МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Кваліфікаційна робота бакалавра

ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СМАРТ-КОНТРАКТУ ДЛЯ СТВОРЕННЯ КРИПТОВАЛЮТНОГО ТОКЕНУ В МЕРЕЖІ BINANCE SMART CHAIN

Здобувач освіти гр. ІН–82 Владислав СЕРГЄЄВ

Науковий керівник

кандидат фізико-математичних наук,
асистент кафедри комп'ютерних наук Ольга ШУТИЛЄВА

Завідувач кафедри
доктор технічних наук, професор Анатолій ДОВБИШ

СУМИ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Затверджую_____
Зав. кафедрою Довбиш А.С.
"_____" _____2022 р.

ЗАВДАННЯ

до кваліфікаційної роботи

Здобувача вищої освіти четвертого курсу, групи ІН-82 спеціальності «122 – Комп'ютерні науки» денної форми навчання Сергєєва Владислава Сергійовича.

Тема: «ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СМАРТ-КОНТРАКТУ ДЛЯ СТВОРЕННЯ КРИПТОВАЛЮТНОГО ТОКЕНУ В МЕРЕЖІ BINANCE SMART CHAIN»

Затверджена наказом по СумДУ
№_____ від _____2022 р.

Зміст пояснювальної записки: 1) Інформаційний огляд. Огляд проблемної області. Актуальність створення крипто-токену. Постановка задачі. 2) Опис основних понять і положень. Вибір програмної реалізації смарт-контракту. 3) Програмна реалізація. Практичне застосування.

Дата видачі завдання "_____"_____2022 р.

Керівник роботи _____ Ольга ШУТИЛЄВА

Завдання прийняв до виконання _____ Владислав СЕРГЄЄВ

РЕФЕРАТ

Записка: 52 стор., 25 рис., 1 табл., 1 додаток, 39 джерел.

Об’єкт дослідження – смарт-контракти в мережі Binance Smart Chain.

Мета роботи – розробка смарт-контракту токена, його розгортання та тестування в мережі BSC.

Методи дослідження – методи збору та аналізу даних.

Результати – розгорнутий смарт-контракт токену GRT на BSC. Створені функції необхідні для коректної роботи токену та підтримки токеноміки. Смарт-контракт розроблений за допомогою мови програмування Solidity на Remix Solidity IDE, версія компілятора 0.8.4.

КРИПТОВАЛЮТА, БЛОКЧЕЙН, СМАРТ-КОНТРАКТ,
ТОКЕН, SOLIDITY.

ЗМІСТ

ВСТУП

Актуальність роботи визначається тим що, у процесі глобалізації, економічного та технічного розвитку на початку XXI століття починає свій розвиток віртуальна економіка, основним завдання якої є обіг цифрової валюти. Спочатку цифрова валюта була представлена як електронні платежі між окремими індивідумами та фінансовими інституціями, але починаючи з 2008 року все змінилося. Адже саме 31 жовтня 2008 року користувач з ніком, нині відомим по всьому світі, Сатоші Накамото, розмістив файли, які описували принципи роботи нової децентралізованої валюти – «Bitcoin». Це спричинило революцію в сфері фінансів не меншу, аніж революція в сфері комунікацій після винайдення інтернету.

Саму цифрову валюту можна розділити на:

- Електронні гроші – це віртуальне відображення реальних грошей, які відносяться до реальної економіки і обертаються серед банківських рахунків.
- Криптовалюта – це віртуальна валюта, яка обертається в цифровому світі.

Високорозвинені країни з сильною економікою прагнуть врегулювати обіг криптовалюти аби зменшити ризики її використання (Японія, США, Канада, Китай і т.д). Держави ж зі слабкою економікою всяко уникають від впровадження таких платіжних засобів (Болівія, Еквадор, В’єтнам і т.д). Це відбувається тому що криптовалюта має свої недоліки які збільшують можливості відмивання грошей та спекулятивність ринку. Це все лише спонукає розвиток нелегальної (тіньової) економіки.

Основними позитивними аспекти є те, що вартість криптовалюти захищена від інфляції, а значна волантильність, що дає широкі можливості для заробітку інвесторів.

Метою кваліфікаційної роботи є розробка смарт-контракту токена, його розгортання та тестування в мережі BSC.

1. АНАЛІЗ ЗАГАЛЬНОГО ПОЛОЖЕННЯ КРИПТОСФЕРИ, ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ВИРІШЕННЯ ПРОБЛЕМИ

1.1 Актуальність тематики роботи

Завдяки активному розвитку блокчейн-технологій кількість інформації, щодо криптовалют, а також кількість обізнаних користувачів у даній сфері зросла значною мірою за останні роки. На сьогоднішній день Україна посідає перше місце за рейтингом країн, відносно значення частки населення, що володіє криптовалютою. 12,7% населення України є власниками тієї чи іншої криптовалюти – це близько 5,6 млн осіб. Ігнорування даного факту є просто неможливим, тому влада узаконила дії з криптовалютою.

16 березня 2022 року президент України Володимир Зеленський підписав закон України «Про віртуальні активи», який Верховна Рада України ухвалила 17 лютого. Це значима подія для створення легального крипторинку і розвитку цієї галузі в Україні. Далі цитата з офіційного сайту Міністерства та Комітету цифрової трансформації України [1]:

«**Підписаний Закон:**

- визначає правовий статус, класифікацію та права власності віртуальних активів;
- визначає регуляторів ринку – Національний банк України та Національну комісію з цінних паперів та фондового ринку;
- створює умови для подальшого формування правового поля на ринку віртуальних активів;
- визначає перелік постачальників послуг віртуальних активів та умови їх реєстрації;
- передбачає впровадження заходів фінансового моніторингу у сфері віртуальних активів».

До того ж з 24.02.2022 р. було отримано більш ніж $100 млн. крипто-донатів на підтримку оборонних зусиль нашої держави.

Таблиця 1.1 – Компанії в Україні, які приймають розрахунки у Bitcoin [2]:

Сфера	Компанія	Вид діяльності
Торгівля	Tix24	Інтернет-магазин товарів
	Digit	Інтернет-магазин техніки
	Rechi.ua	Інтернет-магазин одягу
	BeAngle	Інтернет-магазин нижньої білизни
	Asic Trade	Інтернет-магазин обладнання для майнингу
	SendFlowers	Інтернет-магазин квітів
	12v.ua	Інтернет-магазин акумуляторів
IT	Silença Tech	IT-компанія
	Yaware	Розробники корпоративних додатків
	Unihost	Хостинг, домени
Різне	Juscutum	Юридичні фірма
	Videofabrika	Креативне агентство
	GEK	Агентство нерухомості
	Adventure Tours	Туристична компанія

1.2 Огляд на правову регуляція криптовалют у світі

На сьогоднішній день про криптовалюту є освідомленими багато людей, для частини з яких криптосвіт став невід'ємною частиною життя. Це й не дивно адже після фінансової кризи 2008-2009 років, довіра до американського долара значною мірою похитнулася. Поява криптовалют розв'язала проблему подвійних витрат при використанні фінансових інструментів. Тому після вибуху ціни Bitcoin в кінці 2017 р. та початку 2018 р. (рис.1.1) почалась нова ера для криптовалюти все більше і більше людей зацікавилось даною сферою, адже це щось нове і на цьому збагатилось багато людей.

Рисунок 1.1 – Графік курсу Bitcoin з 28.04.2013 по 19.05.2022

Кожен хотів отримати й собі, якийсь прибуток, тому лише лінивий не знав про криптовалюту. Зараз же дана сфера досі не є повністю контрольованою в світі і ніхто немає чіткого уявлення яким чином можна її врегулювати. Тому на сьогоднішній день перед державами стоїть за мету врегулювати криптовалюти. Ось декілька прикладів, як регулювання в державах, де криптовалютні операції дозволені:

1. Канада дозволила фонди ETF. А також CSA [3] та IIROC [4] випустили вказівки, у яких вимагають від криптотрейдингових платформ у Канаді зареєструватися в місцевих регуляторних органах. У 2021 році Канада додала режим «чистої реєстрації» для торгівельних платформ, які пропонують послуги зберігання. Також були надані рекомендації, щодо реклами та маркетингу криптовалют.

2. США: нормативна база для криптовалют розвивається незважаючи на різні точки зору між агентствами. Хоч SEC і вважається найбільшим регулятором цінних паперів і бірж в США, казначейство FinCEN, Commodity Futures Trading Commission (CFTC) та Internal Revenue Service (IRS) використовують відмінні інтерпретації та рекомендації. Наприклад, SEC [5] зазвичай розглядає криптовалюту, як цінні папери, CFTC [6] називає біткойн товаром, а FinCEN [7] називає його валютою, а IRS [8] визначає криптовалюти, як «цифрове представлення вартості, яка функціонує засобом

обміну/збереження вартості» і також створили податкові інструкції відповідно. Тому Білий дім випустив розпорядження, яке наказує агенціям координувати свої зусилля з регулювання [9].

3. Великобританія: створена спеціальна оперативна група, яка відповідає за криптоактиви в країні. Вона складається з HM Treasury, FCA і The Bank of England. FCA створили правила, які охоплюють KYC, AML та CFT [10]. Також вони створили правила, які відповідають за VASP, але такі щоб не придушити інновації. Усі криптобіржі повинні зареєструватися в FCA для отримання ліцензії. Криптовалюти не вважаються законним платіжним засобом, тому ця діяльність не покривається податками. У лютому 2022 року уряд Великобританії та FCA опублікували реформу, в якій пропонують внести фінансові акції деяких криптоактивів до HM Treasury. У Великобританії не існує спеціального регуляторного режиму, який би охоплював криптомайнерів. Митна служба виклала свій погляд на основі звичайних принципів. Отримання криптовалют від роботодавця розглядаються як «грошова одиниця» і оподатковуються як дохід на основі вартості активів в момент отримання. Якщо криптовалюти зберігаються як особисті інвестиції, застосовується податок на приріст капіталу при вибутті. У випадках, коли йдеться про часту торгівлю, може застосовуватися податок на прибуток, а не приріст капіталу.

4. Австралія :у 2018 році австралійські AUSTRAC, агентство фінансової розвідки та регулятор AML/CTF запровадили закони [11] щодо провайдерів з обміну цифрових валют. Фірми зобов’язані реєструвати та впроваджувати політику KYC, повідомляти про підозрілі транзакції та дотримуватись законодавства щодо боротьби з відмиванням коштів. Казначей Джош Фріденберг заявив, що уряд буде розпочне консультації на початку 2022 року щодо створення системи ліцензування для цифрових бірж, що дозволить купівлю-продаж криптоактивів споживачами в регульованому середовищі. Податки на криптовалюту в Австралії обкладаються податками на приріст капіталу, які варіюються від 19% до 45% [12].

5. Ізраїль: Israeli Securities Authority визнало криптовалюту цінними паперами [13], відповідно до законів Ізраїлю про цінні папери. Регулятор також повідомив громадськість [14] про ризики пов'язані з криптовалютою. 14 листопада 2021 року набули чинності [15] розпорядження про боротьбу з відмиванням грошей за допомогою криптоактивів. Israel Terror Financing Prohibition Authority and Money Laundering приняли подібні до вимог AML/CTF як FATF. Податкова служба Ізраїлю визначає криптовалюту як актив і стягує 25% від приросту капіталу.

6. Швейцарія: Швейцарський фінансовий маркетинговий регулятор, Swiss Financial Market Supervisory Authority (FINMA), створив ліцензійні вимоги для криптовалютного бізнесу всіх можливих типів [16], від біткойн-кіосків до блокчейн компаній. Криптовалютний бізнес підпадає під дію нормативно-правових актів щодо боротьби з відмиванням коштів та вимог ліцензування FINMA. У липні 2021 року Швейцарія ще більше покращила свої правила щодо токенів з Federal Act on the Adaptation of Federal Law до Developments in Distributed Ledger Technology [17]. У Швейцарії приріст капіталу, отриманий від «приватного майна», звільняється від податку на дохід. Це стосується і приросту капіталу від криптовалют, бо згідно з законодавством Швейцарії криптовалюти розглядаються як предмети, які можна оцінити і продати. Отже, вони є активами, які підлягають податку на багатство. Податкові ставки різняться.

7. Польща: як і більшість країн Європи, Польща не регулює криптовалюти за межами вимог ЄС. Польський Національний Банк і KNF попередили про ризики, пов'язані з криптовалютами [18]. KNF заявив, що Ринок криптовалют не є регульованим або контрольованим ринком. «КНФ не уповноважує, здійснювати нагляд або здійснювати будь-які інші наглядові повноваження щодо торгівлі криптовалютами. Деякі організації, що працюють на ринку криптовалют, уповноважені здійснювати оплату послуги, зокрема розрахунки, здійснені законним платіжним засобом (фіатні гроші) в обмін на криптовалюти, які купуються чи продаються». Польський режим

боротьби з відмиванням коштів AML приийняв AMLD5, що суттєво вплинуло на підхід для крипто-бізнесу. Основною метою було підвищення прозорості та захисту від підозрілі операції. Станом на 31 жовтня 2021 року компанії повинні були зареєструватися в Ministry of Finance. Реєстрація не пов'язана з жодним контролюючим аспектом, однак і не надає повноважень на діяльність або правове забезпечення. Польща підписала декларацію про приєднання до Європейського блокчейн-партнерства. Криптовалюти не вважаються законним платіжним засобом. Прибуток від цифрових активів залежить від податків на приріст капіталу та ПДВ. Польські податкові ставки на криптовалюту становлять 19% плюс додаткові 4% для тих, хто має дохід понад 1 млн. злотих.

1.3 Криптовалюта, монета і токен

Криптовалюта – це вид децентралізованої валюти, яка працює на основі блокчейн технологій, що повинна стати альтернативним або ж додатковим способом до сучасної фінансової системи [19]. Взагалі, Сатоші Накамото використовував поняття «electronic cash», в своїй праці, а термін «криптовалюта» почав розповсюджуватись після того, як журнал Forbes опублікував статтю Енді Грінберга «Crypto Currency» [20].

У 1990 році була створена компанія DigiCash із її грошовою системою eCash. У системі було реалізовано функцію підтримки конфіденційності електронних платежів та був присутній криптографічний захист даних. Система eCash була повністю централізована. Проіснувала компанія 8 років і в 1998 благополучно збанкрутувала. Проте сама ідея анонімних платежів була помічена іншими ентузіастами.

У 1997 році британський бізнесмен та спеціаліст-криптограф Адам Бек розробив систему Hashcash. Ця система використовувалася як частина алгоритму аналізу даних як у біткоїні, так і в інших криптовалютах.

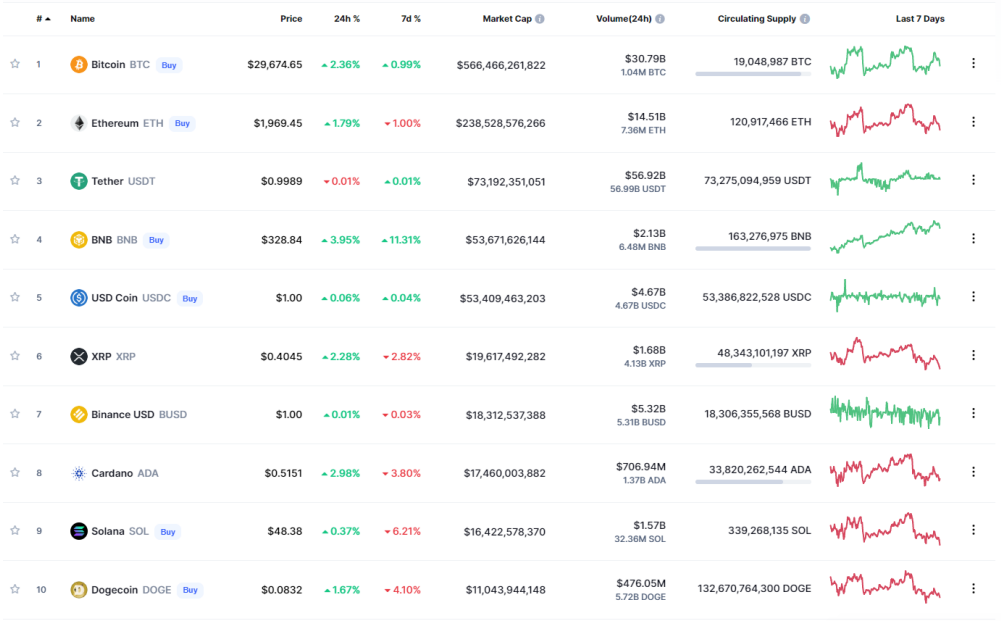
Удосконаленням Hashcash займався Гарольд Фінні, той самий, який був учасником найпершої транзакції з біткоіном.

На основі Hashcash зєявилось два незалежні проекти B-money і Bit-Gold. І саме проект B-money [21] вказаний найпершим в списку літератури того самого документа [22] Сатоші Накамото «Bitcoin: a peer-to-peer electronic cash system».

Альткоїни – дослівно альтернативні монети, тобто всі окрім біткойна. Різні блокчейни або проекти на їх основі (протоколи) виникають, щоб усунути недоліки, притаманні мережі Bitcoin, або запропонувати нові рішення. І вони випускають свої монети, за допомогою яких вирішують різні завдання: управління проектом, залучення фінансування, наймання спеціалістів, надання користувачам доступу до своїх послуг. Не всі альткоїни однаково популярні. Деякі так і не змогли завоювати своє місце на ринку, а деякі, як той самий Ethereum, стали дуже цінними. Хоч у біткоїну досить багато користувачів, але він використовується переважно як засіб накопичення та збереження цінності. Ринок альткоїнів збільшив кількість користувачів криптовалют на порядок. І сталося це багато в чому завдяки тому, що багато альткоїнів мають практичне застосування всередині проекту. Тому на 25.05.2022 року домінація біткойну на ринку криптовалют складає 44,7% при загальній капіталізації крипторинку в $1,267,129,903,731 [23].

Окремим видом альткоїнів є стейблкоіни. Буквально термін означає «стабільні монети». Курс стейблкоїнів найчастіше прив'язаний до реального активу, зазвичай, до долара США. Тому волатильність курсу такого виду криптовалют вкрай низька. Це зрозуміліша для криптоінвестора грошова одиниця, з допомогою якої можна порівняти курс інших криптовалют, зафіксувати прибуток у угоді, зберігати кошти між угодами. На стейблкоини припадає 10,8% капіталізації всіх криптовалют. Стейблкоини виконують роль оборотних засобів під час роботи з криптоактивами, оскільки частка у добовому обороті становить 50 %. Вочевидь, що цей клас активів грає значну роль на ринку криптовалют, надаючи величезну ліквідність. Це можна помітити навіть

неозброєним оком, адже в топ-10 криптовалют по капіталізації на 25.05.2022 р. [24] знаходяться 3 стейблкойна: USDT, USDC і BUSD (рис.1.2).



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	$29,674.65	2.36%	0.99%	$566,466,261,822	$30.79B 1.04M BTC	19,048,987 BTC	
2	Ethereum ETH Buy	$1,969.45	1.79%	1.00%	$238,528,576,266	$14.51B 7.36M ETH	120,917,466 ETH	
3	Tether USDT	$0.9989	0.01%	0.01%	$73,192,351,051	$56.92B 56.99B USDT	73,275,094,959 USDT	
4	BNB BNB Buy	$328.84	3.95%	11.31%	$53,671,626,144	$2.13B 6.48M BNB	163,276,975 BNB	
5	USD Coin USDC Buy	$1.00	0.06%	0.04%	$53,409,463,203	$4.67B 4.67B USDC	53,386,822,528 USDC	
6	XRP XRP	$0.4045	2.28%	2.82%	$19,617,492,282	$1.68B 4.13B XRP	48,343,101,197 XRP	
7	Binance USD BUSD	$1.00	0.01%	0.03%	$18,312,537,388	$5.32B 5.31B BUSD	18,306,355,568 BUSD	
8	Cardano ADA	$0.5151	2.98%	3.80%	$17,460,003,882	$706.94M 1.37B ADA	33,820,262,544 ADA	
9	Solana SOL Buy	$48.38	0.37%	6.21%	$16,422,578,370	$1.57B 32.36M SOL	339,268,135 SOL	
10	Dogecoin DOGE Buy	$0.0832	1.67%	4.10%	$11,043,944,148	$476.05M 5.72B DOGE	132,670,764,300 DOGE	

Рисунок 1.2 – Топ 10 криптовалют за капіталізацією на 25.05.2022 на CoinMarketCap

1.4 Постановка завдань для розробки

Для початку необхідно провести літературний огляд за обраною темою, і також проаналізувати різні варіанти та методики створення смарт-контрактів.

На основі проведеного аналізу літератури було сформовано базовий порядок дій для створення токена:

1. Обрати мережу і мову смарт-контрактів;
2. Створити гаманець MetaMask та додати необхідну мережу;
3. Обрати середовище розробки сумісне з обраним блокчейном;
4. Написати код смарт-контракту токену;
5. Скомпілювати і задеплоїти смарт-контракт;
6. Розгорнути контракт на блокчейні;
7. Перевірити адресу контракту за допомогою BscScan;
8. Змінити необхідну кількість токенів;
9. Протестувати роботу транзакцій.

2. ОСНОВНІ ПОЛОЖЕННЯ ТА ЗАГАЛЬНІ ТЕОРИТИЧНІ ВІДОМОСТІ, НАБІР ІНСТРУКЦІЙ ДЛЯ РЕАЛІЗАЦІЇ ТОКЕНУ

2.1 Аналіз методів створення токенів

Перед тим як створити криптовалюту, необхідно визначитися що створювати монету чи токен. Монета будується на власному блокчейні, в той час як токен вже на існуючій мережі. Створення монети зазвичай потребує зусиль команди розробників і експертів в даній галузі, для створення ж токену необхідні технічні знання та навички.

Хоч токени і будуються у вже існуючий мережі, але вони мають схожі ролі, як і монети. Наприклад, токен біржі PancakeSwap CAKE створений на Binance Smart Chain. І його можна використовувати на PancakeSwap, для оплати деякий транзакцій як мінт NFT або участь в лотереї. В будь якому випадку даний токен активно використовується в додатках заснованих на BSC, в той час як інші токени створені на основі ERC-20 використовуються на блокчейні Ethereum. З цього слідує те, що кожен токен є частиною проекта зі своїми специфічними завданнями [25].

Існує два основних методи створити власний токен: використання спеціалізованої платформи, написання власного смарт-контракту. Щодо першого методу вже давно існує безліч платформ для створення токенів, як приклад ось декілька з них: CoinTool, BakeMyToken, Token Factory, DxSale, DoDoEx [26]. Але якщо краще розібратися то з даним способом не все так гарно як може здатися на перший погляд, зокрема:

1. Велика ціна за створення. Наприклад, створення токену за допомогою CoinTool в мережі BSC обійдеться в 0,7 BNB (≈206$ на 18.05.22).
2. Більшість програм використовують «чорну скриньку» у своїй роботі. Це означає що відомо лише дані, які було передано в програму, а також результат, який отримали, але за рахунок чого він був здобутий невідомо. Також немає доступу до коду смарт-контракту.

Щодо другого методу він є більш підконтрольним розробнику, а також існує можливість для оновлення коду смарт-контракту в залежності від потреб. Також плюсом цього способу є його дешевизна, адже всі необхідні витрати не будуть перевищувати 10$ (у більшості випадків), необхідних для мінту у блокчейні. Взагалі до плюсів децентралізованих платформ над звичайним централізованим можливо віднести:

1. Перевірка транзакцій
2. Безпека даних
3. Незалежність
4. Швидкість і ефективність
5. Доступність інфраструктури даних
6. Рівність учасників

2.2 Принципи та визначення блокчейну

Blockchain перекладається з англійської буквально як «ланцюг блоків». Загалом це база даних, яка може складатися з записів різного роду. Вона зберігається не на якомусь сервері, а децентралізовано, у мережі з комп’ютерних пристроїв. Ці пристрої обмінюються між собою інформацією з бази даних. Таким чином, на кожному пристрої завжди є актуальна інформація, яка зберігається в даному блокчейні. Інформація в блокчейні незмінна, тобто будь-який запис, який був доданий до блокчейну, залишається там назавжди. Ця надійність досягається за рахунок хешування, де хеш кожної наступного запису хешується з хешем попереднього запису, тобто щоб змінити якийсь запис, необхідно розшифрувати всі записи до нього, а також змінити всі, які йдуть після, на всіх пристроях мережі блокчейну. Так, технологія блокчейну навмисно ускладнена і так, в світі не існує потужностей здатних до чогось подібного як зміна такої великої кількості даних на такій кількості пристроїв одночасно.

Більш просте формулювання терміну блокчейн можна знайти від журналу Forbes [27]. Блокчейн – це відкритий розподілений реєстр, який записує транзакції в коді. На практиці це трохи нагадує чекову книжку, яка поширюється на незліченну кількість комп'ютерів по всьому світу. Транзакції записуються в «блоки», які потім пов'язуються разом у «ланцюжку» попередніх транзакцій з криптовалютою.

Загалом, блокчейн заснований на двох технологіях:

1. Децентралізована мережа, в якій кожен пристрій-учасник взаємодіє з іншими в одноранговому форматі. В такій мережі немає одного загального сервера, а кожен пристрій одночасно є клієнтом і виконує функціїї сервера. Такий принцип побудови архітектури більше живучий, працездатний, захищений і масштабований в порівнянні з централізованим. Децентралізовані мережі ще називають: пірінгові, peer-to-peer, p2p.

2. Криптографія, без якої інформація в блокчейні не змогла б знаходитись у безпеці. Завдяки шифруванню сторонні не можуть отримати доступ до секретної інформації і її не вийде непомітно змінити. Криптографія дозволяє перевіряти авторство, властивості, права доступу, дає можливість кодувати дані.

Цікаво, що перша мережа p2p під назвою ARPANET [28] була запущена ще в далекому 1969 році. Вона була створена Агентством Міністерства оборони США по перспективним дослідженням (DARPA) і планувалась як прототип мережі Інтернет.

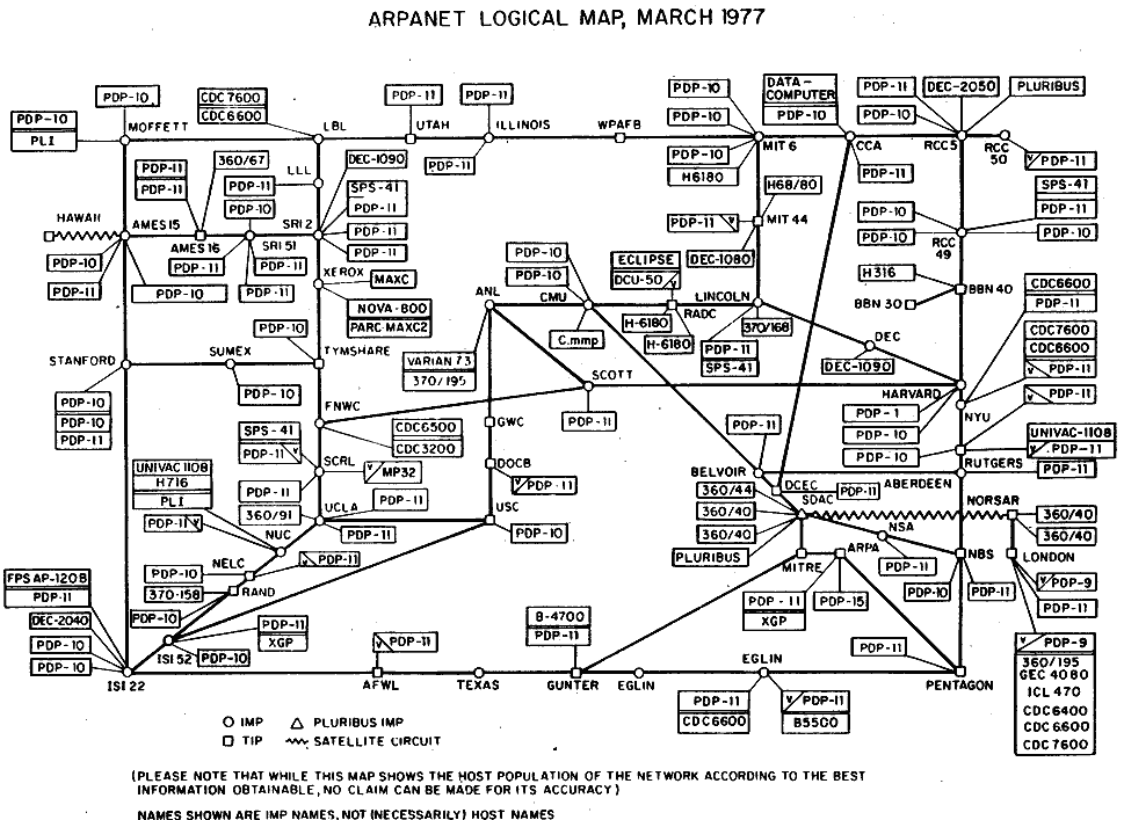


Рисунок 2.1 – Карта логіки ARPANET

Технологія блокчейну була ж започаткована в 1991 році. Саме тоді криптографи Стюарт Хабер і Скотт Сторнетт опублікували працю [29] під назвою: «Як створити часову мітку в цифровому документі», в якій були описані принципи сучасного блокчейну. Їхньою метою було вирішення питання про права володіння інтелектуальною власністю. Вони взялись за вирішення одразу двох задач: страхування від зміни документу і мітки часу. Вони вбачали наступні сфери застосування даної технології: журнали аудитів, докази у кримінальних справах, журнали телефонних розмов, судові протоколи, біржова торгівля, криптографічні сертифікати та багато іншого.

Сучасний блокчейн з’явився в 2009 році. А за рік до цього, в 2008, людина або група людей під іменем Сатоші Накамото опублікували на сайті Bitcoin.org документ, який і вважають історичним: «Bitcoin: A Peer-to-Peer Electronic Cash System». В ньому описані [22] принципи роботи мережі Bitcoin, одною з яких була виключення третьої сторони в здійсненні цифрових транзакцій. Першими учасниками транзакції з переводу десяти біткоїнів були Сатоші Накамото та

американський програміст Гарольд Фінні. Першою з відомих покупок за біткоїни стало придбання піци за 10 000 BTC 22 травня 2010 р.

Декілька важливих визначень, необхідні для розуміння принципу роботи блокчейна:

1. Транзакція – це переказ криптовалюти, при цьому інформація про цей переказ збирається в блоками.

2. Блок – це місце в блокчейні, де інформація зберігається і шифрується. Блоки ідентифікуються довгими числами, які включають зашифровану інформацію про транзакції з попередніх блоків і інформацію про нову транзакцію. Блок обмежений об’ємом інформації, яку можна в нього записати. В різних блокчейнах різний розмір блоків, чим більше розмір, тим більше транзакцій можна записати в блок, мережа при цьому буде працювати швидше.

3. Хеш – це математичний алгоритм, який може дані будь-якого розміру перетворити в масив бітів фіксованого розміру.

У результаті маємо хеш блоку – це всі транзакції цього блоку, які пропускаються через хеш-функцію, яка в свою чергу видає хеш-суму блоку, яка записується в заголовок блоку, в який також записується хеш-сума попереднього блоку. Виникає логічне питання: «Що в якості хешу попереднього блоку записується в першому блоці блокчейну?». Відповідь проста: нічого, окрім хешу цього блоку. До речі, перший блок в блокчейні має назву генезіс-блок (genesis block).

Наступний крок в еволюції блокчейну відбувся в 2013 році, поява Ethereum. Блокчейн Bitcoin, у спрощеному вигляді, рахує скільки в кого біткоїнів є і перераховує їх баланси після кожної транзакції. Ethereum же є повноцінною віртуальною машиною. Ця машина дозволяє запускати програми (смарт-контракти) та цілі програмні комплекси, які будуть спрацьовувати автоматично, у випадку виконання належних умов.

2.3 Смарт-контракти

Вперше технологію смарт-контрактів в 1990-х роках описав Нік Сабо [30]. Він визначив смарт-контракти як інструмент, який захищає комп'ютерні мережі шляхом об'єднання протоколів з призначеним для користувача інтерфейсом. Сабо також обговорював потенційне застосування смарт-контрактів в різних областях, які включають в себе суспільні відносини договірного характеру, такі як кредитні угоди, обробка платежів і управління авторськими правами

Смарт-контракт – це інформаційний аналог звичайних угод, який виконує записану в ньому логіку при виконанні сторонами договору певних умов. Вони дають можливість безпечно обмінюватися криптовалютою, цінними паперами, грошима, а також іншими товарами і послугами, без участі посередників [31]. Код угоди, що містяться в ньому, існують у розподіленій децентралізованій мережі. Код контролює виконання всіх умов, а потім і умови, а транзакції можна відстежувати і вони є незворотними, тобто працюють автоматично.

Смарт-контракти виконує віртуальна машина. Віртуальні машини опрацьовують низько-рівневі мови програмування – байт-код. Для цього використовується обчислювальна потужність блокчейну. Велика кількість одночасно викликаних смарт-контрактів можуть зупини роботу блокчейну, щоб цього уникнути розробники обмежують максимальний розмір контрактів за рахунок обсягу коду і розміру комісій.

Застосування розумних контрактів є неосяжним, зараз це в більшості своїй від продажів токенів до управління децентралізованими проектами, наприклад:

1. Алгоритмічні стейблкоїни, створюють токени і змінюють їхню вартість, для підтримки сталої ціни, в залежності від курсу основної монети. Смарт-контракт Kolibri [32] змінює ціну на нові kUSD в прямій залежності від tez. Але недосконаліть яких на сьогоднішній день чув напевно кожен, після

обвалу Terra LUNA [33], від 90$ до 0,00018$ за монету буквально за тиждень 05.05.2022-12.05.2022.

2. Оракули, які збирають інформацію з різних джерел і надають усереднені ціну на активи чи іншу інформацію. Саме так працює оракул Harbringer [34]. Він отримує ціни на різні криптовалюти з бірж або торгових площадок.

3. Вестинг-контракти [35], робота яких заключається у відправці токенів користувачам в намічений час.

Загалом, на нашу думку, людство ще не використовує дану технологію на повну, в найближчому майбутньому нас чекає багато вдосконалень від смарт-контрактів в онлайн-магазинах до дверей будинків, які не будуть відкриватись без сплати за оренду.

Для порівняння було обрано три мови програмування для розумних контрактів: Solidity, Clarity, Move.

На сьогоднішній день Solidity [36] є основною мовою розробки смарт-контрактів. Спочатку він був розроблений виключно для створення розумних контрактів у мережі Ethereum. Це об'єктно-орієнтована мова високого рівня з фігурними дужками, яка має багато запозичень з інших мов програмування, таких як JavaScript, C++ і Python. Solidity може дозволити розробникам створювати сценарії додатків, які залежать від бізнес-логіки, що самовиконується. Дизайн Solidity є спорідненим до синтаксису JavaScript, що забезпечує кращу легкість розуміння та впровадження JavaScript для розробників.

До основних відмінностей Solidity можна віднести:

1. Підтримка множинного успадкування разом із лінеаризацією C3.

2. Надання складних змінних-членів у випадках контрактів, які включають структури, а також довільні ієрархічні відображення.

3. Підтримка об'єктів стану або змінних поряд із типами даних та багатьма іншими функціями програмування.

4. Бінарний інтерфейс програми в Solidity забезпечує можливість використання різних безпечних для типу функцій в одному контракті.

5. Широкий спектр блокчейн-платформ, які підтримують Solidity, включають Tendermint, Ethereum, ErisDB, Counterparty і Ethereum Classic.

6. Підтримка різні типи даних, такі як цілі числа, модифікатори, логічні значення та рядкові літерали.

7. Завдяки синтаксису, подібному до інших загальних мов програмування, Solidity також забезпечує підтримку як одно-, так і багатовимірних масивів.

Як одна з популярних мов програмування смарт-контрактів, Solidity є багатообіцяючим вибором для таких випадків, як голосування, краудфандинг та сліпі аукціони.

Мова програмування Move смарт-контрактів є мовою нового покоління, розроблена спеціально для блокчейну Diem [37], для забезпечення офіційно перевіреного, безпечного та ізольованого програмування. Це дозволяє розробникам писати програми, які могли б підтримувати гнучке управління та передачу активів, покращуючи тим самим захист відповідних активів. Крім того, дизайн мови програмування Move також зосереджено на деяких важливих випадках використання за межами блокчейну.

До основних відмінностей Move від інших представників можна віднести:

1. Можливість визначення користувацьких типів ресурсів із семантикою, подібною до лінійної логіки.

2. Першокласні ресурси являють собою дуже поширену концепцію, яку використовують програмісти для впровадження безпечних цифрових активів.

3. Підтримка написання правильної бізнес-логіки для застосування політики контролю доступу та упаковки активів.

4. Можливість використання мови поза блокчейном.

5. Під час запуску мережі Diem Payment Network (DPN) важко знайти підтримку для користувацьких модулів Move.

Отже, Move розроблено як безпечну та перевірену мова програмування з надзвичайно бажаною гнучкістю.

Основне визначення Clarity говорить про те, що це мова програмування для створення смарт-контрактів на блокчейні Stacks 2.0 [38]. Цікаво, що це також може забезпечити підтримку програмного контролю над цифровими активами.

До основних відмінностей Clarity від інших представників можна віднести:

1. Користувачі задають власні умови для транзакцій. В результаті він може забезпечити високий рівень безпеки, запобігаючи несподіваній передачі маркерів, які належать користувачу.
2. Мова програмування Clarity не має компілятора.
3. Точний і надзвичайно зрозумілий синтаксис.
4. Підтримка перевірки приведення типів, таким чином усуваючи групи помилок, такі як помилки повторного входу, зчитування неініціалізованих значень і ненавмисне приведення.
5. Можливість аналізу коду для визначення використання даних і витрат на час виконання.

Загалом, за допомогою Clarity вирішуються проблеми, які, можливо, потребували спірних хардфорків, які не можна було б вирішити. Оскільки Clarity застрахований від помилок компілятора, які можуть завдати значної шкоди.

2.4 Remix Solidity IDE

Для написання смарт-контрактів на Solidity існує основне інтегроване середовище розробки - це Remix Solidity IDE. І для написання контракту токену я обрав саме його, адже немає гідних аналогів, які могли б надати такі самі можливості для створення, дебагу та тестування смарт-контрактів. До головних плюсів Remix я би відніс:

1. Підтримка різних мов смарт-контрактів.

2. Багато плагінів, тому можна повозитися з кодом.

3. Присутня можливість дебагу контракту.

4. Можливість обрати свою версію компілятора.

5. Можливість тестування на віртуальній машині.

У загальному вигляді програми є два найбільш важливих та гарно сформованих розділи: Solidity compiler та Deploy & run transactions.

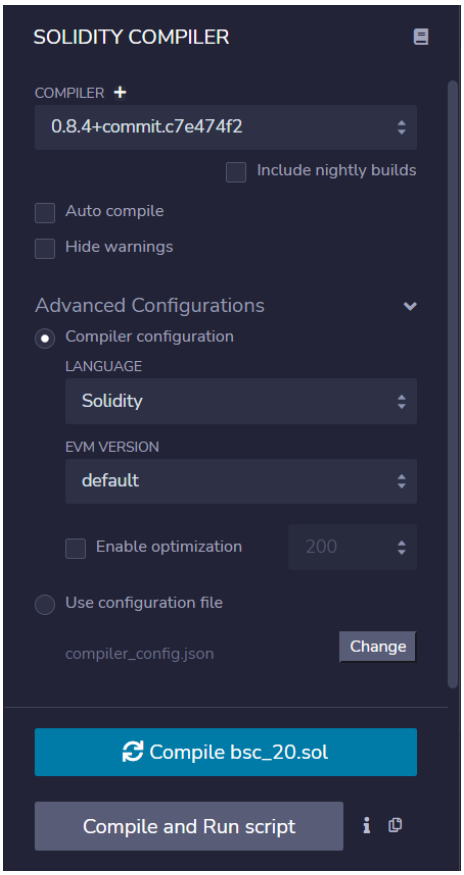


Рисунок 2.2 – Вигляд налаштувань компілятора

У базових можливостях налаштувань компілятора існує вибір мови компілятора та версія оточення. Головним же плюсом є можливість обрати версію компілятора починаючи з 0.1.1 і до актуальної, а це більше ніж 100 версій. Також присутня налаштувань авто-компіляції контракту та ігнорування попереджень.

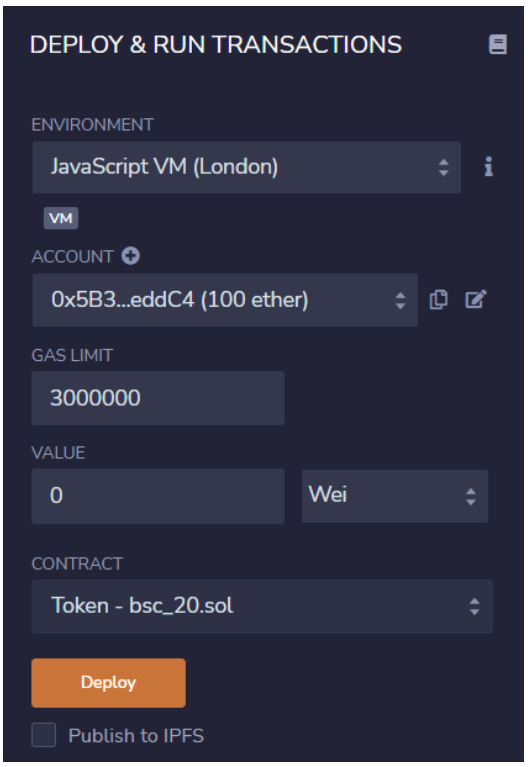


Рисунок 2.3 – Вигляд налаштувань деплою

Основною перевагою Remix над іншими аналогами є саме деплой програми. В ньому присутня можливість вибору оточення, сім варіантів. При виборі оточення віртуальної машини будь то Лондон чи Берлін, надається 15 адрес гаманців, на яких вже є велика кількість ether необхідна для тестування смарт-контракту на локальному блокчейні. Також є оточення за допомогою якого можливо завантажити свій контракт на реальний блокчейн прямо з додатку.

2.5 Токеноміка

Токеноміка (економіка токенів) – це зведення політик та алгоритмів створення та розподілу токенів проекту [39]. До неї входить наступне.

1. Спосіб випуску і роподілу перших токенів. Розподілятись токени можуть різними способами. Мережі винагороджують валідаторів або майнерів, щойно викарбуваних монет, продають частину токенів потенційним користувачам у рамках первинної пропозиції монет (наприклад, ICO). Токени

можуть поширюватися серед користувачів за допомогою певних дій та поведінки.

2. Первинна пропозиція, тобто оцінка токенів випущених на початку.

3. Вид емісії. Регулювання випуску нових монет.

4. Максимальна межа пропозиції (Supply cap) – чи є емісія жорстко обмеженою чи постійною.

5. Цінова стабільність. Якщо монет в обігу достатньо, щоб відповідати рівням пропозиції, учасники ринку здатні вплинути на волатильність меншою мірою.

6. Основна команда, яка стоїть за кожним проектом, розробляє правила того, як токени створюються, а також як вони вводяться в мережу і виводяться з неї. У різних проектах використовуються різні підходи.

7. Майбутня адаптація до ринку. Більшість розробників знають, що те, що вони створюють зараз, не обов'язково працюватиме в майбутньому так, як замислювалося спочатку. У міру зростання та розвитку мережі може знадобитися змінити спосіб управління токенами. Деякі проекти розробили положення про те, як користувачі мережі можуть ефективно змінити спосіб керування токенами в екосистемі за допомогою консенсусу.

Приклади токеноміки в дії:

1. Bitcoin. Максимально буде лише 21 000 000 біткоїнів, і вони випускаються зі швидкістю, що скорочується вдвічі кожні чотири роки. Приблизно 19 000 000 вже існує, так що протягом найближчих 120 років буде випущено лише 2 000 000. Після чого майнінг припиниться. Це означає, що 90% пропозиції вже перебуває в обігу, і через 100 років біткоїнів буде лише на 10,5% більше, тому не слід очікувати на серйозний інфляційний тиск, що знижує вартість монети.

2. Ethereum. В обігу знаходиться близько 119 000 000 монет, і немає обмежень на кількість ефіру. Але емісія Ефіріуму нещодавно була скоригована за допомогою механізму спалювання, щоб вона досягла стабільної пропозиції або, можливо, навіть була дефляційною. З огляду на це особливого

інфляційного тиску на ефір також очікувати не варто. Може навіть бути дефляція.

3. Dogecoin. Також не має обмеження на пропозицію, і в даний час інфляція становить близько 4% на рік. Таким чином, очікується, що інфляційна токеноміка підірве цінність DOGE більше, ніж біткоїну або ефіру.

Загалом існує дві моделі токеноміки: інфляційна та дефляційна.

Інфляційний токен не має максимальної пропозиції і випускатиметься з часом. Існує багато варіантів інфляційних моделей токенів. Деякі обмежують щорічне створення токенів, інші засновані на встановленому графіку випуску нових токенів. Прикладом інфляційного токена може бути токен CAKE децентралізованої криптовалютної біржі PancakeSwap. У токена CAKE інфляційна модель і він не має обмеження максимальної циркуляції, у кожному новому блоці «друкуються» нові токени, частина яких згодом спалюється. Розробники окремо пояснюють випуск нових токенів необхідністю стимулювати користувачів надавати ліквідність, що розумно, оскільки наявність ліквідності запорука працездатності будь-якої біржі.

Якщо ж загальна кількість токенів в обігу обмежена наперед заданою кількістю, цей токен називається дефляційним. У цій моделі буде створено певну кількість токенів, і ліміт ніколи не збільшуватиметься. Це створює дефляційну валюту, навіть якщо попит зросте, пропозиції не буде.

Принципи регулювання випуску нових монет:

1. Блокування частини монет та поступовий висновок на ринок. Метод використовується у проектах з одноразовою емісією. Розробники створюють штучний дефіцит активу та отримують резерв для залучення нових інвесторів.

2. Підвищення складності майнінгу. Нові криптомонети в мережі створюються з певним часовим інтервалом. Для Bitcoin це 10 хвилин, для Ethereum – 14,2 секунди. Час залишається незмінним незалежно кількості майнерів і залучених потужностей. Складність видобутку криптомонету поступово підвищується: в мережі Біткоїн — кожні 2016 блоків (приблизно раз на 2 тижні), Ефіріуму — кожні 1000 блоків.

3. Зниження нагороди за майнінг. У мережі BTC оплата за знаходження нових блоків зменшується вдвічі за кожні 4 роки. Одночасно уповільнюється випуск нових монет та створюється помірний дефіцит активу на ринку. Схожі процеси відбуваються в інших проектах.

4. Механізм спалювання. Для боротьби з інфляцією та підвищення вартості токена деякими проектами практикується спалювання. Цей спосіб застосовується, наприклад, біржею Binance. Біржа спрямовує частину чистого прибутку на скупку токенів BNB з ринку, що неминуче підвищує ціну. Акт спалювання відбувається, коли валюта відправляється на гаманець, адресу якого ніхто не знає. Усі операції зі спалювання токенів записуються в блокчейн як транзакція. Тому будь-хто може перевірити, що монети було знищено.

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Програмна реалізація

Для початку необхідно створити новий робочий простір на https://remix.ethereum.org. Саме за допомогою Remix IDE буде відбуватись вся подальша робота. Далі створюємо файл з розширенням .sol. Ми отримаємо пустий проект і тепер можна перейти до створення смарт-контракту.

Почнем з того, що токен складається з: назви, символу токена, загальної кількості та кількості знаків після крапки.

```
contract Token {
    string public name = "GraduationToken";
    string public symbol = "GRT";
    uint256 public totalSupply = 0;
    uint8 public decimals = 4;
    }
```

Для рефакторингу коду необхідно створити два мапінги: для відображення залишків та для відображення надбавок.

```
    mapping(address => uint256) public balanceOf;
    mapping(address => mapping(address => uint256)) public allowance;
```

Це зменшить обсяг коду та зекономить час.

У основі будь-якого токену є задумка, що ним можна буде торгувати, тобто пересилати з одної адреси на іншу. Але для переводу необхідна перевірка на доступну кількість для переводу, яка вирішить чи взагалі можливо здійснити такий переказ. Створимо функцію approve, яка буде перевіряти на кількість токенів та викликати подію Approval, для того щоб записати підтвердження до транзакції.

```
event Approval(
  address indexed _owner,
  address indexed _spender,
  uint256 _value
);
function approve(address _spender, uint256 _value)
  public
  returns (bool success)
{
  allowance [msg.sender] [_spender] = _value;
```

```
    emit Approval(msg.sender, _spender, _value);
    return true;
  }
```

Тепер вже можна створити функції для переведення. Їх буде дві: для переведення зі свого гаманця та для переведення з одної адреси гаманця до іншої. А також подія, яка буде записувати трансфер до транзакції.

```
event Transfer(
  address indexed _from,
  address indexed _to,
  uint256 _value
  );
function transfer(address _to, uint256 _value)
    public
    returns (bool success)
  {
    require(balanceOf [msg.sender] >= _value);
    balanceOf [msg.sender] -= _value;
    balanceOf [_to] += _value;
    emit Transfer(msg.sender, _to, _value);
    return true;
  }
function transferFrom(
    address _from,
    address _to,
    uint256 _value
  ) public returns (bool success) {
    require(_value <= balanceOf [_from]);
    require(_value <= allowance [_from] [msg.sender]);
    balanceOf [_from] -= _value;
    balanceOf [_to] += _value;
    allowance [_from] [msg.sender] -= _value;
    emit Transfer(_from, _to, _value);
    return true;
  }
```

Далі необхідно застосувати мінтдля того щоб отримати початкову суму токенів, яка на початковому етапі рівна нулю.

```
  function mint(uint256 _amount, address _to) public returns (bool success) {
    require(msg.sender == owner, "Operation unauthorised");

    totalSupply += _amount;
    balanceOf [_to] += _amount;

    emit Transfer(address(0), _to, _amount);
    return true;
  }
```

Ця функція може виконуватися лише власником контракту, якого необхідно вказати вище, як того хто розгорнув цей контракт на блокчейні.

```
address payable public owner = payable(msg.sender);
```

Для того щоб уникнути великої емісії за необхідності необхідно застосувати функцію спалювання.

```
function burn(uint256 _amount) public returns (bool success) {
 require(msg.sender != address(0), "Invalid burn recipient");

 uint256 accountBalance = balanceOf [msg.sender];
 require(accountBalance > _amount, "Burn amount exceeds balance");

 balanceOf [msg.sender] -= _amount;
 totalSupply -= _amount;

 emit Transfer(msg.sender, address(0), _amount);
 return true;
}
```

3.2 Тестування в віртуальному блокчейні

Після успішної компіляції виконаємо деплой контракту на віртуальній машині.

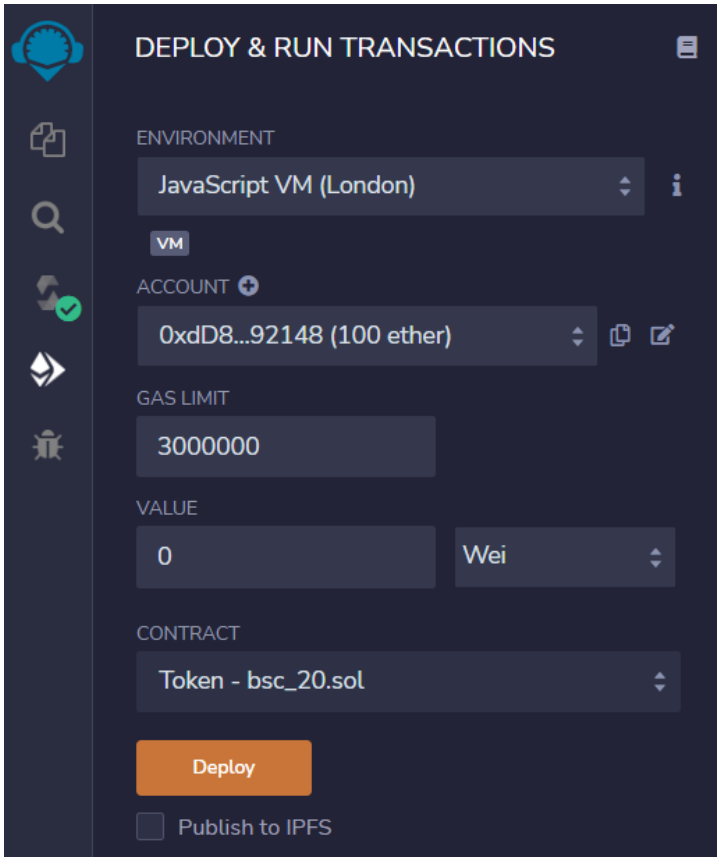


Рисунок 3.1 – Деплой смарт-контракту на віртуальній машині JavaScript VM (London)

Після чого отримуємо контракт з наявними усіма функціями.

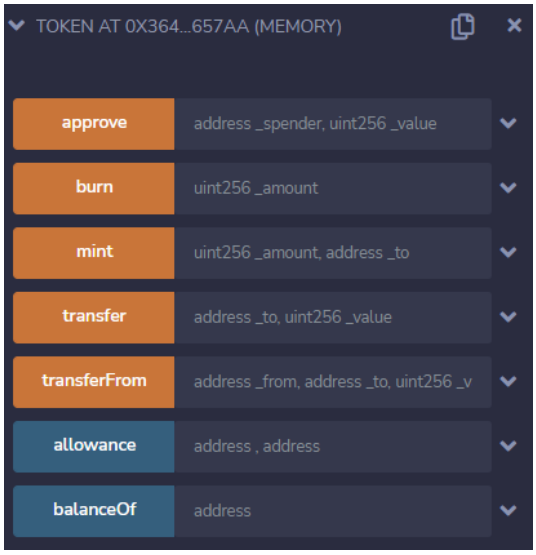


Рисунок 3.2 – Функції смарт-контракту

Синім позначені функції, які не записуються до блокчейну і не використовють газ для роботи. Оранжевим позначені функції, які записуються в транзакцію в блокчейні, відповідно використовують газ для виконання.

Для початку перевіримо власника, кількість символів після коми, ім’я, символ та загальну кількість токенів.

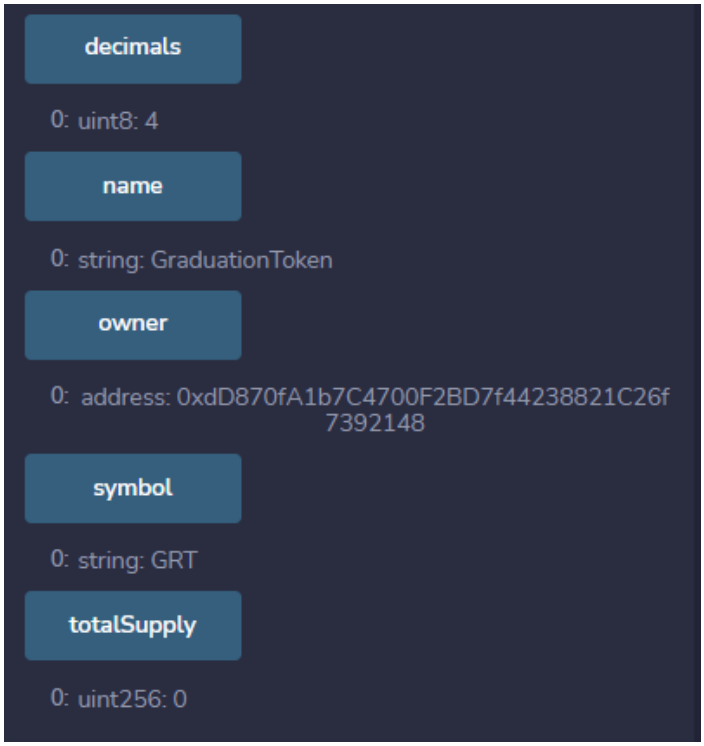


Рисунок 3.3 – Загальна перевірка токена

Оскільки всі дані вірні можна переходити до наступного етапу – мінту токенів. Для цього обираємо гаманець власника контракту та змінтимо, якусь кількість на цю адресу.

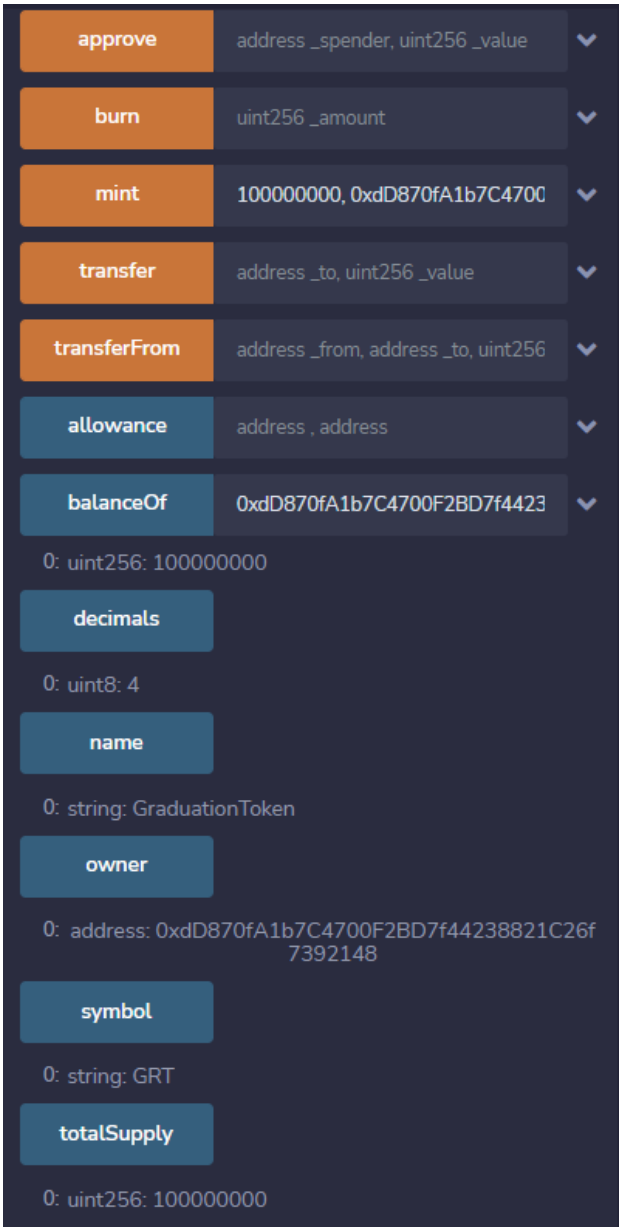


Рисунок 3.4 – Мінт токенів

Як бачимо загальна кількість токенів та кількість токенів на балансі власника змінилась після виконання мінту, отже все працює вірно. Спробуємо тепер перевести токени з акаунта власника на будь-який інший і перевіримо чи змінилась кількість токенів на гаманці отримувача.

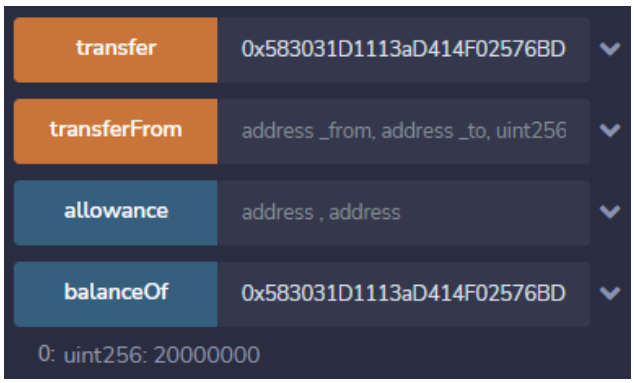


Рисунок 3.5 – Кількість токенів на гаманці отримувача після транзакції

Перевірка токенів з гаманця власника на інший гаманець після чого кількість токенів змінилась на обох гаманцях на визначене число. Перевіримо чи працює спалювання. Для цього спалимо 200 токенів з гаманця.

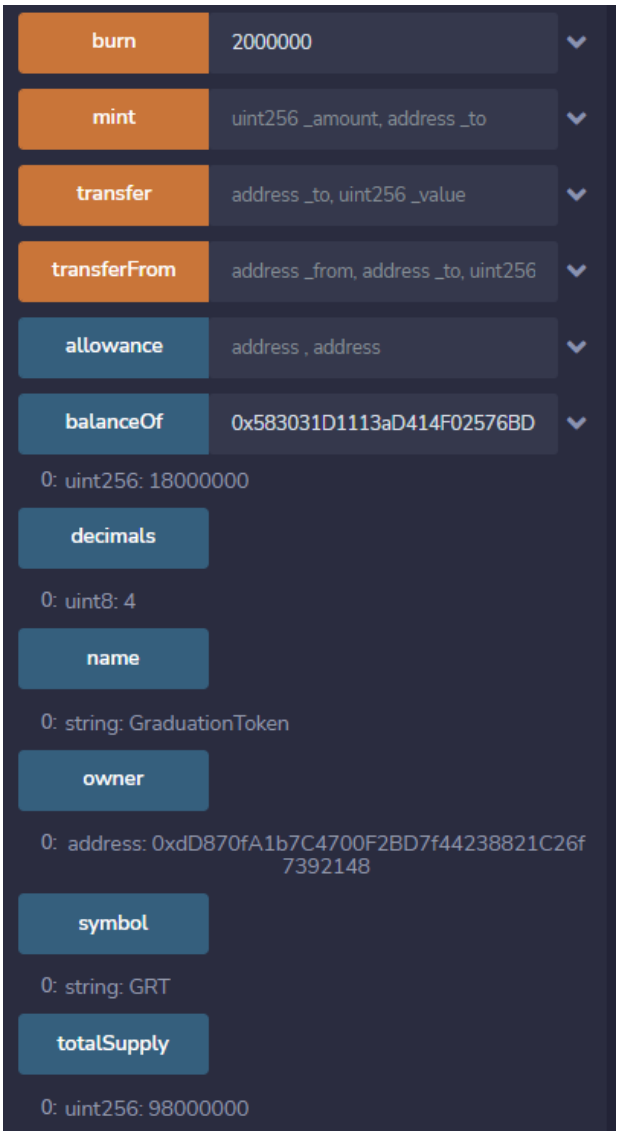


Рисунок 3.6 – Результат роботи спалювання токенів

Після спалення 200 токенів з гаманця їхня кількість на гаманці успішно змінилась, як і загальна кількість токенів. Оскільки все працює коректно, то можна переходити до наступного етапу.

3.3 Розгортання токену в мережі BSC

Для початку необхідно підключити свій гаманець метамаск з підключеною мережею BSC з деякою кількістю токенів BNB необхідних для сплати транзакцій.

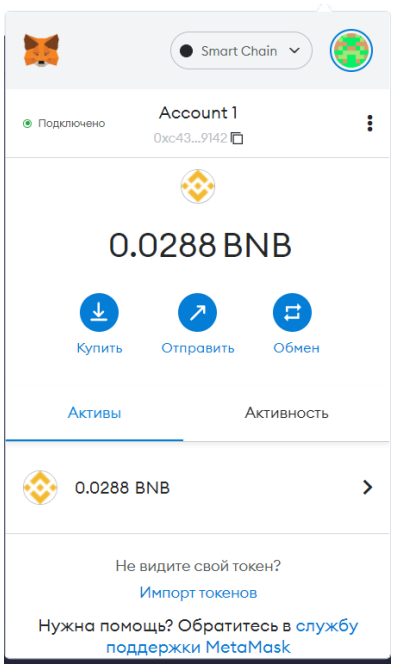


Рисунок 3.7 – Приклад власного гаманця метамаск

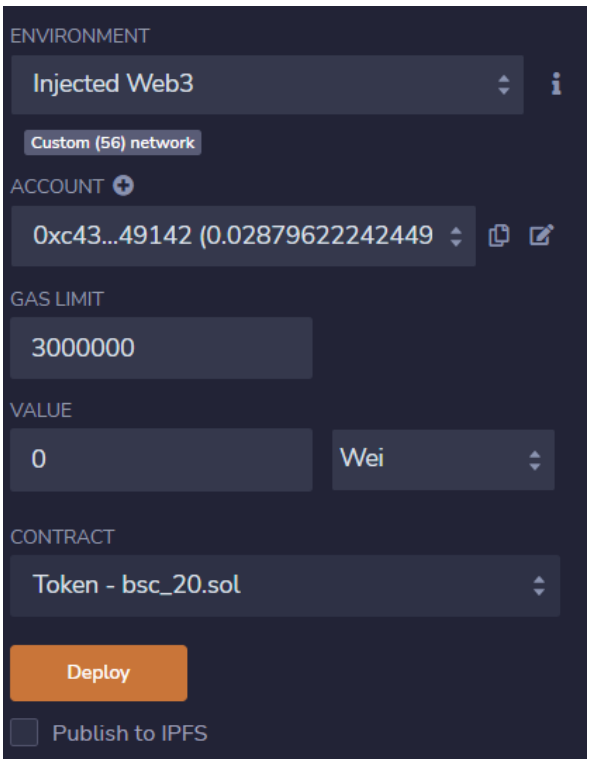


Рисунок 3.8 – Деплой на BSC

Для того щоб задеплоїти контракт необхідно обрати Injected Web3 і підключити гаманець.

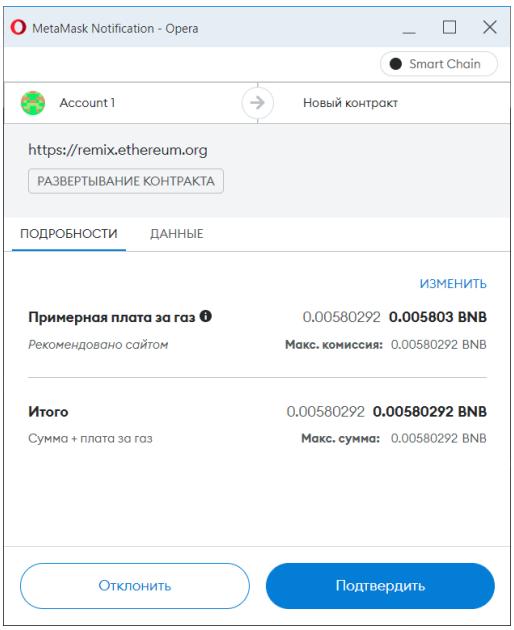


Рисунок 3.9 – Транзакція на розгортку контракту

Після оплати транзакції про розгортання контракту на BSC переходимо по даним транзакції і знаходимо адресу контракту в мережі.

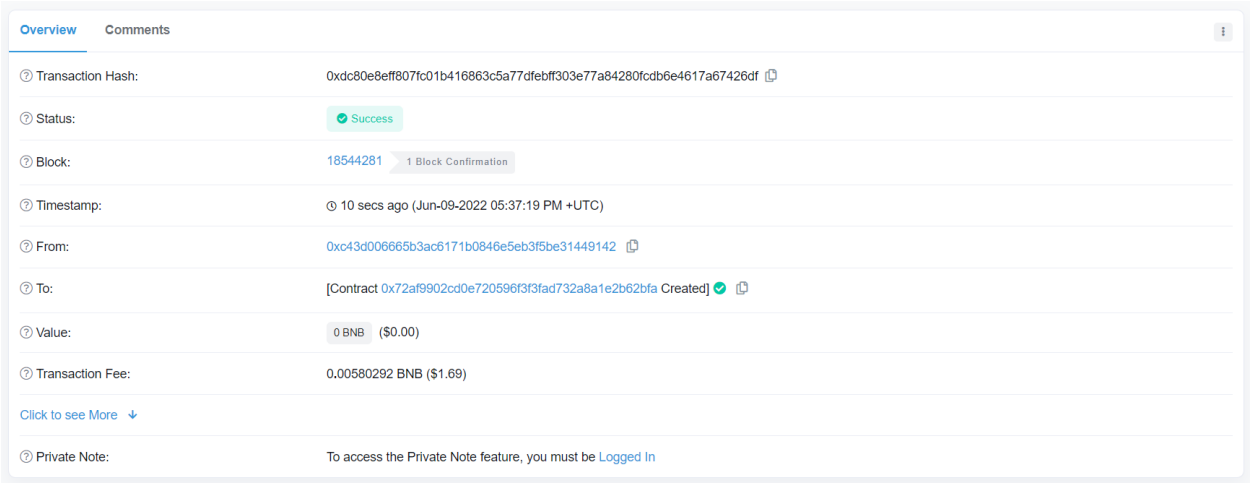


Рисунок 3.10 – Деталі транзакції

Переходимо на сторінку контракту.

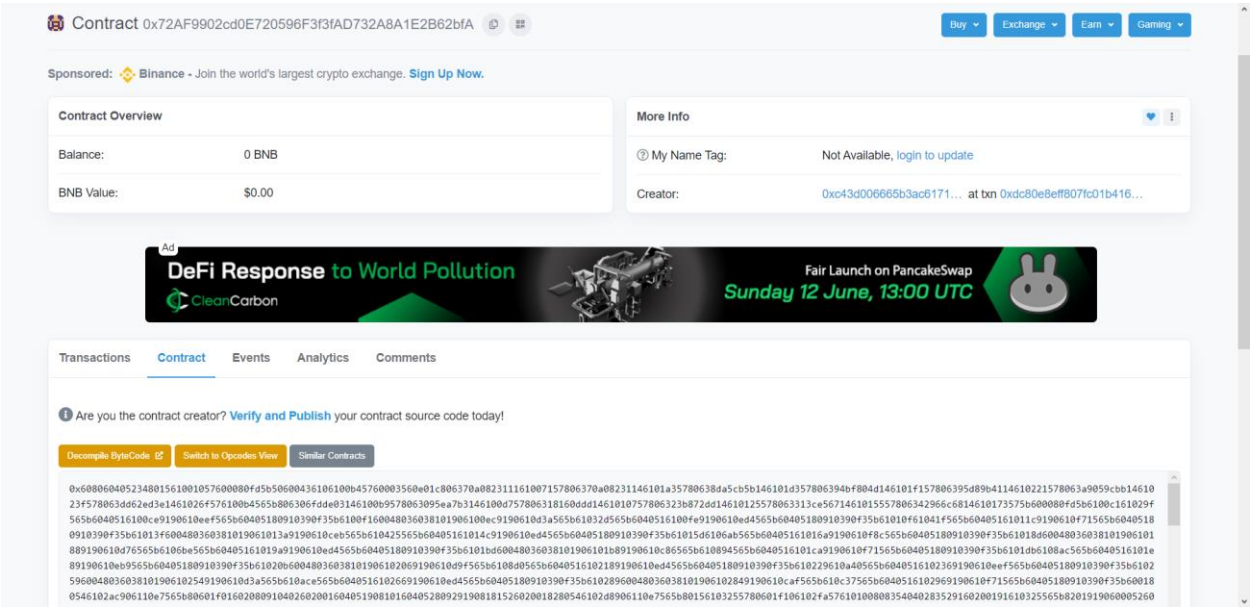


Рисунок 3.11 – Адреса контракту

На цей момент контракт вже розміщується в мережі, але є не верифікованим тому будь-які дії з цим контактом не доступні. Для цього необхідно натиснути «Verify and Publish» для того щоб його верифікувати.

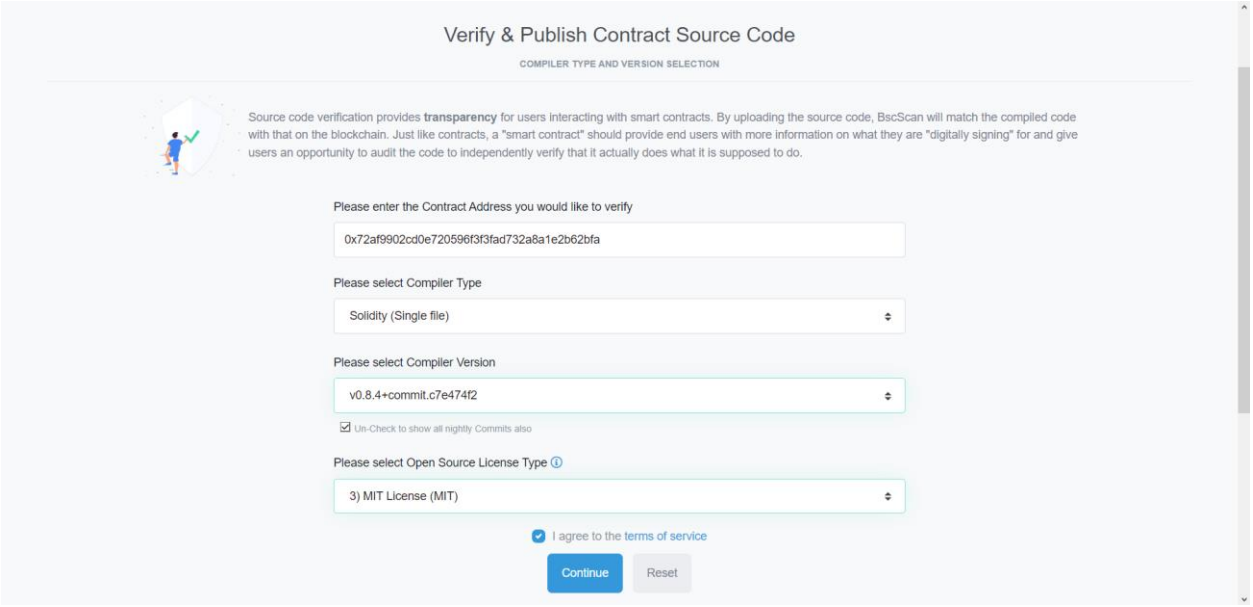


Рисунок 3.12 – Верифікація, ліцензування та публікація контракту

На цій сторінці обираємо мову та тип смарт-контракту, версію компілятора та ліцензію, якщо вона в вас є. На наступній сторінці просто вставляємо код контракту і програма перевіряє чи збігаються байт-коди вставленого коду та коду задпелоїного контракту.

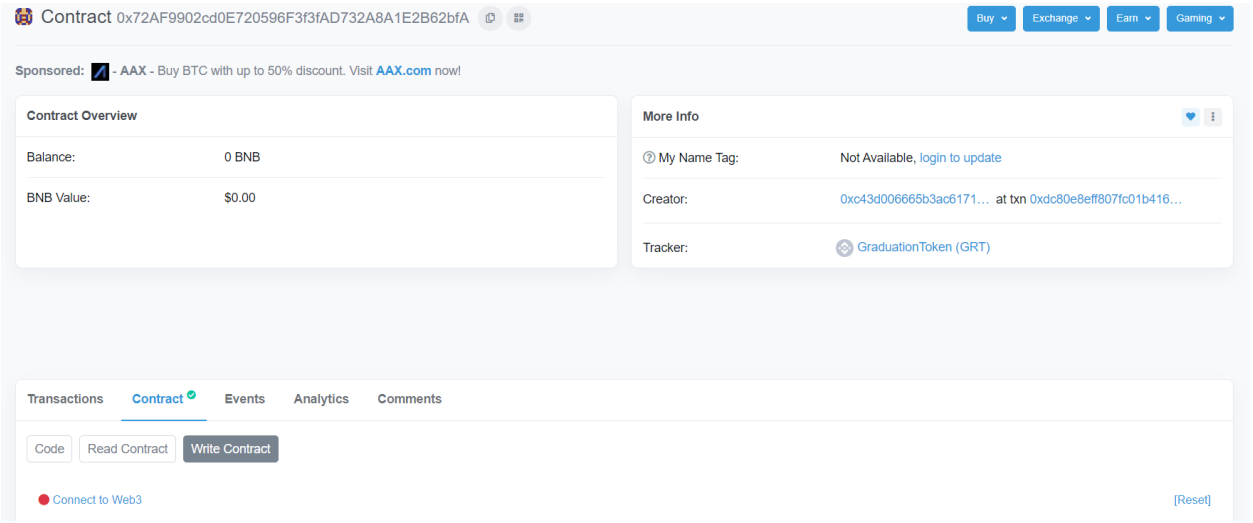


Рисунок 3.13 – Верифікований контракт

Після цього отримуємо повністю верифікований контракт з ліцензією. На цьому токен створений, але необхідно протестувати його роботу на

блокчейні. Для цього натискаємо «Connect to Web3» та підключаємо гаманець. Змінтимо 420000 токенів.

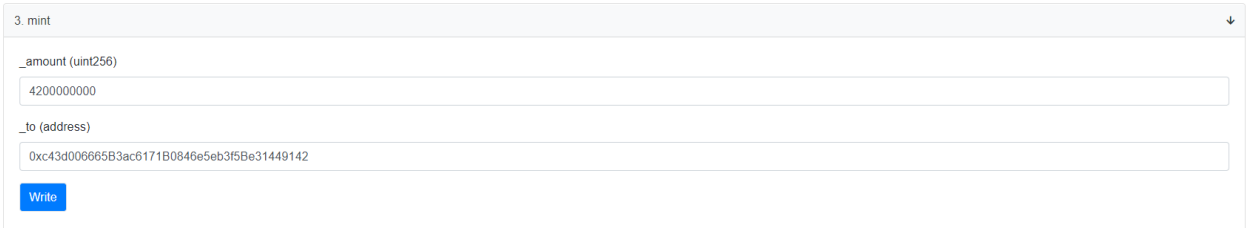


Рисунок 3.14 – Мінт токенів

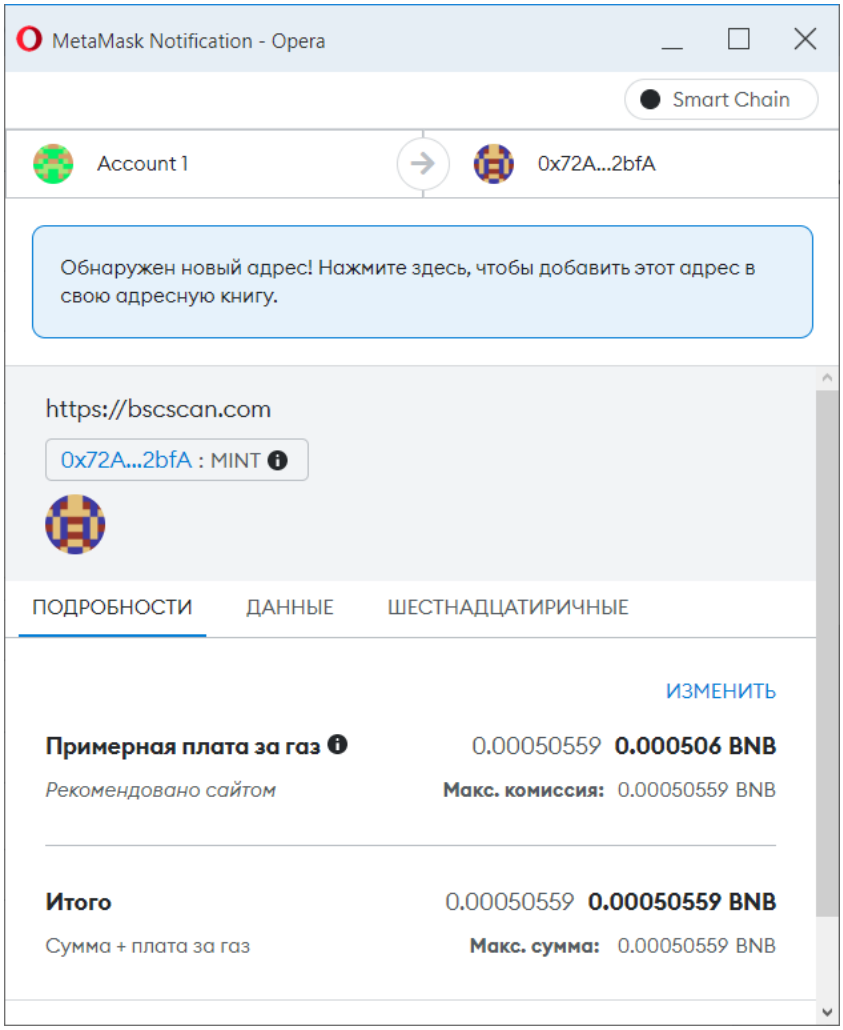


Рисунок 3.15 – Транзакція про мінт

Після підтвердження та оплати транзакції про мінт токенів, вони відправляються на дану адресу.

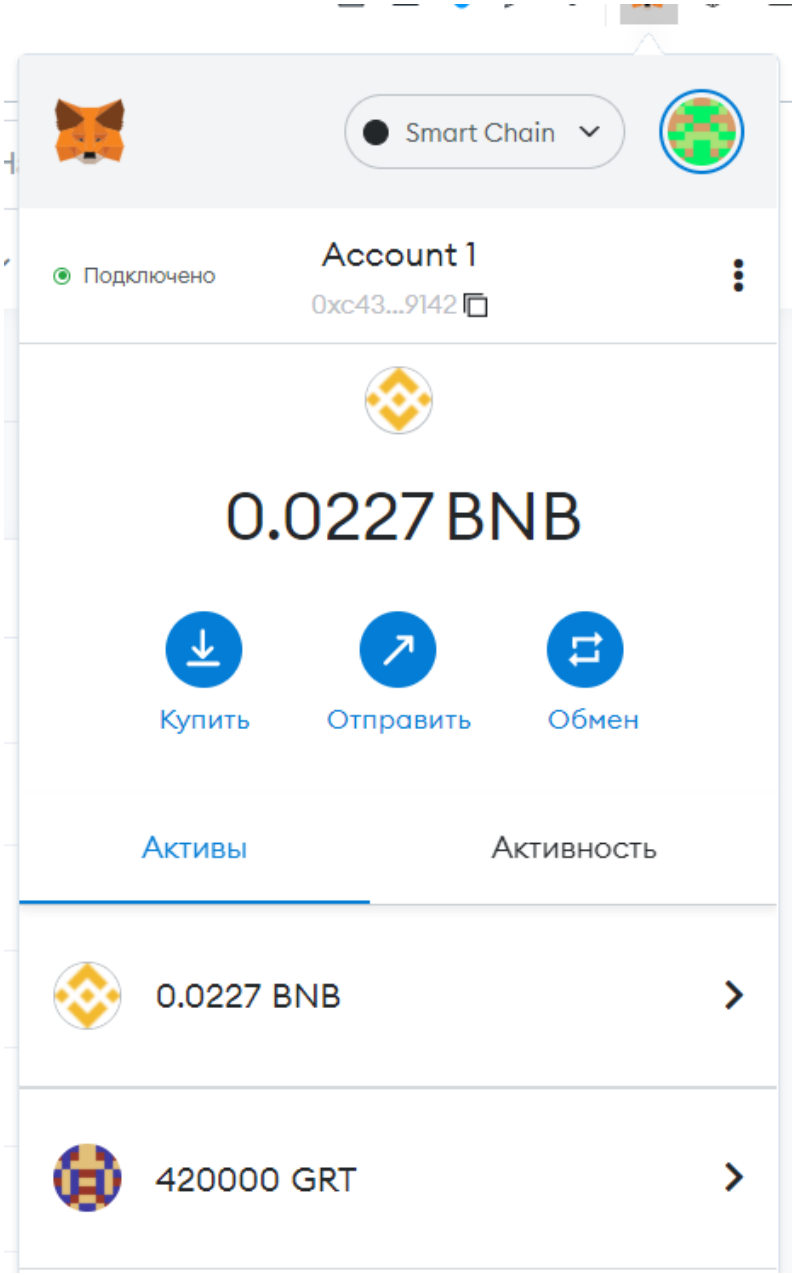


Рисунок 3.16 – Токени на гаманці

Для того щоб перевірити чи прийшли токени, необхідно їх імортувати в метамаск за допомогою адреси смарт-контракту.

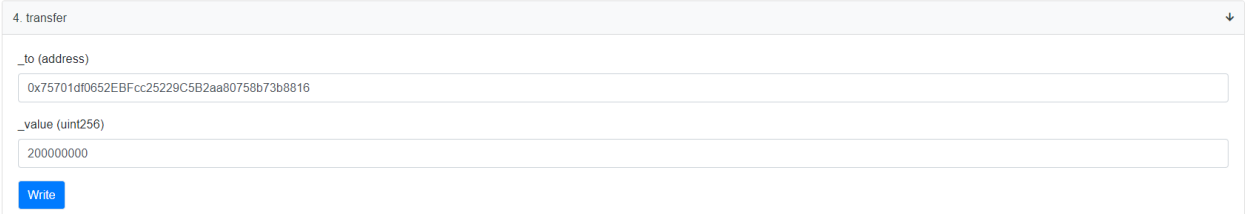


Рисунок 3.17 – Трансфер на інший гаманець

Перевіримо як працює переказ токенів з одного рахунку на інший.

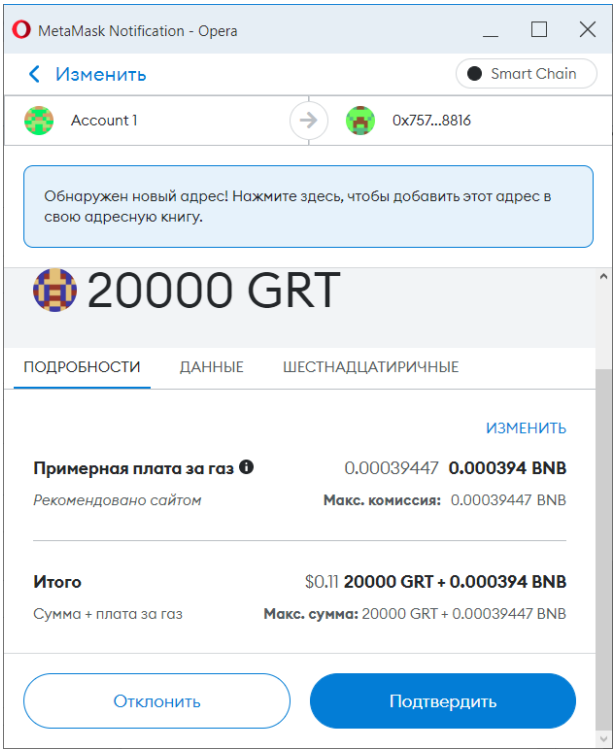


Рисунок 3.18 – Транзакція про трансфер

Після оплати транзакції 20000 токенів були відправлені на адресу іншого гаманця.

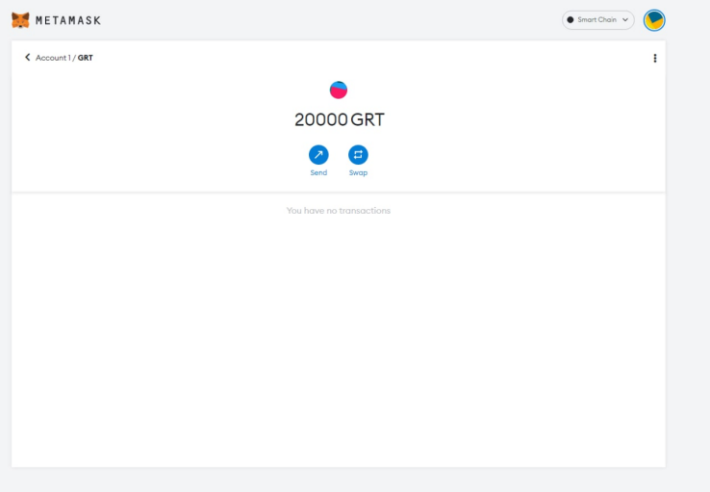


Рисунок 3.19 – Токени успішно прийшли на інший гаманець

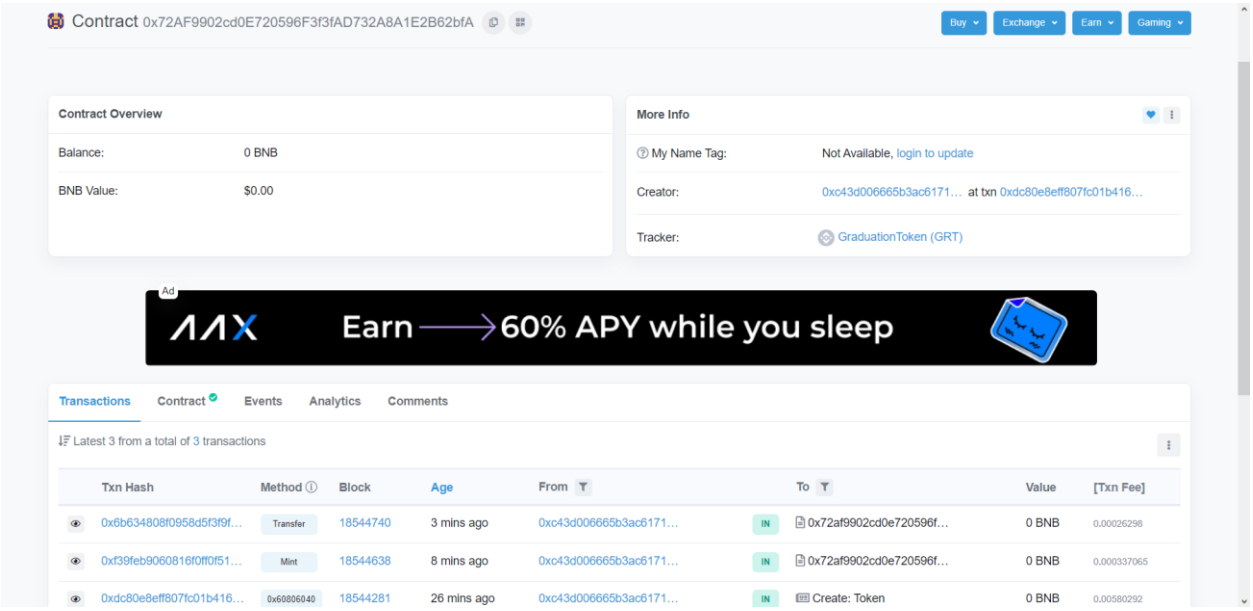


Рисунок 3.21 – Історія транзакцій токену

Повертаючись на головну сторінку смарт-контракту в розділі «Transactions» можна переглянути всі транзакції, які відбувались з даним токеном від моменту його створення.

ВИСНОВОК

Під час виконання кваліфікаційної бакалаврської роботи було:

– проаналізовано методи створення токенів;

– розглянуто регулювання криптовалют, вирішення поставленого завдання та використання їх на практиці;

– сформовано загальні положення та принципи роботи блокчейн-технології;

– виконано ознайомлення зі смарт-контрактами та варіантами їх написання.

– розглянуто токеноміку, як визначну частину будь-якого токену.

Результатом практичної реалізації було написання смарт-контракту, який був протестований за допомогою можливостей віртуальної машини на базі Remix Solidity IDE. Після його успішного тестування відбувся деплой на Binance Smart Chain, а також тестування роботи контракту на справжньому блокчейні. Таким чином виконані всі вимоги, які ставились на етапі проектування – протестований та запущений смарт-контракт токену.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт Міністерства та Комітету цифрової трансформації України. [Електронний ресурс] – Режим доступу до ресурсу: https://thedigital.gov.ua/news/ukraina-legalizuvala-kriptosektor-prezident-pidpisav-profilniy-zakon.
2. Жувагіна І. О., Замарайкін О. В., Будна Т. С. Bitcoin: українські реалії використання криптовалют в сучасних економічних системах. Економіка та держава. 2018. № 6. С. 97-100.
3. Canadian securities regulators outline regulatory framework for compliance for crypto asset trading platforms. [Електронний ресурс] – Режим доступу до ресурсу: https://www.securities-administrators.ca/news/canadian-securities-regulators-outline-regulatory-framework-for-compliance-for-crypto-asset-trading-platforms/.
4. Joint CSA/IIROC Staff Notice 21-329 — Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iiroc.ca/news-and-publications/notices-and-guidance/joint-csaiiroc-staff-notice-21-329-guidance-crypto-asset-trading-platforms-compliance-regulatory.
5. The Division of Examinations' Continued Focus on Digital Asset Securities*. [Електронний ресурс] – Режим доступу до ресурсу: https://www.sec.gov/files/digital-assets-risk-alert.pdf.
6. CFTC Staff Issues Advisory on Virtual Currency for Futures Commission Merchants. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cftc.gov/PressRoom/PressReleases/8291-20.
7. The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transctions. [Електронний ресурс] – Режим доступу до ресурсу: https://home.treasury.gov/news/press-releases/sm1216.

8. CFTC Staff Issues Advisory on Virtual Currency for Futures Commission Merchants. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cftc.gov/PressRoom/PressReleases/8291-20.
9. IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply [Електронний ресурс] – Режим доступу до ресурсу: https://www.irs.gov/newsroom/irs-virtual-currency-guidance.
10. Executive Order on Ensuring Responsible Development of Digital Assets. [Електронний ресурс] – Режим доступу до ресурсу: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.
11. FCA provides clarity on current cryptoassets regulation. [Електронний ресурс] – Режим доступу до ресурсу: https://www.fca.org.uk/news/press-releases/fca-provides-clarity-current-cryptoassets-regulation.
12. New Australian laws to regulate cryptocurrency providers. 11.04.2018 [Електронний ресурс] – Режим доступу до ресурсу: https://www.austrac.gov.au/new-australian-laws-regulate-cryptocurrency-providers.
13. Cryptocurrency and tax. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ato.gov.au/General/Other-languages/In-detail/Information-in-other-languages/Cryptocurrency-and-tax/.
14. The Israeli Securities Authority has ruled that cryptocurrency is a security. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isa.gov.il/מפוקחים%20גופים/Corporations/Staf_Positions/Preliminary_Inquiries/Prospectuses/Documents/T3121.pdf.
15. Unregulated investments. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isa.gov.il/sites/ISAEng/Pages/unregulated-investments.aspx.

16. Наказ про боротьбу з відмивання грошей 2018р. [Електронний ресурс] – Режим доступу до ресурсу: https://perma.cc/JN4X-F7P5.
17. Virtual currencies. [Електронний ресурс] – Режим доступу до ресурсу: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-virtuelle-waehrungen.pdf?la=en.
18. Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology. [Електронний ресурс] – Режим доступу до ресурсу: https://www.newsd.admin.ch/newsd/message/attachments/60601.pdf.
19. Warning about fraudsters claiming to hold KNF authorisation to engage in cryptocurrency exchange. [Електронний ресурс] – Режим доступу до ресурсу: https://www.knf.gov.pl/en/news?articleId=71711&p_id=19#:~:text=In%20the%20light%20of%20the,to%2C%20the%20trade%20in%20cryptocurrencies.
20. In Bitcoin's Orbit: Rival Virtual Currencies Vie for Acceptance. [Електронний ресурс] – Режим доступу до ресурсу: https://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0.
21. W. Dai, "b-money," , 1998. [Електронний ресурс] – Режим доступу до ресурсу: http://www.weidai.com/bmoney.txt.
22. Bitcoin: A Peer-to-Peer Electronic Cash System. [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf.
23. Total Cryptocurrency Market Cap. [Електронний ресурс] – Режим доступу до ресурсу: https://coinmarketcap.com/charts/.
24. Top 100 Crypto Coins by Market Capitalization. [Електронний ресурс] – Режим доступу до ресурсу: https://coinmarketcap.com/coins/.
25. Binance Academy. [Електронний ресурс] – Режим доступу до ресурсу: https://academy.binance.com/en/articles/how-to-create-your-own-cryptocurrency.

26. MLSDev: How to Create a Cryptocurrency: Everything You Need to Know. [Електронний ресурс] – Режим доступу до ресурсу: https://mlsdev.com/blog/how-to-create-your-own-cryptocurrency.
27. What Is Cryptocurrency? [Електронний ресурс] – Режим доступу до ресурсу: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/.
28. Андрей Воленко. В начале была ARPA... // UP Special : журнал. — 2011. — № 3. — С. 46—49.
29. How to Time-Stamp a Digital Document*. [Електронний ресурс] – Режим доступу до ресурсу: https://www.anf.es/pdf/Haber_Stornetta.pdf.
30. Smart Contracts: Building Blocks for Digital Markets Copyright (c) 1996 by Nick Szabo [Електронний ресурс] – Режим доступу до ресурсу: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
31. Smart Contracts By JAKE FRANKENFIELD Updated March 24, 2022 Reviewed by ERIKA RASURE Fact checked by SUZANNE KVILHAUG [Електронний ресурс] – Режим доступу до ресурсу: https://www.investopedia.com/terms/s/smart-contracts.asp.
32. Kolibri Stablecoin. [Електронний ресурс] – Режим доступу до ресурсу: https://kolibri.finance.
33. CoinMarketCap: Terra (LUNA). [Електронний ресурс] – Режим доступу до ресурсу: https://coinmarketcap.com/uk/currencies/terra-luna/.
34. Harbinger. [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/tacoinfra/harbinger.
35. KT1KCYaULopm8i2CBbGF5EHXeXLUr4R6r2dA [Електронний ресурс] – Режим доступу до ресурсу: https://tzkt.io/KT1KCYaULopm8i2CBbGF5EHXeXLUr4R6r2dA/operations/.
36. The Solidity Contract-Oriented Programming Language. [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/ethereum/solidity.

37. Diem: Vision To enable universal access to financial services. [Електронний ресурс] – Режим доступу до ресурсу: https://www.diem.com/en-us/vision/.
38. Stacks Docs: Clarity overview. [Електронний ресурс] – Режим доступу до ресурсу: https://docs.stacks.co/write-smart-contracts/overview.
39. Understanding Tokenomics: The Real Value of Crypto. [Електронний ресурс] – Режим доступу до ресурсу: https://www.finextra.com/blogposting/20638/understanding-tokenomics-the-real-value-of-crypto.

ДОДАТОК А

Код смарт-контракту токена

```
// SPDX-License-Identifier: UNLISCENSED

pragma solidity 0.8.4;

contract Token {
  address payable public owner = payable(msg.sender);
  string public name = "GraduationToken";
  string public symbol = "GRT";
  uint256 public totalSupply = 0;
  uint8 public decimals = 4;

  /*
  Створюється, коли токени передаються з одної адреси до іншої.
  */

  event Transfer(
  address indexed _from,
  address indexed _to,
  uint256 _value
  );

  /*
  Генерується після виклику (approve), для підтвердження.

  Від _spender до _owner.
  */
```

```
event Approval(
  address indexed _owner,
  address indexed _spender,
  uint256 _value
);


//Створює відображення з усіма залишками.

mapping(address => uint256) public balanceOf;

//Створює відображення з усіма надбавками.

mapping(address => mapping(address => uint256)) public allowance;


/*
Передає кількість токенів від адреса виклику до адреси отримувача.

Повертає булеве значення про успіх транзакції.

Викликає подію (Transfer).
*/

function transfer(address _to, uint256 _value)
  public
  returns (bool success)
{
  require(balanceOf [msg.sender] >= _value);
  balanceOf [msg.sender] -= _value;
```

```
  balanceOf [_to] += _value;
  emit Transfer(msg.sender, _to, _value);
  return true;
 }

 /*
 Встановлює кількість токенів `spender` до токенів викликаючого.

 Повертає булеве значення про успіх транзакції.

 Викликає подію (Approval).
 */

 function approve(address _spender, uint256 _value)
  public
  returns (bool success)
 {
  allowance [msg.sender] [_spender] = _value;
  emit Approval(msg.sender, _spender, _value);
  return true;
 }

 /*
 Передає кількість токенів від відправника до отримувача, використовуючи механізм резерву.

 Повертає булеве значення про успіх транзакції.

 Викликає подію (Transfer).
 */
```

```
function transferFrom(
  address _from,
  address _to,
  uint256 _value
) public returns (bool success) {
  require(_value <= balanceOf [_from]);
  require(_value <= allowance [_from] [msg.sender]);
  balanceOf [_from] -= _value;
  balanceOf [_to] += _value;
  allowance [_from] [msg.sender] -= _value;
  emit Transfer(_from, _to, _value);
  return true;
}

/*
Мінтить кількість токенів на адресу.

Виконується лише власником контракту.
*/

function mint(uint256 _amount, address _to) public returns (bool success) {
  require(msg.sender == owner, "Operation unauthorised");

  totalSupply += _amount;
  balanceOf [_to] += _amount;

  emit Transfer(address(0), _to, _amount);
  return true;
}
```

```
  /*
  Спалює кількість токенів.

  Виконується з адреси відправника.
  */

  function burn(uint256 _amount) public returns (bool success) {
   require(msg.sender != address(0), "Invalid burn recipient");
   uint256 accountBalance = balanceOf [msg.sender];
   require(accountBalance > _amount, "Burn amount exceeds balance");
   balanceOf [msg.sender] -= _amount;
   totalSupply -= _amount;
   emit Transfer(msg.sender, address(0), _amount);
   return true;
  }
}
```