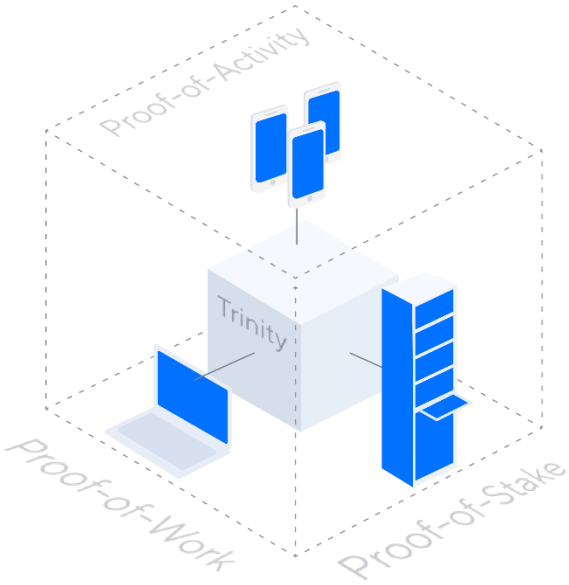


Рисунок 6. Схема роботи консенсусу Trinity [17]

Ноди Proof-of-Work створюють основу для блоків. Вони формують відсічення і інтервали часу, в яких працюють вузли на інших видах консенсусу.

Ноди Proof-of-Activity створюють мікроблоки з транзакціями. Таким чином вони знижують навантаження на PoS-ноди та здійснюють контроль за основними валідаторами. Через те що їх дуже багато, вони створюють необхідну ступінь децентралізованості мережі.

Ноди Proof-of-Stake займаються остаточним збором блоків та записом їх у блокчейн.

У протоколі Trinity вузли, що знаходяться не мобільних платформах, займаються обробкою основного потоку транзакцій, а саме валідацією проміжних мікроблоків. За цю роботу вони отримують нагороди в монетах ENQ.

На рисунку 7 можна побачити як розподіляється здобута криптовалюта.

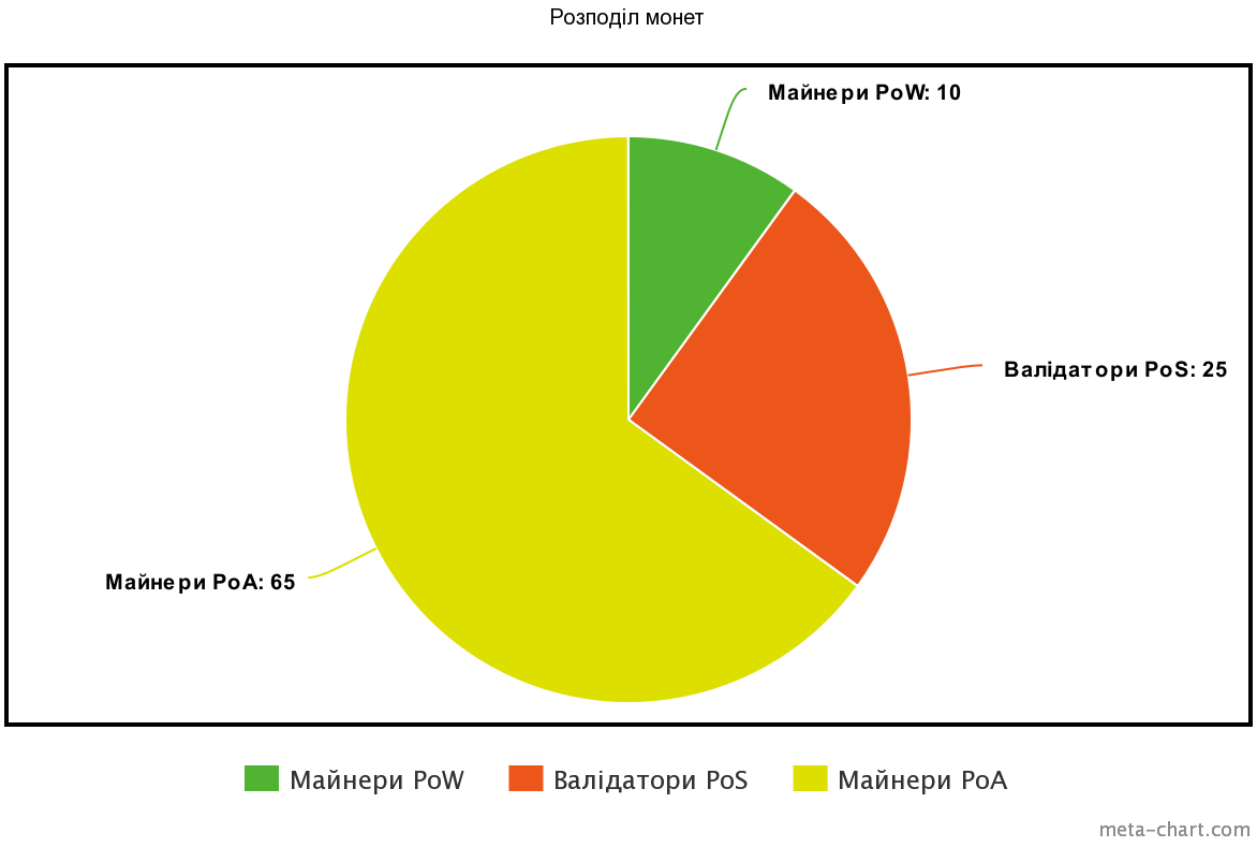


Рисунок 7. Розподіл здобутих монет у проекті Enecuum

На рисунку можна помітити, що найбільший відсоток отримують майнери PoA – тобто користувачі мобільних пристроїв.

В екосистемі Enecuum є додаток мобільного мастерноди (вузол PoA) для ОС Android [18]. Для того щоб розпочати майнінг, на рахунку необхідно мати 25 ENQ.

Елемент консенсусу PoS в Trinity має назву Smart Staking і найближчим часом почне працювати в тестовій мережі. Валідаторами в мережі стають 100 вузлів з найбільшими балансами ENQ [17].

Система Enecuum заснована на смартконтрактах. Учасники, що делегують свої монети отримують гарантовану фіксовану винагороду за передачу своїх монет

PoS-валідаторам. Тобто для валідаторів необхідність виплачувати «проценти за користування» змушує краще виконувати свою роботу, а для людей, що віддають монети у позику це виглядає як чудова гарантована інвестиція.

Отже, проект Enecuum хоче дати доступ до майнінгу усім охочим. Їх протокол у майбутньому може вирішити проблеми масштабованості та децентралізації, від яких страждають класичні алгоритми консенсусу.

4. Розробка EIP

4.1. Огляд Ethereum та стандарту ERC-20

Ethereum – це децентралізована обчислювальна платформа. У неї немає власника або будь-якого конкретного пристрою на якому вона працює. Також Ethereum – назва протоколу, а ETH (ефір) – криптовалюта [19].

Критовалюти дають можливість обмінюватися користувачам цифровими грошима. Ethereum теж це вміє, але на відміну від інших криптовалют, ця платформа також надає можливість створити власну програму на її основі, а також взаємодіяти з іншими програмами.

Створивши програмний код на основі Ethereum та додавши його до бази даних ефіріуму, кожен бажаючий зможе переглянути як він працює, а також які дані зберігає. Такий програмний код називають смарт-контрактами (від англ. smart contract). Смарт-контракти пишуть спеціальною мовою – Solidity.

Смарт-контракти можна запустити за допомогою транзакцій – або зі сторони користувача, або зі сторони іншого смарт-контракту. За допомогою віртуальної машини ефіріума (від англ. Ethereum Virtual Machine, EVM) код смарт-контрактів перетворюється у інструкції, що зчитуються комп’ютером. За транзакцію, що щось додає до блокчейну необхідно сплатити плату, що залежить від поточної ціни газу, а також кількості даних, що необхідно записати.

У певній мірі Ethereum – це стейт машина (state machine). У будь-який момент часу у нас є інформація про кількість користувачів, їх баланси, які є смарт-контракти та які дані вони зберігають. Будь-яка активність учасника мережі буде змінювати стан усієї системи і усі вузли повинні будуть оновити свої дані про стан мережі. Для оновлення стану використовується майнінг.

Смартконтракти дозволяють користувачам створювати власні активи – токени. Їх можна передавати та зберігати, так само як і ефір. Правила, за якими токени існують у мережі задають смарт-контракти. Кожен користувач може створити власний токен, який може підпорядковуватися певним правилам або ж створити новий стандарт.

Такі стандарти мають назву EIPs (від англ. Ethereum Improvement Proposals).

Вони описують стандарти для платформи Ethereum, включаючи основні специфікації протоколу, клієнтські API та стандарти контракту.

Один з найпопулярніших EIPів - ERC-20, а його токени - ERC-20 токени. ERC-20 має багато переваг, серед яких можна виділити можливість гаманцям надавати баланси для сотень різних токенів і створювати засоби для обміну, щоб надсилати токени не надаючи нічого, крім адреси токена. На сьогоднішній день, більшість токенів створені за стандартом ERC-20.

Загалом, ERC-20 – це просто інтерфейс, який токен повинен реалізувати.

У токена повинно бути:

- Ім’я – повна назва токена (можна з пробілами);
- Символ – скорочене позначення, зазвичай це 3-4 символи;
- Кількість знаків – показує наскільки токен «ділиться» (кількість знаків після коми). Причина існування десяткових знаків полягає в тому, що Ethereum не працює з десятковими числами, представляючи всі числові значення як цілі числа.

Варто зауважити, що ім’я, символ та кількість знаків не гарантують унікальність. Унікальність гарантує лише адрес токена (смарт-контракту).

Токен ERC-20 повинен реалізовувати такі функції:

```
/// Загальна кількість токенів
/// supply - кількість токенів
function totalSupply()
    public
    virtual
    view
    returns (uint256 supply)
{}

/// Отримання балансу користувача
/// _owner - адреса користувача
/// balance - баланс
function balanceOf(address _owner)
    public
    virtual
    view
    returns (uint256 balance)
{}

/// Пересилання токенів
```

```
    /// _to - адреса отримувача
    /// _value - кількість токенів для надсилання
    /// success - чи операція завершилася успіхом
    function transfer(address _to, uint256 _value)
        public
        virtual
        returns (bool success)
    {}

    /// Пересилання токенів від from до to, за умови, що from дозволив це
пересилання
    /// _from - адреса надсилача
    /// _to - адреса отримувача
    /// _value - кількість токенів для надсилання
    /// success - чи операція завершилася успіхом
    function transferFrom(address _from, address _to, uint256 _value)
        public
        virtual
        returns (bool success)
    {}

    /// Надсилач дозволяє spender витратити не більше value токенів
    /// _spender - адреса аккаунту, що може надсилати токени
    /// _value - кількість токенів для надсилання
    /// success - чи операція завершилася успіхом
    function approve(address _spender, uint256 _value)
        public
        virtual
        returns (bool success)
    {}

    /// Показує скільки токенів від імені owner може надіслати spender
    /// _owner - адреса аккаунту, на якому знаходяться токени
    /// _spender - адреса аккаунту, що може пересилати токени
    /// remaining - кількість токенів, що ще можна надіслати
    function allowance(address _owner, address _spender)
        public
        virtual
        view
        returns (uint256 remaining)
    {}
```

Також є 2 події (events), що виконуються коли контракт виконує відповідну дію:

```
/// Показує деталі операції надсилання токенів від однієї адреси до іншої
    event Transfer(address indexed _from, address indexed _to, uint256 _value);

/// Показує деталі операції утвердження від однієї адреси до іншої на задану кількість
токенів
    event Approval(
```

```
        address indexed _owner,
        address indexed _spender,
        uint256 _value
    );
```

Випуск токенів сворює подію `Transfer`, де адреса _from – нульова.

4.2. Ідея та реалізація нового EIP

Створення токенів надає величезні можливості для розширення існуючих можливостей блокчейну.

В основі Ethereum лежить PoW консенсус. А за допомогою нового EIP є можливість додати елементи PoS консенсусу. Таким чином ми отримаємо гібридну систему.

PoS (Proof of Stake) базується на стейкінгу. Стейкінг (від англ. stake – «ставка», «частина прибутку») - отримання пасивного доходу від криптовалюти на PoS-алгоритмі та його варіації.

Ідея нового стандарту буде базуватися на тому, що у нас будуть зберігатися опитування для токенів, що реалізують цей стандарт. У кожному опитування є варіанти відповіді, за які можна проголосувати. Голос – певна кількість токенів, яку користувач стейкає на користь того чи іншого варіанту.

Логіка голосування та дані щодо опитувань та відповідей зберігаються у смартконтракті BusinessVoter.

У таблиці 1 можна побачити як у смартконтракті зберігаються відповіді – сутність Answer (тут і далі – типи вказані у мові Solidity, якою реалізовано стандарт).

Поле	Тип даних
id	uint256
answer	string
voters	mapping(address => uint256)
voterCount	uint256

totalStaked	uint256

Таблиця 1. Поля, що зберігає у собі сутність Answer

У Solidity кожна транзакція має змогу отримати інформацію про її надсилача – тому ми завжди знаємо адресу користувача.
Кожна відповідь належить до певного опитування. У таблиці 2 можна побачити як зберігається сутність опитування - Poll.

Поле	Тип даних
id	uint256
question	string
answers	mapping(uint256 => Answer)
answerCount	uint256
created	uint256
endTime	uint256
stakeInterestNumerator	uint256
stakeInterestDenominator	uint256
unstakedVoters	mapping(address => bool)

Таблиця 2. Поля, що зберігає у собі сутність Poll

У Solidity є певні обмеження – наприклад, тут є тільки цілі числа. Тому для зберігання відсотків, що нараховуються після отримання стейку назад необхідно 2 поля – stakeInterestNumerator та stakeInterestDenominator.
Головна ідея нового EIP – надати можливість створювати токени, що за замовчуванням будуть підтримувати реалізацію стейкінгу без необхідності викликати функцію allowance.
Для цього реалізовано новий стандарт, що реалізує всі функції стандарту ERC-20, а також додає дві нові – стейк та анстейк. Сигнатура методів виглядає так:

```
/// Стейкінг коштів
/// _erc20TokenAddress - ERC-20 адреса токена
/// _value – кількість токенів, що треба застейкати
/// _pollId – ідентифікатор опитування
/// _answerId – ідентифікатор відповіді
/// success – чи операція завершилася успіхом
function stake(
    address _erc20TokenAddress,
    uint256 _value,
    uint256 _pollId,
    uint256 _answerId
) public virtual payable returns (bool success) {}

/// Отримання коштів
/// _erc20TokenAddress - ERC-20 адреса токена
/// _pollId – ідентифікатор опитування
/// success – чи операція завершилася успіхом
function unstake(address _erc20TokenAddress, uint256 _pollId)
    public
    virtual
    returns (bool success)
{}
```

Новостворені методи викликають смартконтракт BusinessVoter. BusinessVoter має власні методи для стейкінгу та анстейкінгу, тому він вносить необхідні зміни у свою базу даних, та повертає результат – чи була операція успішною.

5. Опис програмного продукту

5.1. Практичне значення

Рішення у компаніях приймаються збором аукціонерів. Чим більшою кількістю акцій володіє аукціонер - тим більший він має голос. Перевага ERC-20 токенів - вони можуть легко передаватися між аукціонерами. Даний проект допоможе автоматизувати процес прийняття бізнес рішень, за допомогою того, що акції будуть виражатися у токенах. Пропозиції та варіанти голосування надаватимуться адміністраторами - користувачі криптогаманця зможуть лише переглядати наявні пропозиції.

Криптогаманець дозволятиме користувачу ідентифікувати себе за допомогою приватного ключа для Ethereum та адреси токена, що реалізує новостворений EIP. Також у зручному для користувача форматі будуть реалізовані основні функції, що необхідні аукціонеру:

- перегляд балансу;
- список опитувань;
- показ кількості застейканих токенів;
- можливість проголосувати за відповідь;
- можливість забрати гроші після закінчення опитування;
- можливість пересилати токени іншим користувачам.

Оскільки безпека криптоактивів є однією з найважливіших характеристик для такого роду програмного забезпечення, то безпека розробленого застосунку також буде враховуватися. Тому криптогаманець будет некастодіальним.

Некастодіальний криптогаманець – такий, що не передає приватні ключи або сід-фрази користувача третім застосункам та/або серверу. Уся приватна інформація користувача зберігається на пристрої цього ж користувача.

5.2. Готова система

Робота складається з 3 частин - декількох пов’язаних між собою смартконтрактів, бекенду та фронтенду.

Мережа смартконтрактів - головна частина роботи. Складається з 3 смартконтрактів:

- BusinessVoter [21] – реалізує функціонал голосувань та зберігає усі основні дані щодо стану мережі;

- Eip [22] – реалізує усі можливості ERC-20 токенів, а також додає нову функціональність стейку та анстейку;

- BRK [23] – токен, що був створений для показу функціональності системи. Деталі токену можна переглянути у таблиці 3.

Назва поля	Значення
Повна назва	Beyrak Token
Символ	BRK
Кількість знаків (ділимість)	18
Випущена кількість	10000
Адреса	0x39A29c6B886ceEbFfdD663163a3C11FF4DBd0A9F

Таблиця 3. Дані BRK токена

Усі методи смартконтракту викликаються з серверної частини. Сервер написаний мовою Go.

Сервер знаходиться за покликанням http://business-voter.herokuapp.com/ . Також доступною є серверна документація [24].

Бекенд частина реалізує усі необхідні функції для того, або клієнт міг зв’язкутися зі смартконтрактами:

1) Get /polls

Отримання усіх доступних опитувань для даного користувача.

Необхідна авторизація.

2) Get /polls/id

   Отримання інформації про конкретне опитування.

   Необхідна авторизація.

3) Get /user

   Отримання усієї інформації про користувача – його балансів, опитувань та відповідей.

   Необхідна авторизація.

4) Post /user/login

   Генерує валідний токен, що у майбутньому дозволить ідектифікувати користувача.

5) Get /user/eth/gas_price

   Отримання поточної ціни газу (вона необхідна для формування транзакції на стороні клієнта).

   Необхідна авторизація.

6) Get /user/eth/nonce

   Отримання nonce для даного користувача (вона необхідна для формування транзакції на стороні клієнта).

   Необхідна авторизація.

7) Post /user/eth/transaction

   Надсилання транзакції у блокчейн.

   Необхідна авторизація.

Важливою частиною, що зв’язує клієнт та сервер, є токен, що генерується сервером. Цей токен містить у собі інформацію про користувача та генерується з адреси користувача, підпису та адреси контракту за допомогою бібліотеки Web3j (приклад взято з клієнтської частини системи, написаного мовою Kotlin):

```
// Генерація приватного ключа з введеної користувачем поля
val privateKey: ByteArray = Hex.decode("PRIVATE_KEY_HERE")
val credentials: Credentials = Credentials.create(ECKeyPair.create(privateKey))

// Генерація адреси
```

```
val address: String = credentials.address

// Генерація хешу підпису
val signatureHash: ByteArray = Hash.sha3(hexStringToByteArray(address))

// Підпис за допомогою приватного ключа
val sign: Sign.SignatureData = Sign.signMessage(signatureHash, credentials.ecKeyPair,
false)
val signature: String = Numeric.toHexString(toByteArray(sign))
```

Тобто, на сервер не передається приватний ключ користувача. Отриманий на етапі реєстрації токен зберігається на клієнті та у майбутньому допомагає однозначно ідентифікувати користувача та дозволяє йому здійснювати виклики до методів серверу.

Клієнтська частина представляє собою застосунок під операційну систему Android.

Коли користувач вперше заходить до додатку, він бачить екран входу, де є дві опції – ввійти за вже існуючим приватним ключем, або ж створити новий аккаунт (рисунок 8).

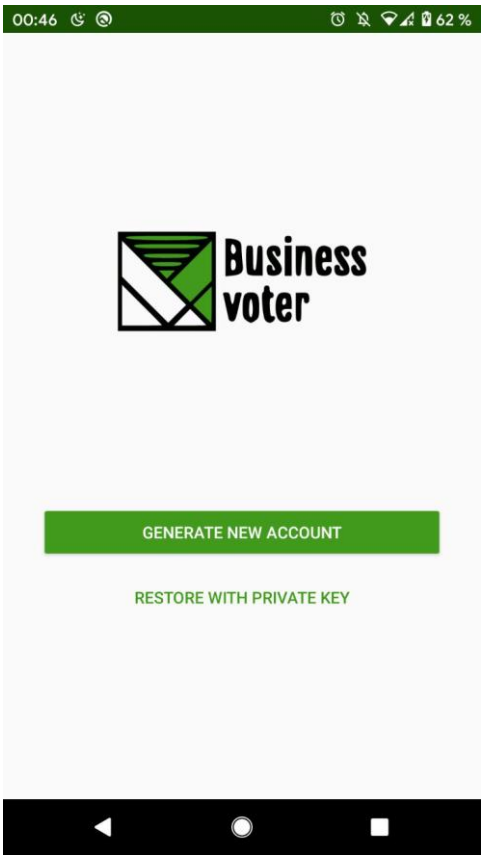


Рисунок 8. Екран входу

Якщо користувач уже має приватний ключ, йому достатнього його лише ввести (рисунок 9). При натисненні кнопки відбувається валідація введеної стрічки.

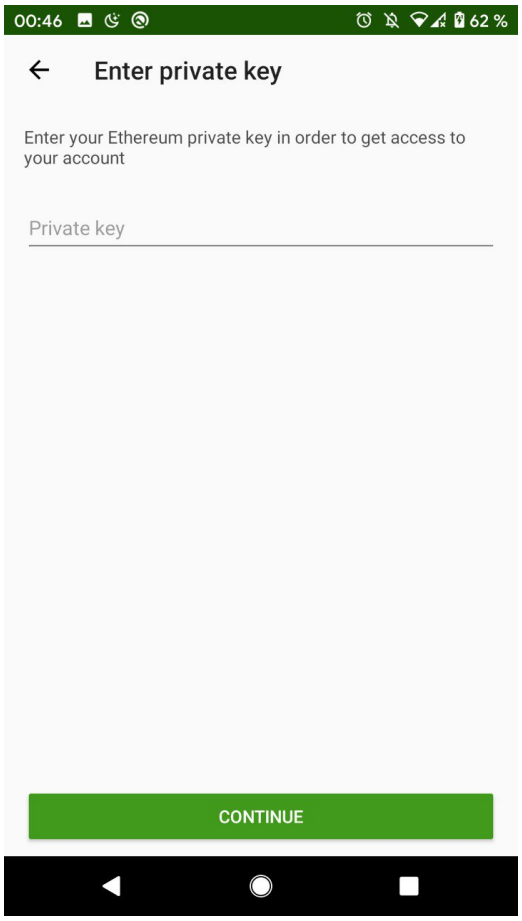


Рисунок 9. Екран введення вже існуючого приватного ключа

Якщо ж у користувача немає приватного ключа, у нього є можливість його згенерувати та одразу зберегти (рисунок 10).

Рисунок 10. Екран генерації нового приватного ключа

Після цього користувач повинен ввести адресу токена (рисунок 11).

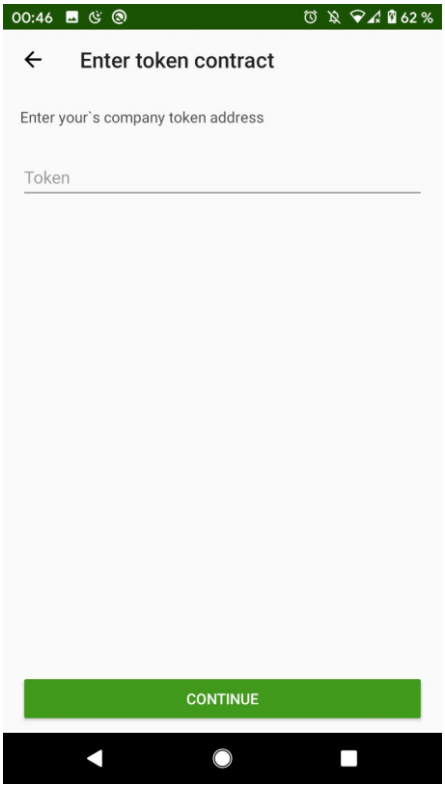


Рисунок 11. Екран вводу адреси токена

На завершення реєстрації необхідно ввести та підтвердити пароль (рисунок 12). У майбутньому цей пароль слугуватиме підтвердженням для здійснення транзакцій.

Рисунок 11. Екран вводу та підтвердження пароля

Після завершення реєстрації, користувач потрапляє на головний екран, де він може переглянути свій баланс токенів, кількість застейканих токенів, а також список опитувань у яких він приймав участь (рисунок 12).

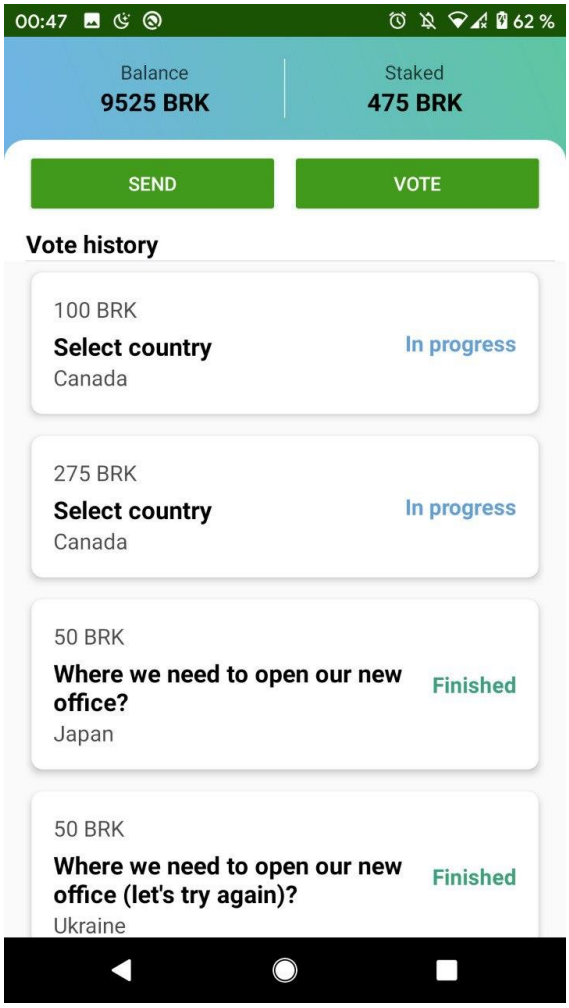
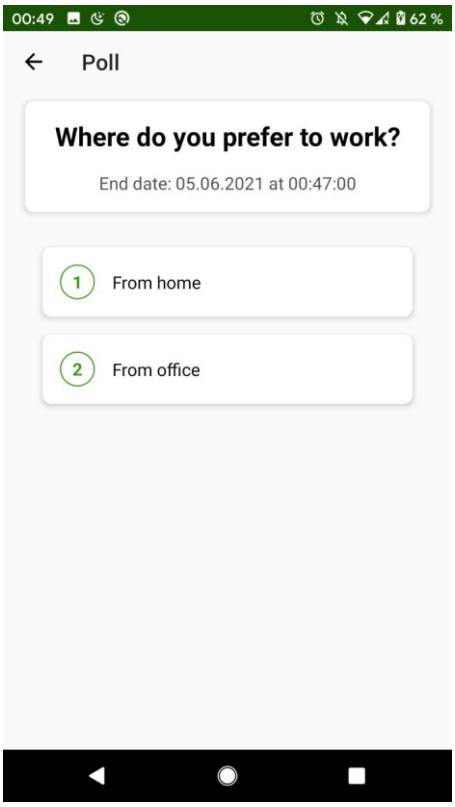
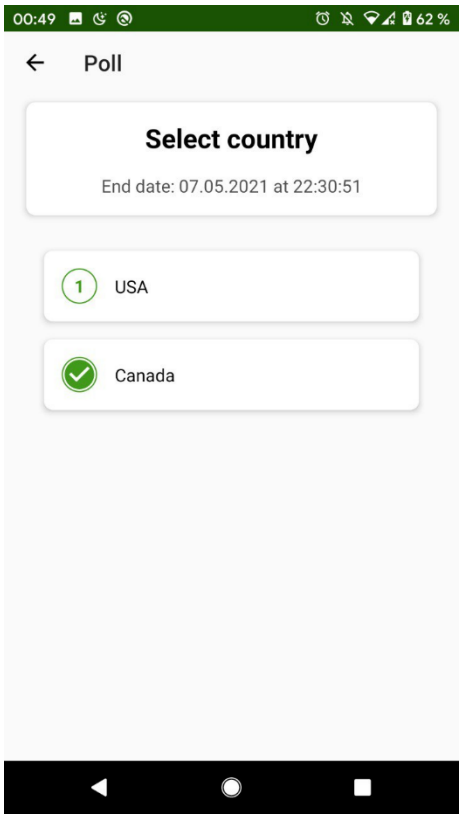


Рисунок 12. Головний екран

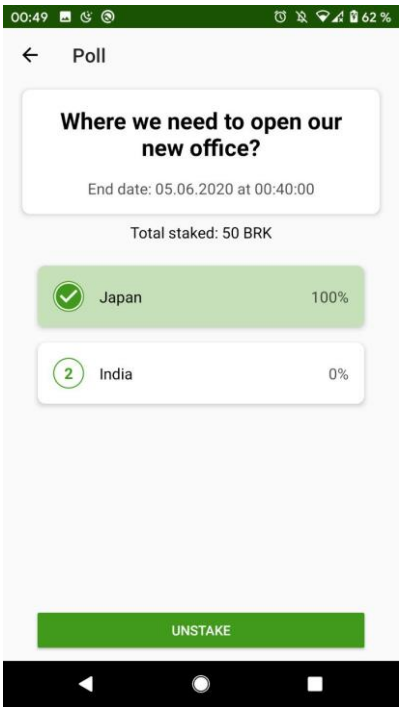
З головного екрану користувач може перейти до деталей певного опитування (рисунок 13). У ньому можна переглянути дату закінчення опитування, питання, обрану відповідь (якщо така є), а також можна проголосувати за відповідь (якщо опитування активне) та анстейкнути гроші (якщо користувач уже голосував та голосування завершилося).



а



б



в

Рисунок 13. Екран деталей опитування. а) Коли користувач ще не голосував. б) Коли користувач проголосував, але опитування ще не завершено. в) Коли опитування завершилося

Якщо користувач хоче проголосувати, він обирає певний варіант та у нього з’являється екран, де він вводить суму, яку хоче застейкати (рисунок 14). В екрані є валідація що не можна застейкати більше ніж баланс, що у нього вже є.

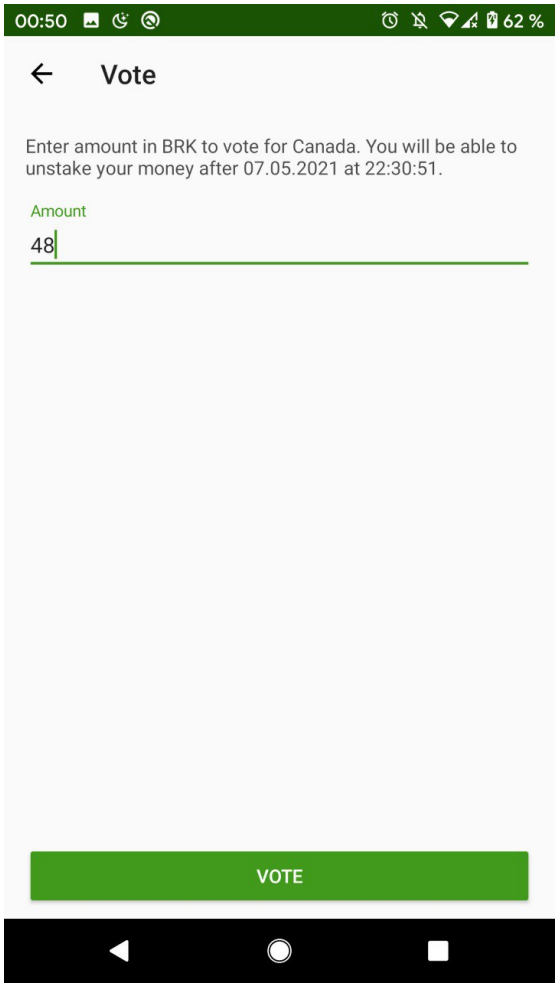


Рисунок 14. Екран голосування

Для здійснення будь-якої транзакції (стейк, анстейк, переказ коштів), з’являється екран підтвердження операції (рисунок 15).

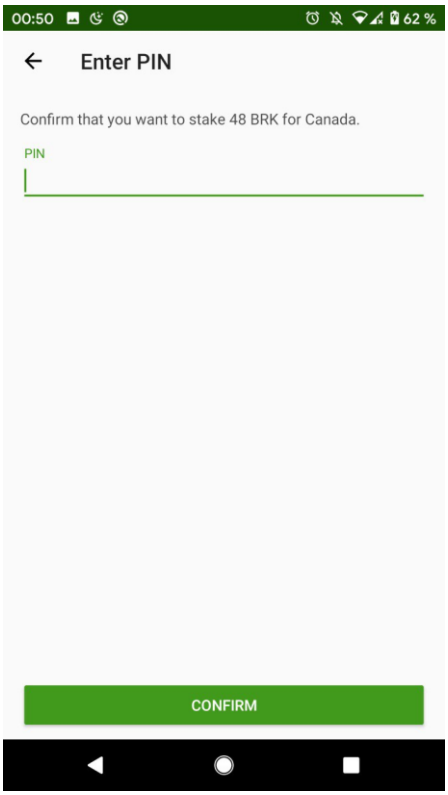


Рисунок 15. Екран підтвердження транзації

Після успішної транзакції, користувач потрапляє в екран успіху, де за допомогою кнопки може перейти до блок-експлореру та переконатися, що транзакція записана до блокчейну (рисунок 16).

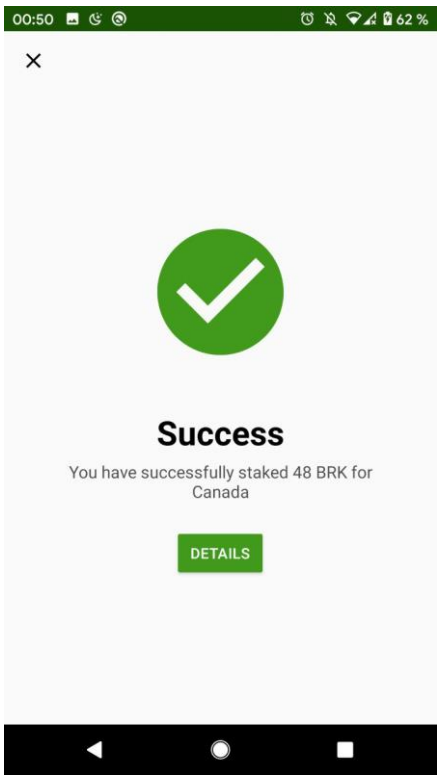


Рисунок 16. Екран успіху транзакції

Також, з головного екрану є можливість потрапити до сторінки, де можна переглянути усі доступні опитування (рисунок 17).

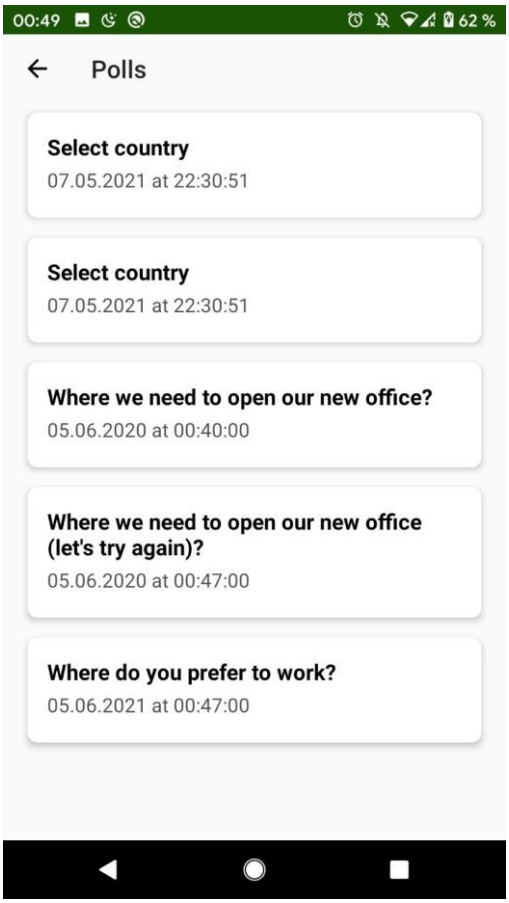


Рисунок 17. Екран усіх опитувань

Як і інші криптогаманці, цей програмний продукт може пересилати кошти з одного рахунку на інший. Для цього необхідно лише вказати адресу отримувача та необхідну суму (рисунок 18). В екрані відбувається валідація адреси та введеної суми.

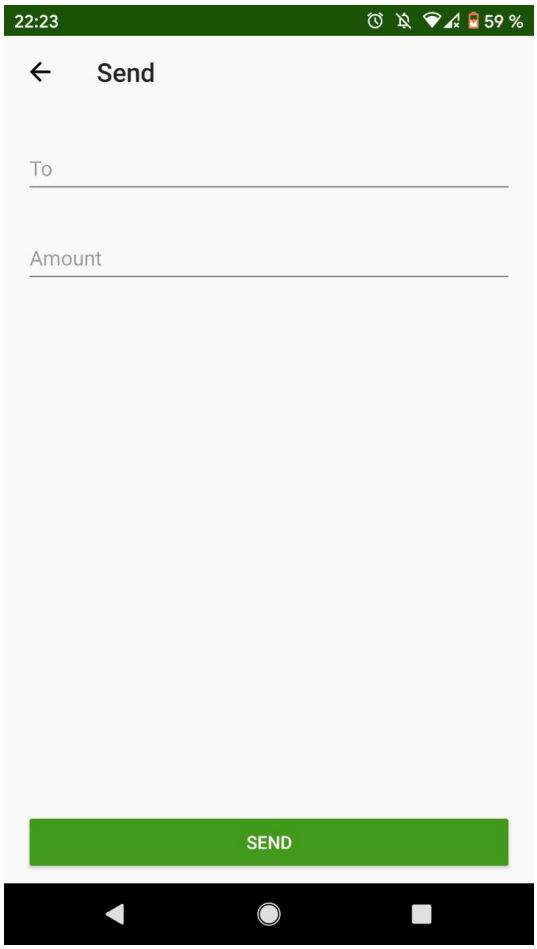


Рисунок 18. Екран надсилання коштів

Отже, програмний продукт повністю задовольняє усі базові потреби користувача.

Висновок

Блокчейн – актуальна на сьогодні технологія, яка активно входить у життя людей. На сьогоднішній день, її використовують не лише у якості пересилання електронних грошей, але й як потужні сховища даних.

У роботі було розглянуто вже існуючі системи консенсусів, описано їх переваги та недоліки. Особливу увагу було приділено гібридним системам консенсусу, що вже є реалізованими та успішно займають своє місце серед інших проектів.

На основі аналізованої інформації, було запропоновано та розроблено новий EIP на базі Ethereum. Новий стандарт додає функціонал Proof-of-Stake консенсусу, що допомагає реалізувати гібридну систему PoW/PoS. Новий EIP розширює найпопулярніший стандарт ERC-20, тому усі токени нового стандарту сумісні з ним.

В якості прикладу використання такої системи було розроблено програмний продукт, що допомагає приймати рішення зборам аукціонерів. Акції компанії виражаються у вигляді токенів нового стандарту. Такий проект допоможе автоматизувати процес прийняття бізнес рішень у компаніях.

Розроблена система складається з 3 частин - декількох пов’язаних між собою смартконтрактів написаних на Solidity, серверу на Go та клієнту під операційну систему Android, написаного на Kotlin. На сервері та клієнті використовувалася бібліотека Web3J для генерації та валідації відповідних даних (приватних ключів, підписів) для Ethereum.

Отже, блокчейн – це потужна концепція, що показує свої переваги не лише в сфері криптовалют. Є багато систем консенсусів, кожна з яких має свої переваги та недоліки, тому обирати ту, що більш пасує до певного проекту, необхідно виходити з того, які цілі ставить проект. Наприклад, нещодавно в українському суспільстві виникла ідея щодо того, аби використовувати АЕС для майнінгу криптовалюти – враховуючи відносну дешеву вартість електроенергії, цей варінт може мати право на життя [25].

Хорошим компромісом є використання гібридних систем консенсусу, що можуть поєднувати у собі переваги двох або більше вже відомих консенсусів та намагатися компенсувати недоліки один одного, але такий варіант все ж не можна вважати ідеальним.

Перелік використаних джерел

1. Что такое Блокчейн (Blockchain)? Технология распределенного реестра простыми словами [Електронний ресурс]. – URL : https://mining-cryptocurrency.ru/blockchain/
2. AN INTRODUCTION TO BLOCKCHAIN [Електронний ресурс]. – URL : https://www.mindtory.com/an-introduction-to-blockchain/
3. CoinMarketCap [Електронний ресурс]. – URL : https://coinmarketcap.com/
4. Report: Japan is working on its own digital currency in retaliation to China’s [Електронний ресурс]. – URL : https://thenextweb.com/hardfork/2020/01/24/japan-working-own-digital-currency-compete-facebooks-libra-china-yuan/
5. Inside China's mission to create an all-powerful cryptocurrency [Електронний ресурс]. – URL : https://www.wired.co.uk/article/china-digital-currency-crypto
6. USA Is Looking Closely To Launching Its Own Cryptocurrency, According To Fed Governor Lael Brainard [Електронний ресурс]. – URL : https://cryptopotato.com/usa-is-looking-closely-to-launch-its-own-cryptocurrency-according-to-fed-governor-lael-brainard/
7. DOD Digital Modernization Strategy [Електронний ресурс]. – URL : https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
8. Electronic Voting With Blockchain: An Experience From Naples, Italy [Електронний ресурс]. – URL : https://cointelegraph.com/news/electronic-voting-with-blockchain-an-experience-from-naples-italy
9. Что такое Алгоритм Консенсуса в Blockchain? [Електронний ресурс]. – URL : https://www.binance.vision/ru/playlists/how-blockchains-achieve-consensus/what-is-a-blockchain-consensus-algorithm
10. Что такое Proof-of-Work и Proof-of-Stake? [Електронний ресурс]. – URL : https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/

11. Proofs of Work and Bread Pudding Protocols [Електронний ресурс]. – URL : http://www.hashcash.org/papers/bread-pudding.pdf
12. Delegated Proof of Stake Explained [Електронний ресурс]. – URL : https://www.binance.vision/ru/blockchain/delegated-proof-of-stake-explained
13. Proof of Authority Explained [Електронний ресурс]. – URL : https://www.binance.vision/ru/blockchain/proof-of-authority-explained
14. Proof-of-importance (PoI) – алгоритм доказательства важности [Електронний ресурс]. – URL : https://profit-life.net/proof-of-importance-poi/
15. Что Такое Критовалюта Decred [Електронний ресурс]. – URL : https://altcoinlog.com/what-is-decred/
16. Politea [Електронний ресурс]. – URL : https://proposals.decred.org/
17. Enecuum и протокол Trinity в развитии индустрии блокчейна [Електронний ресурс]. – URL : https://bits.media/pr/enecuum-i-protokol-trinity-v-razvitii-industrii-blokcheyna/
18. Enecuum app [Електронний ресурс]. – URL : https://app.enecuum.com/
19. What is Ethereum [Електронний ресурс]. – URL : https://www.binance.vision/ru/blockchain/what-is-ethereum
20. Ethereum Improvement Proposals [Електронний ресурс]. – URL : https://github.com/ethereum/EIPs
21. BusinessVoter on Etherscan [Електронний ресурс]. – URL : https://ropsten.etherscan.io/address/0x4c8dae8e3a5c87baab169a9b1f2d98c293ad8c93
22. EIP on Etherscan [Електронний ресурс]. – URL : https://ropsten.etherscan.io/address/0x430cb82724af09fa88a66d49bcfa3e1ac4f96b54
23. Beyrak Token on Etherscan [Електронний ресурс]. – URL : https://ropsten.etherscan.io/address/0x39a29c6b886ceebffdd663163a3c11ff4dbd0a9f

24. Серверна документація [Електронний ресурс]. – URL : http://business-voter.herokuapp.com/api/v1/docs/#/
25. Невмержицький Є.І. Майнінг на атомних станціях — перспективи чи нова афера? [Електронний ресурс]. – URL : http://ukrpres.info/2020/05/07/mayninh-na-atomnykh-stantsiyakh-perspektyvy-chy-nova-afera/?fbclid=IwAR3jGj5z5cWJK-Fs26mBeOt0NML3nQqRqQOj1Nz4IV1BCM4a_vBt-xt8-ns