Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко
«_____»_____2022 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Мережеві та інтернет технологій»

на тему:

БЛОКЧЕЙН ТЕХНОЛОГІЯ ДЛЯ ВПРОВАДЖЕННЯ Е-ГРИВНІ

Виконав: студент групи МІТм - 21

Ложкін Юрій Володимирович _____
(прізвище ім'я по-батькові) (підпис)

Керівник: доктор технічних наук, доцент кафедри мережевих та інтернет технологій

д.т.н. Плющ Олександр Григорович. _____
(посада, прізвище ім'я по-батькові) (підпис)

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко
«_____»_____2022 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Ложкін Юрій Володимирович
(прізвище, ім'я, по батькові)

1. Тема роботи:

«Блокчейн технологія для впровадження Е-гривні»

затверджена на засіданні кафедри МІТ «31» серпня 2022 р. протокол № 1
2. Термін здачі закінченої роботи «01» грудня 2022р
3. Вихідні дані до проекту (роботи)

Програмне забезпечення для реалізації токена в блокчейн мережі

4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-50 стор.)

1. дослідження технології. структурна концепція blockchain та децентралізація

2. порівняння цільових актуальних систем. рішення для нбу. принцип токенізації завдяки blockchain мережі

3. розробка токену е-гривні на обраній технології. оптимальна блокчейн мережі згідно вимог та теоретичних напрацювань

5. Перелік графічного матеріалу 8-12 слайдів

Блокчейн та інтернет мережі.

Актуальність технології для України.

Вибір технології та потреби України.

Результати роботи .

Висновки

Дата видачі завдання
Керівник роботи д.т.н., доцент МІТ Плющ О.Г.
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий		
2	Розділ 1		
3	Розділ 2		
4	Розділ 3		
5	Доповідь та слайди		
6	Пояснювальна записка		

Здобувач вищої освіти _____
(підпис)
(прізвище, ім'я, по батькові)

Керівник _____
(підпис)
(прізвище, ім'я, по батькові)

РЕФЕРАТ

Пояснювальна записка: ХХ с., ХХ рис., ХХ табл., ХХ додатків, ХХ джерел.

Мета роботи: приклад правильного застосування blockchain мережі для вирішення проблеми довіри. Реалізація власного крипто токена на базі blockchain мережі.

Об'єкт дослідження: проблема ненадійності традиційних систем збереження інформації, проблема довіри між учасниками в мережі Інтернет.

Предмет дослідження: blockchain мережі для вирішення проблеми довіри. Актуальність blockchain технології та перспективи. Актуальність Е-гривні для потреб НБУ.

Наукова новизна: розробка моделі електронної гривні. Офіційних аналогів не представлено. Додає до реальної валюти державного значення цифрову валюту "Е-гривню" номіналом 1:1, відкриту для публічного моніторинга зі швидкими та дешевими транзакціями. Наприклад, оплата по реквізитам займає до 1 робочого дня та потребує додаткових верифікацій від банків, "Е-гривня" виконує транзакцію близько 5 секунд та одразу верифікується, ID транзакції дозволяє будь-кому побачити результат та учасників, що спрямовано на подолання корупції в державних установах та контрактах.

Методи дослідження: теоретичний аналіз blockchain технології, моделювання самої валюти для демонстрації роботи, аналіз транзакцій для пересвідчення правильного функціонування та переваг, емпіричні дослідження роботи, порівняльний аналіз зі звичайними банківськими транзакціями.

Короткий зміст роботи: аналітичний огляд blockchain технології як Distributed Ledger Technology, проблема довіри в мережі та загальна модель blockchain як рішення, актуальність технології та приклади використання, аналізі правового сектору та вибір інструменту для реалізації, рекомендації та власне

бачення реалізації , реалізація крипто токена, тестування та порівняння результатів.

Ключові слова: БЛОКЧЕЙН, DLT, ЦИФРОВІЗАЦІЯ, ДЕЦЕНТРАЛІЗАЦІЯ, ДОВІРА, КРИПТОВАЛЮТНИЙ ТОКЕН, ЦИФРОВА ВАЛЮТА, КРИПТОВАЛЮТНА ТРАНЗАКЦІЯ, РОЗПОДІЛЕНІ ДАНІ.

ABSTRACT

Explanatory note: XX p., XX figures, XX tables, XX appendices, XX sources.

Purpose of work: an example of the correct application of blockchain network to solve the problem of trust. Implementation of own crypto token based on blockchain network.

Object of research: the problem of invalidity of traditional information storage systems, the problem of trust between participants in the Internet.

The subject of research: Blockchain networks to solve the problem of trust. Relevance of blockchain technology and prospects. Relevance of E-hryvnia for the needs of the NBU.

Scientific novelty: development of the electronic hryvnia model. No official analogues are presented. It adds to the real currency of state importance the digital currency "E-hryvnia" with a nominal value of 1:1, open for public monitoring with fast and cheap transactions. For example, payment by requisites takes up to 1 working day and requires additional verifications from banks, "E-hryvnia" performs a transaction in about 5 seconds and is immediately verified, transaction ID allows anyone to see the result and participants, which is aimed at overcoming corruption in public institutions and contracts.

Research methods: theoretical analysis of blockchain technology, modeling of the currency itself to demonstrate the work, analysis of transactions to verify the correct functioning and benefits, empirical research of work, comparative analysis with conventional banking transactions.

Summary of the work: analytical overview of blockchain technology as Distributed Ledger Technology, the problem of trust in the network and the general model of blockchain as a solution, the relevance of the technology and examples of use, analysis of the legal sector and the choice of tool for implementation, recommendations

and own vision of implementation, implementation of crypto token, testing and comparison of results.

Keywords: BLOCKCHAIN, DLT, DIGITALIZATION, DECENTRALIZATION, TRUST, CRYPTOCURRENCY TOKEN, DIGITAL CURRENCY, CRYPTOCURRENCY TRANSACTION, DISTRIBUTED DATA

ЗМІСТ

РЕФЕРАТ 4
ABSTRACT 6
ЗМІСТ 8
ВСТУП 10
1 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ. СТРУКТУРНА КОНЦЕПЦІЯ BLOCKCHAIN ТА ДЕЦЕНТРАЛІЗАЦІЯ 12
1.1 Як і для чого виник blockchain 12
1.1.1 Загальна історія появи технології 12
1.1.2 Хронологія популяризації технології 12
1.2 Поняття про технологію 15
1.2.1 Термінологія 15
1.2.2 Distributed Ledger Technology 16
1.2.3 Базова архітектура blockchain мережі 17
1.3 Принципи blockchain. Порівняння з Інтернетом та переваги. 20
1.4 Децентралізовані системи 22
1.4.1 Концепція та переваги 22
1.4.2 Обмеження та проблеми 24
2 ПОРІВНЯННЯ ЦІЛЬОВИХ АКТУАЛЬНИХ СИСТЕМ. РІШЕННЯ ДЛЯ НБУ. ПРИНЦИП ТОКЕНІЗАЦІЇ ЗАВДЯКИ BLOCKCHAIN МЕРЕЖІ 27
2.1 Аналіз існуючих блокчейн підходів для позиціонування валютного токена 27
2.1.1 Рівні блокчейну(Layers) 0, 1, 2, 3 27
2.1.2 Публічні блокчейни 32
2.1.3 Приватні блокчейни 34
2.2 Проблематика токенізації активів 37
2.2.1. Чому токенізація і що це таке. 37
2.2.2. Відмінність токенізації від оцифровки. 39
2.2.3 Що таке платформа токенізації 40
2.2.4 Базові принципи та можливості токенізації 41

2.3 Вибір блокчейн технології для банківських рішень та відбір необхідної для втілення Е-гривні 43
2.3.1 Для чого взагалі потрібно рішення не власної розробки 43
2.3.2 Очікування Національного банку України та рішення Міністерства цифрової трансформації України 46
3 РОЗРОБКА ТОКЕНУ Е-ГРИВНІ НА ОБРАНІЙ ТЕХНОЛОГІЇ. ОПТИМАЛЬНА БЛОКЧЕЙН МЕРЕЖІ ЗГІДНО ВИМОГ ТА ТЕОРЕТИЧНИХ НАПРАЦЮВАНЬ 50
3.1 Вибір мережі. Публічні популярні рішення для банківських сфер 50
3.2 Stellar як blochain рішення для фінансових задач 51
3.3 Покрокова розробка токена Е-гривня та тестування транзакцій 53
3.3.1 Створення аккаунта емітента, дистриб'ютора та випадкового користувача 53
3.3.2 Встановлення рівня довіри до емітента та емісії токена 57
3.3.3 Тестування здійснення транзакції та перерахування коштів 61
ВИСНОВКИ 65
ПЕРЕЛІК ПОСИЛАНЬ ТА ВИКОРИСТАНІ ДЖЕРЕЛА 67
ДОДАТКИ 69

ВСТУП

У 2021 році Президент України - Володимир Зеленський підписав Закон України № 1591-IX “Про платіжні послуги” [1] та в 2022 підписав закон, який ще не набрав чинності, але дає орієнтир економічного напрямку - Закон України № 2074-IX “Про віртуальні активи” у якому описаний правовий статус криптоактивів та криптовалют в Україні [2]. У лютому 2020 року Національний Банк України на міжнародній конференції “CBDC2020” вперше на офіційному рівні заговорив про створення так званої “Е-гривні” - офіційної цифрової валюти від Національного Банку України на базі blockchain технологій.

У процесі написання цієї роботи , 28.11.2022 НБУ презентував офіційну концепцію Е-гривні [3] для представників банків, небанківських фінансових установ та ринку віртуальних активів, для подальшого спільного обговорення проєкту.

Від того часу проект був заморожений, а розробки, якщо і велись, були непублічними або формальними. Я, вже користуючись blockchain мережами декілька років та оцінивши їх модель роботи, захист, швидкість та інші параметри, вирішив, що нереалізована “Е-гривня” є дуже вдалим інструментом для прозорого використання державних коштів, підприємницької діяльності, моніторингу податкової сфери та інших сфер української економіки. Саме через факт заморозки такої розробки, я хочу її реалізувати, аби актуалізувати, популяризувати рішення та продемонструвати свої навички, як розробника так і навички оцінки трендів потреб в IT сфері.

Кожен криптотокен можна назвати унікальною розробкою, адже це в цьому полягає суть, що скопіювати, змінити , замінити його не вийде, хіба відтворити інший токен з таким ж функціоналом. Тому говорячи про унікальність розробки необхідно звернутись до більш абстрактних розробок, які мають такі ж принципи. Офіційних аналогів та реалізацій “Е-гривні” ще не має, інші держави також не створювали свою офіційну валюту в blockchain мережах, проте є країни, які

прийняли існуючу криптовалюту офіційним платіжним засобом. Наприклад, Сальвадор перша в світі країна , яка дозволяє розраховуватись Біткоіном за будь-які послуги [4]. Важливість такого прикладу в тому , що криптовалютні рішення вже втілюються та тестуються , збитки від власних невдалих тестів можуть бути непідйомні, а мережа Біткоіна доводить свою стабільність , з 2011 року вона функціонує без збоїв , незважаючи на несчисленні кількості та різновиди атак на неї консенсус мережі не був порушений, а час напрацювання тільки підсилює математичне сподівання в результат надійності.

Тема blockchain індустрії здобуває популярність завдяки криптовалютам та через це нажаль в більшості людей асоціюється з ризиковими активами , валютними спекуляціями , фінансовими махінаціями та подібним. Насправді ж blockchain мережі мають значно ширший сенс та значення для користувачів, можливо планетарного масштабу , оскільки більшість людей на Землі , користується інтернетом , а blockchain дозволяє побороти проблеми довіри та зробити усіх рівноправними та рівноважливими. Коли багатьма рівноправність та відсутність третіх сторін вважається утопією , blockchain вже з 2011 року тільки доводить теорію практичними напрацюваннями та фактичними досягненнями.

Робота має на меті продемонструвати простоту та ефективність функціонування валюти з допомогою blockchain мереж , популяризувати технологію серед людей , висвітлити переваги цифровізації державних активів та фінансів. Звернутись до проблематики довіри в мережі Інтернет , показати можливість рішення. Презентувати один з багатьох можливих підходів для використання blockchain технології , як рішення актуальних проблем між користувачами , у вигляді інтерфейсу для прозорої фінансової взаємодії в напрямках держава - держава , держава - громадяни , громадяни-громадяни.

1 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ. СТРУКТУРНА КОНЦЕПЦІЯ BLOCKCHAIN ТА ДЕЦЕНТРАЛІЗАЦІЯ

1.1 Як і для чого виник blockchain

1.1.1 Загальна історія появи технології

Ідея технології blockchain почала зароджуватись ще в 1980-х, а перший подібний до blockchain протокол був представлений 1982 року американським криптографом Девідом Чаумом, в своїй дисертації “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”[5]. Далі вже безпосередньо blockchain як технологія була описана в 1991 році , вчені-дослідники Стюарт Хабер та Скотт Шторнетта впровадили та описали обчислювально-практичне рішення для цифрових документів зі штампом часу, щоб вони не могли бути оформлені заднім числом і підробитись. Система використовувала криптографічно захищений ланцюг блоків [6]. Вже в 1992 році до проекту доєднався Дейв Бейер та було вдосконалено технологію з допомогою дерева хешів , що збільшило ефективність , дозволяючи збирати декілька документів в один блок [7]. Але ця технологія не здобула моментальної популярності , а патент втрачено в 2004, за 4 роки до створення рушійного потяга технології - Біткоіна.

1.1.2 Хронологія популяризації технології

Хоч і blockchain далеко не тільки про Біткоін , але факт залишається таким , що існування, тестування технології та довіра до неї завдячує саме Біткоіну, його стрімкій історії розвитку та зах.

Першочергово Біткоін був покращенням концепції b-money (вигадана Вей Даєм в 1999 році , де сервери мусили внести гарантійний внесок в нечітко

розкритий механізм) та технології bitgold (описаної в 2005 році Ніком Самбо , яка просувала ідею використання доказів на основі математичних розрахунків)

Хронологія технології 1977-2005 рік: період до появи Біткоіна та його винахідника.

1977: перший опис шифрування RSA, в якому використовується відкритий ключ для шифрування конфіденційних даних і закритий ключ для їх розшифровки.

1979: Ральф Меркле створив механізм стиснення «дерево Меркле». Він використовується для ефективного та безпечного зберігання та перевірки великих обсягів даних і використовується в протоколі біткоін, щоб обчислити корінь Меркле всіх операцій, що містяться в блоці даних.

1990: американський математик Девід Шаум винайшов DigiCash - електронну валюту (централізовану і власну) на основі криптографічних протоколів

1992: Скотт Ванстоун (Certicom) запропонував з алгоритм ECDSA (Elliptic curve digital signature algorithm), який використовує більш короткі ключі і дозволить виконувати операції підпису та шифрування швидше, ніж RSA.

1994: Нік Сабо висунув ідею смарт-контракту, чи розумного договору.

18 липня 1996 року: NSA публікує доповідь під назвою «Як виробляти валюту: криптографія анонімної електронної готівки»

1997: Адам Бек створив HashCash - систему підтвердження виконання роботи на базі ідеї, висунутої Стітією Дворк і Моні Наором в доповіді, яка опублікована в 1993 році, Pricing via Processing or Combatting Junk Mail.

Пізніше Адам Бок став першим партнером Сатосі Накамото

1998: банкрутство DigiCash. Вей Дай подовжує ідею цифрової готівки на основі регістру, розподіленого по розсилочній відомості The Cypherpunks.

1999: Шон Феннінг у співпраці з Napster винайшов технологію peer to peer (P2P) (Рівний рівному, або однорангову). Платформа обміну аудіофайлами

Napster працювала з центральним сервером (farm), який грав роль центрального реєстру всіх файлів, які належать учасникам або запитувані ними (рівними партнерами). У цій централізованій системі сформувалася єдина точка відмови (Single Point of Failure - SPOF) платформи Napster, і сайт був закритий ФБР у 2001 році за порушення прав інтелектуальної власності.

2000 : Том Пепер і Джастін Франкель розробили Gnutella - першу повністю розподілену платформу для передачі даних файлів P2P.

1998-2005 роки:Hix Сабо розробляє проект BitGold- децентралізовану цифрову валюту, засновану на стійких до фальсифікацій ланцюжках підтвердження про завершення роботи, в якій були використані багато елементів, які врешті-решт увійшли в біткоін: автоматичне проставлення дати і часу, електронні підписи, відкриті ключі... Проте система виявилася надто вразливою до атак.

2004 рік: розробка Ripplepay -спроба створити децентралізовану валютну систему.

2007-2010 роки: поява блокчейна біткоін та його валюти біткоін.

19 серпня 2008 року: Сатосі Накамото зарезервував доменне ім'я bitcoin.org.

31 жовтня 2008 року: було оголошено про появу біткоіну. Сатосі Накамото опублікував статтю Bitcoin: A Peer-to-Peer Electronic Cash System, в якій представив метод розв'язання криптографічного завдання, над яким багато хто бився протягом кількох десятиліть - проблеми подвійної оплати, або завдання візантійських генералів. Ця проблема заважала двом контрагентам обмінюватися активами, зокрема грішми, без участі довіреної особи.

3 січня 2009: створюється перший блок (вихідний блок).

12 січня 2009 року: перша біткоін-транзакція.

Лютий 2009 року: Сатосі Накамото поширює першу версію програми Bitcoin на сайті P2P Foundation і створює перші біткоіни.

2009 та 2010 рік: Сатосі Накамото розробляє та створює біткоін та програмне забезпечення Bitcoin-Qt.

Середина 2010 року: розробники та спільнота Bitcoin поступово втрачають контакт із Сатосі Накамото.

12 грудня 2010: Накамото написав останнє повідомлення на форумі Bitcointalk.

Незадовго до зникнення Накамото назначає Гевіна Андресена наступником, передавши йому доступ до проекту Bitcoin на SourceForge і копію аварійного ключа - унікальний особистий криптографічний ключ, який дозволяє зменшити наслідки потенційної атаки на системи біткоіна - наприклад, в разі виявлення вразливостей, що дозволяють заднім числом змінити операції, або захоплення більше 51% вузлів мережі. Оператори вузлів мережі можуть при отриманні попередження сповістити своїх користувачів або зупинити всі реєстрації договорів.

1.2 Поняття про технологію

1.2.1 Термінологія

Дати визначення blockchain в короткому змістовному терміні важко, оскільки кожен вкладе в термінологію свій досвід, знання та буде сприймати не обов’язково відповідно думці автора. Blockchain (англ. Blockchain) , як поняття вже обросло багатьма термінами, основним, на мою думку, можна вважати поняття від 2008 року анонімного розробника мережі біткоін Сатоші Накамото:

Blockchain[8] (від первинного англ. block chain - ланцюг блоків) - ланцюг блоків, кожен з яких посилається на блок , який йому передував. Найскладніший для відтворення ланцюг - найкращий blockchain.

Для більш точного і широкого розуміння нижче можна розділити по наростаючій термінології [9] по Лоран Лелу.

- *Спрощене*: Blockchain - велика бухгалтерська книга, або журнал, куди кожен може вносити записи і кожен може прочитати, розподілена по величезній кількості комп’ютерів по всьому світу.

- *Базове*: Blockchain - програмний продукт, який дозволяє зберігати і перетворювати дані за допомогою Інтернету захищеним і прозорим способом , не маючи при цьому центрального керуючого органу.

- *Буквальне*: Blockchain описує ланцюг блоків (числових контейнерів) , у яких зберігається інформація різного виду : транзакції, контракти, документи про власність, витвори мистецтва і т.д.

- *Узагальнене*: Blockchain - технологія, яка використовується в додатках для тразакцій нового покоління, яка завдяки алгоритму колективного консенсуса і розподіленому децентралізованому журналу, створює довіру, відповідальність і прозорість серед всіх учасників.

Від себе я ще б додав уточенння , що blockchain - це частина (рис. 1) ще більшої технології , яка має назву: Distributed Ledger Technology

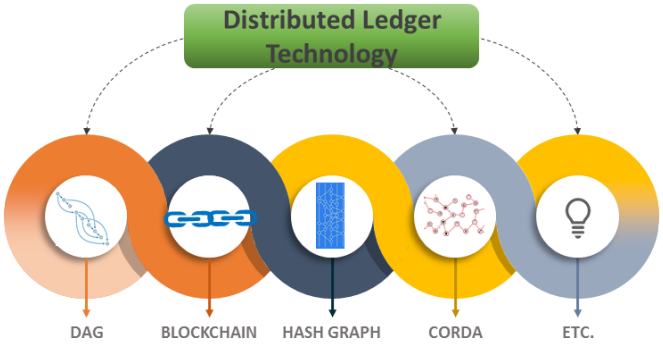
1.2.2 Distributed Ledger Technology

Оскільки blockchain це лише частина DLT (рис. 1) варто розглянути і це поняття. Distributed Ledger Technology - технологія розподіленого реєстру , яка дозволяє спільно записувати та використовувати дані в мережах.

У своєму розумінні технологія передбачає консенсус реплікованих , спільних та синхронізованих цифрових даних , які географічно рознесені на багато місць в різних частинах Землі, що забезпечує завадостійкість, не має єдиного центрального адміністратора і не має точки відмови [10].

Усі вузли в такій технології тісно зв’язані між собою, можуть вносити зміни в реєстр (незалежно від інших) , після чого усі вузли голосують і при досягнені консенсуса реєстр доповняється новими даними.

Першим ефективним і повністю робочим прикладом DLT вважається саме blockchain.



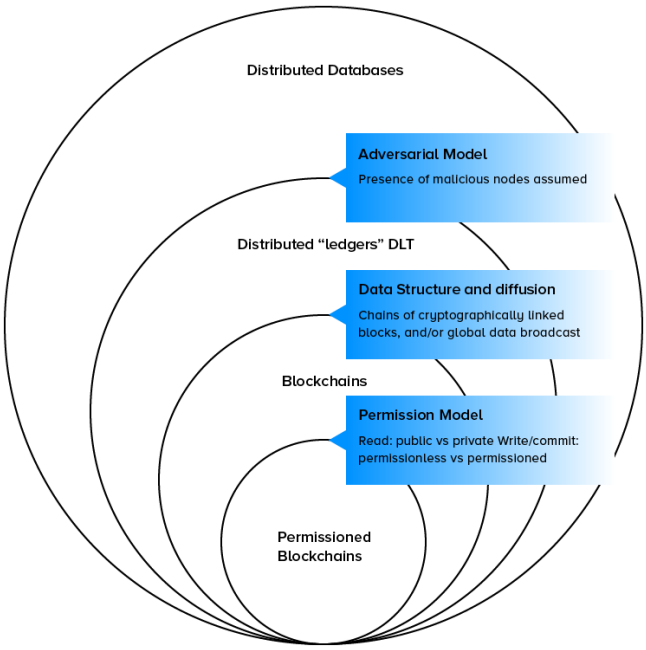


Рисунок 1.1 Blockchain частина DLT

1.2.3 Базова архітектура blockchain мережі

Блокчейн - це децентралізована, розподілена база даних, яка дозволяє декільком сторонам безпечно зберігати і передавати дані без необхідності в центральному органі. Вона складається з ланцюжка блоків, кожен з яких містить перелік транзакцій, які були перевірені та додані до блокчейну. Базова архітектура мережі блокчейн включає наступні компоненти:

● Блоки: Кожен блок в ланцюжку містить унікальний код, який називається "хеш", що відрізняє його від інших блоків. Він також включає хеш попереднього блоку, що створює ланцюжок блоків, який не може бути змінений , бо зміна призводить до утворення нового ланцюга (рис. 1.2) . Крім хешу, кожен блок може містити інші дані, такі як мітка часу і список транзакцій.

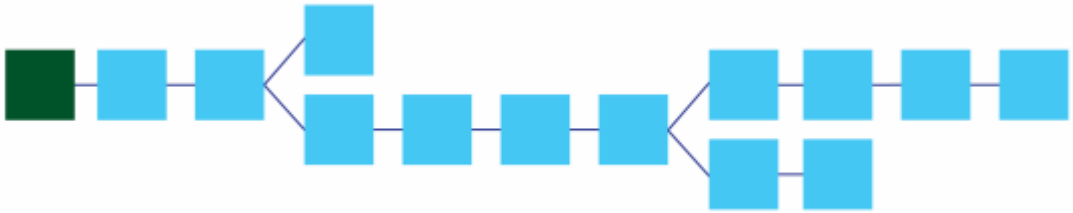


Рисунок 1.2 Організація бази даних в системах, що використовують технологію blockchain

● Ноди: Ноди - це комп'ютери, які беруть участь в мережі блокчейн і підтримують копію реєстру. Існує два типи вузлів: повні вузли і полегшені вузли. Повні вузли зберігають всю історію транзакцій і підтверджують нові транзакції, в той час як полегшені вузли зберігають тільки останні транзакції і покладаються на повні вузли для перевірки.

● Алгоритм консенсусу: Алгоритм консенсусу - це набір правил, яких дотримуються вузли для перевірки транзакцій (рис. 1.3) і додавання їх до реєстру. Найпоширенішим алгоритмом консенсусу є алгоритм доказу роботи, в якому вузли змагаються у вирішенні складної математичної задачі, і той, хто першим її вирішить, отримує право додати наступний блок до ланцюжка. Інші алгоритми консенсусу включають доказ частки, в якому вузли вибираються для підтвердження транзакцій на основі їх частки в мережі, і делегований доказ частки, в якому вузли вибираються для підтвердження транзакцій на основі голосів, які вони отримують від інших вузлів.

Рисунок 1.3 Досягнення консенсусу в мережі

- Майнінг: Процес додавання транзакцій в блокчейн називається майнінгом. Майнери, які є вузлами, що беруть участь в алгоритмі консенсусу, використовують потужні комп'ютери для перевірки транзакцій і вирішення математичної задачі. Коли майнер успішно додає блок до ланцюжка, він отримує винагороду у вигляді певної кількості одиниць криптовалюти.

- Криптографія: Криптографія - це практика безпечного спілкування в присутності третіх осіб. У мережі блокчейн криптографія використовується для захисту даних в блоках і гарантує, що транзакції не можуть бути змінені після їх додавання в ланцюжок. Це досягається шляхом використання криптографічних хеш-функцій, які приймають вхідні дані будь-якого розміру і видають вихідні дані фіксованого розміру, які є унікальними для цих вхідних даних.

В цілому, базова архітектура мережі блокчейн дозволяє створити децентралізовану, безпечну та прозору систему для запису та перевірки транзакцій. Вона має потенціал революціонізувати широкий спектр галузей, включаючи фінанси, управління ланцюгами поставок та системи голосування

1.3 Принципи blockchain. Порівняння з Інтернетом та переваги.

Через стрімкий розвиток та популярність Bitcoin масово виникає порівняння блокчейн мереж із мережею Інтернет (рис. 1.4). Звучать тези про те , що блокчейн витіснить чи замінить інтернет. Ця думка є популярною але не вірною. Вірне твердження буде таким , що блокчейн мережі це доповнення до звичного усім Інтернету. Блокчейн доповнює та оновлює принципи роботи в мережі інтернет , а не конкурує з ними. Тобто блокчейн не може функціонувати без інтернету , а інтернет без блочейну здається неповною технологією для взаємодії між будь-якими кінцевими точками.

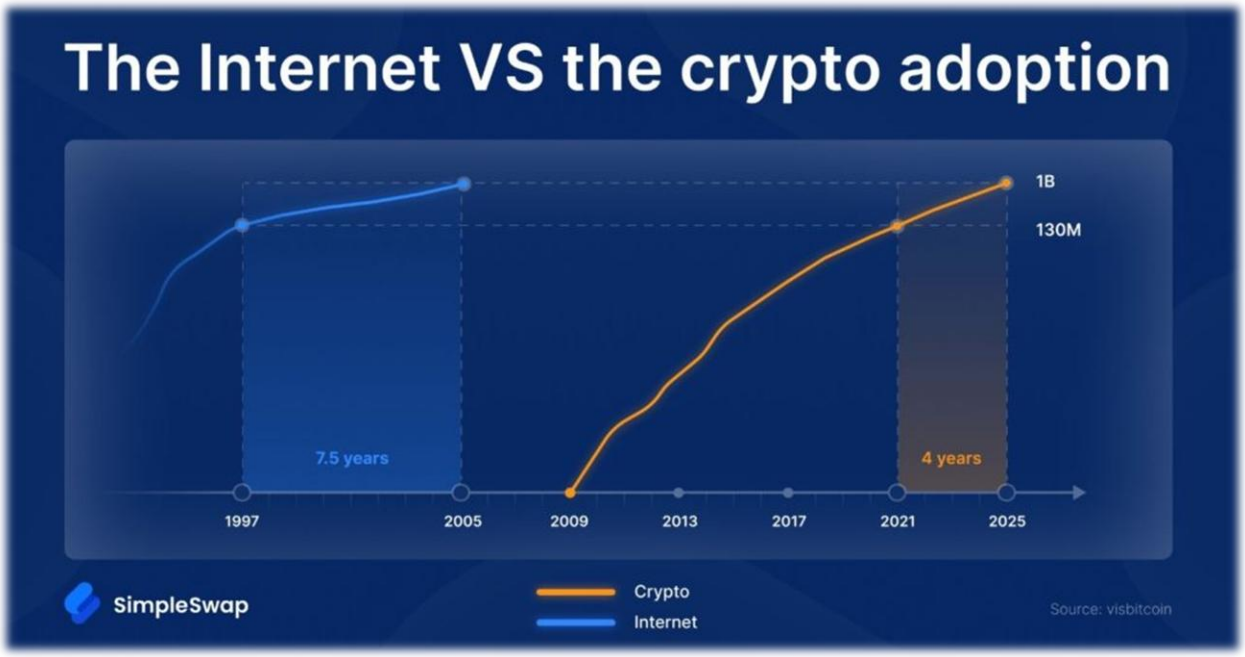


Рисунок 1.4 Порівняння кількості користувачів інтернету та криптовалют.

Основні принципи, на яких базується blockchain, наступні :

- *Розподілений регістр 2.0* , побудований по моделі книги обліку і розподілений між кожним учасником.
- *Децентралізація та відмова від посередників:* blockchain не контролюється ніяким центральним органом, в цій довірчому системі стосунків між двома учасниками немає третіх осіб.

- *Консенсус*: Факт прийняття транзакції або відмови від неї є результатом розподіленого консенсусу, а не рішення деякого централізованого інституту.
- *Незмінність і стійкість* : Неможливо змінити або знищити записи.
- *Розподілена довіра і прозорість* : Розділяються дані, операції і консенсус.

Важливо зазначити : blockchain не обмежується тільки на Bitcoin чи Ethereum та інших криптовалютах. Єдиного блокчейну поки не існує, тілкьи їх різноманітні типи які існують незалежно та навіть можуть взаємодіяти між собою.

Таким чином, у blockchain можуть виявлятися специфічні технічні особливості використання його з тими або іншими застосуваннями.

Технологія blockchain може міняти правила гри : менше централізації, менше влади, більше розподілення. Таким чином, blockchain несе в собі інфраструктуру розподіленої алгоритмічної довіри, або консенсус на вимогу.

Саме завдяки цим властивим інфраструктурі аспектам численні спостерігачі порівнювали blockchain з Інтернетом, але в результаті пришли до висновку, що він перевершить.

У моєму баченні blockchain стане таким ж популярним , як інтернет , оскільки не перечить йому , а доповнює технологію, звернемось до порівняння в таблиці 1.1 .

Таблиця 1.1 - Порівняння Інтернету так Блокчейн мережі.

Інтернет мережа	***Блокчейн мережа***
Дозволяє автоматизувати зв’язки (і встановлення зв’язків та спілкування)	Дозволяє автоматизувати транзакції, скасувавши треті сторони
Система децентралізованої публікації	Система розподіленої довіри

Інфраструктура публікацій	Інфраструктура підтвердження прав доступу
Зробив революційні досягнення в: Міжособове спілкування; Автоматична публікація; Електронна комерція; Соціальні мережі.	Робить революційні досягнення в: Децентралізація; Довіра; Оборот цінностей без посередників; Цифрова власність та віртуальна реальність.

1.4 Децентралізовані системи

1.4.1 Концепція та переваги

Було 2 жабки, одну кинули в окріп - вона випригнула та вижила, іншу поливали тепліюшою водою поступово і вона зварились заживо.

Едвард Сноуден

Децентралізація - це концепція, за якою система, додаток або мережа працює незалежно від якого-небудь центрального органу управління чи контролю (рис. 1.5). Децентралізація в даній роботі є фундаментальним принципом блокчейн-технологій. Але не усі блокчейн мережі є децентралізованими.

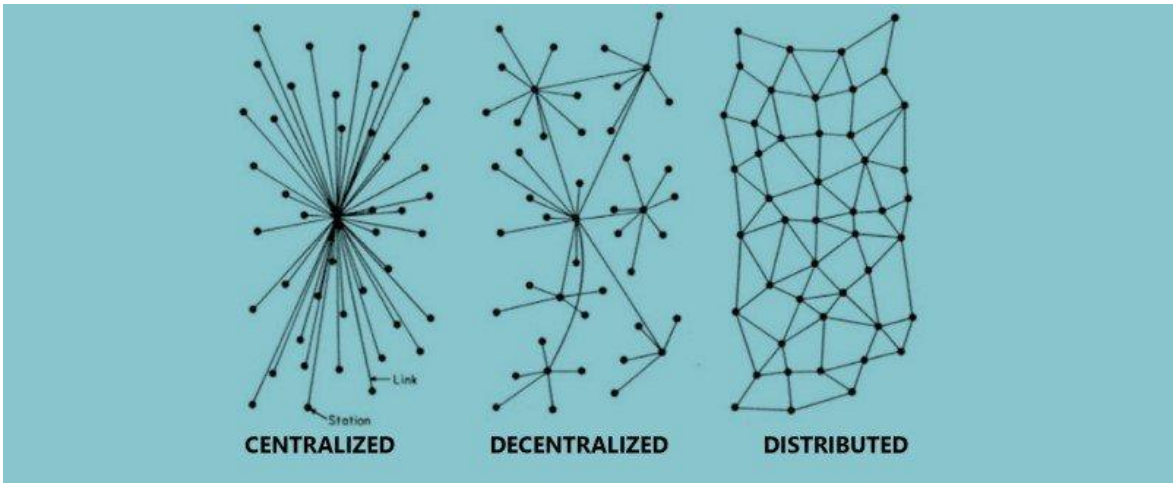


Рисунок 1.5 Види систем в залежності від способу взаємодії користувачів між собою

Децентралізація є протилежним до централізації процесом і передбачає розподілення функцій системи (зберігання даних, обчислення тощо) між її учасниками, причому без єдиного керуючого органу. Важливо розуміти, що це поняття можна застосувати далеко поза межами інформаційних технологій, і воно вже давно використовується в таких галузях суспільного життя як політика, менеджмент, юриспруденція, економіка тощо. Саме слово децентралізація увійшло у вжиток в 1820-і рр.

У теорії передачі даних децентралізація передбачає створення умов, за яких зникає потреба в існуванні центрального сервера, а учасники мережі мають однаковий ранг. Децентралізація також має місце і у глобальній мережі Інтернет, маршрутизатори якої працюють незалежно один від одного. У більшості випадків існує більше одного маршруту доставки пакета даних, а вихід з ладу одного з маршрутизаторів не є критичним для користувачів.

Централізовані системи та ієрархічні моделі управління, що застосовуються в них, мають низку недоліків. Наприклад, будь-яка централізована соціальна мережа, подібна до Facebook, має можливість здійснювати цензуру та блокувати акаунти користувачів. Непрозорість процесів, які відбуваються у централізованих інформаційних системах, не залишає клієнтам можливості доведення факту порушення конфіденційності їх приватних даних. Такий стан речей дозволяє власникам системи навіть модифікувати історію змін на свій розсуд, у тому числі заднім числом. Очевидно, що в таких системах процес прийняття рішень носить суб’єктивний характер.

Децентралізована система передбачає наявність великої кількості незалежних учасників, які спільно здійснюють управління процесами. Подібний підхід вимагає від учасників узгоджених дій, що потрібні для досить ефективної взаємодії за відсутності

Переваги концепції:

- Незалежність від якоїсь єдиної точки вразливості, контролю.

- Надійність завдяки відсутності точки вразливості.
- Прозорість даних у відкритому доступі, що дозволяє усім перевірити точність ті цілісність.
- Безпека системи завдяки розподіленому ризику і відповідальності між багатьма учасниками.
- Стійкість до цензури ускладнює маніпулювання даними та цільову пропаганду , оскільки потребує консенсусу в мережі.

Важливо розуміти, що децентралізація вже доступна, але штучно стримується через непопулярність серед не технічного суспільства. Популяризація концепції працює на довгострокову виграшну стратегію для людей. Відповідальність освічених людей глобалізувати кращі технології.

1.4.2 Обмеження та проблеми

Поряд з беззаперечними перевагами (які, у свою чергу, залежать від рівня децентралізації системи), у децентралізованих системах наявні деякі обмеження.

Перше з них полягає у відсутності служби підтримки (за визначенням), яка здатна вплинути на акаунти користувачів або транзакції. Це означає, що якщо ви випадково відправили транзакцію,і вона була додана до загальної бази даних, то вам буде нікуди звернутися за відшкодуванням, виправдовуючи це тим, що транзакція була випадковою.

Другим обмеженням є підвищена вартість підтримки системи. З плином часу база даних тільки зростає у розмірі. Це означає, що кожен її учасник повинен відводити все більше і більше ресурсів для зберігання та обробки даних.

Третім обмеженням є складність реалізації на децентралізованих платформах деяких функцій, що доступні централізованим системам.В якості прикладу можна навести підрахунок статистики чи оцінку стану системи у конкретний момент часу

Фактори, які вповільнюють впровадження децентралізованих систем :

- Складнощі оновлення протоколу

Складність впровадження будь-якого оновлення протоколу взаємодії у децентралізованому середовищі полягає в тому, що запропоноване оновлення повинно бути підтримано більшістю активних вузлів мережі. Для цього стороні, що пропонує оновлення, необхідно довести необхідність його впровадження решті вузлів системи, що само собою є дуже складним завданням.

- Проблема відповідальності

Проблема відповідальності. Будь-яке рішення в децентралізованій системі є результатом згоди більшості учасників (обраних певним чином). Тому не існує єдиної сторони, яка могла б скасувати рішення, прийняте спільно, або нав'язати своє. Але якщо користувач з власної неуважності все-таки стане жертвою шахраїв, то йому нікуди буде скаржитися, бо в загальному випадку немає відповідальної сторони та будь-яких гарантій. Тут йде мова саме про прийняття ризиків самими користувачами. А розрахунок цих ризиків є досить складним процесом

- Складний процес монетизації розробки

Монетизувати централізовану систему зазвичай легше, ніж децентралізовану. Так відбувається, тому що централізована система більш керована та може мати юридичну підтримку, оскільки адміністрація системи відповідальна за ведення діяльності в межах правового поля. При таких умовах простіше побудувати бізнес-модель і монетизувати проект. У децентралізованій системі, навпаки, досить складно ввести ефективну цензуру, забезпечити захист авторського права та контролювати використання сервісу. Створюються умови, в яких стає набагато складніше підтримувати діяльність системи у рамках правового поля. Тому розробникам протоколів децентралізованих систем складно навіть мати прибуток зі своїх проектів

- Надлишковість і високі вимоги до обладнання
- Проблема масштабованості

У разі використання механізму розподіленого прийняття рішень, потрібно, щоб всі учасники обмінялися новими даними та погодилися, які з них вважати правильними. Пропускна здатність облікової системи знижується з ростом кількості валідаторів (рис. 1.6). Децентралізовані системи також стикаються з необхідністю зберігання надлишкового обсягу даних і високими вимогами до обладнання.

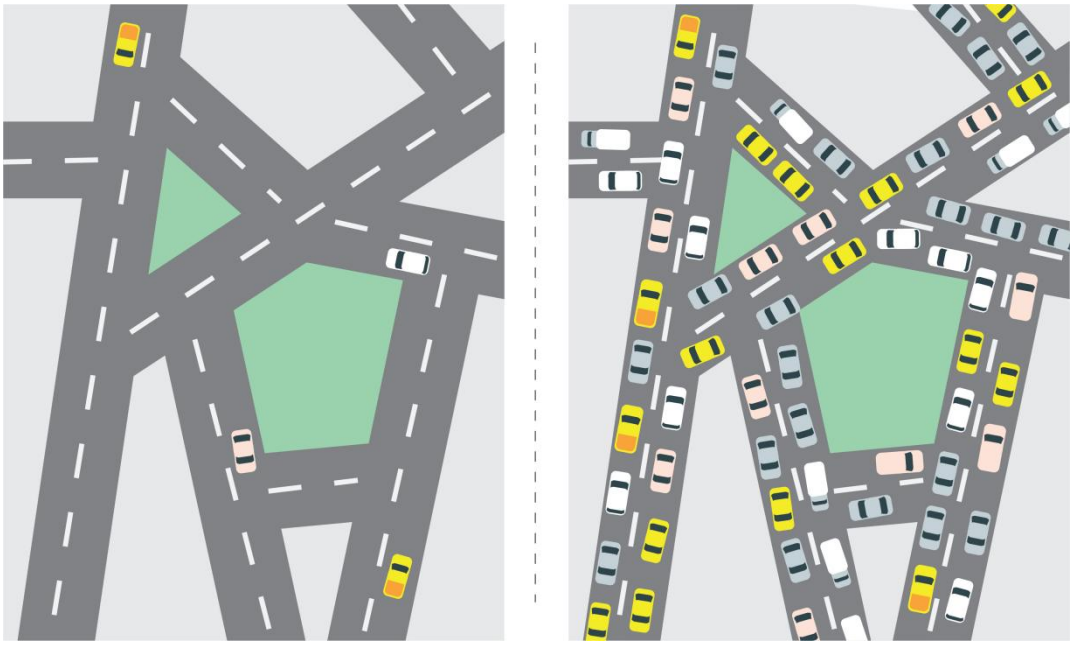


Рисунок 1.6 Приклад зниження пропускної здатності системи у зв’язку зі збільшенням кількості її користувачів

2 ПОРІВНЯННЯ ЦІЛЬОВИХ АКТУАЛЬНИХ СИСТЕМ. РІШЕННЯ ДЛЯ НБУ. ПРИНЦИП ТОКЕНІЗАЦІЇ ЗАВДЯКИ BLOCKCHAIN МЕРЕЖІ

2.1 Аналіз існуючих блокчейн підходів для позиціонування валютного токена

2.1.1 Рівні блокчейну(Layers) 0, 1, 2, 3

Рівні блокчейну(Layers) 0, 1, 2 і 3 - це терміни, що використовуються для опису різних аспектів технології блокчейн (рис. 2.1). Ці рівні формально не визначені і не стандартизовані, і конкретні визначення можуть відрізнятися в залежності від контексту.

Однак при сучасній розробці та презентаціях криптопроектів усі користуються такою термінологію , тому варто її також формалізувати .

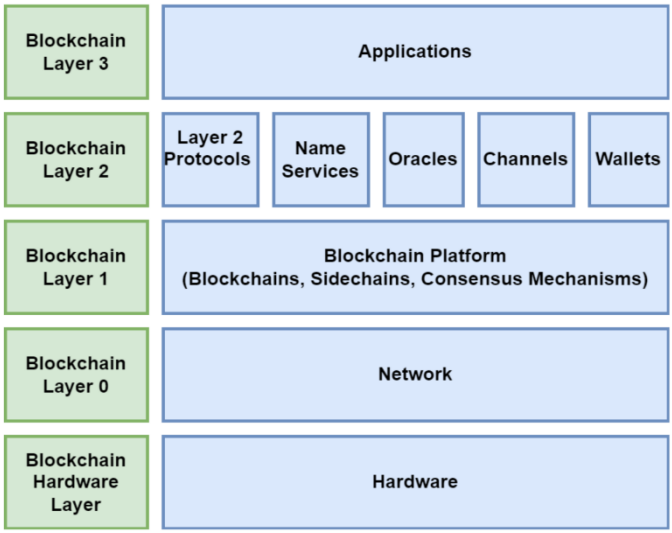


Рисунок 2.1 Візуалізація Blochain layers

Більш детальне пояснення кожного рівня не затиснуто в конкретні рамки термінології та виглядає приблизно так:

Рівень 0: відноситься до фізичної інфраструктури або апаратного забезпечення, яке підтримує блокчейн. Сюди входять сервери, комп'ютери та інші пристрої, на яких розміщується програмне забезпечення блокчейну та зберігаються дані. Сюди також входить інфраструктура, яка підтримує зв'язок і синхронізацію вузлів у мережі блокчейн.

У децентралізованій мережі блокчейн вузли, з яких складається мережа, розподілені по різних місцях і, як правило, управляються волонтерами або організаціями. Ці вузли спілкуються один з одним за допомогою однорангового протоколу і працюють разом для перевірки і передачі транзакцій, а також для досягнення консенсусу щодо стану блокчейну. Апаратне та програмне забезпечення, яке використовується для роботи вузлів, вважається частиною 0-го рівня.

Рівень 0 є основою блокчейну, і він має важливе значення для роботи і безпеки мережі. Апаратне забезпечення та інфраструктура, що використовуються на рівні 0, повинні бути надійними і безпечними, щоб забезпечити цілісність і доступність блокчейну. Однак, рівень 0 також є найбільш вразливим до атак і збоїв, оскільки він є точкою входу для зовнішніх загроз, таких як хакери або шкідливе програмне забезпечення. Таким чином, важливо забезпечити належний захист та обслуговування апаратного та програмного забезпечення, що використовується на рівні 0

Рівень 1: відноситься до основних протоколів і механізмів консенсусу, які формують основу блокчейну. До них відносяться правила перевірки транзакцій і додавання блоків в ланцюжок, а також алгоритми і механізми, що використовуються для досягнення консенсусу щодо стану блокчейна.

У децентралізованій мережі блокчейн вузли, з яких складається мережа, спілкуються один з одним за допомогою однорангового протоколу і спільно працюють над перевіркою і передачею транзакцій, а також над досягненням консенсусу щодо стану блокчейну. Правила і механізми, які регулюють цей процес, вважаються частиною рівня 1.

Різні блокчейн-платформи використовують різні алгоритми консенсусу, такі як доказ роботи, доказ частки та інші. Ці алгоритми визначають, як нові блоки додаються в ланцюжок і як вузли в мережі досягають консенсусу щодо стану блокчейну. Вони є ключовою частиною першого рівня і відіграють вирішальну роль у безпеці та децентралізації блокчейну.

Рівень 1 є базовою основою блокчейну і має важливе значення для роботи і безпеки мережі. Він визначає правила і механізми, які регулюють перевірку і додавання нових блоків до ланцюжка, а також процес досягнення консенсусу щодо стану блокчейну. Таким чином, важливо забезпечити, щоб протоколи і механізми, які використовуються на рівні 1, були безпечними, ефективними і децентралізованими.

Рівень 2: відноситься до протоколів або технологій, які надбудовуються над основними протоколами блокчейну для додавання нових можливостей або поліпшення масштабованості і продуктивності. Ці технології працюють за межами основних протоколів блокчейну і можуть пропонувати додаткову функціональність або більш ефективні способи використання блокчейну.

Прикладами технологій другого рівня є платіжні канали, які дозволяють користувачам здійснювати безліч платежів без необхідності транслювати кожну транзакцію на всю мережу; сайдчейни, які дозволяють користувачам передавати активи між різними платформами блокчейну без необхідності використовувати централізовану біржу; і шардинг, який ділить блокчейн на менші частини (шарди) для збільшення пропускної здатності і зниження навантаження на окремі вузли.

Технології другого рівня можуть використовуватися для усунення деяких обмежень масштабованості та продуктивності основних протоколів блокчейну, оскільки вони дозволяють користувачам здійснювати транзакції та взаємодіяти з блокчейном більш ефективно. Вони також можуть надавати додаткову функціональність, яка недоступна в основних протоколах, наприклад, можливість проводити позамережеві транзакції або передавати активи між різними платформами блокчейну.

Технології другого рівня не є необхідними для функціонування блокчейну, але вони можуть бути корисними для підвищення продуктивності і можливостей блокчейну для конкретних додатків або випадків використання. Важливо ретельно зважити компроміси і ризики, пов'язані з використанням технологій другого рівня, оскільки вони можуть внести додаткову складність і потенційні точки відмови.

Рівень 3: Третій рівень блокчейну - це додатки та сервіси, які використовують блокчейн як платформу для створення нових продуктів та послуг. Вони можуть включати криптовалютні гаманці, платформи децентралізованих фінансів (DeFi), ринки прогнозування та інші види програмного забезпечення, які використовують можливості блокчейну. Ці додатки побудовані на основі основних протоколів блокчейну і можуть запропонувати користувачам широкий спектр можливостей і функціональності.

Додатки третього рівня можуть використовуватися для доступу і взаємодії з блокчейном різними способами, наприклад, шляхом відправки і отримання транзакцій, створення і управління смарт-контрактами або доступу до децентралізованих додатків (DApps). Вони також можуть надавати додаткові можливості і функціональність, такі як можливість відстежувати і управляти криптовалютними портфелями, брати участь в децентралізованих фінансових ринках або отримувати доступ до ринків прогнозування.

Додатки 3-го рівня не є обов'язковими для роботи блокчейну, але вони можуть надавати користувачам широкий спектр корисних інструментів і послуг. Важливо ретельно розглянути питання безпеки та надійності додатків третього рівня, оскільки вони можуть створювати додаткові точки відмови і можуть залежати від базової інфраструктури блокчейну для належного функціонування.

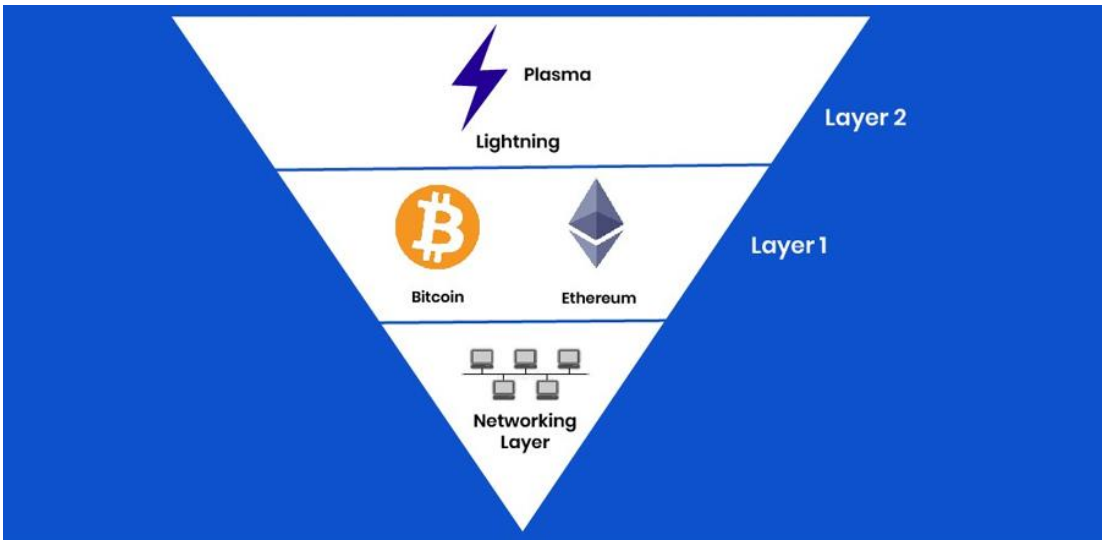


Рисунок 2.2 Приклади рівнів блокчейн мережі

Отже, наше рішення також буде якимось рівнем, це буде залежати від обраної для нього бази та його функціоналу. Із прикладів існуючих рішень (рис. 2.3.) це буде щось біля третього рівня.

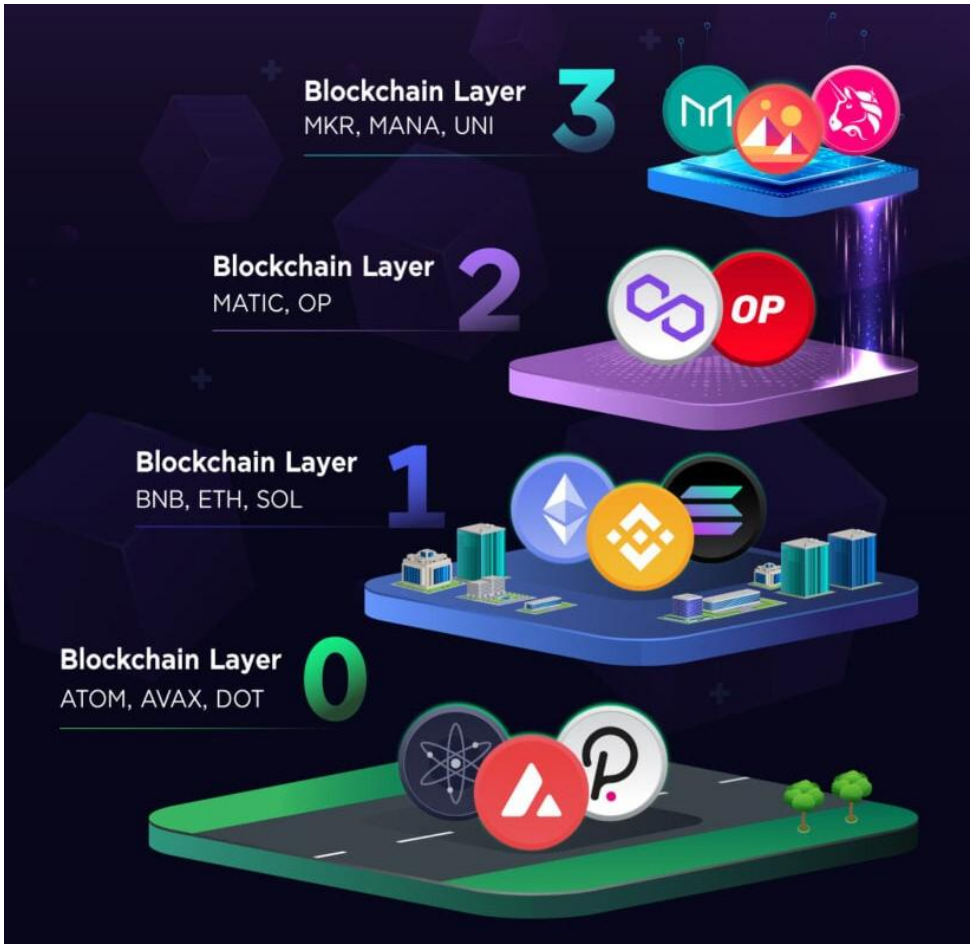


Рисунок 2.3 готові проекти на блокчейни посортовані відповідно рівнів

2.1.2 Публічні блокчейни

Технології з часом та розвитком потреб розділились на приватні блокчейн мережі та публічні блокчейн мережі, як спосіб задоволення різних потреб та варіантів використання . Публічні блокчейни також відомі як permissionless (рис. 2.4).

Як публічні, так і приватні блокчейни мають свої переваги та недоліки, і вони підходять для різних випадків використання.

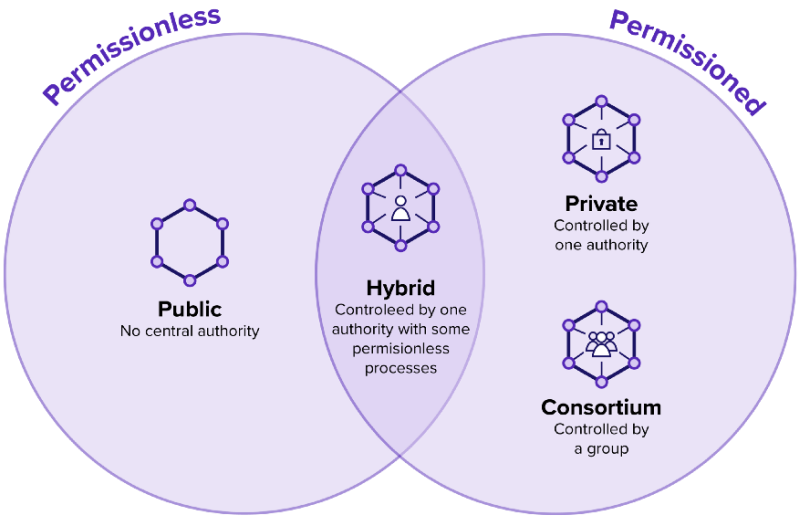


Рисунок 2.4 Типи блокчейнів за правом доступу

Публічні блокчейни - це децентралізовані мережі, до яких може приєднатися та брати участь будь-хто. Вони, як правило, не потребують дозволу, що означає, що будь-хто може читати, писати і підтверджувати транзакції в блокчейні без необхідності отримання дозволу або схвалення.

Публічні блокчейни підтримуються мережею вузлів, які працюють разом для перевірки і передачі транзакцій, а також для досягнення консенсусу щодо стану блокчейну. Вузли в мережі публічного блокчейну, як правило, управляються волонтерами або організаціями, і вони розподілені по декількох місцях. Така децентралізація ускладнює втручання будь-якої окремої особи в дані блокчейну, оскільки для цього необхідне схвалення більшості вузлів мережі.

Як і всі рішення технологія публічних блокчейнів має свої переваги та недоліки.

Серед ***переваг*** публічних блокчейнів варто виділити наступні:

- ✓ *Деценралізація:* Публічні блокчейни є децентралізованими мережами, що означає, що вони не контролюються жодним органом влади або організацією. Це робить їх стійкими до цензури та фальсифікації, оскільки для внесення будь-яких змін до блокчейну потрібна згода більшості вузлів мережі.

- ✓ *Безпека:* Публічні блокчейни використовують криптографічні методи та механізми консенсусу для забезпечення безпеки та цілісності даних у блокчейні. Транзакції підтверджуються та реєструються у прозорий спосіб, який можна перевірити, що ускладнює зміну даних у блокчейні будь-яким окремим суб'єктом.

- ✓ *Прозорість:* Публічні блокчейни є відкритими та прозорими, що означає, що будь-хто може переглядати транзакції та дані в блокчейні. Це може сприяти підвищенню довіри та підзвітності, оскільки всі транзакції реєструються на постійній основі та піддаються перевірці.

- ✓ *Доступність:* Публічні блокчейни є відкритими та доступними для будь-кого, що означає, що будь-хто може брати участь у мережі та використовувати можливості блокчейну. Це може сприяти просуванню інновацій та заохочувати розробку нових додатків і послуг.

Втім, публічні блокчейни мають і певні ***недоліки***, в тому числі:

- ■ *Масштабованість:* Публічні блокчейни можуть мати обмеження щодо масштабування, оскільки вони зазвичай вимагають, щоб всі вузли в мережі підтверджували та передавали кожну транзакцію. Це може призвести до уповільнення швидкості транзакцій і підвищення комісійних, оскільки мережа зростає в розмірах.

- *Продуктивність:* Публічні блокчейни можуть мати обмеження по продуктивності, оскільки децентралізований характер мережі може ускладнити оновлення і поліпшення базових протоколів.

- *Відсутність конфіденційності:* Публічні блокчейни є прозорими, що означає, що будь-хто може переглядати транзакції та дані в блокчейні. Це може бути недоліком для користувачів, які цінують свою конфіденційність, оскільки всі транзакції є загальнодоступними.

Публічні блокчейни часто використовуються для фінансових транзакцій, наприклад, у випадку криптовалют, оскільки вони пропонують безпечний і прозорий спосіб зберігання та перевірки фінансових записів. Вони також можуть використовуватися для інших цілей, таких як відстеження права власності на активи або автоматизація контрактів та інших процесів за допомогою смарт-контрактів.

Деякі приклади відомих публічних блокчейнів включають Bitcoin, Ethereum та Litecoin. Це все децентралізовані платформи, які використовують технологію блокчейн для зберігання та перевірки фінансових транзакцій. Існує також багато інших типів публічних блокчейнів, які використовуються для різних цілей, таких як управління ланцюгами поставок, системи голосування та перевірка особи.

Загалом, переваги та недоліки публічних блокчейнів залежать від конкретного випадку використання та потреб користувачів. Публічні блокчейни можуть бути потужним інструментом для зберігання та перевірки даних у безпечний та прозорий спосіб, але вони можуть не підходити для всіх застосувань або галузей.

2.1.3 Приватні блокчейни

Приватні блокчейни, також відомі як permissioned (рис. 2.4), є системами розподіленого реєстру, які не є відкритими для широкої громадськості. Замість цього, доступ до приватного блокчейну обмежується обраною групою осіб або організацій, які зазвичай отримують дозвіл на участь у мережі від адміністраторів блокчейну.

На противагу публічним блокчейнам переваги та недоліки здавалися б очевидними(рис. 2.5) , але не все так поверхнево, тому варто виділити і їх особливості.

Серед ***переваг*** приватних блокчейнів варто виділити наступні:

- ✓ *Безпека:* Оскільки приватні блокчейни мають обмежену базу користувачів, вони, як правило, вважаються більш безпечними, ніж публічні блокчейни. Це пов'язано з тим, що існує менший ризик несанкціонованого доступу або зловмисної діяльності в мережі.
- ✓ *Швидкість і ефективність:* Приватні блокчейни часто використовують інший механізм консенсусу, ніж публічні блокчейни, що може зробити їх швидшими та ефективнішими. Це може бути особливо корисно для додатків, які вимагають високої швидкості транзакцій або низьких транзакційних витрат.
- ✓ *Налаштовуваність:* Приватні блокчейни можуть бути налаштовані для задоволення конкретних потреб і вимог організації або групи користувачів. Це дозволяє адаптувати їх до конкретного випадку використання і може зробити їх більш ефективними та дієвими.

Відповідні приватним блокчейнам ***недоліки*** будуть наступні :

- ■ *Обмежений доступ:* Оскільки приватні блокчейни мають обмежену базу користувачів, вони, як правило, вважаються більш безпечними, ніж публічні блокчейни. Це пов'язано з тим, що існує менший ризик несанкціонованого доступу або зловмисної діяльності в мережі.
- ■ *Централізація:* Приватні блокчейни можуть бути більш централізованими, ніж публічні блокчейни, оскільки мережа, як правило, контролюється одним суб'єктом або групою суб'єктів. Це може зробити їх більш вразливими до цензури і може обмежити їх здатність досягти справжньої децентралізації.

- *Відсутність прозорості:* Приватні блокчейни можуть не забезпечувати такий же рівень прозорості, як публічні блокчейни, оскільки вони не є відкритими для широкої громадськості. Це може ускладнити перевірку цілісності даних в блокчейні та обмежити їх використання в певних додатках.

Однією з ключових відмінностей між публічними та приватними блокчейнами є те, що останні, як правило, використовують механізм консенсусу, який спирається на довіру та авторитет вузлів-учасників, а не вимагає алгоритму підтвердження роботи або підтвердження частки для підтвердження транзакцій. Це означає, що приватні блокчейни часто можуть досягати більшої швидкості транзакцій і менших витрат, ніж публічні блокчейни, але можуть не пропонувати такий же рівень безпеки і децентралізації.

Приватні блокчейни часто використовуються в бізнесі та на підприємствах, де метою є створення безпечного та ефективного способу для групи довірених осіб обмінюватися даними та здійснювати транзакції. Приватні блокчейни пропонують деякі з тих же переваг, що і публічні блокчейни, такі як незмінність, прозорість і децентралізація, але з додатковою безпекою і контролем, який забезпечується обмеженою базою користувачів.

Деякі приклади приватних блокчейнів включають Hyperledger Fabric, Corda та Quorum.

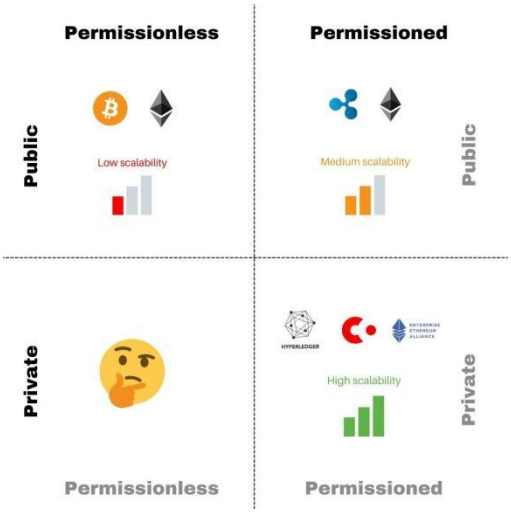


Рисунок 2.5 Площина переваг та недоліків блокчейнів від типу доступу.

2.2 Проблематика токенізації активів

2.2.1. Чому токенізація і що це таке.

Від самого початку слово токен використовувалося, коли люди говорили про випуск проектами власних монет. У цих випадках токен являв собою право власності, що створюється і передається в межах облікової системи, що може знаходитися як під управлінням однієї компанії, так і групи незалежних валідаторів. Якщо ця облікова система стає основним джерелом інформації для визначення права власності на певний актив, то він називається токенізованим.

Мета токенізації полягає у пришвидшенні та підвищенні безпеки роботи з активами [11].

Токенізація – це процес трансформації облікової системи, що полягає у тому, що всі баланси знаходяться під управлінням користувачів за допомогою криптографічних ключів, і право власності на актив надається у вигляді цифрового токену.

Якщо замислитися, з токенами ми знайомі досить давно. Ваучер на одну стрижку в перукарні також можна вважати токеном. Ще один приклад – жетон в метрополітені. Навіть долар США до моменту,коли відмінили золотий стандарт, також був токеном, який мав на увазі право на відповідну кількість золота.

Термін токен може вживатися у контексті автентифікації – так називають деякі ідентифікатори чи секрети, що використовуються для електронної автентифікації. Токен може бути представлений у вигляді бітового рядка чи у вигляді фізичного пристрою для підтвердження доступу до відповідних систем, інформаційних ресурсів тощо. Далі спробуємо надати більш чітке і компромісне визначення токену як цифрового активу.

Токен (як цифровий актив) – це одиниця обліку, що використовується для представлення цифрового балансу в деякому активі, причому володіння токеном

доводиться за допомогою криптографічних механізмів, наприклад цифрового підпису [12].

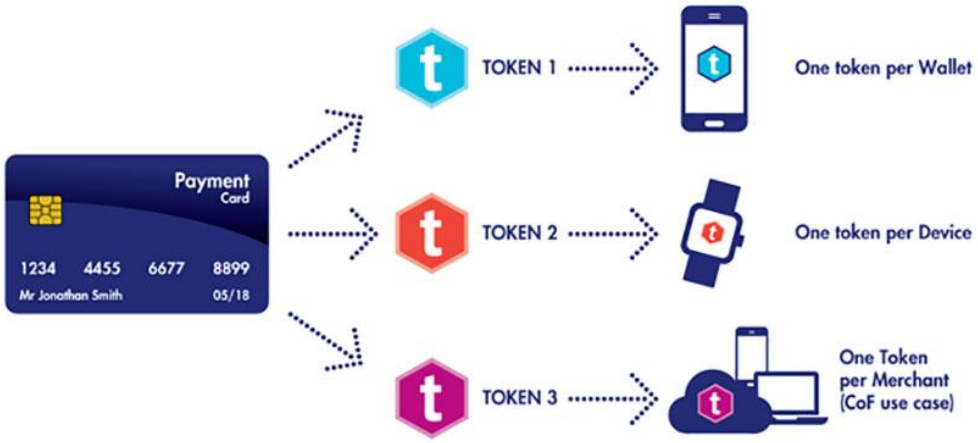


Рисунок 2.6 Токенізація платіжних засобів

Токени та токенізація можуть бути розглянуті на чотирьох концептуально різних рівнях:

- *Рівень користувача*. Власнику токена надається юридичне право власності на відповідний актив. Він також може швидко і надійно передати це право іншим користувачам, не переміщуючи при цьому сам актив. Передбачається, що власники токенів визнають законність і унікальність конкретного реєстру, в якому ведеться облік токенів. Також вони повинні довіряти хранителю фізичних активів (у випадку, якщо токен закріплюється саме фізичним активом).

- *Рівень бізнес-процесів*. Насамперед токенізація передбачає наявність заснованого на blockchain реєстрі прав власності. Передача токена з рук у руки означає зміну власника ресурса з внесенням відповідного запису до реєстру, який вважається основним джерелом інформації для всіх користувачів системи

- *Рівень IT-інфраструктури*. У цьому випадку токен можна розглядати в якості підходу до запису в реєстрі, що відображає баланс користувача в системі. У той же час з токеном пов’язані функції резервного копіювання

даних, управління ролями та інфраструктурою в цілому, перевірки цілісності історії транзакцій і ведення автоматичного аудиту в режимі реального часу

- *Рівень технології.* Токен є структурою акаунту, де всі поля захищені за допомогою криптографічних механізмів, таких як цифровий підпис, zero-knowledge proofs тощо. Кожен акаунт самостійно підтримує операції, пов'язані з оновленням його стану, визначає набір можливих транзакцій, модель їхнього життєвого циклу, правила обробки тощо.

2.2.2. Відмінність токенізації від оцифровки.

Звичайної оцифровки документів, рахунків і прав власності недостатньо, щоб вийшла самодостатня автоматизована облікова система, яку можна використовувати повністю віддалено. Токенізація трансформує управління активами: модель виконання заявок оператором (наприклад, у банку) змінюється на модель прямого управління активом за допомогою криптографічних механізмів. Основною відмінністю є виключення ролі (наприклад, адміністратора чи модуля, що працює з відповідними дозволами), яка може напряму змінювати баланс на рахунках користувачів. Саме на цьому базується модель системи, що побудована за принципом виконання замовлень. Токенізація передбачає, що користувачі контролюють свої баланси за допомогою криптографічних ключів, які ніхто інший (в т. ч. адміністратори) не знає.

Також є принципова різниця між реєстром справжності і реєстром прав власності. Реєстр справжності пов'язує відповідний актив (наприклад, дизайнерську сумку) із його виробником і дозволяє перевірити справжність цього об'єкту. Цей реєстр містить лише об'єкти (без їхніх поточних власників). Реєстр прав власності є інформаційним ресурсом, що містить дані про існуючі і минулі права власності на конкретні активи.

2.2.3 Що таке платформа токенізації

Платформа токенізації – це сукупність компонентів, які дозволяють проводити облік та операції з певним активом за допомогою використовування цифрового токена, а також забезпечити безпеку його зберігання, обробки та управління.

Компоненти платформи токенізації наступні:

- реєстр;
- внутрішня платіжна система;
- внутрішня біржа;
- модуль управління аккаунтами;
- шлюзи та інтеграційні модулі;
- гаманці;
- модуль управління адмініструванням

Щоб знизити ризик шахрайства та змови, різні (іноді незалежні)суб'єкти повинні виконувати різні типи дій. Отже існує набір ролей,які повинні підтримуватися платформою токенізації. Найважливішими з них є валідатор, аудитор, хранитель, емітент і адміністратор.

Валідатор підтримує нормальне функціонування системи у відповідності до протоколу обліку токенів. Роль валідатора може виконувати як окрема людина, так і ціла організація.

Аудитор є призначеною стороною, яка має право перевіряти транзакції, і саме аудитор натискає на «тривожну кнопку», якщо помічає щось підозріле. Аудитор зберігає повну копію реєстру транзакцій і перевіряє законність дій, що відбуваються на платформі.

Хранитель (custodian) – це особа, що відповідає за надання зовнішніх активів, які токенізовані на платформі (якщо вони є). Ця роль є дуже важливою, оскільки IT-платформа самостійно не може запобігти крадіжці.

Емітент є стороною, що здійснює емісію на підставі даних, отриманих від хранителя (у деяких випадках ролі емітента і хранителя можуть виконуватися однією стороною). Токени можуть випускатися або централізованим (суму, яку необхідно видати, призначає відповідальна сторона), або децентралізованим (декілька валідаторів досягають консенсусу відносно кількості токенів, що потрібно випустити) чином.

Адміністратор приймає рішення згідно оновлення і налаштування платформи, а також щодо налаштування бізнес- правил.

2.2.4 Базові принципи та можливості токенізації

Для правильно функціювання і досягнення переваг токенізації необхідно аби були дотримані наступні принципи:

- ❖ Пряме управління активом за його власником
- ❖ Надійний і автоматизований аудит усієї історії транзакцій
- ❖ Розподілення відповідальності за управління процесами на платформі згідно ролей
- ❖ Підвищення відмовостійкості інструментів зберігання, передачі та обміну активів
- ❖ Відкритість специфікації облікової системи і цифрових гаманців
- ❖ Відокремлення процесів зберігання активу від процесів управління активами

За рахунок технічних особливостей нової інфраструктури з’являється низка нових можливостей.

- ✓ Створення глобальних децентралізованих реєстрів даних.

- ✓ Створення щільно інтегрованих систем, що мають високу модульність і розподілення відповідальності за роботу кожного конкретного модуля.
- ✓ Простий аудит системи обліку в режимі реального часу.
- ✓ Переміщення активів і торгівля ними в Інтернеті без меж (можливість створення Фінансового Інтернету)

Також вагомою можливістю , яку надає токенізація є прозорість облікової системи. За допомогою платформи токенізації можна побудувати прозорі бізнес-процеси. Як показує практика, ефективнішим є попередження нечесної поведінки, а не боротьба з нею. Платформа токенізації може працювати за жорсткими правилами, метою яких є запобігання злонамірних дій. У межах такої облікової системи партнери по бізнесу завжди можуть перевірити дії один одного.

Що більше незалежних валідаторів в обліковій системі, тим стійкіша вона до відмов у роботі. Оскільки локальні копії синхронізуються в режимі реального часу і автоматично створюються резервні копії, токенізація підвищує надійність системи.

Тому можна заявити , що токенізація є новим трендом вдосконалення облікових систем і відповідної інфраструктури (IT infrastructure) в цілому.Платформи токенізації надають свої переваги при роботі з цифровими активами: прозорість їхнього обліку, простий аудит,надійність зберігання та синхронізації даних між валідаторами облікової системи, а також можливість доведення цілісності і незмінності цих даних. Завдяки цим властивостям можна створювати облікові системи, в яких довіра між сторонами не обов’язкова –чесність їхньої поведінки буде гарантуватися правилами системи.Тому логічно припустити, що в майбутньому всі активи будуть токенізованими.

2.3 Вибір блокчейн технології для банківських рішень та відбір необхідної для втілення Е-гривні

2.3.1 Для чого взагалі потрібно рішення не власної розробки

У розділі 2.1 цієї роботи було описано про рівні блокчейн мереж та їх типи по доступу. Тепер необхідно виділити потреби перед технологією яка буде задовільняти потреби *державної* валюти.

На мою думку, існує кілька потенційних переваг використання технології блокчейн для державної валюти:

- ✓ *Підвищення безпеки:* Технологія блокчейн пропонує безпечну і децентралізовану платформу для проведення транзакцій, що може зробити її менш вразливою до шахрайства, хакерства та інших видів фінансових злочинів.
- ✓ *Швидші та дешевші транзакції:* Використовуючи блокчейн, транзакції можуть оброблятися швидше і з меншими комісіями, в порівнянні з традиційними фінансовими системами. Це може полегшити фізичним та юридичним особам проведення фінансових операцій, особливо в транскордонному або міжнародному середовищі.
- ✓ *Підвищення прозорості:* Технологія блокчейн забезпечує прозорий і незмінний запис транзакцій, що може підвищити загальну прозорість і підзвітність фінансової системи.
- ✓ *Покращена фінансова інклюзія:* Використання валюти на основі блокчейну може полегшити фізичним та юридичним особам, які проживають у районах з недостатнім рівнем банківського обслуговування, доступ до фінансових послуг та участь у світовій економіці.
- ✓ *Підвищення фінансової стабільності:* Децентралізований характер технології блокчейн може зробити її більш стійкою до ринкових коливань та інших зовнішніх факторів, які можуть вплинути на стабільність валюти.

Однак важливо зазначити, що існують також потенційні виклики та ризики, пов'язані з використанням валюти, заснованої на блокчейні, і для держави було б важливо ретельно розглянути ці питання, перш ніж приймати таку систему.

Отже , для будови ефективної валютної системи необхідно виконати такі вимоги , аби використати усі переваги , або їх можливий максимум.

При побудові власної системи від держави layer 0 або layer 1 необхідні величезні ресурси як людські так і грошові, а змісту особливого не має.

Переваги власного рішення :

1. *Налагоджуваність(Customizability)*:Коли ви створюєте свій власний блокчейн, у вас є можливість гнучко налаштувати його відповідно до ваших конкретних потреб і вимог. Це може бути особливо корисно, якщо у вас є унікальні або спеціалізовані вимоги, які не можуть бути задоволені існуючими блокчейн-платформами.

2. *Контроль*: Створення власного блокчейну дає вам більше контролю над мережею, включаючи можливість встановлювати правила і структуру управління. Це може бути важливо, якщо ви хочете забезпечити відповідність мережі вашим бізнес-цілям і цінностям.

3. *Право власності*: Коли ви створюєте власний блокчейн, ви володієте і контролюєте мережу, що може бути важливо для бізнесу, який хоче підтримувати високий рівень контролю і автономії.

Недоліки побудови власного блокчейну:

1. *Вартість*: створення блокчейну з нуля може бути дорогим, оскільки вимагає значних ресурсів і досвіду. Це може бути суттєвим недоліком для підприємств, які не мають бюджету або ресурсів для інвестування в створення власного блокчейну.

2. *Час*: Створення блокчейну з нуля також може зайняти багато часу, оскільки вимагає тривалого планування, розробки та тестування. Це може бути недоліком для підприємств, яким потрібно рухатися швидко або які

мають обмежений час і ресурси, щоб присвятити їх створенню власного блокчейну.

3. *Відсутність підтримки спільноти*: Коли ви створюєте власний блокчейн, у вас може не бути підтримки і ресурсів великої спільноти розробників і користувачів, які доступні на встановлених блокчейн-платформах. Це може ускладнити отримання допомоги у вирішенні проблем або доступ до ресурсів та інструментів, які можуть допомогти вам у створенні та підтримці вашого блокчейну.

Переваги використання готового блокчейну:

1. *Вартість і час*: Використання готового блокчейну може бути швидшим і економічно ефективнішим, ніж створення його з нуля, оскільки дозволяє використовувати ресурси і досвід існуючої платформи.

2. *Підтримка спільноти*: Створені блокчейн-платформи часто мають великі і активні спільноти розробників і користувачів, які можуть надати цінну підтримку і ресурси для створення і підтримки ваших додатків.

3. *Безпека*: Готові блокчейни часто мають більш тривалий послужний список і були ретельно протестовані і розглянуті спільнотою, що може забезпечити більш високий рівень безпеки в порівнянні з користувацьким блокчейном, який ще не отримав широкого поширення.

Недоліки використання готового блокчейну.

1. *Відсутність можливості кастомізації:* Коли ви використовуєте готовий блокчейн, ви можете бути обмежені в своїх можливостях налаштувати його для задоволення ваших конкретних потреб і вимог.

2. *Відсутність контролю*: Використання готового блокчейну означає, що у вас менше контролю над мережею, оскільки ви повинні дотримуватися правил і структури управління, встановлених платформою.

3. *Залежність*: Коли ви використовуєте готовий блокчейн, ви стаєте залежними від платформи та її розробників щодо оновлень, обслуговування та

підтримки. Це може бути недоліком, якщо платформа не відповідає вашим бізнес-цілям або якщо у неї виникають якісь проблеми або простої.

У підсумку моє рішення все ж суб'єктивне, але усі недоліки використання готового блокчейну вирішуються, або домовленістю і контрактами між державою та розробниками блокчену, або невеликими фінансовими затратами, натомість отримуються величезні переваги в людському часі , грошах та стабільності системи.

На мою думку , ОДНОЗНАЧНО потрібно використовувати готове рішення з правильним аудитом. Це дасть змогу зосередитись на виконанні ключових функцій самої технології та користуватись можливостями і перевагами на загально корисну ціль , а не витрачати даремно величезні сили на розробку рішення , яке буде вразливе та не відтестоване роками безперебійних років та мільйонами атак.

Також це ОДНОЗНАЧНО повинен бути публічний блокчейн , адже головна ціль це досягнення результатів , які є перевагами публічних блокчейнів , в той час як приватні блокчейни підходять більше для бізнес рішень.

2.3.2 Очікування Національного банку України та рішення Міністерства цифрової трансформації України

Національний банк презентував[3] представникам банків, небанківських фінансових установ та ринку віртуальних активів для обговорення та отримання зворотного зв'язку проєкт концепції е-гривні – цифрових грошей Національного банку України.

Е-гривня – це електронна форма грошової одиниці України(рис. 2.7), що буде прямим зобов'язанням центрального банку. Її ключове призначення, на думку регулятора – ефективно виконувати всі функції грошей, доповнюючи готівкову та безготівкову форми гривні. Використання е-гривні має бути зручним та

доступним для всіх верств населення, юридичних осіб, державних органів, банків та небанківських фінансових установ.

"Розробка та впровадження е-гривні може стати наступним кроком еволюції платіжної інфраструктури України, сприятиме цифровізації економіки, подальшому поширенню безготівкових розрахунків, зменшенню їх вартості, зростанню рівня їх прозорості і підвищенню довіри до національної валюти загалом. Це може позитивно вплинути на забезпечення економічної безпеки та посилення монетарного суверенітету держави, посилить спроможність Національного банку підтримувати цінову та фінансову стабільність як запоруку стійкого економічного зростання", – зазначав заступник Голови Національного банку Олексій Шабан.

Під час обговорення з учасниками зазначених вище ринків Національний банк презентував також можливий дизайн е-гривні, її архітектуру, характеристики та переваги для надавачів платіжних послуг. Зокрема використання технологічної платформи для миттєвих розрахунків е-гривнею, програмування послуг та аналізу потоків даних створить широкі можливості для виникнення нових бізнес-кейсів, цифровізації послуг, залучення нових клієнтів, оптимізації витрат тощо.

Під час створення проєкту концепції е-гривні регулятор враховував результати опитування експертів фінансового ринку щодо попиту на е-гривню (проводилося Національним банком у 2021 році), світовий досвід розробки цифрових валют центральних банків та власні дослідження.

Наразі Національний банк розглядає та опрацьовує такі можливі варіанти використання е-гривні, від яких залежатимуть її дизайн та основні характеристики:

- е-гривня для роздрібних безготівкових платежів із можливим функціоналом “програмованих” грошей: для здійснення цільових соціальних виплат, зниження державних видатків на адміністрування та контроль цільового використання коштів, а також використання технології смартконтрактів для програмування різноманітної логіки розрахунків залежно від настання тих чи інших обставин та фактів;

- е-гривня для використання у сфері, пов’язаній з обігом віртуальних активів (наприклад, для обміну, забезпечення випуску та інших операцій з віртуальними активами). Е-гривня може стати одним із ключових елементів якісного розвитку інфраструктури для ринку віртуальних активів в Україні;
- е-гривня для забезпечення можливості здійснення транскордонних платежів: забезпечить можливість здійснювати транскордонні платежі швидше, дешевше та прозоріше.

Національний банк продовжує опрацьовувати проєкт концепції е-гривні з учасниками платіжного ринку, учасниками ринку віртуальних активів та державними органами.

Результатом опрацювання стане створення концепції е-гривні – із комплексним урахуванням інтересів й потреб учасників ринків та потенційних користувачів.

Водночас Національний банк, як і більшість центробанків світу, підходитиме до питання випуску власної цифрової валюти зважено та враховуючи, зокрема, потенційний вплив від її запровадження на фінансову систему держави.

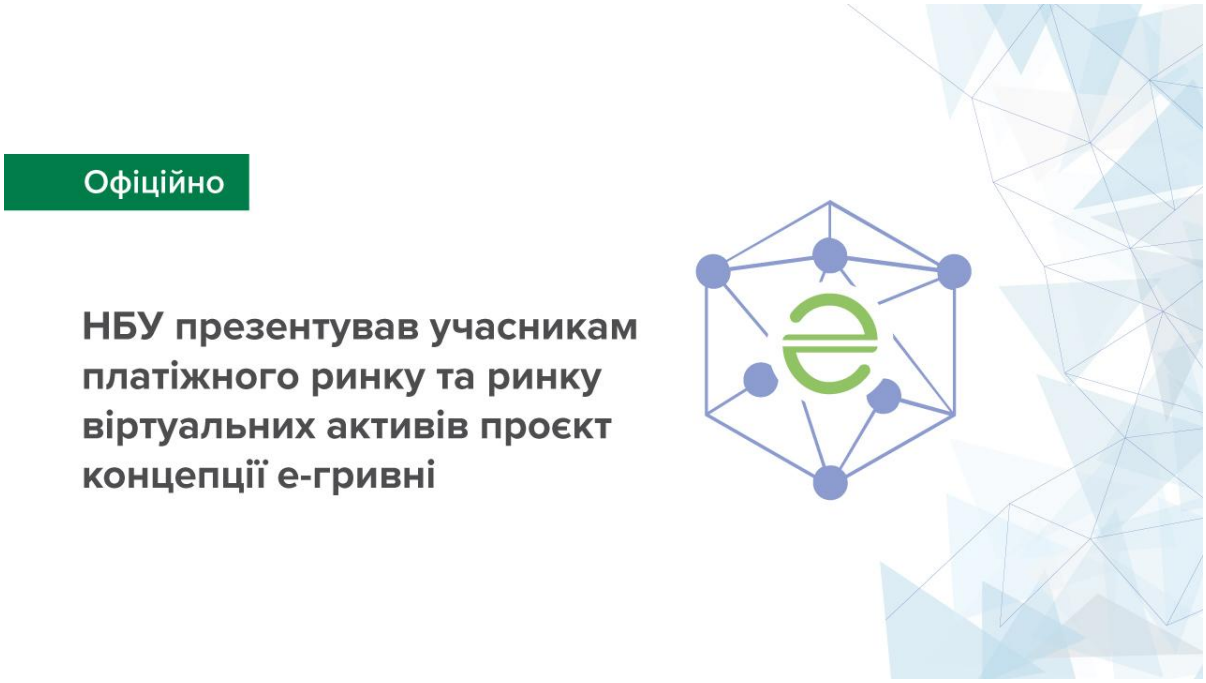


Рисунок 2.7 Офіційна презентації Е-гривні 28.11.2022

Можна підсумувати , що моє власне бачення застосування блокчейну сильно корелює з побажаннями НБУ і вибір вимог до технології є об’єктивно актуальним та правильним.

Важливо ще звернути увагу на цікаву співпрацю та бачення Міністерства цифрових технологій України. Від 04.01.2021 [13] де публічно представлена співраця Мінцифри України та Stellar Development Foundation (рис. 2.8) над розвитком ринку віртуальних активів.

Меморандумом передбачається співпраця за такими напрямами:

- розвиток ринку віртуальних активів в Україні;
- надання підтримки проєктам, які спеціалізуються на віртуальних активах;
- імплементація та врегулювання обігу стейблкоїнів в Україні;
- сприяння розвитку цифрової валюти Національного банку в Україні.

Отже, ще один важливий та об’єктивний факт того , що моє бачення та орані напрямки мають компетентне підґрунтя і реалізація необхідна на ГОТОВОМУ публічному блокчейні.

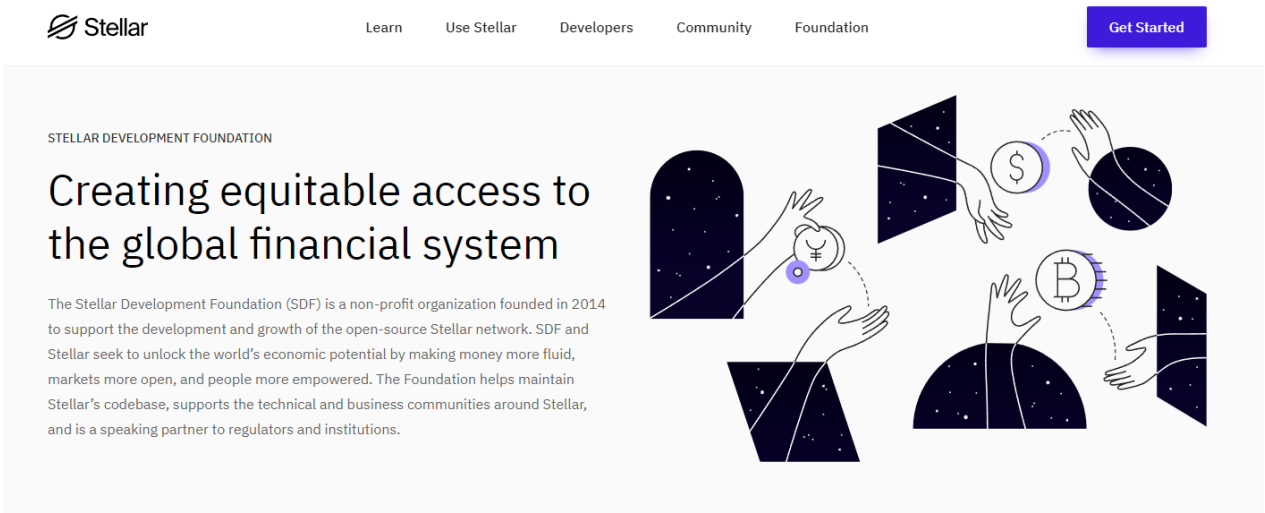


Рисунок 2.8 Головна сторінка офіційного сайту Stellar Development Foundation

3 РОЗРОБКА ТОКЕНУ Е-ГРИВНІ НА ОБРАНІЙ ТЕХНОЛОГІЇ. ОПТИМАЛЬНА БЛОКЧЕЙН МЕРЕЖІ ЗГІДНО ВИМОГ ТА ТЕОРЕТИЧНИХ НАПРАЦЮВАНЬ

3.1 Вибір мережі. Публічні популярні рішення для банківських сфер

Із найпопулярніших публічних блокчейн мереж для банківських установ себе вже зарекомендували наступні:

- ✓ Ripple: це система валових розрахунків в режимі реального часу, обміну валюти та мережа грошових переказів, яка базується на технології розподіленого реєстру. Вона призначена для забезпечення швидких, безпечних і недорогих фінансових транзакцій і часто використовується банками та фінансовими установами.
- ✓ Stellar: це децентралізований протокол з відкритим вихідним кодом для передачі цифрової валюти та активів. Він призначений для полегшення недорогих транскордонних транзакцій між різними валютами та активами, включаючи фіатні валюти, криптовалюти та товари. Мережа Stellar використовує розподілений реєстр для швидкого і дешевого підтвердження транзакцій, має високу масштабованість і можливість обробляти тисячі транзакцій в секунду. Блокчейн Stellar був використаний для створення цілого ряду додатків, включаючи децентралізовані біржі, стейблкоіни і багато іншого.
- ✓ Corda: це децентралізована блокчейн-платформа з відкритим вихідним кодом, яка спеціально розроблена для фінансових додатків. Вона використовується консорціумом банків і фінансових установ для розробки рішень на основі блокчейну, таких як торгове фінансування, перевірка особи і системи розрахунків.

- ✓ Hyperledger Fabric: це блокчейн-платформа з відкритим вихідним кодом, яка призначена для розробки блокчейн-рішень корпоративного рівня. Вона часто використовується банками та фінансовими установами для розробки таких додатків, як обробка платежів, управління ланцюжками поставок і перевірка особистих даних.

- ✓ Quorum: це блокчейн-платформа корпоративного рівня з відкритим вихідним кодом, яка базується на Ethereum. Вона призначена для забезпечення швидких, безпечних і приватних фінансових транзакцій і часто використовується банками та фінансовими установами для розробки таких додатків, як торгове фінансування, обробка платежів і відстеження активів.

Це лише кілька прикладів багатьох публічних мереж блокчейн, які були розроблені для використання банківськими установами. Важливо зазначити, що кожна мережа має свої унікальні особливості та можливості, і дуже важливо ретельно розглянути конкретні вимоги та потреби фінансового додатку, перш ніж обирати платформу блокчейн.

Аби спростити задачу з ретельним та трудомістким вибором мереж із представлених можемо довіритись і скористатись напрацюваннями спеціалістів із Мінцифри України та обрати Stellar. Дана мережа є публічною, децентралізованою, має швидкі тразакції, прозорість, блокчейн є готовим Layer 1 рішенням, добре відтестованим та функціонує з 2014 року. Отже, фаворит blochain Stellar

3.2 Stellar як blochain рішення для фінансових задач

Stellar - це децентралізований протокол з відкритим вихідним кодом для передачі цифрової валюти і активів, який може використовуватися фінансовими установами різними способами (рис. 3.1). Окрім вже відомих фактів технології в загальному Stellar цілеспрямовано позиціонується як рішення для фінансів та грошових інституцій.

Серед завдань, які виконує Stellar для фінансових установ, варто виділити:

✓ *Транскордонні платежі*: Stellar може сприяти швидким, недорогим транскордонним платежам між різними валютами та активами. Це може бути особливо корисно для фінансових установ, яким необхідно здійснювати часті міжнародні платежі, оскільки це може заощадити їм гроші на комісіях і скоротити час, необхідний для завершення транзакцій.

✓ *Грошові перекази*: Stellar також може використовуватися для полегшення грошових переказів, які є переказами грошей від однієї особи або організації до іншої. Це може бути корисно для фінансових установ, які хочуть пропонувати послуги грошових переказів своїм клієнтам, оскільки це може дозволити їм відправляти і отримувати гроші швидко і дешево.

✓ *Мікрофінансування:* Stellar також може використовуватися для підтримки ініціатив з мікрофінансування, які є фінансовими послугами, покликаними допомогти людям в країнах, що розвиваються, отримати доступ до кредитів та інших фінансових послуг. Використовуючи Stellar, фінансові установи можуть пропонувати послуги мікрофінансування більш ефективно і з меншими витратами.

✓ *Емісія активів*: Фінансові установи також можуть використовувати Stellar для випуску власних цифрових активів, таких як стейблкоіни або токени безпеки. Це може дозволити їм залучати капітал, передавати право власності на активи і створювати нові фінансові продукти і послуги.

✓ *Децентралізовані фінанси:* Stellar також може використовуватися для створення додатків децентралізованого фінансування (DeFi), які є фінансовими послугами, побудованими на основі блокчейну Stellar, що дозволяють користувачам отримувати доступ до фінансових послуг децентралізовано і без довіри.

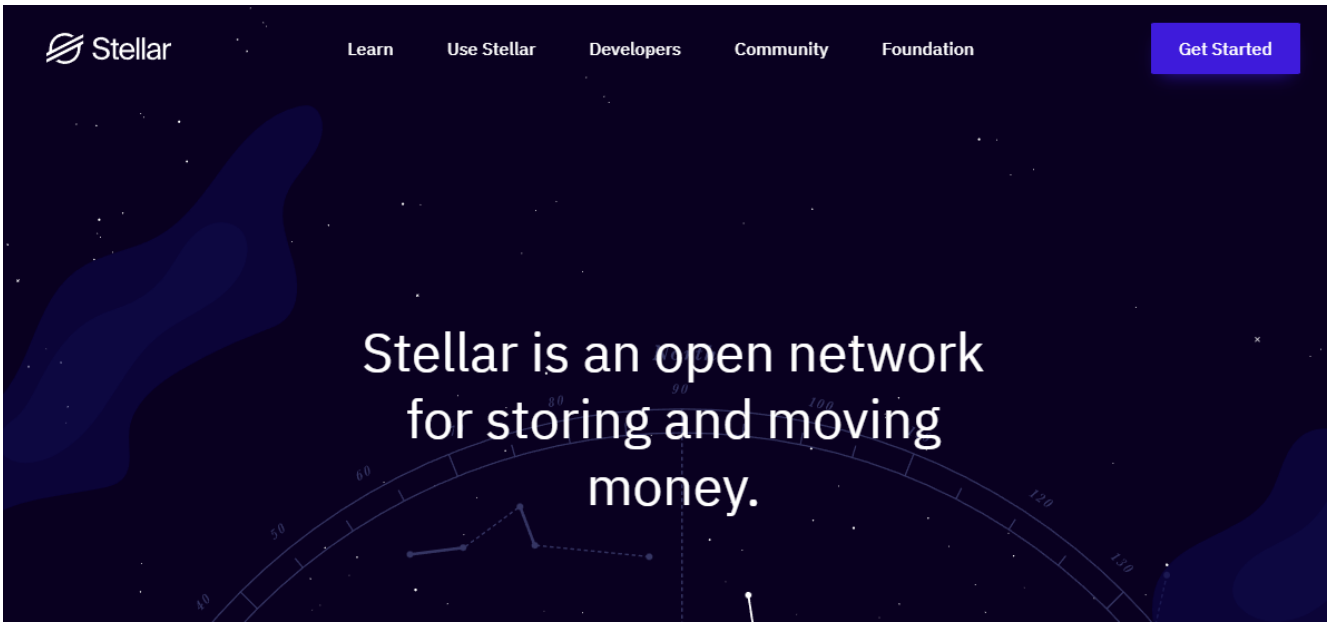


Рисунок 3.1 Головна сторінка Stellar акцентує на рішенні для фінансів.

3.3 Покрокова розробка токена Е-гривня та тестування транзакцій

3.3.1 Створення аккаунта емітента, дистриб'ютора та випадкового користувача

Емітент - це компанія, уряд або інша організація, яка випускає цінні папери, такі як акції, облігації або інші фінансові інструменти. Емітент відповідає за створення та продаж цінних паперів і використовує кошти, отримані від продажу цінних паперів, для фінансування своєї діяльності або для фінансування конкретних проектів.

Рахунок емітента - ведеться окремо від рахунку, який ви будете використовувати для розповсюдження вашого нового Активу. Чому? Це дозволяє вам легко довести світові економічне обґрунтування вашого активу. Наприклад, ви можете заблокувати акаунт емітента після створення фіксованої кількості токенів, і це дасть зрозуміти світові, що більше ніяких ваших токенів не може бути створено.

Створення ключів для Issuer в графічному інтерфейсі на платформі Stellar та присвоєння 10000 XLM для тестових транзакцій (рис. 3.2) та присвоєння значень в коді (рис. 3.3). Утворені наступні ключі:

IssuerPublicKey:="GBB3N4JUOVKO6ZDP6LGYF6TWCYVES4MQL5GWHODCVMOY2HVIE7UD43PD"

IssuerSecretKey:="SALYSZ5LM5YFX6ZDYVY64P2ARS3QJIKXO7Y5BAX4NC6ZUTJUAQACIY77"

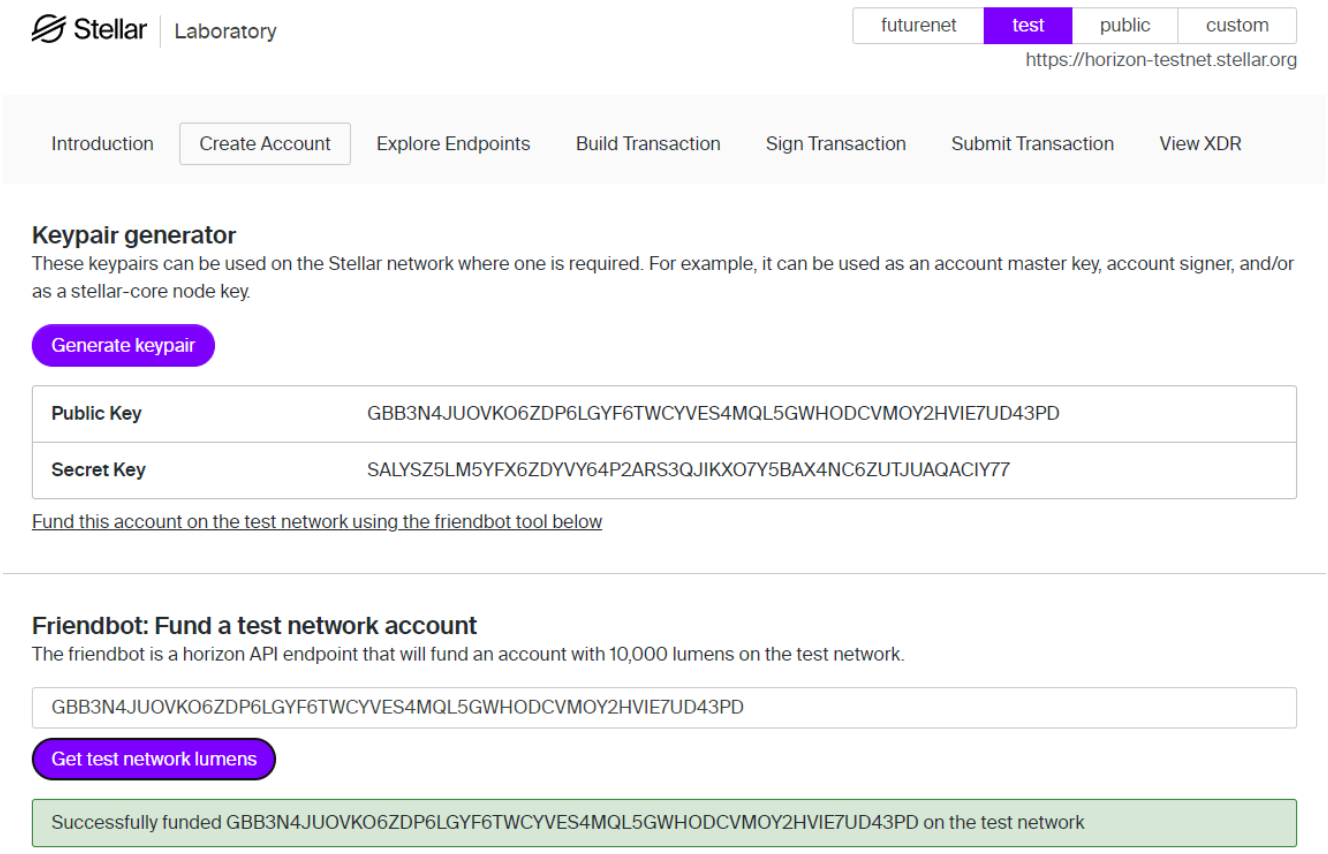


Рисунок 3.2 Створення Issuer Keys на платформі

```
12  func main() {
13      // Issuer Credentials - replace with your respective keys
14      IssuerPublicKey := "GBB3N4JUOVKO6ZDP6LGYF6TWCYVES4MQL5GWHODCVMOY2HVIE7UD43PD"
15      IssuerSecretKey := "SALYSZ5LM5YFX6ZDYVY64P2ARS3QJIKXO7Y5BAX4NC6ZUTJUAQACIY77"
16      IssuerKeypair, _ := keypair.ParseFull(IssuerSecretKey)
17
```

Рисунок 3.3 Присвоєння ключів на мові Golang

Дистриб’ютор - це особа або організація, яка купує цінні папери у емітентів і продає їх інвесторам. Дистриб'ютори зазвичай працюють з інвестиційними банками, брокерськими фірмами та іншими фінансовими установами для сприяння продажу цінних паперів, таких як акції, облігації та пайові інвестиційні фонди. Вони також можуть надавати підтримку та послуги інвесторам, наприклад, надавати інформацію про цінні папери, які вони пропонують, та допомагати інвесторам зрозуміти ризики та потенційні прибутки, пов'язані з різними інвестиціями. Дистриб'ютори відіграють важливу роль на фінансових ринках, з'єднуючи емітентів з інвесторами та допомагаючи забезпечити ефективний розподіл капіталу.

Рахунок дистриб'ютора - отримує токени з рахунку Емітента і є рахунком, який ви потім будете використовувати для розповсюдження своїх токенів на інші гаманці Stellar тощо.

Створення ключів для Distributor в графічному інтерфейсі на платформі Stellar та присвоєння 10000 XLM для тестових транзакцій (рис. 3.4) та присвоєння значень в коді (рис. 3.5). Утворені наступні ключі:

DistributorPublicKey:="GAXLOAX27HXOHSBW54EI6DFLSF4TFAGXREIRB5OTOKECKHKVECPESWYB"

DistributorSecretKey:="SBSYGPGES2MGXPKAUERY7WV5X33Q57ISGV4LZKBBD6LVJGP4G7O7OUQ5"

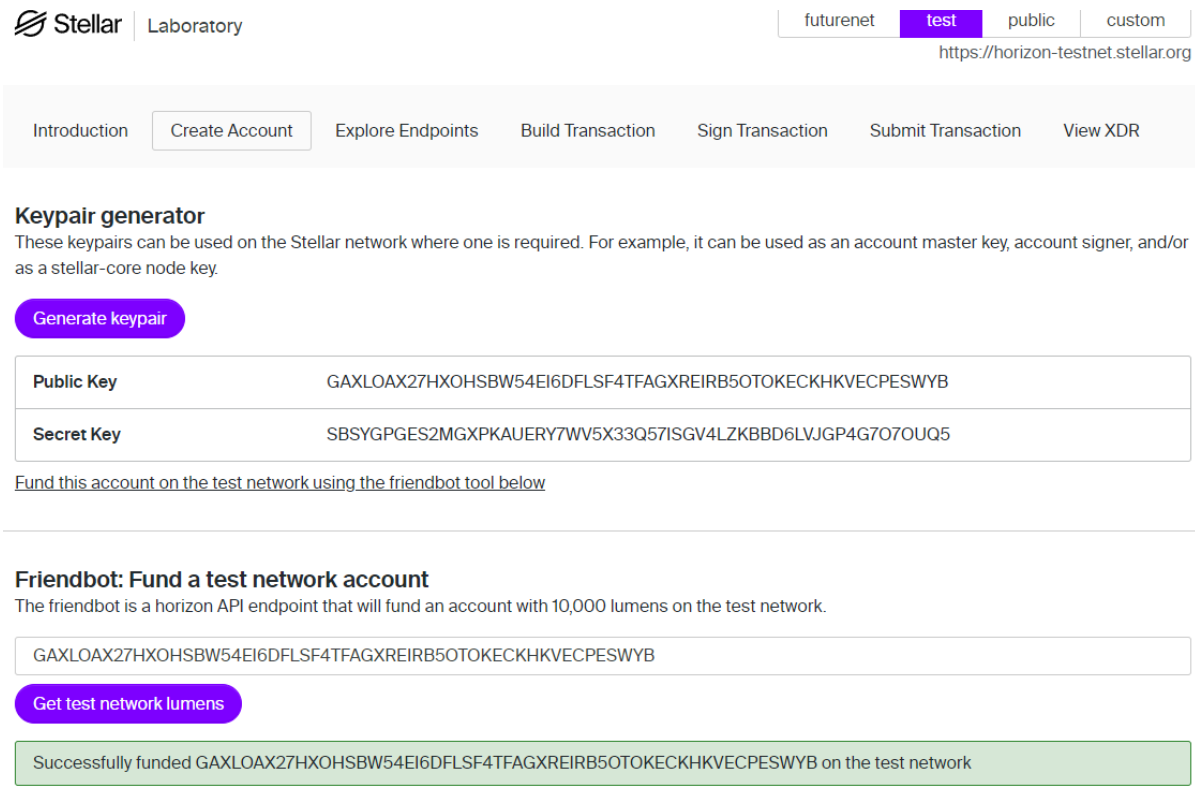


Рисунок 3.4 Створення Distributor Keys на платформі

```
17
18      // Distributor Credentials - replace with your respective keys
19      DistributorPublicKey := "GAXLOAX27HXOHSBW54EI6DFLSF4TFAGXREIRB5OTOKECKHKVECPESWYB"
20      DistributorSecretKey := "SBSYGPGES2MGXPKAUERY7WV5X33Q57ISGV4LZKBBD6LVJGP4G7O7OUQ5"
21      DistributorKeypair, _ := keypair.ParseFull(DistributorSecretKey)
22
```

Рисунок 3.5 Присвоєння ключів на мові Golang

Таким ж чином створиться аккаунт громадянина (рис. 3.6).

UserPublicKey:="GDCCY3U2OJ3CD2H36W72GSFE2ALPIF6FCE5EJT5BNIITZJAPY3NEA6ET"

UserSecretKey:="SCNVCYVRBL5JJ5U6RS4YHRIOM3SBSQJMOOQLDCH7PTE572VKTBAE54JN

```
23      // User Credentials - replace with your respective keys
24      // UserPublicKey := "GDCCY3U2OJ3CD2H36W72GSFE2ALPIF6FCE5EJT5BNIITZJAPY3NEA6ET"
25      UserSecretKey := "SCNVCYVRBL5JJ5U6RS4YHRIOM3SBSQJMOOQLDCH7PTE572VKTBAE54JN"
26      UserKeypair, _ := keypair.ParseFull(UserSecretKey)
```

Рисунок 3.6 Присвоєння ключів на мові Golang

3.3.2 Встановлення рівня довіри до емітента та емісії токена

Необхідно, щоб обліковий запис Дистриб'ютора довіряв обліковому запису Емітента - тому на сторінці "Build Transaction page", необхідно вставити відкритий ключ облікового запису Дистриб'ютора в поле "Source account"" і натиснути кнопку "Fetch next sequence number..." (рис. 3.7) (рис. 3.8)

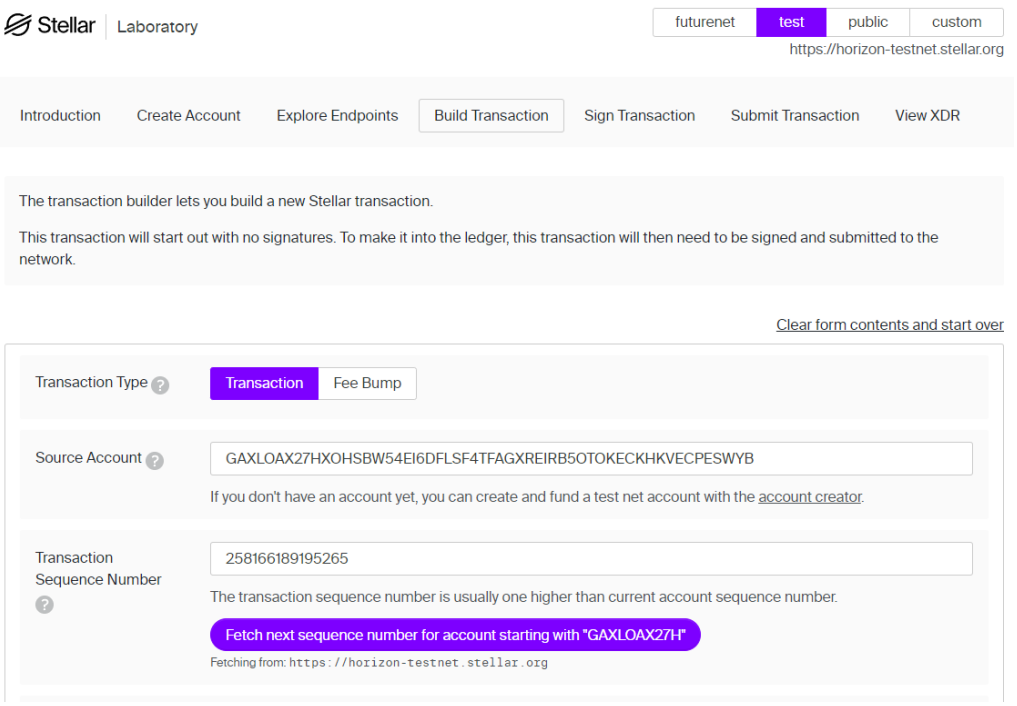


Рисунок 3.7 Процес встановлення довіри на платформі

```
58  // ChangeTrust creates and submits the create trust operation
59  func ChangeTrust(DistributorKeypair *keypair.Full, IssuerPublicKey string,
60      client *horizonclient.Client) <-chan string {
61
62      res := make(chan string)
63
64      go func() {
65          defer close(res)
66
67          // Get information about the Distributor account
68          accountRequest := horizonclient.AccountRequest{AccountID: DistributorKeypair.Address()}
69          Account, err := client.AccountDetail(accountRequest)
70          if err != nil {
71              log.Fatal(err)
72          }
73
74          // Construct the operation
75          changeTrustOp := txnbuild.ChangeTrust{
76              Line: txnbuild.CreditAsset{
77                  Code:   "eHryvnia",
78                  Issuer: IssuerPublicKey,
79              },
80              Limit:         "200000000000",
81              SourceAccount: &Account,
82          }
83
84          // Construct the transaction that will carry the operation
```

Рисунок 3.8 Процес встановлення довіри мовою Golang

Прокрутивши сторінку вниз і обравши «Change Trust». Я вибрав «Буквено-цифровий 12», тому що ім'я мого токена складається з 4+ літер - eHRYVNIA. Після визначення назви токена, необхідно вставити відкритий ключ свого облікового запису-емітента. Trust Limit, він же кількість токенів які можна буде випустити я встановив на 200 000 000 000 (рис. 3.9).(рис. 3.10)

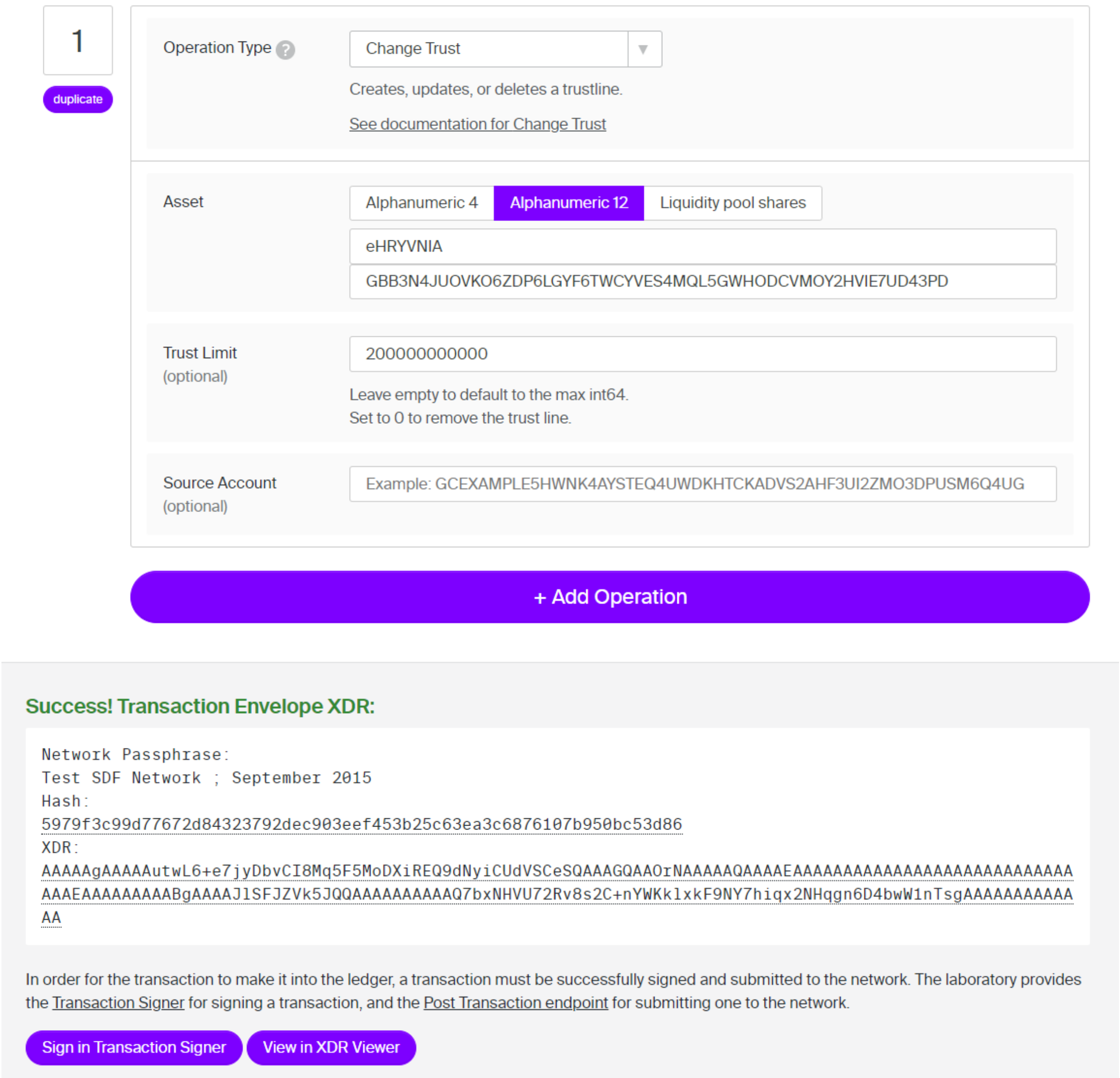


Рисунок 3.9 Встановлення емісії валюти та довіреного емітента на платформі

```go
// ChangeTrust creates and submits the create trust operation
func ChangeTrust(DistributorKeypair *keypair.Full, IssuerPublicKey string,
    client *horizonclient.Client) <-chan string {

    res := make(chan string)

    go func() {
        defer close(res)

        // Get information about the Distributor account
        accountRequest := horizonclient.AccountRequest{AccountID: DistributorKeypair.Address()}
        Account, err := client.AccountDetail(accountRequest)
        if err != nil {
            log.Fatal(err)
        }

        // Construct the operation
        changeTrustOp := txnbuild.ChangeTrust{
            Line: txnbuild.CreditAsset{
                Code:   "eHryvnia",
                Issuer: IssuerPublicKey,
            },
            Limit:         "200000000000",
            SourceAccount: &Account,
        }

        // Construct the transaction that will carry the operation
```

Рисунок 3.10 Встановлення емісії валюти та довіреного емітента мовою Golang

Наступною дією буде “Sign in Transaction Signer” після чого створиться контракт на підписання випуску токенів (рис.3.11). Заповнивши поле приватного ключа підпишемо транзакцію від Distributor натиснувши “Submit in Transaction Submitter” та створимо токен eHRYVNIA (рис. 3.12).

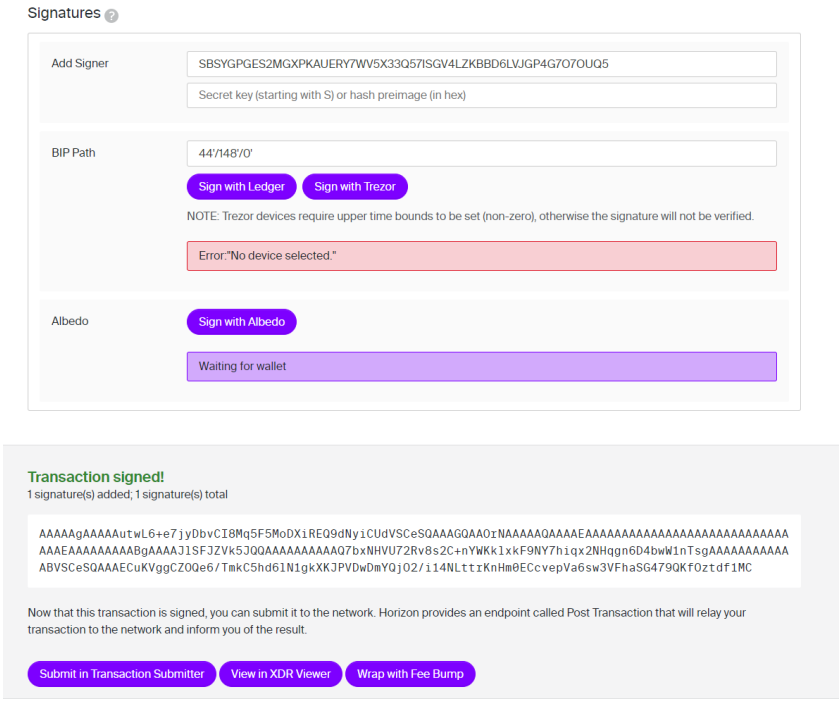


Рисунок 3.11 Створення контракта на підписання про емісію на платформі

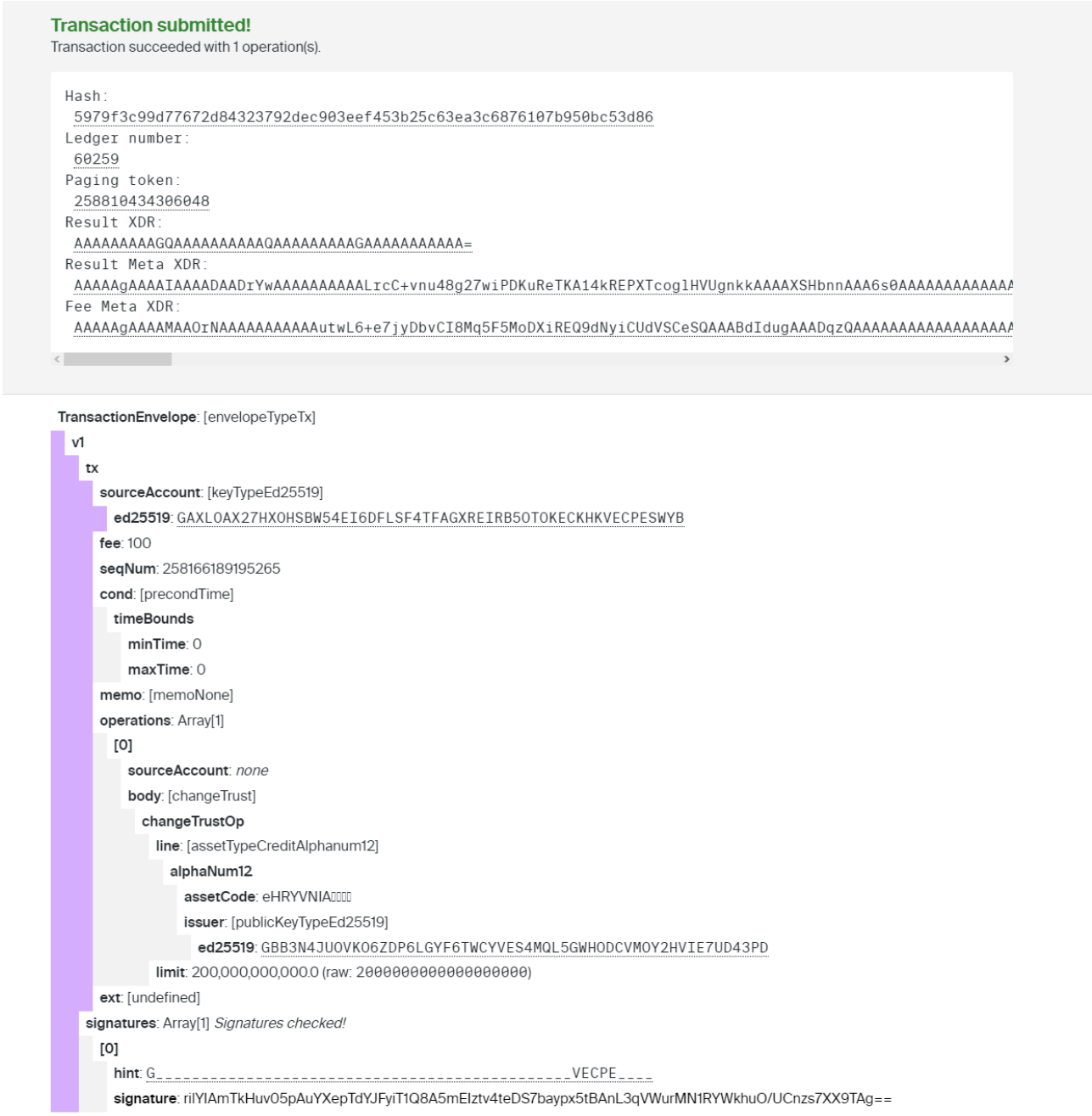


Рисунок 3.12 Підписаний контракт та створення токен eHryvnia емісією для довіреного обличчя в 200000000000

Оскілкьи блокчейн відкритий та прозорий кожен бажаючий може скористатись https://testnet.stellarchain.io та по адресу токена , транзакції, власника побачити токени, їх кількість та усі транзакції в історії (рис 3.13).

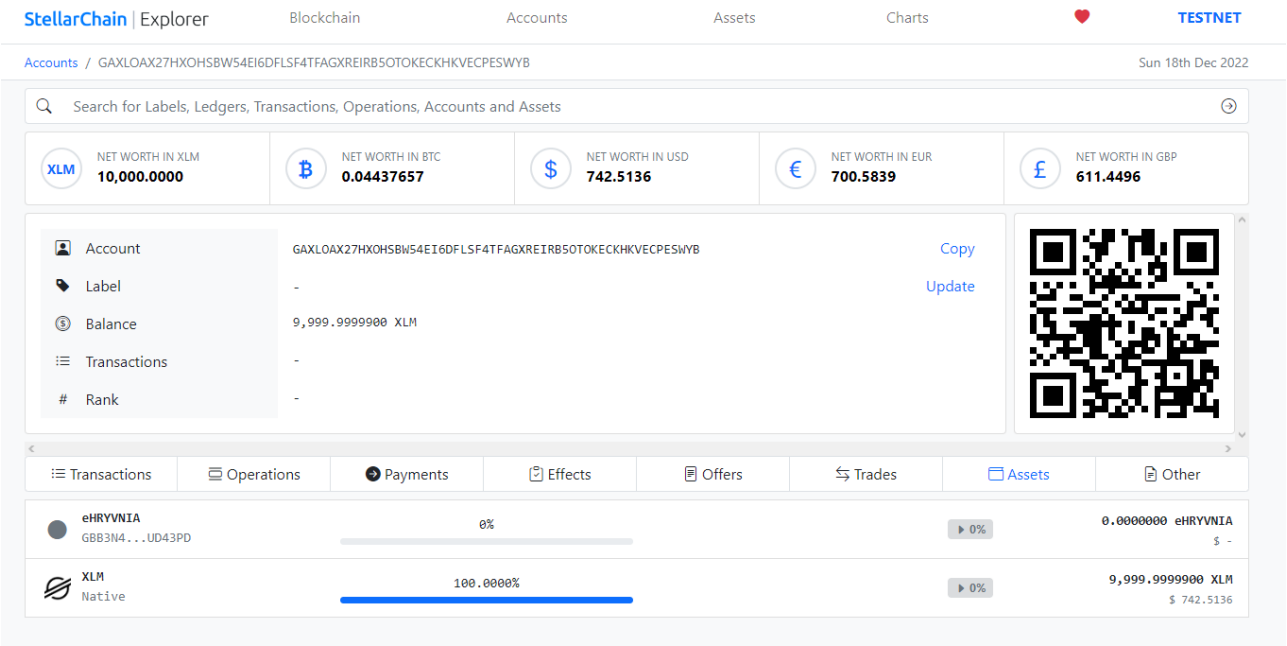


Рисунок 3.13 Публічна історія власника, токена та транзакцій

3.3.3 Тестування здійснення транзакції та перерахування коштів

Тепер відправимо токени від Issuer до Distributor, аби протестувати як працють транзакції в мережі. Генеруємо транзакцію від імені Емітента (рис. 3.14)

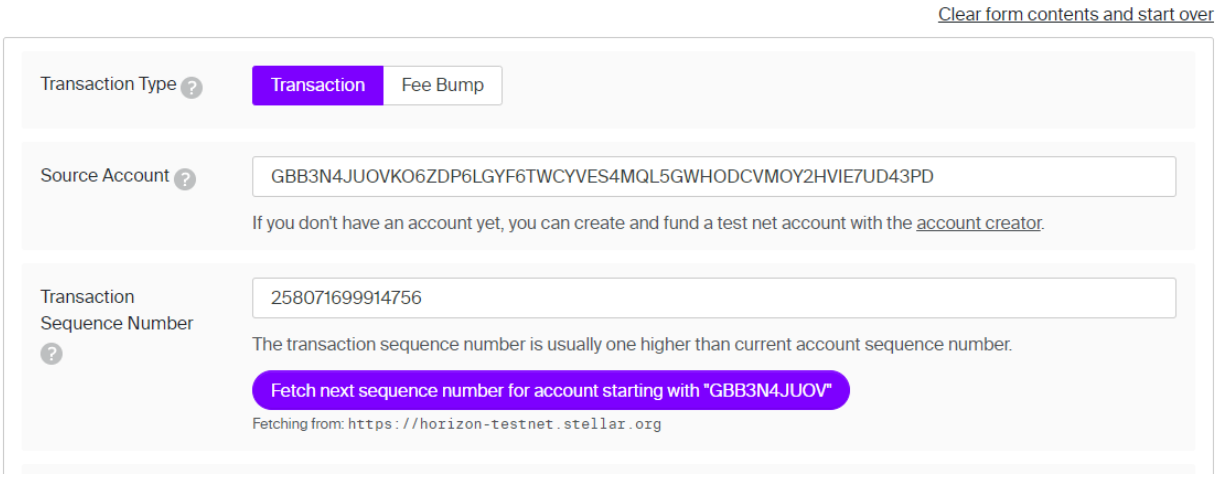


Рисунок 3.14 Транзакція від імені емітента на платформі.

Після цього необхідно вибрати тип транзакції “Payment” обрати місце призначення (адреса цільового учасника, публічний ключ) , емітента (довірене обличчя) , вказати назву токену який хочемо відправити та кількість , я вказую 5001 гривню. (рис. 3.15)

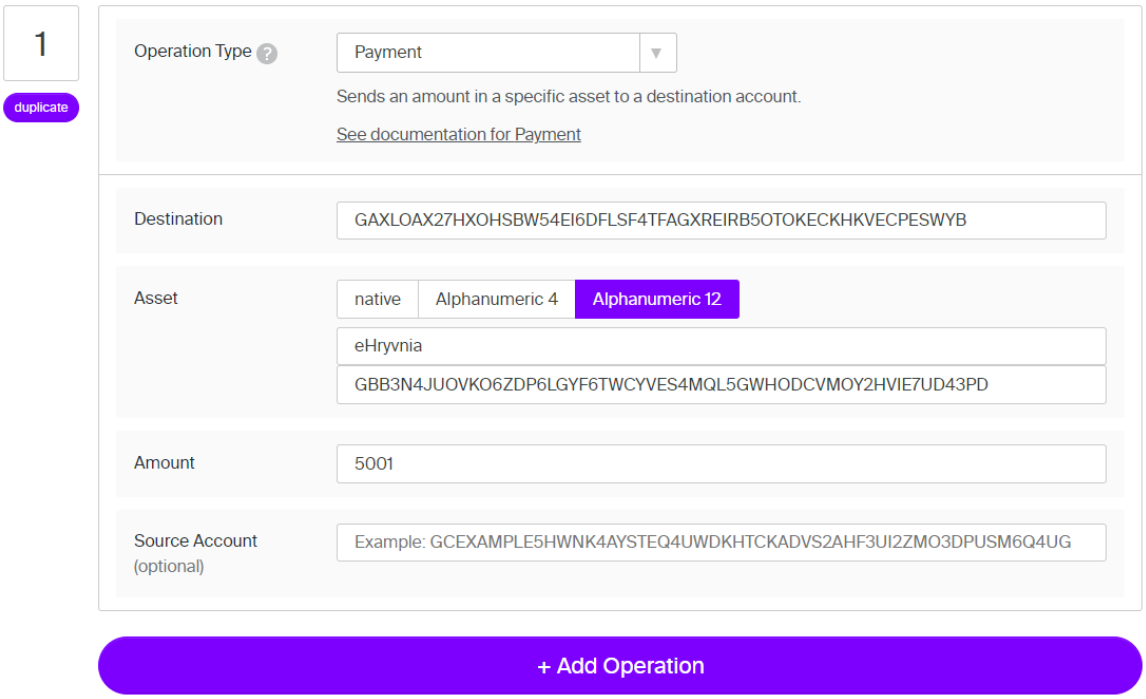


Рисунок 3.15 Тип транзакції відправка на платформі.

Підпис транзакції вже по відомій процедурі (рис 3.16).

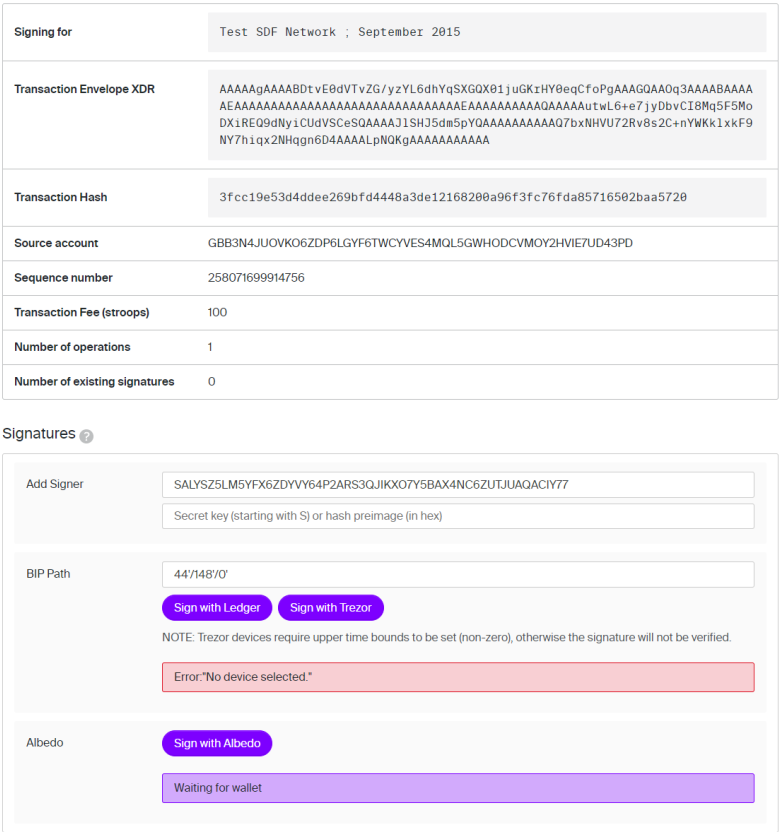
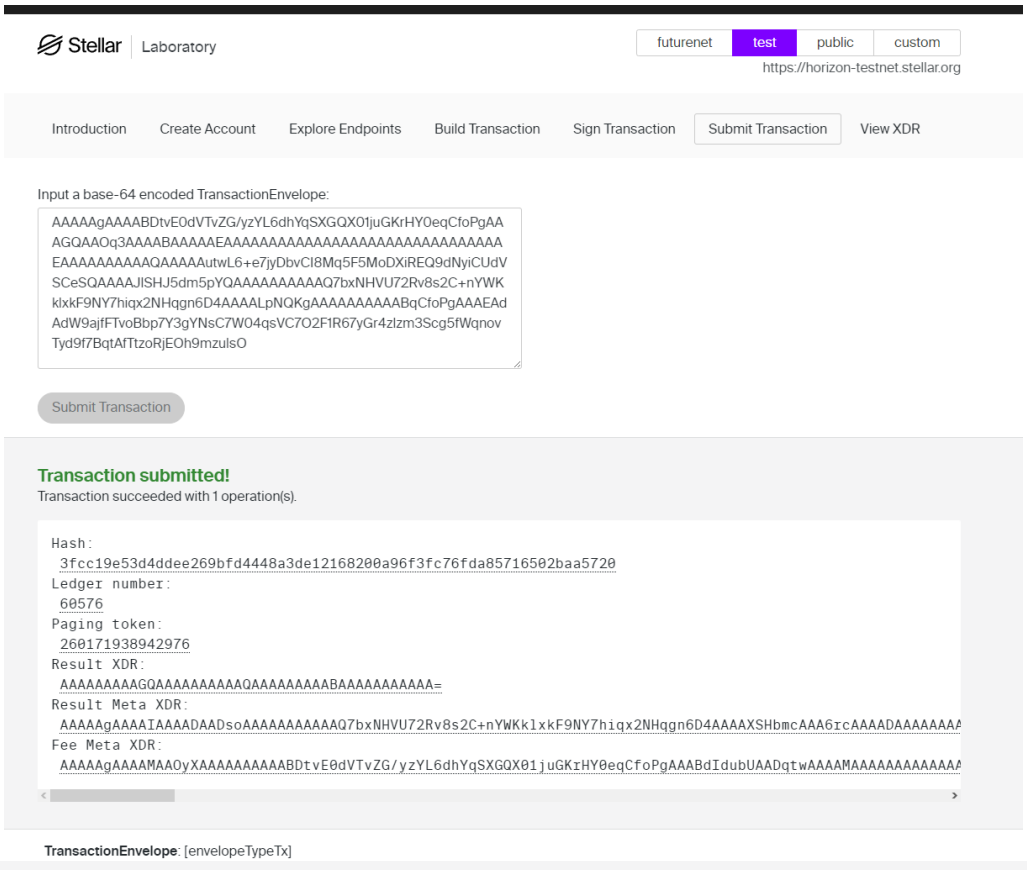


Рисунок 3.16 Підпис транзації відправки 5001 гривні на платформі

Підтверджуємо транзакцію та бачимо звіт про її виконання (рис. 3.17)



TransactionEnvelope: [envelopeTypeTx]

- **v1**
  - **tx**
    - **sourceAccount**: [keyTypeEd25519]
      - **ed25519**: GBB3N4JUOVKO6ZDP6LGYF6TWCYVES4MQL5GWHODCVMOY2HVIE7UD43PD
    - **fee**: 100
    - **seqNum**: 258071699914756
    - **cond**: [precondTime]
      - **timeBounds**
        - **minTime**: 0
        - **maxTime**: 0
    - **memo**: [memoNone]
    - **operations**: Array[1]
      - **[0]**
        - **sourceAccount**: *none*
        - **body**: [payment]
          - **paymentOp**
            - **destination**: [keyTypeEd25519]
              - **ed25519**: GAXLOAX27HXOHSBW54EI6DFLSF4TFAGXREIRB5OTOKECKHKVECPESWYB
            - **asset**: [assetTypeCreditAlphanum12]
              - **alphaNum12**
                - **assetCode**: eHryvnia□□□□
                - **issuer**: [publicKeyTypeEd25519]
                  - **ed25519**: GBB3N4JUOVKO6ZDP6LGYF6TWCYVES4MQL5GWHODCVMOY2HVIE7UD43PD
            - **amount**: 5,001.0 (raw: 50010000000)
    - **ext**: [undefined]
  - **signatures**: Array[1] *Signatures checked!*
    - **[0]**
      - **hint**: G_____IE7UD___
      - **signature**: HQHVvWo3xU76AW6e2N4GDbAu1tOKrFQuzthdUeu8hq+M5c5t0nIOX1qp6L08nfX+warQH07c6EYxDofZs7pbDg==

Рисунок 3.17 Підтвердження та звіт про успішну транзакцію в мережі

Слід зазначити , що виконалась транзакція досить швидко.ю час близько моментального, навідміну від конкуруючих фіатних шлюзів типу Visa, Mastercard чи SWIFT. Оскільки блокчейн є прозорим будь-хто може переконатись в виконаних діях в блокчейн сканері мережі Stellar за посиланням (рис. 3.18) :

https://testnet.stellarchain.io/accounts/GAXLOAX27HXOHSBW54EI6DFLSF4TFAGXREIRB5OTOKECKHKVECPESWYB

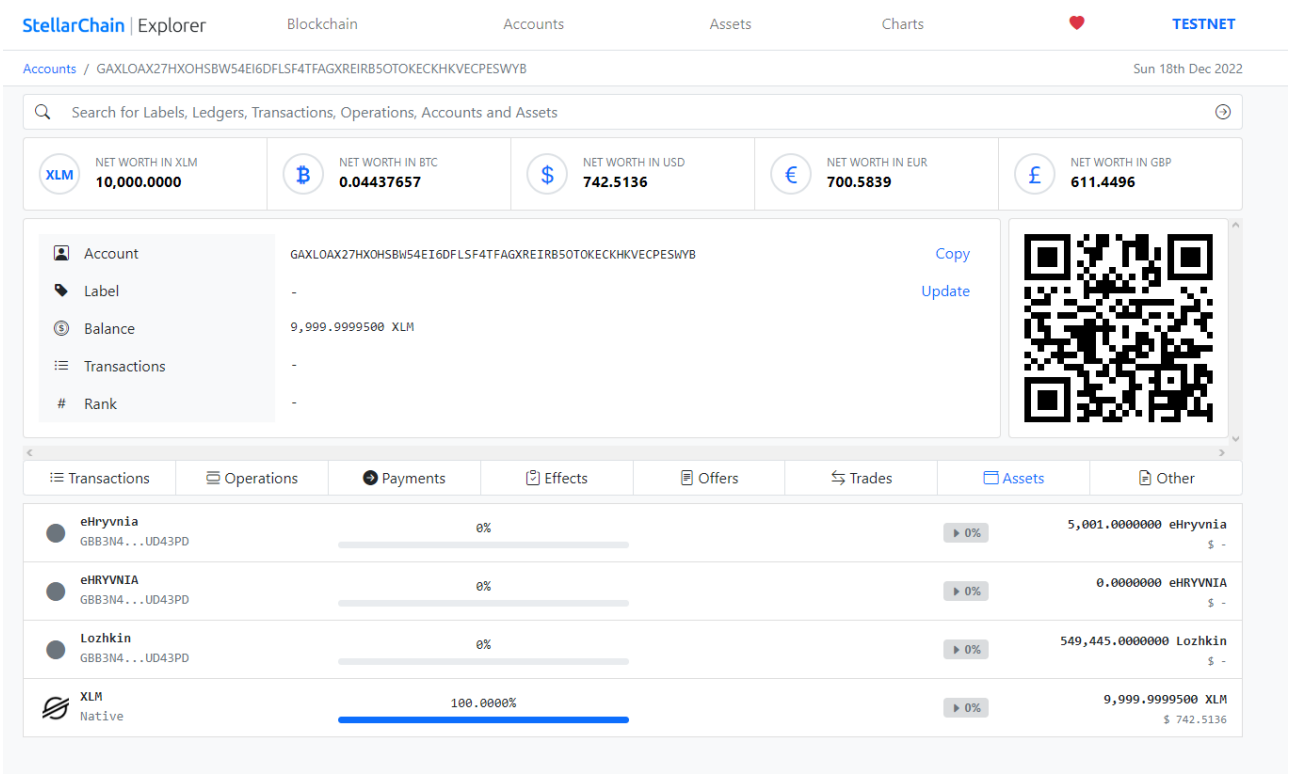


Рисунок 3.18 Результат транзакції доступний для всіх

ВИСНОВКИ

Дана кваліфікаційна робота була успішно виконана. Я продемонстрував свою компетентність у роботі та реалізував власний токен в блокчейн мережі Stellar який функціонує відповідно до очікувань та потреб.

Протягом виконання роботи було якісно розібрано та досліджено багато джерел інформації та відсортована корисна складова. Здійснено аналітичний огляд на такі актуальні теми ,як поняття блокчейн технології та блокчейн мережі. Детальніше по цих темах були опрацьовані такі складові як базова архітектура , принципи роботи, розібрана технологія.

Окрім блокчейн технологій було розглянуто концепцію децентралізації, описані переваги та недоліки такої концепції, проблематика.

Для виконання роботи та вибору актуальної та правильної блокчейн технології було проаналізовано які бувають рівні блокчейну, типи блокчейну за доступом.

Розглянута та описана проблематика токенізації , відмінність токенізації від оцифровки та можливості які відкриває перед нами ця технологія.

Протягом усієї роботи я висловлював свою думку по темі та намагався об’єктивно виокремлювати якісь аспекти.

Після проведеного аналізу та набутими знаннями переконався та оцінив, що технологія буде корисною для України, що обраний Міністерством цифрової трансформації України блокчейн - Stellar є актуальною та справді потрібною технологією , яка вдало вирішує покладені на проект завдання.

Розробив та реалізував власний токен за відповідно потребам НБУ та перевагам технології.

Реалізований токен дійсно відповідає поставленим задачам децентралізації , прозорості та швидкості транзакцій , які перевершую класичні платіжні шлюзи в сотні разів.

Вважаю виконану роботу корисною а тему актуальною для подальшої популяризації та розробки.

ПЕРЕЛІК ПОСИЛАНЬ ТА ВИКОРИСТАНІ ДЖЕРЕЛА

1. Закон України « Про платіжні послуги » від 30.07.2021 р. № 1591-IX URL: https://zakon.rada.gov.ua/laws/show/1591-20 (дата звернення 12.11.2022)

2. Закон України «Про віртуальні активи" від 17.02.2022 р. № 2074-IX URL: https://zakon.rada.gov.ua/laws/show/2074-20 (дата звернення 12.11.2022)

3. Національний банк представив учасникам платіжного ринку та ринку віртуальних активів проєкт концепції е-гривні URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-predstaviv-uchasnikam-platijnogo-rinku-ta-rinku-virtualnih-aktiviv--proyekt-kontseptsiyi-e-grivni (дата звернення 12.11.2022)

4. El Salvador's world-first adoption of bitcoin endures bumpy first day URL: https://www.reuters.com/business/finance/el-salvador-leads-world-into-cryptocurrency-bitcoin-legal-tender-2021-09-07/ (дата звернення 12.11.2022)

5. Sherman, Alan T.; Javani, Farid; Zhang, Haibin; Golaszewski, Enis (January 2019). "On the Origins and Variations of Blockchain Technologies". IEEE Security Privacy. 17 (1): 72—77.

6. Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. 3 (2): 99—111.

7. Bayer, Dave. Improving the Efficiency and Reliability of Digital Time-Stamping / Dave Bayer, Stuart Haber, W. Scott Stornetta. — March 1992. — Vol. 2. — P. 329–334.

8. Bitcoin: A Peer-to-Peer Electronic Cash System URL: https://bitcoin.org/bitcoin.pdf (дата звернення 14.12.2022)

9. Laurent Leloup Blockchain від А до Я France, Groupe Eyrolles, Paris 2017

10. Distributed Ledger Technology: beyond block chain (Report). Government Office for Science (UK). January 2016.

11. Kravchenko P. Tokenization in a nutshell [Електронний ресурс] /Pavel Kravchenko. – Режим доступу: https://medium.com/@pavelkravchenko/tokenization-in-a-nutshell-349968702e33.

12. Кравченко П. Теория токенизации / П. Кравченко, Б. Скрябин. – Харьков : Промарт, 2018. – 46 с.

13. Мінцифра співпрацюватиме зі Stellar Development Foundation над розвитком ринку віртуальних активів URL: https://thedigital.gov.ua/news/mintsifra-spivpratsyuvatime-zi-stellar-development-foundation-nad-rozvitkom-rinku-virtualnikh-aktiviv (дата звернення 15.12.2022)

14. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ.освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків :ПРОМАРТ.

ДОДАТКИ

```
import (
        "log"

        "github.com/stellar/go/clients/horizonclient"
        "github.com/stellar/go/keypair"
        "github.com/stellar/go/network"
        "github.com/stellar/go/txnbuild"
)
func main() {
        // Issuer Credentials - replace with your respective keys
        IssuerPublicKey :=
"GBB3N4JUOVKO6ZDP6LGYF6TWCYVES4MQL5GWHODCVMOY2HVIE7UD43PD"
        IssuerSecretKey :=
"SALYSZ5LM5YFX6ZDYVY64P2ARS3QJIKXO7Y5BAX4NC6ZUTJUAQACIY77"
        IssuerKeypair, _ := keypair.ParseFull(IssuerSecretKey)

        // Distributor Credentials - replace with your respective keys
        DistributorPublicKey :=
"GAXLOAX27HXOHSBW54EI6DFLSF4TFAGXREIRB5OTOKECKHKVECPESWYB"
        DistributorSecretKey :=
"SBSYGPGES2MGXPKAUERY7WV5X33Q57ISGV4LZKBBD6LVJGP4G7O7OUQ5"
        DistributorKeypair, _ := keypair.ParseFull(DistributorSecretKey)

        // User Credentials - replace with your respective keys
        // UserPublicKey :=
"GDCCY3U2OJ3CD2H36W72GSFE2ALPIF6FCE5EJT5BNIITZJAPY3NEA6ET"
        UserSecretKey := "SCNVCYVRBL5JJ5U6RS4YHRIOM3SBSQJMOOQLDCH7PTE572VKTBAE54JN"
        UserKeypair, _ := keypair.ParseFull(UserSecretKey)

        // Set Horizon Client to Testnet
        client := horizonclient.DefaultTestNetClient

        // Distributor Creates Trustline to Asset Issuer
        log.Println("STEP 1:Distributor Creates Trustline to Asset Issuer")
        ChangeTrustResponse := <-ChangeTrust(DistributorKeypair, IssuerPublicKey,
client)
        log.Println("Transaction Hash: ", ChangeTrustResponse)

        // Issuer Funds Distributor Account with total coin allocation
```

```
        log.Println("STEP 2:Issuer Funds Distributor Account with total coin
allocation")
        FundDistributorResponse := <-FundDistributor(IssuerKeypair,
DistributorPublicKey, client)
        log.Println("Transaction Hash: ", FundDistributorResponse)

        // Issuer locks itself by nullifying Master Threshold
        log.Println("STEP 3:Issuer locks itself by nullifying Master Threshold")
        LockIsuerResponse := <-LockIsuer(IssuerKeypair, client)
        log.Println("Transaction Hash: ", LockIsuerResponse)

        // User Creates Trustline to Asset Issuer
        log.Println("STEP 4:User Creates Trustline to Asset Issuer")
        ChangeTrustResponse2 := <-ChangeTrust(UserKeypair, IssuerPublicKey, client)
        log.Println("Transaction Hash: ", ChangeTrustResponse2)

        // User Buys the Coin in exchange for XLMS
        log.Println("STEP 5:User Buys the Coin in exchange for XLMS")
        OfferCoinExchangeResponse := <-OfferCoinExchange(UserKeypair,
DistributorKeypair, IssuerPublicKey, client)
        log.Println("Transaction Hash: ", OfferCoinExchangeResponse)

}
// ChangeTrust creates and submits the create trust operationfunc
ChangeTrust(DistributorKeypair *keypair.Full, IssuerPublicKey string,
        client *horizonclient.Client) <-chan string {

        res := make(chan string)

        go func() {
                defer close(res)

                // Get information about the Distributor account
                accountRequest := horizonclient.AccountRequest{AccountID:
DistributorKeypair.Address()}
                Account, err := client.AccountDetail(accountRequest)
                if err != nil {
                        log.Fatal(err)
                }

                // Construct the operation
                changeTrustOp := txnbuild.ChangeTrust{
                        Line: txnbuild.CreditAsset{
                                Code:   "eHryvnia",
                                Issuer: IssuerPublicKey,
                        },
```

```
                Limit:         "200000000000",
                SourceAccount: &Account,
            }

            // Construct the transaction that will carry the operation
            tx := txnbuild.Transaction{
                SourceAccount: &Account,
                Operations:    []txnbuild.Operation{&changeTrustOp},
                Network:       network.TestNetworkPassphrase,
                Timebounds:    txnbuild.NewInfiniteTimeout(),
            }

            // Sign the transaction, serialise it to XDR, and base 64 encode it
            txeBase64, err := tx.BuildSignEncode(DistributorKeypair)
            if err != nil {
                hError := err.(*horizonclient.Error)
                log.Fatal("Error submitting transaction:", hError)
            }
            // log.Println("txeBase64: ", txeBase64)

            // Submit the transaction
            resp, err := client.SubmitTransactionXDR(txeBase64)
            if err != nil {
                hError := err.(*horizonclient.Error)
                log.Fatal("Error submitting transaction:", hError)
            }

            res <- resp.Hash
        }()

        return res

}
// FundDistributor creates and submits the payment operation to fund the
distributorfunc FundDistributor(IssuerKeypair *keypair.Full, DistributorPublicKey
string,
        client *horizonclient.Client) <-chan string {

        res := make(chan string)

        go func() {
            defer close(res)
            // Get information about the Distributor account
            accountRequest := horizonclient.AccountRequest{AccountID:
IssuerKeypair.Address()}
            Account, err := client.AccountDetail(accountRequest)
```

```
		if err != nil {
			log.Fatal(err)
		}

		// Construct the operation
		paymentOp := txnbuild.Payment{
			Destination: DistributorPublicKey,
			Amount:      "1000000",
			Asset: txnbuild.CreditAsset{
				Code:   "eHryvnia",
				Issuer: IssuerKeypair.Address(),
			},
			SourceAccount: &Account,
		}

		// Construct the transaction that will carry the operation
		tx := txnbuild.Transaction{
			SourceAccount: &Account,
			Operations:    []txnbuild.Operation{&paymentOp},
			Network:       network.TestNetworkPassphrase,
			Timebounds:    txnbuild.NewInfiniteTimeout(),
		}

		// Sign the transaction, serialise it to XDR, and base 64 encode it
		txeBase64, err := tx.BuildSignEncode(IssuerKeypair)
		if err != nil {
			hError := err.(*horizonclient.Error)
			log.Fatal("Error submitting transaction:", hError)
		}
		// log.Println("txeBase64: ", txeBase64)

		// Submit the transaction
		resp, err := client.SubmitTransactionXDR(txeBase64)
		if err != nil {
			hError := err.(*horizonclient.Error)
			log.Fatal("Error submitting transaction:", hError)
		}

		res <- resp.Hash
	}()
	return res

}
// LockIsuer creates and submits the set option operation to lock accountfunc
LockIsuer(IssuerKeypair *keypair.Full, client *horizonclient.Client) <-chan string
{
```

```
	res := make(chan string)

	go func() {
		// Get information about the Issuer account
		accountRequest := horizonclient.AccountRequest{AccountID:
IssuerKeypair.Address()}
		Account, err := client.AccountDetail(accountRequest)
		if err != nil {
			log.Fatal(err)
		}

		// Construct the operation
		setOptionsOpp := txnbuild.SetOptions{MasterWeight:
txnbuild.NewThreshold(0)}

		// Construct the transaction that will carry the operation
		tx := txnbuild.Transaction{
			SourceAccount: &Account,
			Operations:    []txnbuild.Operation{&setOptionsOpp},
			Network:       network.TestNetworkPassphrase,
			Timebounds:    txnbuild.NewInfiniteTimeout(),
		}

		// Sign the transaction, serialise it to XDR, and base 64 encode it
		txeBase64, err := tx.BuildSignEncode(IssuerKeypair)
		if err != nil {
			hError := err.(*horizonclient.Error)
			log.Fatal("Error submitting transaction:", hError)
		}
		// log.Println("txeBase64: ", txeBase64)

		// Submit the transaction
		resp, err := client.SubmitTransactionXDR(txeBase64)
		if err != nil {
			hError := err.(*horizonclient.Error)
			log.Fatal("Error submitting transaction:", hError)
		}

		res <- resp.Hash

	}()
	return res

}
```

```
// OfferCoinExchange creates and submits the coin exchange payment multi-signature transactionfunc OfferCoinExchange(UserKeypair *keypair.Full, DistributorKeypair *keypair.Full,
	IssuerPublicKey string, client *horizonclient.Client) <-chan string {
	res := make(chan string)

	go func() {
		defer close(res)

		// Get information about the User's account
		UserAccountRequest := horizonclient.AccountRequest{AccountID: UserKeypair.Address()}
		UserAccount, err := client.AccountDetail(UserAccountRequest)
		if err != nil {
			log.Fatal(err)
		}

		// Get information about the DistributorRequest's account
		DistributorRequest := horizonclient.AccountRequest{AccountID: DistributorKeypair.Address()}
		DistributorAccount, err := client.AccountDetail(DistributorRequest)
		if err != nil {
			log.Fatal(err)
		}

		log.Println("User's Wallet Before")
		//View account balance
		for _, Bal := range UserAccount.Balances {
			if Bal.Asset.Code == "" {
				log.Println("Asset Type:"+Bal.Asset.Type, "Asset Code:XLM", "Asset Balance:"+Bal.Balance)
			} else {
				log.Println("Asset Type:"+Bal.Asset.Type, "Asset Code:"+Bal.Asset.Code, "Asset Balance:"+Bal.Balance)
			}
		}

		//Assign Native Asset Interface
		nativeAsset := txnbuild.NativeAsset{}

		// Construct the operation
		paymentOp1 := txnbuild.Payment{
			SourceAccount: &UserAccount,
			Destination:   DistributorKeypair.Address(),
			Amount:        "5",
			Asset:         nativeAsset,
```

```
	}

	paymentOp2 := txnbuild.Payment{
		SourceAccount: &DistributorAccount,
		Destination:   UserKeypair.Address(),
		Amount:        "1",
		Asset: txnbuild.CreditAsset{
			Code:   "eHryvnia",
			Issuer: IssuerPublicKey,
		},
	}

	// Construct the transaction that will carry the operation
	tx := txnbuild.Transaction{
		SourceAccount: &UserAccount,
		Operations:    []txnbuild.Operation{&paymentOp1,
&paymentOp2},
		Network:       network.TestNetworkPassphrase,
		Timebounds:    txnbuild.NewInfiniteTimeout(),
	}

	// User signs the transaction, serialise it to XDR, and base 64
encode it
	txeBase64A, err := tx.BuildSignEncode(UserKeypair)
	if err != nil {
		log.Fatal("Error Building transaction:", err)
	}

	//Distributor receives xdr and opens as xdr
	txn, errXDR := txnbuild.TransactionFromXDR(txeBase64A)
	if errXDR != nil {
		log.Fatal("Error decoding xdr:", errXDR)
	}

	txn.Network = network.TestNetworkPassphrase
	// Distributor signs the transaction if right, serialises it to XDR,
and base 64 encode it
	errS := txn.Sign(DistributorKeypair)
	if errS != nil {
		log.Fatal("Error submitting transaction:", errS)
	}

	txeBase64B, err := txn.Base64()
	if err != nil {
		log.Fatal("Error encoding transaction:", err)
	}
```

```
                // Submit the transaction
                resp, err := client.SubmitTransactionXDR(txeBase64B)
                if err != nil {
                        hError := err.(*horizonclient.Error)
                        log.Fatal("Error submitting transaction:", hError)
                }

                // log.Println("Transaction Hash: ", resp.Hash)

                UserAccount, err = client.AccountDetail(UserAccountRequest)
                if err != nil {
                        log.Fatal(err)
                }

                log.Println("User's Wallet After")
                //View User account balance
                for _, Bal := range UserAccount.Balances {
                        if Bal.Asset.Code == "" {
                                log.Println("Asset Type:"+Bal.Asset.Type, "Asset
Code:XLM", "Asset Balance:"+Bal.Balance)
                        } else {
                                log.Println("Asset Type:"+Bal.Asset.Type, "Asset
Code:"+Bal.Asset.Code, "Asset Balance:"+Bal.Balance)
                        }
                }

                res <- resp.Hash

        }()

        return res

}
```