Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Чорного Дмитра Віталійовича*
академічної групи *125м-22-1*
спеціальності *125 Кібербезпека*
спеціалізації[1]
за освітньо-професійною програмою *Кібербезпека*
на тему *Розробка рекомендацій щодо застосування blockchain технології в системах електронних платежів*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Чорному Дмитру Віталійовичу* **академічної групи** *125м-22-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка рекомендацій щодо застосування blockchain технології в системах електронних платежів***

затверджену наказом ректора НТУ «Дніпровська політехніка» від р. №

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання та постановка завдання	28.10.2023
Розділ 2	Інтеграція та інновації: Stellar як ключовий інструмент для модернізації банківських електронних платежів в Україні.	16.11.2023
Розділ 3	Економічний аналіз: визначення впливу інтеграції Stellar на фінансові показники Національного банку України.	08.12.2023

Завдання видано _____ _____
(підпис керівника) (ім'я, прізвище)

Дата видачі: 16.10.2023 р.

Дата подання до екзаменаційної комісії: 11.12.2023 р.

Прийнято до виконання _____ Дмитро Чорний
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 154 с., 16 рис., 34 табл., 4 додатка, 29 джерел.

Об`єкт дослідження: процес ідентифікації інформаційних активів в системах електронних платежів з використанням блокчейн-технології.

Мета роботи: Підвищити рівень безпеки систем електронних платежів шляхом впровадження блокчейн-технології.

Методи розробки: спостереження, порівняння, аналіз та опис.

У першому розділі роботи проведено аналіз технології блокчейн та її застосування у системах електронних платежів, досліджено впровадження стандарту ISO 20022 в платіжну інфраструктуру України та роль компанії Stellar, з порівняльними характеристиками з іншими провідними технологіями.

У другому розділі надано детальний опис взаємодії НБУ та користувачів з технологією Stellar, розглянуто архітектуру та встановлення платформи Anchor, а також платформи Stellar Disbursement Platform. Також описано процес запуску та інтеграції Stellar, включаючи, налаштування та моніторинг.

У третьому розділі досліджено економічний аспект впровадження технології у систему електронних платежів, включаючи аналіз капітальних та операційних витрат, а також загальний економічний ефект від оновлення системи. Проведено розрахунки показників окупності інвестицій та оцінку терміну окупності проекту, а також аналіз ризиків та невизначеностей проекту.

Наукова новизна роботи полягає у розробці рекомендацій щодо застосування блокчейн-технології для підвищення рівня безпеки та ефективності систем електронних платежів, а практичне значення - у наданні конкретних напрямків для оптимізації та розвитку таких систем.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІДЕНТИФІКАЦІЯ, ІНФОРМАЦІЙНИЙ АКТИВ, КІБЕРБЕЗПЕКА, РЕЄСТР ІНФОРМАЦІЙНИХ АКТІВІВ, БЛОКЧЕЙН, STELLAR, НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

ABSTRACT

Explanatory note: 154 p., 16 pics., 34 tabl., 4 app., 29 sources.

Object of research: the process of identifying information assets in electronic payment systems using blockchain technology.

Objective: To improve the security of electronic payment systems by implementing blockchain technology.

Research methods: observation, comparison, analysis, and description.

The first section of the paper analyzes the blockchain technology and its application in electronic payment systems, examines the implementation of the ISO 20022 standard in Ukraine's payment infrastructure and the role of Stellar, with comparative characteristics with other leading technologies.

The second section provides a detailed description of the interaction of the NBU and users with Stellar technology, describes the architecture and installation of the Anchor platform and the Stellar Disbursement Platform. It also describes the process of launching and integrating Stellar, including configuration and monitoring.

The third section examines the economic aspect of implementing the technology in the electronic payment system, including the analysis of capital and operating costs, as well as the overall economic effect of the system upgrade. The article calculates the return on investment and estimates the payback period of the project, as well as analyzes the risks and uncertainties of the project.

The scientific novelty of the work lies in the development of recommendations for the use of blockchain technology to improve the security and efficiency of electronic payment systems, and the practical significance lies in the provision of specific areas for optimizing and developing such systems.

INFORMATION SECURITY, IDENTIFICATION, INFORMATION ASSET, CYBERSECURITY, REGISTER OF INFORMATION ASSETS, BLOCKCHAIN, STELLAR, NATIONAL BANK OF UKRAINE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСД - Автоматизовані системи документообігу.

БД - Бази даних.

БТ - Блокчейн технологія.

БФ - Банківська функція.

ДБ - Діяльність банку.

ЕП - Електронні платежі.

ЗМГ - Засоби масової комунікації та зв'язку.

ІРК - Індивідуальний рахунок клієнта.

ІТ - Інформаційні технології.

КБ - кібербезпека

КР - Комісійні розрахунки.

ЛК - Лічильник транзакцій.

МБ - Методи блокчейну.

НДР - Національна документація та звітність.

ППД - Публічний розподіл даних.

РР - Розподілений реєстр.

СА - Спеціальний агент.

СЕП - Системи електронних платежів.

СМК - Системи масових комунікацій.

ТЗ - Технічне завдання.

ФС - Фінансовий сектор.

AML - Anti-Money Laundering (Боротьба з відмиванням грошей).

API - Application Programming Interface (Інтерфейс програмування додатків).

CBDC - Central Bank Digital Currency (Центральна банківська цифрова валюта).

Consensus - Консенсус (у контексті блокчейн технології).

Cryptocurrency - Криптовалюта.

DLA - Distributed Ledger Application (Додаток для розподіленого реєстру).

DLT - Distributed Ledger Technology (Технологія розподіленого реєстру).

Decentralized - Децентралізований.

Fintech - Фінтех (фінансові технології).

Immutable - Незмінний (про дані в блокчейні).

IoT - Internet of Things (Інтернет речей).

KYC - Know Your Customer (Знай свого клієнта).

NBU - Національний банк України.

Node - Вузол (у мережі блокчейн).

PoS - Proof of Stake (Доказ власності).

PoW - Proof of Work (Доказ роботи).

Q - Квартал

Smart Contract - Розумний контракт.

Stellar - Сама назва блокчейн-платформи.

Tokenization - Токенізація.

Transaction - Транзакція.

ЗМІСТ

ВСТУП

Актуальність дослідження

У сучасному світі, який постійно розвивається в галузі інформаційних технологій та фінансових послуг, питання кібербезпеки та ефективного управління електронними транзакціями стають все більш важливими та актуальними. З впровадженням стандарту ISO20022 та блокчейн-технології з'явилися нові можливості та виклики, які вимагають глибокого дослідження та розробки відповідних рекомендацій.

Проблема, яку розглядає дана магістерська робота, полягає в необхідності оптимізації процесу ідентифікації інформаційних активів об'єктів захисту в системах ЕП з використанням технології блокчейн. Ця проблема стає особливо актуальною в умовах зростаючих загроз кібербезпеці та зменшення довіри до традиційних фінансових послуг.

Актуальність даного дослідження в сучасному контексті визначається необхідністю забезпечення безпеки та ефективності ЕП у глобальному масштабі. Національний банк України за міжнародним стандартом ISO20022 вже інтегрував технологію від компанії Stellar, що свідчить про реальну можливість використання цієї технології в сфері фінансів. Таким чином, дослідження, спрямоване на розробку рекомендацій щодо застосування БТ в системах електронних платежів, є актуальним та важливим для подальшого розвитку цієї галузі.

Дана магістерська робота ставить за мету внести вклад у розв'язання цієї проблеми та надати практичні рекомендації для покращення ідентифікації інформаційних активів, що використовують блокчейн-технологію.

Об'єкт дослідження

Об'єктом дослідження є процес ідентифікації інформаційних активів в системах електронних платежів, які використовують технологію блокчейн від Stellar.

Мета дослідження

Основною метою даної магістерської роботи є розробка рекомендацій щодо застосування БТ в системах ЕП, зокрема в НБУ, який інтегрував цю технологію. Головною метою є покращення системи електронних платежів, забезпечення її безпеки та надійності з використанням інноваційних технологій.

Завдання дослідження

Для досягнення основної мети магістерської роботи передбачається виконання завдань зазначених у таблиці 1.

Таблиця 1. Завдання дослідження

№	Завдання
1	Аналіз літературних джерел та нормативно-правової бази у сфері блокчейн-технології, систем електронних платежів і кібербезпеки.
2	Вивчення організаційного забезпечення ідентифікації інформаційних активів у системах електронних платежів.
3	Аналіз існуючих автоматизованих засобів для збору інформації та їхньої застосовності у контексті ідентифікації інформаційних активів.
4	Розробка методики проведення ідентифікації інформаційних активів у системах електронних платежів на базі блокчейн-технології.
5	Визначення економічної доцільності розробки та впровадження розробленої методики.
6	Розрахунок капітальних (фіксованих) та поточних (експлуатаційних) витрат на впровадження рекомендацій.
7	Оцінка загального збитку від можливої атаки на інформаційну безпеку систем електронних платежів.
8	Аналіз загального ефекту від впровадження рекомендацій та блокчейн-технології у системи електронних платежів.

Ці завдання є необхідними кроками для досягнення мети роботи та розробки конкретних рекомендацій щодо ідентифікації інформаційних активів в системах електронних платежів з використанням БТ.

Предмет дослідження

Предметом дослідження є процес ідентифікації інформаційних активів в системах ЕП та розробка рекомендацій для покращення цього процесу з використанням технології стандарту ISO20022.

Методи дослідження

Для здійснення дослідження в магістерській роботі використовуються методи зазначені у таблиці 2.

Таблиця 2. Методи дослідження

№	Метод	Опис
1	Аналіз літературних джерел	Проведення огляду та аналізу наукової літератури та публікацій з питань блокчейн-технології, систем електронних платежів, кібербезпеки та ідентифікації інформаційних активів.
2	Спостереження	Аналіз та спостереження за функціонуванням систем електронних платежів, які використовують технологію блокчейн, з метою збору практичних даних та вивчення їхнього функціонування.
3	Порівняння	Порівняння різних підходів та методів ідентифікації інформаційних активів у системах електронних платежів з використанням блокчейн-технології з метою визначення найкращих практик.
4	Аналіз	Глибокий аналіз отриманих даних та інформації з метою визначення проблем, можливостей та ризиків ідентифікації інформаційних активів у системах електронних платежів на основі блокчейн-технології.
5	Опис	Розробка детального опису розробленої методики ідентифікації інформаційних активів з використанням блокчейн-технології та рекомендацій щодо її впровадження

Ці методи дослідження дозволять систематизувати інформацію, провести аналіз та розробити конкретні рекомендації щодо ідентифікації інформаційних активів в системах електронних платежів з використанням блокчейн-технології.

Наукова новизна

Науковою новизною даної магістерської роботи є:

- Розробка методики ідентифікації інформаційних активів в системах електронних платежів на основі блокчейн-технології, що враховує специфіку цієї технології та вимоги до кібербезпеки.
- Визначення економічної доцільності та розрахунок витрат та можливого збитку від атаки на інформаційну безпеку систем електронних платежів з використанням блокчейн-технології.
- Встановлення практичного значення розробленої методики та рекомендацій для систем електронних платежів, зокрема для Національного банку України, який інтегрував технологію блокчейн від компанії Stellar.

Дана робота спрямована на заповнення наукового та практичного пустоти у галузі ідентифікації інформаційних активів у сучасних системах електронних платежів з використанням блокчейн-технології, що відкриває перспективи для подальшого розвитку цього напрямку та підвищення рівня кібербезпеки в фінансовій сфері.

Практичне значення

Практичне значення даної магістерської роботи полягає в наступному:

- Надання конкретних рекомендацій для покращення систем електронних платежів, що використовують технологію блокчейн, зокрема в Національному банку України, з погляду ідентифікації інформаційних активів.
- Підвищення ефективності процесу ідентифікації інформаційних активів у системах електронних платежів, що дозволить забезпечити вищий рівень кібербезпеки та надійності фінансових операцій.
- Розрахунок економічної доцільності впровадження рекомендацій та блокчейн-технології, що допоможе раціоналізувати витрати та зменшити можливий збиток від кібератак.
- Посилення захисту інформаційної безпеки в системах електронних платежів, що є критично важливим для фінансового сектору та забезпечує довіру користувачів до електронних фінансових послуг.

Отже, результати даного дослідження мають практичне застосування і можуть бути використані фінансовими установами, в тому числі НБУ, для покращення систем ЕП та забезпечення їхньої безпеки та ефективності.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Технологія Блокчейн

Блокчейн (англ. blockchain, block chain від block — блок, chain — ланцюг, тобто ланцюжок блоків) — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево. Інформація про транзакції зазвичай надається відкритою, не шифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку у наступний блок. Тому внесення змін в один з блоків вимагає відповідних змін в усіх блоках після нього, що зазвичай виявляється або дуже складно, або дуже коштовно.

Таку розподілену базу даних закладено в основу криптовалюти Bitcoin (вона була описана 2008 і реалізована 2009 року). По суті, це своєрідна книга обліку всіх операцій.

Наглядно блок схема транзакцій показана на Рисунку 1.1.

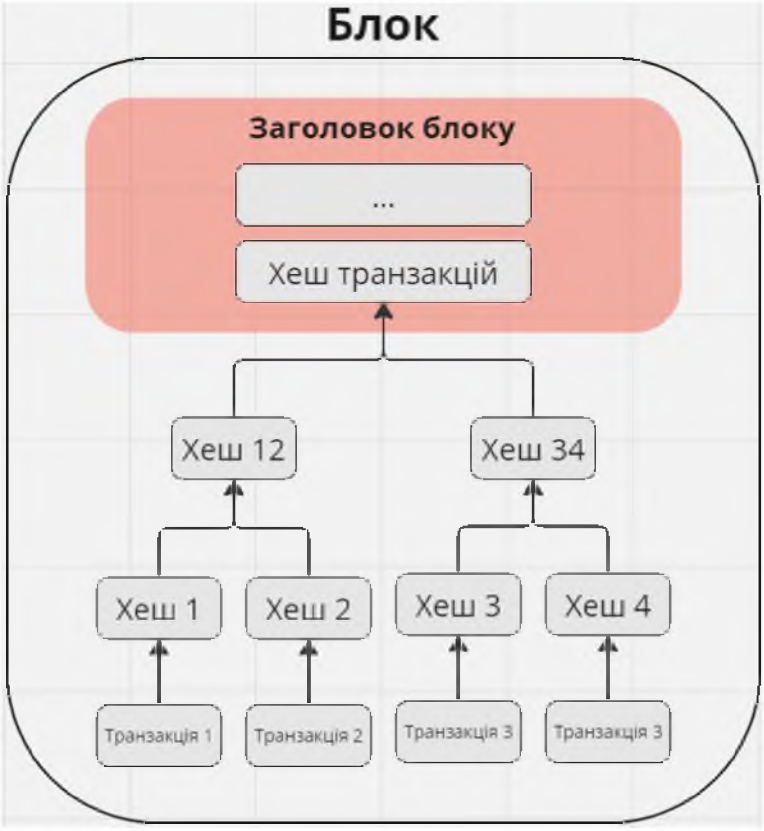

Рисунок 1.1. Схема блоку транзакій

1.1.1. Блок транзакцій

Блок транзакцій — спеціальна структура для запису нових транзакцій в системі Біткоїн та аналогічних їй

Блок містить відомості про транзакції, дерево їхніх хешів, а також заголовок зі службовими даними, де зокрема наведено і хеш попереднього блока, тож кожен наступний блок є також підтвердженням попереднього.

Щоб транзакція вважалася достовірною («підтвердженою»), її формат та підписи мусять перевірити й записати (разом з іншими транзакціями) в новий блок. Але справді надійна перевірка достовірності транзакції потребує наявності декількох наступних блоків. Кожен наступний блок посилається на попередній, тож усі блоки можна вишикувати в один ланцюжок, що являтиме собою історію транзакцій за ввесь час існування системи. Перший блок ланцюжка — первинний блок (англ. genesis block) — то окремий випадок, бо в нього відсутній материнський блок

Блок складається із заголовка та списку транзакцій. Заголовок блоку містить свій хеш, хеш попереднього блоку, хеші транзакцій та додаткову службову інформацію. Першою транзакцією в блоку завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоку використовується деревисте хешування, аналогічне формуванню хеш-суми файлу в протоколі BitTorrent. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію, за якою на цей рахунок були отримані біткоїни. Комісійні операції можуть містити в атрибуті будь-яку інформацію (для них це поле носить назву англ. Coinbase parameter), оскільки у них немає батьківських транзакцій.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка менше або дорівнює певному числу, величина якого періодично коригується. Оскільки результат хешування (функції SHA-256) необоротний, немає алгоритму отримання бажаного результату, окрім повного перебору чи пошуку навмання. Якщо хеш не задовольняє умову, то

довільно змінюється блок службової інформації в заголовку, а хеш обчислюється знов. Зазвичай потрібно чимало переобчислень. Коли умову дотримано, вузол висилає створений блок іншим підключеним вузлам, а ті його перевіряють. Якщо помилок немає, то блок вважається доданим в ланцюжок, і вже його хеш міститиме наступний блок.

Величина цільового числа, з яким порівнюється хеш, коригується через кожні 2016 блоків. Заплановано, що вся мережа витрачатиме на створення одного блоку приблизно 10 хвилин, на 2016 блоків — близько двох тижнів. Якщо 2016 блоків сформовано швидше, то ціль трохи зменшують і досягти її стає важче, інакше ціль збільшують. Зміна складності обчислень не впливає на надійність мережі Біткоїн і потрібна лише для того, щоб система створювала блоки з майже постійною швидкістю незалежно від потужності мережі.

1.1.2. Ланцюжок блоків

Над створенням нових блоків одночасно працює чимало «майнерів». Новостворений блок, що відповідає певним умовам, негайно надсилається решті членів мережі і має стати наступною ланкою ланцюжка. Постійно трапляється таке, що з різних частин мережі (від різних учасників) надходять блоки, що попереднім називають той самий блок, тобто відбувається галуження. Навмисне чи ненароком можна обмежити поширення новостворених блоків (наприклад, одне з галужень ланцюжка може деякий час розвиватися в межах локальної мережі). Тоді одночасно відбувається створення кількох гілок одного ланцюжка, що суперечать одна одній.

Коли поширення блоків поновлюється, майнери розв'язують суперечність, обираючи найдовшу гілку з найбільшим рівнем складності за єдину «достовірну». За однакової складності і довжини перевага віддається гілці, кінцевий блок якої з'явився раніше. Суперечні гілки можуть містити різні множини транзакцій, тобто не всяка транзакція конче присутня в усіх

гілках. Тож транзакції, що входять лише до відхиленої гілки (зокрема, транзакції з виплати винагороди), втрачають підтвердженість.

Кожну транзакцію переказу коштів, що містилась лише у відхилених гілках, знов буде поставлено в чергу, а відтак включено в черговий блок. Натомість транзакції з одержання винагороди за створення відхилених зрештою блоків не отримають дальших підтверджень і відповідні «зайві» кошти буде втрачено.

Розподілена база даних Blockchain — це ланцюжок блоків, що постійно зростає, зберігаючи всю історію транзакцій. Копія бази даних або її частини одночасно зберігаються на безлічі комп'ютерів та синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Дані блоків не шифровані і доступні у відкритому вигляді, проте захищені від змін криптографічно через хеш-ланцюжок.

Зазвичай умисна зміна інформації в будь-якій копії бази або навіть в багатьох копіях не буде визнана істинною, бо не відповідатиме правилам. Деякі зміни може бути прийнято, якщо їх внести в усі копії бази (наприклад, видалення кількох останніх блоків через помилку в їхньому формуванні).

До версії 0.8.0 для зберігання ланцюжка блоків основний клієнт використовував Berkeley DB, починаючи з версії 0.8.0 розробники перейшли на LevelDB

Приклад ланцюжка блоків показаний на Рисунку 1.2.

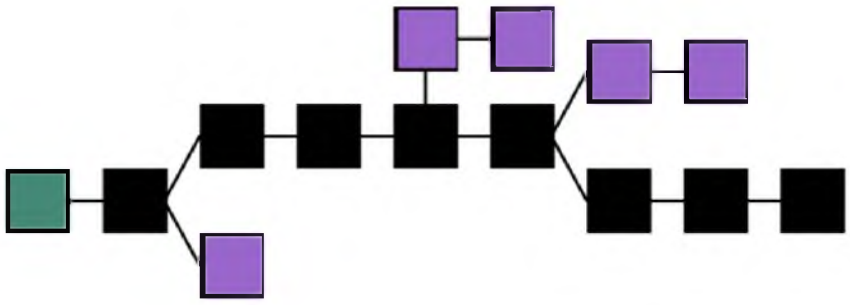

Рисунок 1.2. Ланцюг блоків

Основна послідовність блоків (чорні) є найдовшою від початкового (зелений) до поточного. Побічні гілки (фіолетові) відсікаються.

1.1.3. Підтвердження транзакцій

Поки транзакція не включена в блок, система вважає, що кількість біткоїнів за якоюсь адресою залишається незмінною. У цей час є технічна можливість оформити кілька різних транзакцій для передачі з однієї адреси одних і тих же біткоїнів різним одержувачам. Але як тільки одна з подібних транзакцій буде включена в блок, то інші транзакції з цими ж біткоїнами система вже буде ігнорувати.

Наприклад, якщо в блок буде включена більш пізня транзакція, то більш рання буде вважатися помилковою. Є невелика ймовірність, що при розгалуженні дві подібні транзакції потраплять в блоки різних гілок. Кожна з них буде вважатися правильною, лише при відмиранні гілки одна з транзакцій стане вважатися помилковою. При цьому не буде мати значення час здійснення операції.

Отож попадання транзакції в блок є підтвердженням її достовірності незалежно від наявності інших транзакцій з тими ж біткоїнами. Кожен новий блок вважається додатковим підтвердженням транзакцій з попередніх блоків. Якщо в ланцюжку три блоки, то транзакції з останнього блоку будуть підтверджені один раз, а поміщені в перший блок будуть мати три підтвердження. Досить дочекатися декількох підтверджень, щоб звести ймовірність скасування транзакції до мінімуму.

Для зменшення впливу таких ситуацій на мережу існують обмеження на розпорядження щойно отриманими біткоїнами. Згідно сервісу blockchain.info до травня 2015 року максимальна довжина відкинутих ланцюжків була 5 блоків. Необхідне число підтверджень для розблокування отриманого залежить від програми-клієнта або від вказівок приймаючої сторони. Клієнт «Bitcoin-qt» для відправлення не потребує наявності підтверджень, однак у більшості одержувачів за замовчуванням виставлено вимогу 6 підтверджень, тобто реально скористатися отриманим зазвичай можна через годину. Різні онлайн-сервіси часто встановлюють свій поріг підтверджень.

Біткоїни, отримані за створення блоку, протокол дозволяє використовувати після 100 підтверджень, але стандартна програма-клієнт показує комісію через 120 підтверджень, тобто зазвичай скористатися комісією можна приблизно через 20 годин після її нарахування.

1.1.4. Складність

За вимогу до хешів блоків відповідає спеціальний параметр, званий «складність». Оскільки обчислювальні потужності мережі непостійні, цей параметр перераховується клієнтами мережі через кожні 2016 блоків таким чином, щоб підтримувати середню швидкість формування розподіленої БД на рівні 2016 блоків за два тижні. Таким чином 1 блок повинен створюватися приблизно раз на десять хвилин. На практиці, коли обчислювальна потужність мережі зростає — відповідні часові проміжки коротші, а коли знижується — довші.

Перерахунок складності з прив'язкою до часу можливий завдяки наявності в заголовках блоків часу їх створення. Він записаний в Unix-форматі і взятий за системним годинником автора блоку (якщо блок створений у пулі, то за системним годинником сервера цього пулу). Використання технології показано у таблиці 1.1. Використання блокчейну

Таблиця 1.1. Використання блокчейну

Використання	Опис
Україна	В 2017 році технологія блокчейн була використана для оновленої системи електронних торгів арештованим майном СЕТАМ. У жовтні 2017 року із використанням блокчейн було реалізовано оновлену версію інформаційної системи державного земельного кадастру.
У світі	Мер столиці Південної Кореї оголосив про намір зробити з Сеула «розумне» місто на блокчейні. Стратегія має назву Blockchain Urban Plan, розрахована на 2018 - 2022 роки.

Продовження таблиці 1.1.

	Інновації охоплять 14 державних служб у 5 галузях. Основні служби, які переведуть на блокчейн, - це соцзабезпечення, архів експлуатації транспортних засобів, видача сертифікатів, керування пожертвами та система голосування
Військова сфера	Різні випадки потенційного використання блокчейну у мультидоменних операціях обговорюються у військових спільнотах. У цьому контексті блокчейн визначають як цифрову інформаційну систему для передачі даних у зашифрованому розподіленому форматі на полі бою в різних доменах. Вважається, що технологія блокчейну є перехідною від традиційної мережі даних до використання квантово заплутаного зв'язку. До переліку можливих випадків застосування блокчейну у військових операціях слід віднести крипто-захищену цифрову ідентифікацію та доступ до цифрових близнюків, смарт-контракти як процедуру видачі наказів військам і виконання логістичних запитів, обмін даними доповненої реальності на полі бою, моніторинг здоров'я солдат та стану озброєння чи військової техніки тощо. З іншого боку, технологію блокчейну слід поєднувати з машинним навчанням. Як приклад, блокчейн доцільно використовувати для узгодженого оновлення кількох ідентичних нейронних мереж дронів у складі рою з метою адаптації до нових ситуацій або підвищення точності.

1.2. Блокчейн-ноди та види криптовалютних нод

1.2.1. Технічні особливості нод

Нода (вузол) - це точка в блокчейн-мережі, основна функція якої зводиться до розподілу даних між іншими вузлами. Це потрібно для передачі інформації всередині блокчейна з одночасним збереженням ефекту

децентралізації. Нода може бути проміжною ланкою або кінцевим одержувачем даних.

Нода - це комп'ютер (сервер) зі встановленим криптовалютним гаманцем, який синхронізовано з іншими такими ж комп'ютерами. Зв'язка таких вузлів утворює блокчейн. Використання подібної мережі дає можливість швидко розподіляти великі потоки даних.

Робота ноди забезпечується за рахунок потужностей сервера. Для цього підійде будь-який пристрій, який може передавати інформацію через інтернет. Також для функціонування вузла необхідне спеціальне програмне забезпечення.

У більшості випадків node використовується для виконання 3 завдань:

- Зберігати та поширювати між вузлами інформацію про транзакції та кількість коштів у гаманцях учасників мережі.
- Контролювати виконання правил мережі (алгоритм консенсусу PoS, PoW тощо).
- Підтримувати роботу розподілених реєстрів, у яких зберігається інформація про транзакції за весь час існування мережі.

Ноди не можуть працювати без підключення до інтернету. Офлайн-пристрій для зберігання інформації теж не здатний виконувати функцію вузла. Але він стає повноцінною нодою, якщо його під'єднати до інтернету.

1.2.2. Навіщо потрібні ноди

Для підтримки стабільної роботи блокчейну потрібна мережа серверів, які синхронізовані між собою. Основна цінність такої мережі полягає в забезпеченні ефекту децентралізації без втрати швидкості взаємодії масивів інформації.

З огляду на те, що комп'ютери-вузли розташовані в різних країнах і містах, навіть блокування інтернету в окремому регіоні не призведе до зупинки роботи блокчейна. Але якщо всі ноди будуть зосереджені в руках

однієї групи людей, то вони зможуть повністю контролювати мережу, що може призвести до обмеження ефекту децентралізації.

Водночас децентралізація - це одна з ключових переваг криптовалют. Щоб її забезпечити та отримати ефект розподілу даних, блокчейн використовує численні незначущі вузли. Вони не беруть участі в майнінгу, але зберігають у собі всю історію транзакцій. Завдяки цьому одна обмежена група людей не може взяти контроль над розподіленим реєстром.

Користувачі, які надали свої обчислювальні потужності для забезпечення роботи блокчейна, отримують за це винагороду. Так проєкт мотивує людей підключати свої ПК до розподіленої мережі.

1.2.3. Види нод

Повні ноди (Full nodes)

Це найперший варіант вузла, який був спочатку створений для роботи біткоїна. Повні ноди формують основу блокчейна і беруть участь у завершенні транзакцій.

Така нода містить у собі всю інформацію про транзакції та блоки з моменту запуску мережі до поточного часу. Коли один користувач переказує монети, цю операцію "бачать" усі вузли і зберігають у своїй історії.

В одному блокчейні можуть одночасно працювати десятки тисяч повних нод. Усі вони постійно обмінюються інформацією між собою. Для обробки такого великого потоку даних необхідна достатня обчислювальна потужність.

Якщо користувач уперше встановлює повну ноду на свій ПК, вона має синхронізуватися, тобто завантажити весь блокчейн. У разі деяких блокчейнів це займає досить багато пам'яті. Наприклад, обсяг блокчейна біткоїна в листопаді 2022 року становив 438 Гбайт, і на його синхронізацію може знадобитися кілька тижнів.

Якщо нода відключається від мережі на деякий час, то при підключенні вона повинна повторно синхронізуватися, тобто завантажити всю інформацію, яка була згенерована за період її відсутності.

Повні ноди мають певний набір опцій, які відрізняють їх від інших видів нод у мережі. Одна з найважливіших функцій полягає в перевірці підписів (ключів) для підтвердження транзакцій і блоків. У разі виявлення помилки нода може відхилити операцію. Причини можуть бути різні: неправильне форматування, помилки алгоритмів, дублювання, маніпуляції із записами тощо.

Користувачі, у яких є повний вузол мережі, можуть самі перевіряти вхідні перекази. За бажання у них також є можливість брати участь у майнінгу та отримувати за це винагороду.

Полегшені ноди (Light nodes)

Полегшені ноди не містять повної інформації про блокчейн. У такому вузлі зберігається тільки запис про блок, до якого він підключений. У більшості випадків такі ноди не працюють безперервно.

Як правило, полегшена нода - це ПЗ, яке підключається до повної ноди і ретранслює з неї інформацію на комп'ютер користувача - наприклад, відомості про баланс рахунку, вхідні та вихідні транзакції. Фактично, легка нода використовує повну ноду як перехідник для доступу до блокчейну.

Легкий вузол має необхідний набір функцій для використання криптовалюти, при цьому не вимагаючи великих обчислювальних потужностей або обсягу пам'яті. Тому його можна запустити навіть на мобільному пристрої. Як правило, синхронізація займає лічені секунди.

Урізані повні ноди (Pruned full nodes)

Така нода завантажує весь блокчейн і синхронізує його тільки під час першого запуску. Далі вона автоматично довантажує нові блоки і видаляє старі при досягненні певного обсягу пам'яті. Зазвичай користувач може сам встановити в налаштуваннях розмір ноди, наприклад 10 Гбайт.

Майнінг-ноди (Mining nodes)

Майнінг-нода бере участь у процесі майнінгу криптовалюти і застосовується тільки в блокчейнах на алгоритмі Proof of Work. Вона може бути повною або полегшеною.

Для запуску такої ноди користувачеві необхідно мати потужне обчислювальне обладнання:

- центральний процесор (CPU);
- графічний процесор (GPU);
- інтегральну схему спеціального призначення (ASIC).

Також знадобиться встановити спеціальне програмне забезпечення.

Так, у процесі майнінгу біткоїна необхідно розв'язувати складні математичні задачі. У результаті таких обчислень майнер знаходить унікальне значення коду - хеш, який служить доказом виконаної роботи.

Далі майнер пересилає знайдений хеш іншим нодам, які повинні його перевірити на відповідність поставленому завданню. Якщо перевірка буде успішною, майнер може додати новий блок і отримати за це винагороду.

Стейкінг-ноди (Staking nodes)

Це аналог майнінг-нод, який використовується в блокчейнах з алгоритмом Proof of Stake. Такий вузол теж потрібен для перевірки транзакцій і додавання нових блоків, і він також може бути повним або полегшеним.

У цьому разі винагороду нараховують не за математичні обчислення, а за зберігання певної суми монет на рахунку. Відповідно, для запуску стейкінг-ноди не потрібно купувати дороге обладнання. Достатньо правильно налаштувати програмне забезпечення і поповнити рахунок.

Мастерноди (Masternodes)

Мастернода є аналогом повної ноди: вона теж зберігає всю інформацію з блокчейна і синхронізується з ним, але має і додаткові функції. Вони потрібні для забезпечення анонімності шляхом дроблення транзакцій і пересилання їх між гаманцями.

Власник повної ноди може отримати мастерноду, якщо виконає необхідні умови блокчейну. Як правило, основна вимога полягає в поповненні та утримуванні на рахунку певної кількості монет. Також необхідно виконати спеціальні налаштування сервера (у різних криповалют вони різні).

Коли користувач виконує анонімну транзакцію, його монети "перемішуються" в мастернодах. У цьому процесі може брати участь різна кількість вузлів, які розкидані по всьому світу і підбираються випадковим чином. Чисельність раундів перемішування теж варіюється - це можна встановлювати вручну або автоматично. У підсумку простежити зв'язок між відправником і одержувачем стає неможливо.

Мастерноди можуть працювати на алгоритмі Proof of Stake або гібридному консенсусі PoW/PoS. Щоб стимулювати користувачів до створення та управління мастернодами, система нараховує їм частину комісії майнерів. Розмір винагороди теж різниться у різних блокчейнів. Різновид мастерноди, який працює в блокчейні NEM (XEM), називається супернодою.

1.2.4. Валідатори та оракули

Це додаткові функції, якими може володіти нода в децентралізованій мережі:

- Вузол-валідатор - це пристрій, який перевіряє транзакції та затверджує їх. Такі ноди можуть працювати за різними алгоритмами залежно від особливостей блокчейна.
- Оракул - це нода, яка передає інформацію із зовнішніх систем у блокчейн. Прикладом таких даних може бути актуальна вартість валют для обмінного сервісу, що працює на базі блокчейна.

Скрипт-оракул потрібен для того, щоб перетворити інформацію на зрозумілий для смарт-контракту вигляд. Валідатор потім перевіряє дані з оракула нарівні з усією іншою інформацією в блокчейні. При цьому сигнал

від одного оракула перевіряється великою кількістю валідаторів, що підвищує загальну безпеку мережі.

Форки та зміна функцій ноди

Будь-який криптовалютний проєкт може періодично оновлюватися. Щоб оновлення набували чинності на рівні всієї мережі, їх повинні прийняти всі ноди. Іноді у спільноті розробників і валідаторів можуть виникати розбіжності щодо впровадження деяких оновлень, коли одна частина нод може їх прийняти, а інша - відхилити. Процес впровадження змін називається форком.

Форки бувають двох видів:

- Софтфорк — это мягкие изменения и улучшения, которые не противоречат базовым настройкам блокчейна. Чтобы их принять, владельцу ноды нужно обновить программное обеспечение. Если это обновление примут только часть узлов, система все равно продолжит работать стабильно.
- Хардфорк предполагает значительные преобразования блокчейна. В результате такого мероприятия типы сетевых узлов могут вовсе измениться. Например, в сентябре 2022 года криптовалюта Ethereum перешла из алгоритма POS на POW. В результате исчезли майнинг-ноды и появились стейкинг-ноды с функцией валидаторов.

Якщо в співтоваристві виникає розбіжність щодо прийняття хардфорка, мережа розділяється на два несумісних блокчейни. Один із них зберігає базові налаштування, а другий переходить на нові.

1.3. Впровадження стандарту ISO 20022 в платіжній інфраструктурі України

ISO 20022 - це міжнародний стандарт для обміну фінансовою інформацією між різними учасниками фінансового ринку, такими як банки, платіжні системи, корпорації та інші фінансові установи. Цей стандарт визначає спосіб представлення даних про фінансові транзакції та

повідомлення в електронному форматі, забезпечуючи їхню єдність та взаємоповність.

Основні характеристики ISO 20022 показані у таблиці 1.2.

Таблиця 1.2. Характеристики ISO 20022

№	Характеристика	Опис
1	Універсальність	Стандарт може бути використаний для різних видів фінансових транзакцій, включаючи платежі, перекази, виписки з рахунків, операції з цінними паперами, страхування та інші;
2	Міжнародність	ISO 20022 є міжнародним стандартом, який використовується у багатьох країнах і є основою для стандартів з обміну фінансовою інформацією в різних регіонах світу;
3	XML-формат	Велика частина повідомлень в ISO 20022 використовує XML-формат для подачі даних, що робить їх більш доступними для обробки та аналізу комп'ютерними системами;
4	Розширюваність	Стандарт може бути легко розширений для врахування нових фінансових інструментів та потреб користувачів.

1.3.1. Розвиток платіжної інфраструктури України

Національний банк України у партнерстві із компанією SWIFT відповідно до Стратегії розвитку платіжної інфраструктури України та Стратегії ЄЦБ в рамках інтеграції України в ЄС, здійснює впровадження міжнародного стандарту обміну повідомленнями ISO 20022 в платіжній інфраструктурі України з метою підвищення конкурентоспроможності нашої країни та її інтеграції зі світовими ринками. [8]

Перехід на використання міжнародних стандартів обміну фінансовими повідомленнями забезпечується шляхом упровадження системи електронних платежів нового покоління (СЕП 4), що надає можливість:

- гармонізувати український платіжний простір зі світовим з метою подальшого здійснення транскордонних переказів з країнами ЄС на базі SEPA Instant Credit Transfer (підключення до TIPS);
- перейти до гнучких та стандартизованих форматів обміну інформацією на базі XML;
- розширити реквізити платежів додатковою інформацією та підвищити рівень обслуговування та ефективності платежів;
- розширити функціональне наповнення платіжних інструментів на користь банків та їх клієнтів;
- закласти основу для подальшого ефективного розвитку СЕП в частині упровадження миттєвих платежів, реалізації мультивалютності, трекінг-сервісу для платежів та інших інструментів. [8]

Roadmap, або дорожня карта надана на Рисунку 1.2.

Рисинок 1.2. Дорожня карта розвитку СЕП

Карта впровадження ISO 20022 у світі

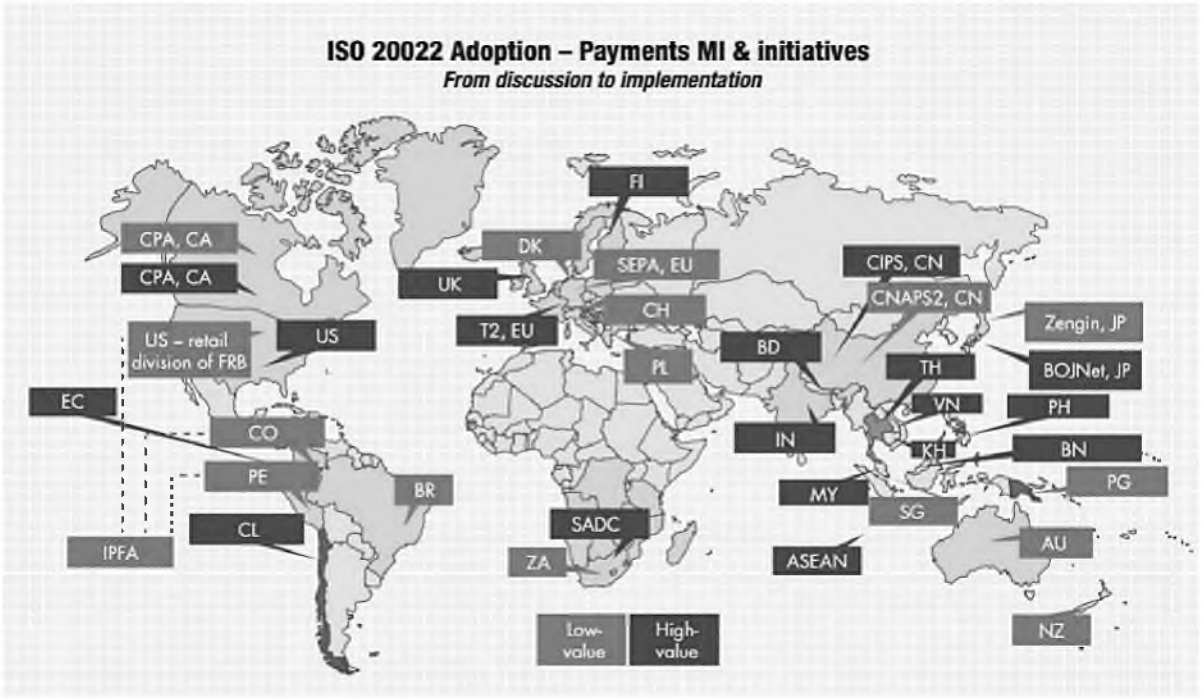

Рисунок 1.3. Карта впровадження ISO 20022

План вдосконалення платіжної інфраструктури України (згідно з проектом «Розвиток платіжної інфраструктури України») на Рисунку 1.4.

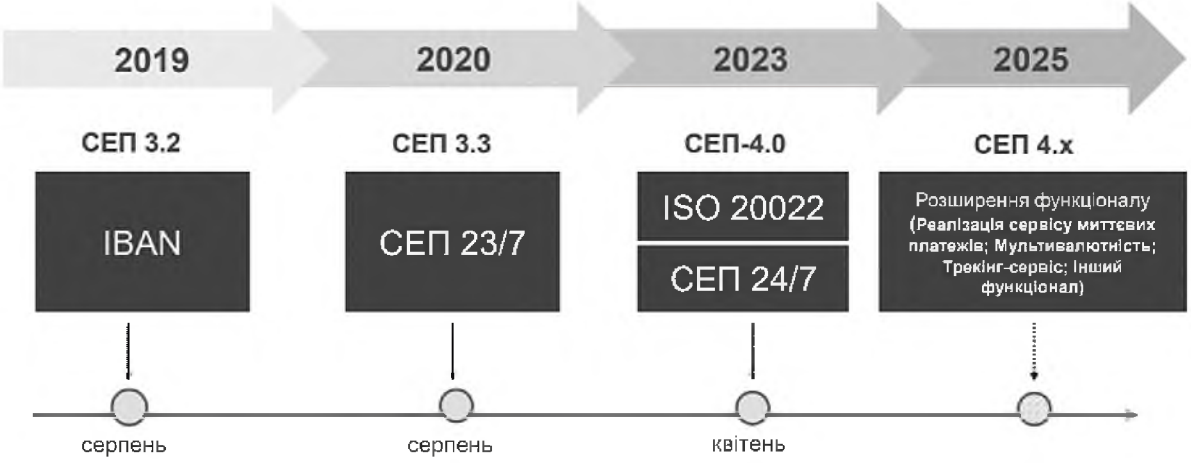

Рисунок 1.4. План вдосконалення платіжної інфраструктури України

Графік реалізації проекту «Розвиток платіжної інфраструктури України» наданий у таблиці 1.5.

Таблиця 1.3. Графік реалізації проекту «Розвиток платіжної інфраструктури України»

Квартал, Q	**Назва етапу**	**Що зроблено**
Q3-2021	Закон про платіжні послуги	Закон підписано;
Q3/Q4-2021	Забезпечення безпеки при переході СЕП на ISO 20022	Розроблення документів щодо вимог до захисту систем банків, захисту ЦОСЕП;
Q3-2020/Q2-2022	Нормативне забезпечення впровадження ISO 20022	Розробка технологічної документації (Специфікації, структури повідомлень, інші документи) / оновлення НПА для впровадження ISO 20022;
Q3-2021 - Q2-2022	Узгодження режиму 24/7	Аналіз та приведення НПА НБУ у відповідність до зміни режиму роботи СЕП на 24/7;
Q3-2021-2023	Тестування режиму 24/7, форматів ISO 20022	Тестування на стенді СЕП-4 повідомлень ISO 20022 в режимі 24/7;
Квітень 2023	Запровадження ISO 20022 та 24/7 в СЕП	СЕП-4 починає працювати в режимі 24/7 та відповідно до стандарту ISO 20022;
2024-2025	Розширення функціоналу СЕП-4 і гармонізація з правилами ЄС	СЕП 4.х - 5.0 – доступний сервіс миттєвих платежів, Мультивалютність (UAH, EUR), Трекінг-сервіс для платежів, інший функціонал відповідно до дорожньої карти розвитку СЕП.

1.3.2. План заходів щодо впровадження ISO 20022

Концептуально план заходів складається з етапів вказаних в таблиці 1.4

Таблиця 1.4. Етапи плану заходів у процесі виконання та при подальшому впровадженні

Виконані і у процесі виконання
- Розробка нормативно-правової бази, яка регламентує порядок застосування методології стандарту ISO 20022 в платіжній інфраструктури України, а також внесення змін до чинних нормативно-правових актів;
- Розробка електронних платіжних документів та фінансових повідомлень, створених відповідно до методології ISO 20022 для платіжної інфраструктури України;
- Впровадження електронних платіжних документів та фінансових повідомлень, створених відповідно до методології ISO 20022, в СЕП-4 та в ПК учасників ринку;
При подальшому впровадженні
Нових інструментів та можливостей, зокрема, після упровадження 1 квітня 2023 року СЕП-4.0 відбудеться розширення функціоналу СЕП в частині впровадження миттєвих платежів та інших інструментів.

Візуальний план показаний на Рисунку 1.5.

Рисунок 1.5. План заходів щодо впровадження ISO 20022

1.3.3. Загальні відомості щодо стандарту ISO 20022

1.3.3.1. Методологія стандарту ISO 20022

Основою в ISO 20022 є не сукупність форматів і правил обміну електронними повідомленнями, а методологія розробки стандартів – формалізованого опису бізнес-процесів, їх елементів і схем взаємодії елементів в ході виконання бізнес-процесу.

У результаті застосування методології ISO 20022 є побудова формалізованого опису бізнес-процесів і отримання форматів та схем обміну електронними повідомленнями, що забезпечують реалізацію бізнес процесів.

Даний підхід у рамках упровадження СЕП 4 дозволяє:

- оптимізувати процес супроводу отриманої моделі і успішно координувати подальший розвиток області що моделюється;
- використовувати нову сучасну криптографічну систему захисту інформації Національного банку за міжнародними стандартами;
- забезпечити цілодобову роботу СЕП 24/7/365;
- максимально автоматизувати регламентні дії усіх учасників СЕП;
- розширити перелік інструментів

1.3.3.2. Бізнес-області ISO 20022

Стандарт ISO 20022 був затверджений в 2004 році, і за декілька років на основі його методології було спроектовано 280 різних типів повідомлень. Стандарт постійно й активно розвивається, представлені моделі вдосконалюються, відображаючи зростаючі потреби учасників ринку.

- Побудовано формалізовані моделі наступних предметних областей:
- Платежі та розрахунки
- Розслідування
- Операції з цінними паперами
- Обслуговування торгових операцій
- Банківські карти
- Операції на валютному ринку

Приклад Бізнес-області ISO 20022 показаний на Рисунку 1.6.

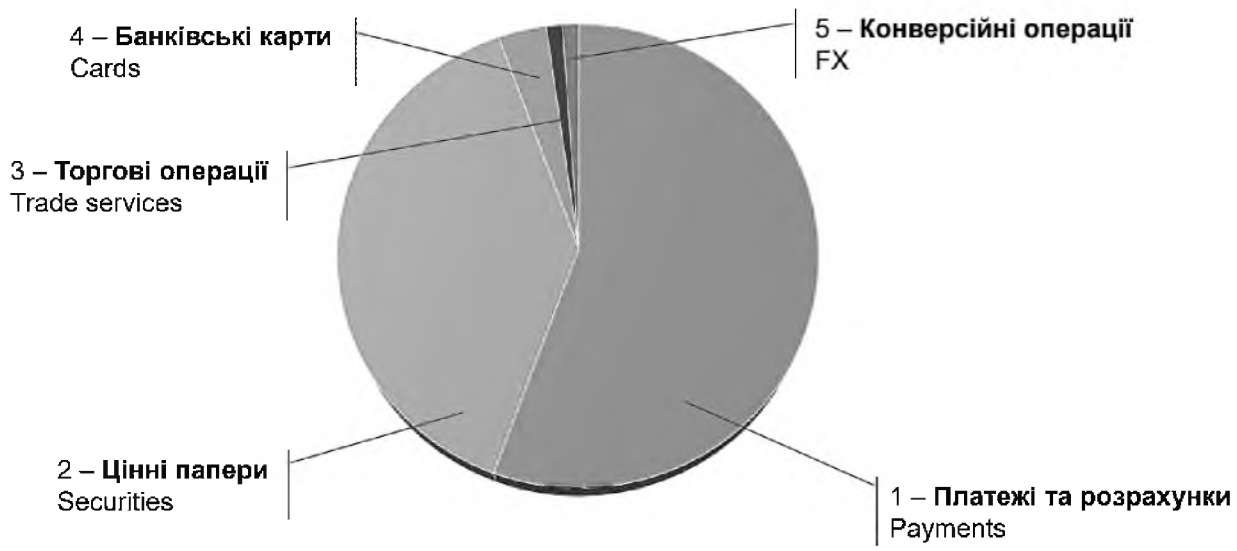

Рисунок 1.6. Бізнес-області ISO 20022

1.3.3.3. Підхід до моделювання

Методологія ISO 20022, що застосовується для стандартизації обміну інформаційними повідомленнями при наданні фінансових послуг, заснована на послідовному застосуванні методу моделювання.

За методологією ISO 20022 моделювання проводиться шляхом структуризації об'єктів стандартизації та даних про них за принципом «зверху вниз» або «від загального – до конкретного». При моделюванні виділяються чотири етапи, що відображають чотири різних рівня абстрактності [8] показаних у Таблиці 1.4.

Таблиця 1.4. Чотири рівня абстрактності моделювання

№	Рівень	Опис
1	Оглядовий рівень Scope Level	Визначення бізнес-області, бізнес-цілей, бізнес-процесів і ролей учасників;
2	Концептуальний рівень Conceptual Level	Опис бізнес-процесів інформаційного обміну та алгоритмів взаємодії учасників, сценаріїв моделі, складу повідомлень і послідовності їх передачі при виконанні транзакцій, визначення відповідних учасників і ролей;

Продовження таблиці 1.4.

3	Логічний рівень Logical Level	Створення точного опису повідомлень та систем без прив'язки до технології;
4	Фізичний рівень Physical Level	Створення точного опису повідомлень та систем по технології, що може бути використана для реалізації.

1.3.3.4. Результати моделювання

Реалізація методології ISO 20022 щодо окремо взятої бізнес-області призводить до створення її комплексної моделі, що складається із сукупності моделей для кожного з чотирьох рівнів Мета моделі ISO 20022.

Моделі перших двох рівнів (Оглядового і Концептуального) в різному ступені деталізації відображають об'єкти і процеси бізнес-області, їх взаємодію між собою, потреби в інформаційному обміні.

Моделі третього і четвертого рівнів (Логічного і Фізичного) дають повний і точний опис процесів інформаційного обміну і складових цих процесів – повідомлень і послідовностей передачі повідомлень різного виду.

Моделі першого-третього рівня використовуються для виконуваних людиною аналізу і вивчення процесів обміну інформацією у відповідній бізнес-області. Моделі Фізичного рівня використовуються для створення систем обміну фінансовими повідомленнями, відповідними до ISO 20022, в конкретних платіжних системах, в рамках фінансових інститутів або окремих структур фінансових ринків [8].

1.4. Інноваційні рішення компанії Stellar у сфері міжнародних платежів за стандартом ISO 20022

- Цифрові активи, що відповідають стандарту ISO 20022, можуть стати стандартом для регуляторних органів, оскільки вони можуть працювати з CBDC. [17]

- XRP від Ripple та XLM від Stellar Lumens - єдині токени, які підходять для створення CBDC.[17]

1.4.1. Огляд компанії Stellar і її ролі у фінансовій індустрії

Stellar — платформа для валютних операцій, що працює в режимі реального часу (система валютних розрахунків в режимі реального часу) [1]. Вона була заснована на початку 2014 року Джедом МакКалебом і Джойс Кім, як відгалуження від системи Ripple і перший час працювала на одноіменному протоколі. У подальшому було розроблено власний open-source протокол Stellar [2]. В процесі роботи використовується власний вид електронної валюти, який раніше називався стелларом (stellar) або зіркою (star), а тепер називається люменом (lumen) або XLM.

Для підтримки платформи був організований некомерційний неакціонерний фонд Stellar Development Foundation. Фінансування фонду було отримано від компанії Stripe.

Оновлена мережа Stellar (на власному протоколі) почала роботу в листопаді 2015 року [9]. І в момент першого виходу, влітку 2014 року, і протягом 2015 року Stellar отримувала доброзичливі відгуки в пресі.

Станом на 11 січня 2018 року Stellar займає 9 місце в списку криптовалют з найбільшою капіталізацією, обсяг капіталізації становить 9 130 804 932 USD.

1.4.1.1. Правила платформи Stellar

При організації платіжної мережі Stellar були здійснені дії і прийняті правила, які повинні допомогти уникнути проблем, властивих мережі Ripple. [16]

1. Був організований Stellar Development Foundation — некомерційний і неакціонерний фонд. Таким чином, засновники фонду не можуть отримати вигоди від його функціонування і від продажу його акцій.

2. Вся програмна реалізація платформи спочатку була відкритою. У момент запуску вона працювала використовуючи open-source протокол Ripple, а потім був створений відкритий протокол Stellar. Фонд розвитку Stellar взяв на себе відповідальність за те, що протокол платформи завжди буде відкритим.
3. Stellar відмовилася від інституту привілейованих учасників.
4. Платформа зобов'язалася публікувати різні звіти, які висвітлюють її діяльність. Наприклад, звіт про зарплату співробітників; звіт про люмен-гранти співробітників; бюджетний розпис; кількість розподілених люменів; механізм розподілу люменів тощо. У даний момент на сайті можна знайти статистику по люменам. Там же можна бачити кількість користувачів, що прийшли з Facebook. Також є фінансовий звіт за II квартал 2014 року.
5. Спочатку було сказано, скільки створено люменів при утворенні платформи (100 млрд.), скільки буде генеруватися щотижня (для створення штучної інфляції 1 % в рік), скільки буде витрачено на розвиток фонду (5 % від загальної кількості).
6. Велика частина люменів повинна бути розподілена безкоштовно (крім 5 % на операційні витрати). Важливим завданням фонду є розподілити їх більш-менш рівномірно.
7. 25 % всіх люменів має відійти некомерційним організаціям.
8. Існує обмежувальний договір, згідно з яким сторони, що мають великі суми люменів, не можуть продавати їх протягом 5 років.

Можна сказати, що організатори платформи Stellar зробили все можливе, щоб виключити будь-яку азартну складову цього проекту.

1.4.1.2. Фонд підтримки Stellar

Фонд підтримки Stellar (Stellar Development Foundation) створений влітку 2014 року. Його членами правління в даний момент є: Кіт Рабоіс,

Джойс Кім, Шівані Сироя і Грег Брокман. Джед МакКалеб вказаний як співзасновник фонду і розробник Stellar, але в правління не входить.

За час роботи складу правління доволі серйозно змінився, оскільки спочатку в ньому були Рабоіс, МакКалеб і Патрік Коллісон. Останній з перерахованих є співзасновником фонду і до недавнього часу, поряд з Кітом Рабоісом, був ветераном правління Stellar, проте в січні 2016 року перейшов в консультанти. Грег Брокман, навпаки, перейшов з консультантів в члени правління. [16]

В якості консультантів фонду вказані відомі в світі IT люди: Метт Малленвег, Грег Стейн, Джої Іто, Сем Альтман, Навал Равикант та ін. У цілому колектив консультантів фонду стабільний.

Команда фахівців, навпаки, мала сильні зміни. Зокрема, за рік, з березня 2015 року, вона була скорочена майже на 40 %, в основному за рахунок розробників. [16]

Фонд фінансується приватними пожертвами і 5 % люменів, відкладених на операційну діяльність. Із зазначеної суми люменів 2 % вже викуплені компанією Stripe за 3 млн дол.

Завданнями фонду є: підвищення цифрової фінансової грамотності, розробка інструментів і сервісів для мережі і управління протоколом Stellar.

1.4.1.3. Схема роботи

Stellar є протоколом з відкритим кодом, і призначений для валютних операцій. Сервери виконують програмну реалізацію протоколу і використовують Інтернет, щоб з'єднуватися і обмінюватися даними з іншими серверами Stellar, утворюючи глобальну мережу обміну валюти. Кожен сервер зберігає записи про «рахунки» в мережі. Ці записи зберігаються в базі даних під назвою «гросбух». Сервери заявляють зміни в бухгалтерській книзі (гросбух), пропонуючи «угоди», які переводять рахунки з одного стану в інший, витрачаючи баланс облікового запису або змінюючи його властивості. Всі сервери намагаються прийти до угоди, яка дозволить застосувати до

поточного гросбуху певний пакет угод, за допомогою процесу, який називається «консенсус». Процес консенсусу запускається через регулярні проміжки часу, як правило, через кожні 2-4 секунди. Це зберігає копію бухгалтерської книги кожного сервера в синхронізованому і ідентичному стані. [16]

При запуску Stellar був заснований на протоколі Ripple. Після того, як були виявлені системні проблеми, пов'язані з існуючим алгоритмом консенсусу, Stellar створив оновлену версію протоколу з новим алгоритмом досягнення консенсусу, що заснований на абсолютно новому коді. Код та технічна документація для цього нового алгоритму були випущені в квітні 2015 року, а оновлена мережа почала функціонувати в листопаді 2015 року.

9 грудня 2020 року один із найстаріших німецьких банків Bankhaus von der Heydt разом в партнерстві з Bitbond створив свій стейблкоїн EURB на базі мережі Stellar. Це був перший стейблкоїн випущений безпосередньо банківською установою на базі Stellar на криптовалютному ринку Європи.

4 січня 2021 року міністерство цифрової трансформації України та Stellar Development Foundation підписали Меморандум про взаєморозуміння та співпрацю, в рамках якого працюватимуть над розробкою стратегії розвитку ринку віртуальних активів в Україні.

1.4.1.4. Протокол консенсусу Stellar

Технічна документація і код для Протоколу консенсусу Stellar (SCP) були опубліковані 8 квітня 2015 року. В документації вводиться поняття інтегрованого візантійського договору (FBA), новий підхід до консенсусу, для якого SCP є першим втіленням. Для визначення надійності системи FBA спирається на кворумні зрізи — коли кожен вузол вибирає, яким іншим вузлам довіряти. Разом кворумні зрізи визначають кворум на системному рівні. SCP дозволяє відкрите членство.

1.5. Провідні блокчейн компанії

1.5.1. Опис та особливості компаніїй

У сфері блокчейн існує багато провідних компаній, які надають платіжні послуги для банківських секторів.

Ряд відомих компаній показаний у таблиці 1.5.

Таблиця 1.5. Опис та особливості блокчейн компаній

№	Назва компанії	Опис	Особливості
1	Ripple (XRP)	Ripple пропонує рішення для міжбанківських платежів, використовуючи свою криптовалюту XRP як міст між різними валютами.	Ripple відомий своєю високою швидкістю транзакцій та низькою вартістю комісій, роблячи його привабливим для міжнародних банківських переказів.
2	Stellar (XLM)	Stellar забезпечує платформу для обробки міжнародних платежів, дозволяючи швидко конвертувати традиційні гроші в свою криптовалюту Stellar Lumens (XLM) та навпаки.	Stellar зосереджений на зменшенні витрат та часу транзакцій, особливо в країнах з обмеженим доступом до банківських послуг.
3	Ethereum (ETH)	Хоча Ethereum відомий переважно як платформа для смарт-контрактів, він також використовується для фінансових транзакцій та платіжних систем.	Його гнучка інфраструктура дозволяє створювати складні фінансові рішення, включаючи децентралізовані фінанси (DeFi).

Продовження таблиці 1.5.

4	Circle (USDC)	Circle - це компанія, що випустила одну з найбільших стабілкойнів, USD Coin (USDC), яка прив'язана до вартості долара США.	USDC використовується для платежів та розрахунків, забезпечуючи стабільність і ефективність блокчейн-технологій.
5	Chainalysis	Хоча Chainalysis не є платіжною платформою, вона забезпечує важливі аналітичні послуги для блокчейн-транзакцій, що допомагає банкам та фінансовим установам відстежувати та аналізувати блокчейн-діяльність.	Забезпечення безпеки, відповідності регулюванню, та прозорості в блокчейн-транзакціях.
6	IBM Blockchain	IBM Blockchain пропонує рішення на базі Hyperledger Fabric, яке використовується для різних бізнес-потреб, включаючи фінансові послуги.	Сприяє підвищенню прозорості, ефективності та безпеки у фінансових операціях.

Ці компанії відіграють ключову роль у розвитку блокчейн-технологій у фінансовому секторі, пропонуючи інноваційні рішення для покращення міжнародних платежів та банківської інфраструктури.

1.5.2. Ripple (XRP) та Stellar (XLM)

Порівняльна характеристика

У 2023 році самими провідними компаніями з надання послух ЕП є Ripple (XRP) та Stellar (XLM). Обидві платформи забезпечують інноваційні рішення в сфері блокчейну та цифрових фінансів, пропонуючи унікальні можливості для міжнародних грошових переказів і фінансової інтеграції. Хоча Ripple та Stellar мають спільну мету – поліпшення та спрощення міжнародних платежів, їхні підходи, технологічні особливості та стратегічні цілі відрізняються.

Ripple, з його фокусом на міжбанківських транзакціях, забезпечує швидкі та ефективні платіжні рішення, спрямовані на інтеграцію з традиційними банківськими системами. З іншого боку, Stellar прагне забезпечити фінансову інклюзію, забезпечуючи доступ до платіжних послуг ширшому колу користувачів, включаючи небанківські сектори та країни з обмеженим доступом до традиційних фінансових послуг.

Подробиці порівняння показані у таблиці 1.6.

Таблиця 1.6. Порівняння компаній Ripple та Stellar

Параметр / Критерій	**Ripple (XRP)**	**Stellar (XLM)**
Основне призначення	Спрощення міжбанківських платежів і розрахунків.	Забезпечення міжнародних переказів та фінансового включення.
Швидкість транзакцій	Дуже висока, до 1500 транзакцій на секунду.	Висока, до 1000-5000 транзакцій на секунду.
Вартість транзакцій	Низька, але залежить від мережевого навантаження.	Дуже низька, майже незначна.
Ринкова орієнтація	Спрямований на співпрацю з банками та фінансовими установами.	Зорієнтований на більш широке фінансове включення, включаючи

Продовження таблиці 1.6.

		небанківські сектори.
Регуляторні питання	Частіше зустрічається з регуляторними викликами, особливо в США.	Зазвичай має менші регуляторні проблеми.
Децентралізація	Частково децентралізований, критика через більш централізовану структуру.	Сильніше децентралізований у порівнянні з Ripple.
Взаємодія з традиційними валютами	Ефективний обмін та ліквідність з традиційними валютами.	Підтримка мультивалютних транзакцій, включаючи обмін фіатних та криптовалют.
Безпека	Високий рівень безпеки, але існують деякі занепокоєння щодо централізованої природи.	Високий рівень безпеки, забезпечений децентралізацією.
Масштабування	Масштабується добре для великих фінансових установ.	Гнучке масштабування, підходить для різноманітних фінансових операцій.
Сприйняття спільнотою	Часом сприймається з підозрою через питання централізації.	Позитивне сприйняття завдяки зосередженню на децентралізації та інклюзії.

Це порівняння висвітлює ключові відмінності між Ripple та Stellar, які включають їхні підходи до децентралізації, цільові аудиторії та регуляторні взаємодії. Обидва пропонують унікальні переваги і мають свої виклики, які важливо враховувати при розгляді їх для міжнародних платіжних систем.

1.5.3. НБУ та Stellar (XLM)

Серед відомих компаній Національний Банк України (НБУ) вибрав Stellar (XLM) для розвитку інфраструктури цифрових активів та впровадження міжнародних платіжних систем з декількох причин які вказані у таблиці 1.7.

Таблиця 1.7. Причини вибору НБУ технології Stellar

Причина	**Опис**
Децентралізація та Прозорість	Stellar відрізняється високим ступенем децентралізації, що забезпечує більшу прозорість і безпеку транзакцій. Це дуже важливо для державного банку, оскільки забезпечує надійність та відкритість валютних операцій.
Низька Вартість та Висока Швидкість Транзакцій	Stellar пропонує швидке проведення транзакцій з мінімальними комісіями, що є ідеальним для міжнародних платежів та переказів, особливо у випадку великого об'єму транзакцій.
Мультивалютність і Гнучкість	Stellar дозволяє легко перетворювати традиційні валюти в цифрові активи і навпаки. Ця мультивалютна платформа дозволяє банкам та їхнім клієнтам легко взаємодіяти з різними валютами, що підвищує гнучкість міжнародних фінансових операцій.
Сумісність з Міжнародними Стандартами	Stellar добре інтегрується з існуючими міжнародними фінансовими стандартами, що є ключовим фактором для державного банку, оскільки це забезпечує легкість інтеграції з існуючою фінансовою інфраструктурою.
Підтримка Цифрових Активів і Цифрової Інтеграції	Stellar підтримує створення, передачу та торгівлю цифровими активами, що відповідає цілям НБУ щодо розвитку цифрової економіки та інтеграції інноваційних фінансових технологій.

Продовження таблиці 1.7.

Потенціал для Розвитку Цифрової Валюти Центрального Банку (CBDC)	Stellar може бути використаний для створення та управління цифровою валютою центрального банку, що є стратегічно важливим напрямком для багатьох центральних банків, включаючи НБУ.

1.5.4. Переваги Stellar (XLM) перед Ripple (XRP) для НБУ

Stellar (XLM) має кілька переваг перед Ripple (XRP), які роблять його привабливим вибором для Національного Банку України (НБУ):

- Вища Децентралізація. Забезпечує більшу децентралізацію у порівнянні з Ripple. Ця характеристика є ключовою для центральних банків, які прагнуть забезпечити безпеку та прозорість фінансових операцій.
- Сприяння Фінансовому Включенню. Зорієнтований на сприяння фінансовому включенню, що допомагає забезпечити доступ до фінансових послуг для широкого спектра користувачів, включаючи тих, хто знаходиться у віддалених або недостатньо обслуговуваних регіонах.
- Підтримка Мультивалютних Транзакцій. Дозволяє легко здійснювати мультивалютні транзакції, що є важливим для НБУ, оскільки це полегшує обмін між різними валютами та сприяє міжнародній торгівлі.
- Гнучкість і Відкрита Архітектура. Пропонує відкриту архітектуру, яка дозволяє легко інтегрувати додаткові фінансові інструменти та сервіси, що може бути корисно для банківських операцій та розвитку цифрових фінансових продуктів.
- Нижча Вартість Транзакцій. Забезпечує дуже низькі витрати на транзакції, що робить його привабливим для центральних банків, особливо при великому обсязі міжнародних переказів.

- Сумісність з Існуючими Фінансовими Системами. Може легко інтегруватися з існуючими фінансовими системами і підтримувати традиційні валюти, що є важливим для центральних банків, які прагнуть впровадити новітні технології без повного переосмислення існуючої інфраструктури.
- Менші Регуляторні Виклики. Має менше регуляторних викликів і складнощів порівняно з Ripple, що важливо для державних установ, що піклуються про відповідність законодавчим та регулятивним стандартам.
- Підходить для Розробки Цифрових Валют Центральних Банків (CBDC). Може бути використаний для створення та управління Цифровою Валютою Центрального Банку (CBDC), що є одним з потенційних напрямків розвитку для НБУ.

Ці фактори роблять Stellar привабливим вибором для Національного Банку України, враховуючи їхні цілі та потреби у контексті розвитку цифрової фінансової інфраструктури.

1.6. Вплив технології блокчейн на безпеку електронних платежів

1.6.1. Зміни в Безпеці та Процесі Транзакцій

Технологія блокчейн може суттєво вплинути на безпеку банківських платежів і транзакцій порівняно з традиційними системами. Ось кілька ключових аспектів, що зміняться з впровадженням технології:

- Децентралізація: На відміну від централізованих банківських систем, блокчейн є децентралізованим, що ускладнює хакерські атаки та фальсифікації.
- Шифрування та Консенсус: Кожна транзакція шифрується та перевіряється через механізм консенсусу мережі, забезпечуючи її надійність.

- Прозорість та Відстежуваність: Транзакції в блокчейні легко відстежувати, але при цьому зберігається конфіденційність сторін.
- Відсутність Посередників: Скорочення кількості посередників знижує ризики зловживань та затримок.
- Швидкість та Ефективність: Блокчейн забезпечує швидкіші транзакції без потреби у багатоденній обробці.

На Рисунку 1.7. буде зображена блок-схема роботи транзакції через блокчейн

Користувач 1 планує відправити гроші Користувачу 2

Рисунок 1.7. Приклад технології блокчейн у вигляді блок-схеми

1.7. Постановка завдання

Це дослідження має на меті аналізувати використання блокчейн-технології, впровадженої в платіжну систему України, з особливим фокусом на інтеграцію технології Stellar у системи Національного Банку України (НБУ). Ключові аспекти дослідження включають:

1) Оцінка ефективності блокчейн-технології: Аналіз, як інтеграція блокчейн покращила функціональність і безпеку платіжних систем України.
2) Технічний аналіз: Огляд технічних особливостей інтеграції Stellar, включаючи сумісність із міжнародним стандартом ISO 20022.
3) Порівняльний аналіз з іншими системами: Порівняння впровадження Stellar з іншими блокчейн-технологіями, що використовуються в фінансових установах.

4) Вплив на кібербезпеку: Дослідження, як блокчейн сприяє захисту даних та транзакцій у платіжних системах.
5) Перспективи розвитку: Прогнозування майбутнього використання блокчейн-технологій у платіжних системах України.

1.8. Висновок

На основі проведеного дослідження можна очікувати, що інтеграція блокчейн-технології в платіжні системи України має значний потенціал для підвищення ефективності, безпеки та прозорості фінансових операцій. Використання Stellar зокрема, з огляду на його сумісність з ISO 20022 та інші технічні переваги, може слугувати прикладом для інших фінансових установ, що розглядають можливості блокчейн. Подальше дослідження та аналіз будуть ключовими для розуміння довгострокових впливів цих технологій на фінансову систему України.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1. Взаємодія НБУ та Користувачів з блокчейн технологією Stellar

2.1.1. Приклад взаємодії Користувача з СЕП-4

Розглянемо приклад взаємодії процесу здійснення платежу від Клієнта 1 (який користується послугами Банку 1) до Клієнта 2 (клієнта Банку 2), використовуючи нову систему СЕП-4 Національного Банку України (НБУ), яка інтегрована з блокчейн технологією Stellar.

2.1.1.1. Попередні Умови

Банки та Клієнти: Банк 1 і Банк 2 є учасниками системи СЕП-4 і мають відповідні додатки/інтерфейси, що дозволяють їхнім клієнтам здійснювати транзакції.

Інтеграція з Stellar: НБУ використовує блокчейн Stellar для обробки транзакцій в рамках СЕП-4. Це означає, що транзакції між банками проводяться через Stellar Network.

2.1.1.2. Процес Транзакції

Спрощений приклад транзакції у СЕП-4 показаний на рисунку 2.1.

Рисунок 2.1. Спрощений приклад транзакції у СЕП-4

Більш розписана схема прикладу транзакції показана на рисунку 2.2.

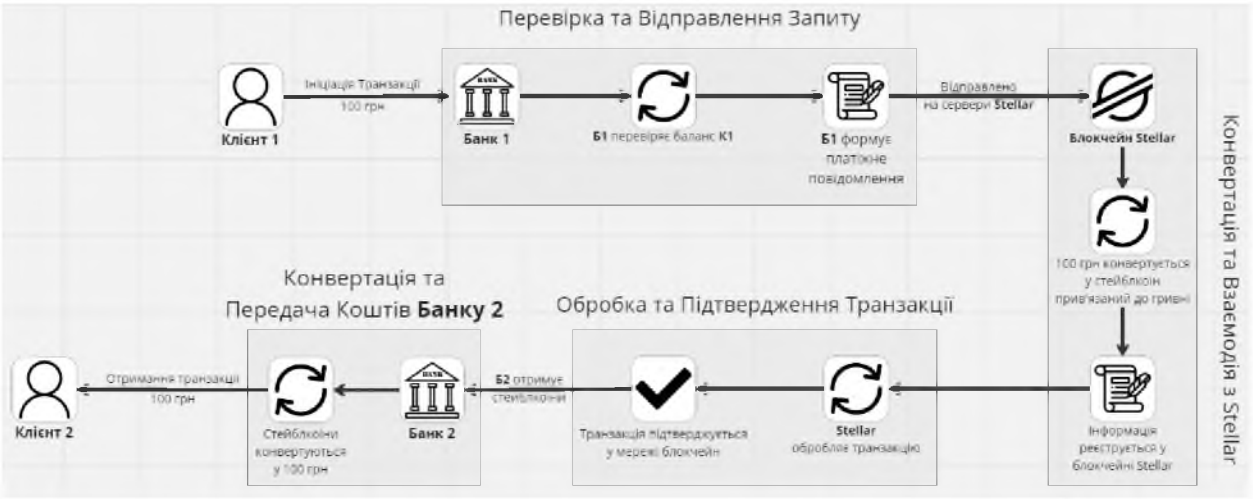

Рисунок 2.2. Розписана схема прикладу транзакції яка використовує систему блокчейн

Крок 1: Ініціація Транзакції

- Клієнт 1(К1) відкриває додаток Банку 1.(Б1)
- Вводить деталі транзакції: суму (100 грн) та отримувача (Клієнт 2, Банк 2).

Крок 2: Перевірка та Відправлення Запиту

- Банк 1 перевіряє інформацію про Клієнта 1 та його баланс.
- Після перевірки, запит на транзакцію пересилається до системи Stellar.

Крок 3: Конвертація та Взаємодія з Stellar

- Сума у гривнях конвертується у відповідний актив Stellar (наприклад, стабілкойн, прив'язаний до гривні).
- Інформація про транзакцію реєструється у блокчейні Stellar.

Крок 4: Обробка та Підтвердження Транзакції

- Stellar обробляє транзакцію, забезпечуючи швидке та безпечне переведення коштів.
- Транзакція підтверджується у мережі блокчейн.

Крок 5: Конвертація та Передача Коштів Банку 2 (Б2)

- Після підтвердження, кошти конвертуються назад у гривні (або валюту Банку 2).
- Кошти передаються на рахунок Клієнта 2(К2) у Банку 2.(Б2)

Крок 6: Повідомлення Клієнтам

- Банк 1 та Банк 2 надсилають повідомлення своїм клієнтам про статус транзакції.

Крок 7: Запис у Бухгалтерській Системі

- Обидва банки роблять відповідні записи у своїх бухгалтерських системах для відображення транзакції.

Схема повідомлення та запису у бухгалтерській системі (Бух. записи) показані на рисунку 2.3.

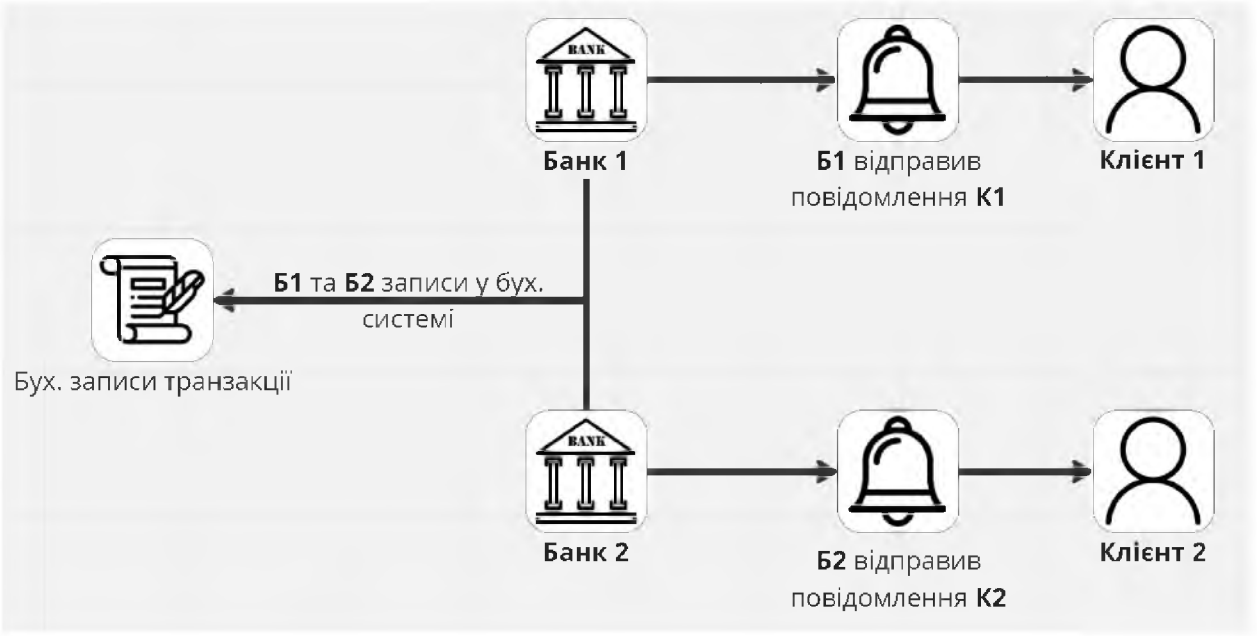

Рисунок 2.3. Схема повідомлення та запису у бухгалтерській системі транзакції

Ці інтегровані схеми показують, як блокчейн технологія може оптимізувати міжбанківські платежі, роблячи їх більш ефективними, безпечними та прозорими. Вона включає всі необхідні етапи від моменту ініціації транзакції клієнтом до кінцевого реєстрування в бухгалтерських системах банків.

2.1.1.3. Особливості

Швидкість і Ефективність

Блокчейн Stellar з власними ресурсами дозволяє швидко обробляти транзакції, знижуючи час переказу коштів.

Безпека і Прозорість

Записи в блокчейні незмінні і відкриті для перевірки, що забезпечує високий рівень безпеки та прозорості.

Стандартизація

Використання ISO 20022 сприяє уніфікації формату платіжних повідомлень.

2.1.2. Приклад взаємодії НБУ з Stellar

Взаэмодія НБУ та Stellar показано на рисунку 2.4.

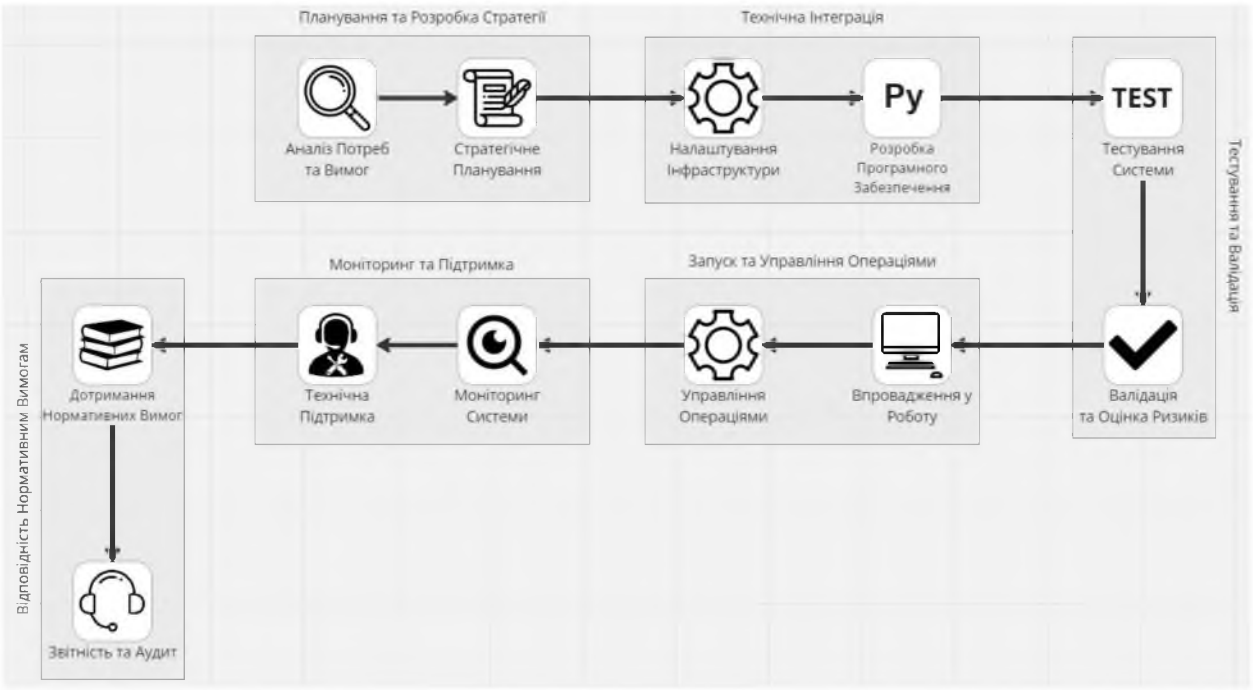

Рисунок 2.4. Схема взаємодії НБУ та Stellar

Крок 1: Планування та Розробка Стратегії

Аналіз Потреб та Вимог

- Обладнання/Ресурси: Комп'ютери, аналітичне програмне забезпечення (наприклад, Tableau, Microsoft Excel).
- Діяльність: Збір даних про поточні платіжні системи, аналіз вимог до безпеки, швидкості транзакцій, вартості.

Стратегічне Планування

- Програмне Забезпечення: Програми для керування проектами (наприклад, Jira, Trello).

- Діяльність: Розробка дорожньої карти проекту, визначення ролей і відповідальностей.

Крок 2: Технічна Інтеграція

Налаштування Інфраструктури

- Обладнання: Сервери, мережеве обладнання.
- Програмне Забезпечення: Системи управління базами даних (наприклад, Oracle, MySQL), мережеві утиліти.

Розробка Програмного Забезпечення

- Мови Програмування: Java, C++, Python для розробки кастомізованих рішень.
- Діяльність: Розробка API для інтеграції з Stellar, створення інтерфейсів користувача.

Крок 3: Тестування та Валідація

Тестування Системи

- Інструменти: Selenium для автоматизації тестування, Postman для тестування API.
- Діяльність: Проведення функціонального та навантажувального тестування.

Валідація та Оцінка Ризиків

- Програмне Забезпечення: Ризик-менеджмент програми (наприклад, Riskified, IBM OpenPages).
- Діяльність: Оцінка впливу на бізнес, аналіз можливих ризиків.

Крок 4: Запуск та Управління Операціями

Впровадження у Роботу

- Діяльність: Поступове впровадження системи, навчання співробітників.
- Моніторинг: Першочерговий моніторинг системи після запуску.

Управління Операціями

- Програмне Забезпечення: CRM системи (наприклад, Salesforce) для управління клієнтськими запитами.

- Діяльність: Підтримка операційних процесів, вирішення проблем користувачів.

Крок 5: Моніторинг та Підтримка

Моніторинг Системи

- Інструменти: Splunk або Datadog для моніторингу системи.
- Діяльність: Виявлення та аналіз збоїв, відстеження продуктивності системи.

Технічна Підтримка

- Обладнання: Центр підтримки з комунікаційним обладнанням.
- Діяльність: Надання допомоги користувачам, управління запитами на сервіс.

Крок 6: Відповідність Нормативним Вимогам

Дотримання Нормативних Вимог

- Програмне Забезпечення: Правові та відповідність нормативним вимогам (наприклад, Thomson Reuters).
- Діяльність: Перевірка на відповідність законодавству, регулярні аудити.

Звітність та Аудит

- Інструменти: Аудиторські програми (наприклад, AuditBoard, TeamMate+).
- Діяльність: Підготовка та подання звітів, внутрішні та зовнішні аудити.

Ця детальна схема включає в себе всі аспекти роботи зі Stellar, від початкового планування до повсякденного управління та забезпечення відповідності нормативним вимогам. Оскільки технології та ринкові умови швидко змінюються, важливо регулярно оновлювати підходи та інструменти, щоб забезпечити ефективність та безпеку системи.

2.1.3. Рекомендації для Національного банку України щодо взаємодії з блокчейн технологією Stellar

Створення рекомендацій для Національного Банку України (НБУ) при взаємодії з блокчейном Stellar включає аспекти безпеки, дотримання правил, використання програмного забезпечення та обладнання показані у таблиці 2.1.

Таблиця 2.1. Рекомендації для НБУ при роботі з блокчейном Stellar

Забезпечення Безпеки	Шифрування Даних	Використання сучасних методів шифрування для захисту транзакцій і персональних даних.
	Багаторівнева Аутентифікація	Впровадження двофакторної аутентифікації для доступу до систем.
	Регулярні Перевірки Безпеки	Виконання регулярних аудитів безпеки та вразливостей.
	Відповідність GDPR	Забезпечення відповідності обробки даних правилам GDPR.
Правила Дотримання	Дотримання Місцевого Законодавства	Слідування фінансовим регуляціям України.
	Політика Конфіденційності	Впровадження чіткої політики конфіденційності та захисту даних.
Програмне Забезпечення	Системи Управління Базами Даних	Наприклад, Oracle Database (версія 19c) або Microsoft SQL Server (версія 2019).
	Інструменти Моніторингу	Splunk (остання версія) для моніторингу даних або Datadog.
	Захист Від Вірусів/Шкідливого ПЗ	Використання рішень типу Norton 360 або McAfee (останні версії).

Продовження таблиці 2.1.

Обладнання	Сервери:	Dell PowerEdge R740 або HP ProLiant DL380 Gen10 для обробки великих даних та забезпечення надійності.
	Засоби Захисту Мережі	Cisco Firepower 2100 Series для забезпечення безпеки мережі.

Інструкція для Роботи	Системи Зберігання Даних	Synology DiskStation DS1621+ або аналоги для надійного зберігання даних.
	Навчання Персоналу	Проведення тренінгів і семінарів для співробітників щодо правильного використання систем та обладнання.
	Документація з Безпеки	Розробка та розповсюдження внутрішніх інструкцій із захисту даних та безпеки.
	План Реагування на Інциденти	Розробка чіткого плану дій у випадку виявлення вразливостей або кібератак.

Забезпечення Безпеки

1) Шифрування Даних. Найсучаснішими методами шифрування є

- Асиметричне Шифрування (RSA, Elliptic Curve Cryptography (ECC))

Застосування: Забезпечує безпечний обмін ключами та шифрування даних. ECC забезпечує високий рівень безпеки при меншому розмірі ключів порівняно з RSA.

- Симетричне Шифрування (AES (Advanced Encryption Standard), DES (Data Encryption Standard))

Застосування: Широко використовується для шифрування великих обсягів даних. AES є одним з найбезпечніших та найшвидших методів.

- Хеш-Функції (SHA-256, SHA-3.)

Застосування: Використовується для створення унікального цифрового відбитка (хешу) даних. Важливо для забезпечення цілісності даних.

- Протоколи Безпечної Передачі Даних (TLS (Transport Layer Security), SSL (Secure Sockets Layer))

Застосування: Забезпечують безпечне з'єднання між серверами та клієнтами в інтернеті.

2) Багаторівнева Аутентифікація

- Дзвінок або SMS-Повідомлення.

Користувач вводить свій пароль (перший фактор), після чого на зареєстрований мобільний номер надсилається унікальний код

верифікації. Користувач має ввести цей код на веб-сайті або в додатку для завершення процесу аутентифікації.

- Додатки для Генерації Кодів (Google Authenticator, Authy.)

Після введення пароля користувач відкриває додаток, який генерує унікальний код, який змінюється кожні кілька секунд. Користувач вводить цей тимчасовий код на веб-сайті або в додатку для підтвердження своєї особи.

- Біометрична Аутентифікація (Відбитки пальців, розпізнавання обличчя)

Після введення пароля користувач підтверджує свою особу за допомогою біометричного сканування. Цей метод забезпечує високий рівень безпеки, оскільки біометричні дані унікальні для кожної особи.

- Фізичні Токени (RSA SecurID)

Фізичний пристрій, який генерує унікальний безпековий код кожні кілька секунд. Користувач використовує цей код разом із своїм паролем для аутентифікації.

- Повідомлення на Електронну Пошту

Користувач отримує унікальний код або посилання для верифікації на свою електронну пошту після введення пароля. Користувач має ввести код або перейти за посиланням для підтвердження своєї особи.

Використання будь-якого з цих методів 2FA значно знижує ризик несанкціонованого доступу до облікових записів та систем, особливо у сфері фінансових послуг, де високий рівень безпеки є критично важливим

3) Регулярні Перевірки Безпеки

- Внутрішні Аудити

Проводяться внутрішньою командою безпеки для оцінки відповідності внутрішнім стандартам безпеки. Проводиться зазвичай регулярно, квартально або щорічно

- Зовнішні Аудити

Проводяться незалежними аудиторами або консалтинговими фірмами для забезпечення об'єктивності та дотримання зовнішніх стандартів. Проводиться щорічно або за потребою.

- Аудити Відповідності

Перевірка дотримання вимогам регуляторних органів та стандартам (наприклад, GDPR, ISO 27001).

- Оцінка Ризиків

Аналіз потенційних ризиків для безпеки інформації та розробка плану їх мінімізації. Проводиться регулярно, зазвичай раз на рік або при зміні умов роботи.

Правила Дотримання

1) Відповідність GDPR

GDPR (General Data Protection Regulation - Загальний регламент захисту даних) – це регулятивний документ Європейського Союзу, який встановлює правила обробки та захисту персональних даних громадян ЄС. GDPR введений у дію з 25 травня 2018 року і є одним з найстрогіших у світі законів про приватність даних. Він стосується всіх організацій, які обробляють дані громадян ЄС, незалежно від того, де знаходиться організація.

- Оцінка Даних та Процесів

Проводиться аудит усіх персональних даних, які обробляються де визначається для чого вони використовуються, і де вони зберігаються.

Цілі обробки: Визначити законні підстави для обробки персональних даних (наприклад, згода, контракт, законні інтереси).

- Політика Приватності та Згоди

Оновлення Політики Приватності. Важливо переконатись що політика приватності чітко описує, як збираються, використовуться та зберігаються дані. Важливо використовувати чіткі механізми для отримання згоди на обробку персональних даних.

- Внутрішні Процедури та Навчання Персоналу

Політики та Процедури. Розроблюються та впроваджуються внутрішні політики та процедури для обробки персональних даних. Проводяться регулярні тренінги для персоналу з питань GDPR та захисту даних.

- Готовність до Порушень

  План Реагування на Порушення. Розроблюється план реагування на порушення безпеки даних.

Таблиця з програмним забезпеченням яке буде використовуватись для захисту БД показано у таблиці 2.2.

Таблиця 2.2. Програмне забезпечення для захисту БД

Назва програмного забезпечення, версія	**Обладнання**	**Робота**
	Системи Управління Базами Даних (СУБД)	
Oracle Database, 19c або 21c.	Ефективна робота на потужних серверах, таких як Dell PowerEdge або HPE ProLiant.	Пропонує розширені можливості для обробки великих обсягів даних, включаючи шифрування даних, автоматизоване управління ресурсами та високу доступність.
Продовження таблиці 2.2.		
Microsoft SQL Server, 2019	Сумісний з більшістю стандартних серверних платформ.	Підтримує розширені аналітичні можливості, бізнес-інтелект, а також інтеграцію з іншими продуктами Microsoft.
	Інструменти Моніторингу	
Splunk, 9.1.2.	Може працювати на різноманітних серверах і хмарних платформах.	Збір та аналіз великих обсягів машинних даних для моніторингу, пошуку порушень, звітності та візуалізації.
Datadog, 2023	Хмарно-орієнтоване рішення, сумісне з	Моніторинг хмарних інфраструктур, аплікацій, логів та інших систем в

	більшістю хмарних платформ.	реальному часі.
Захист Від Вірусів/Шкідливого Програмного Забезпечення		
Norton 360	Комп'ютери та мобільні пристрої	Забезпечує комплексний захист від вірусів, шпигунського програмного забезпечення, мережевих атак. Включає функції VPN та резервного копіювання даних.
Zillya! Антивирус	Комп'ютери та мобільні пристрої	Український антивірус, сертифікований для використання у державних органах та організаціях. Містить брандмауер, WEB-фільтр, USB-захист. Централізоване керування антивірусним захистом. Економне споживання системних ресурсів. Зручний інтерфейс

Продовження таблиці 2.3.

Eset NOD32	Комп'ютери та мобільні пристрої	Бізнес-рішення для централізованого захисту від інтернет-загроз, троянських програм, шпигунського та рекламного ПЗ, руткітів та буткітів, а також фішингу. Ефективний захист усієї корпоративної мережі. Оптимальний рівень безпеки системи, висока продуктивність за мінімальних системних вимог. Компанія зі Словаччини.

Інформація з прикладом обладнанням яке буде використовуватись у проекті показано у таблиці 2.3.

Таблиця 2.3. Приклад обладнання Національного банку України

Назва	**Характеристика**
Сервери	
Dell PowerEdge R740	Процесор: До двох Intel Xeon Scalable процесорів, до 28 ядер кожен.

	Пам'ять: Максимум 3TB (24 слота DIMM): DDR4, 2666MT/s. Жорсткий диск: Підтримка різних варіантів, включаючи SAS, SATA, SSD. Мережеві адаптери: Різні варіанти, включаючи 1GbE, 10GbE, 25GbE. Ціна: Орієнтовно 130 000 гривень, залежно від конфігурації.

Продовження таблиці 2.3.

HPE ProLiant DL380 Gen10	Процесор: До двох Intel Xeon Scalable процесорів, до 28 ядер кожен. Пам'ять: Максимум 3TB (24 слота DIMM) DDR4, до 2933MT/s. Жорсткий диск: Варіанти SAS/SATA/SSD. Мережеві опції: Різноманітність мережевих карт і адаптерів. Ціна: Орієнтовно 100 000 – 150 000 гривень, в залежності від специфікацій.
	Засоби Захисту Мережі
Cisco Firepower 2100 Series	Пропускна здатність: Висока пропускна здатність, до 10 Gbps. Функціональність: Інтегрований захист від загроз, управління трафіком. Інтерфейси: Множинні варіанти інтерфейсів. Ціна: Орієнтовно 150 000 – 250 000 гривень, залежно від моделі.
	Системи Зберігання Даних
Synology DiskStation DS1621+	Процесор: AMD Ryzen Quad-core 2.2 GHz. Пам'ять: 4GB DDR4, розширювана до 32GB. Жорсткі диски: 6 відсіків для HDD/SSD, підтримка RAID. Мережеві інтерфейси: 4 x 1GbE LAN порти. Ціна: Орієнтовно 25 000 – 62 000 гривень.

2.2. Система електронних платежів

2.2.1. Термінологія

Система електронних платежів НБУ – загальнодержавна платіжна система, яка створена Національним банком України і забезпечує здійснення розрахунків із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації. Учасниками системи міжбанківських розрахунків Національного банку України можуть бути банки-резиденти, Державна казначейська служба України та інші суб'єкти, визначені законодавством, за умови дотримання вимог, встановлених Національним банком України.[18]

СЕП створено в 1993 році. Перші платежі через СЕП пройшли 5 січня 1993 року. З 01 січня 1994 року в Україні повністю скасовані паперові та телеграфні авізо у міжбанківських розрахунках. СЕП у 2022 році не дивлячись на повномасштабну війну працювала безперебійно. У 2022 році через СЕП здійснено майже 363 млн платежів на суму 133 трлн грн (у 2021 році – 446 млн платежів на суму 57 трлн грн). У середньому в день СЕП обробляє 1,3 млн платежів на суму майже 700 млрд грн.[18]

2.2.2. Про систему СЕП

Система електронних платежів – є складним та унікальним програмно-технічним комплексом, розробленим фахівцями Національного банку України і є його власністю, вона забезпечує розрахунки в національній валюті України. СЕП базується на повністю безпаперовій технології і передаванні електронних повідомлень через власну телекомунікаційну систему Національного банку.

СЕП забезпечує високий рівень безпеки і надійності переказу коштів між банками та обслуговує 97 % міжбанківських платежів у державі, тому вона визнана системно важливою платіжною системою України.[18]

СЕП — єдина системно важлива державна платіжна система класу RTGS (валові розрахунки у режимі реального часу за міжнародною

класифікацією), яка в реальному часі забезпечує як розрахунки на великі суми, так і роздрібні міжбанківські платежі клієнтів банків.[18]

Національний банк України є не тільки власником, а і оператором СЕП, забезпечує розроблення, удосконалення та експлуатацію програмно-технічних комплексів системи та засобів захисту інформації, розробляє відповідну нормативну базу. НБУ гарантує надійність і безпеку СЕП. НБУ відповідає за нагляд над платіжною системою.[18]

З 1 квітня 2023 року запрацювало нове покоління системи (версія СЕП 4.0), яке дає можливість здійснювати електронні платежі ще швидше, зручніше та безпечніше. Це стало однією з найбільших міграцій, яку будь-коли здійснювали фінансові установи України, і, крім того, потужним поштовхом для майбутнього розвитку і модернізації інформаційних систем українських банків та фінансових установ. Відтепер система функціонує на базі міжнародного стандарту ISO 20022.

Порядок функціонування системи електронних платежів Національного банку України, прийняття і виключення з її членів, проведення переказу за допомогою цієї системи та інші питання, пов'язані з діяльністю системи електронних платежів Національного банку України, визначаються Національним банком України.[18]

Необхідною умовою для проведення переказу через систему електронних платежів Національного банку України є встановлення банком кореспондентських відносин з Національним банком України шляхом відкриття кореспондентського рахунку в Національному банку України.

2.2.3. Розвиток системи

Національний банк України постійно приділяє особливу увагу розвитку СЕП, упровадженню нових механізмів та засобів для задоволення потреб учасників фінансового ринку та їхніх клієнтів.[18]

Після модернізації системи шляхом впровадження нового покоління СЕП версії 4.0 (міжнародний стандарт ISO 20022) з 1 квітня 2023 року, планується подальший розвиток.[18]

Наразі Національний банк працює над упровадженням версії системи СЕП 4.1 з функціоналом миттєвих платежів, який є логічним продовженням розвитку СЕП, зокрема впровадженого режиму роботи 24/7. Початок тестування цього функціоналу заплановано на жовтень 2023 року. В наступних версіях СЕП розглядається впровадження зокрема мультивалютності, трекінг-сервісу для платежів, сервісу оцінки ризику платіжної операції тощо.[18]

2.2.4. Порівняльна характеристика СЕП-3 та СЕП-4

СЕП-4 є принципово новою системою порівняно з СЕП-3 як за функціональним складом, так і за структурами обміну інформацією. Тому спроба представити СЕП-4 як певний розвиток СЕП-3 і обмежитися в САБ тільки реалізацією відмінностей була б хибним підходом. [19]

Порівняння СЕП-3 та СЕП-4 показані у таблиці 2.4.

Таблиця 2.4. Порівняння СЕП-3 та СЕП-4

СЕП-3	**СЕП-4**
За структурами обміну інформацією	
Структура повідомлення – «плоский» файл.	Структура – формат XML
Є два режими роботи СЕП – «файловий» і «онлайновий»	Надається одна технологія обміну учасника з СЕП, не розділена на окремі режими.
Основний набір реквізитів для всіх документів СЕП фіксований, всі з них є обов'язковими. Якщо значення реквізиту за змістом відсутнє, то	Реквізити поділяються на обов’язкові та необов’язкові. Необов’язкові реквізити можуть бути відсутніми, і

Продовження таблиці 2.4.

поле має бути заповненим визначеним	тоді вони фізично не включаються в

«порожнім» значенням	повідомлення.
Є можливість введення нових реквізитів електронного розрахункового документа/ повідомлення, які не входять в основний набір реквізитів. Усі вони вміщуються в окреме поле «Допоміжні реквізити»	Не надається можливість додання реквізитів, що не передбачені стандартом ISO 20022. Кожний з необов'язкових реквізитів розглядається окремо, визначено його найменування, призначення і місце в структурі документа. Реквізити, специфічні для України, розміщуються в максимально наближених за змістом реквізитах ISO 20022, можливо, з особливими правилами їх заповнення.
Електронний розрахунковий документ і електронне розрахункове повідомлення незалежно від їх функціонального призначення вміщуються в одну й ту саму структуру обміну інформацією (файл А, пакет 1.08) і відрізняються одне від одного реквізитами «ознака дебет/кредит» і «Умовний числовий код документа».	Платіжні і неплатіжні повідомлення оформляються в різних типах повідомлень ISO 20022. Зокрема: Електронні розрахункові документи тепер мають назву «платіжні інструкції». Вони поділяються на 4 типи і кожному з них відповідає окреме повідомлення ISO 20022: – клієнтські платежі (у тому числі платежі в бюджет) – pacs.008 – платежі між фінансовими установами (за винятком платежів від/на Державну казначейську

Продовження таблиці 2.4.

	службу) – pacs.009; – повернення коштів – pacs.004;
	– безспірне списання, стягнення з коррахунків учасників СЕП – pacs.010.
	Для кожної з функцій, для яких у СЕП-3 використовувались електронні розрахункові повідомлення, передбачено окремий тип повідомлень ISO 20022,

	наприклад, для запиту на виконання платежу – pain.013, для запиту на повернення помилково перерахованої суми – camt.056, для уточнення реквізитів платежу – набір повідомлень інструменту “Exceptions and Investigations”.
В одному файлі $A припускається вміщення кількох дебетових платежів щодо безспірного списання, стягнення	У повідомленнях, що використовуються для безспірного списання, стягнення, допускається тільки одна трансакція. А саме: у повідомленні pacs.010 дозволяється тільки одна трансакція; якщо повідомлення pain.013 використовується для примусового списання, стягнення (в інструменті Forced Debit), то в ньому дозволяється тільки одна трансакція

Продовження таблиці 2.4.

«Платіжне доручення» і «Меморіальний ордер» виокремлюються як різні документи з різним «умовним числовим кодом»	Така класифікація документів у повідомленнях ISO не використовується.
У файл $A вміщуються платежі, які можуть бути адресовані різним учасникам СЕП	У повідомлення pacs.008, pacs.009 вміщуються платежі, для яких реквізит «Агент отримувача» є однаковим
Коли відправником файла $A є головний банк за 3 моделлю, то у файлі можуть міститися платежі від різних його філій та від його самого	У повідомлення pacs.008, pacs.009 вміщуються платежі, для яких реквізит «Агент платника» є однаковим. Оскільки головний банк і його філія розглядаються як різні «Агенти платника», то одне повідомлення pacs.008, pacs.009, сформоване головним банком за 3 моделлю, може містити платежі тільки від головного банку або тільки від однієї з його філій
Розмір вхідного файлу $A обмежується за	Розмір вхідного повідомлення pacs.008,

кількістю платежів – 1000. У режимі реального часу розмір пакету 1.08 – завжди одна трансакція.	pacs.009 обмежується за його фізичним розміром
Зміни до довідника учасників СЕП подаються у вигляді файлу $U, що містить тільки зміни. Повний стан довідника учасників надається	Повний стан довідника учасників СЕП подається автоматизовано, на запит учасника (повідомлення

Продовження таблиці 2.4.

учаснику за його клопотанням в ручному режимі	admi.998), причому можна отримати як поточний стан «на сьогодні», так і стан зі змінами, який буде актуальний на наступний календарний день.
Назва учасника в Довіднику учасників СЕП – «Технологічна», завдовжки 38 символів	Назва учасника в Довіднику учасників СЕП – із статуту, скорочена, завдовжки 80 символів Дорівнює реквізиту SHORTNAME із Електронного технологічного довідника банків України та інших установ (колишній RCUKRU)
За правилами оброблення повідомлень	
Наявні три різні моделі обслуговування консолідованого коррахунку з безпосередньою участю філій: 4, 7, 8	Моделі 7 і 8 вилучено, залишено тільки одну модель з безпосередньою участю філій «4»
Для кожного безпосереднього учасника ведеться технічний рахунок «ТРФ»	ТРФ ведуться тільки для тих учасників, які працюють за 4 моделлю (з безпосередньою участю філій). Для безмодельних учасників і тих, хто працює за 3 моделлю, ведеться тільки ТКР.
Зарахування коштів на технічний рахунок отримувача за платежем, прийнятим до СЕП, здійснюється: - у файловому режимі – після отримання квитанції $S від учасника	Зарахування коштів на технічний рахунок отримувача здійснюється в момент надходження платежу до СЕП, негайно, одночасно з списанням з технічного рахунку

Продовження таблиці 2.4.

-отримувача;	відправника і незалежно від дій

- у режимі реального часу – негайно, незалежно від дій отримувача	отримувача – аналогічно режиму реального часу СЕП-3
Якщо у файлі $A виявлено помилку хоча б в одному платежі, то файл відхиляється в цілому (включаючи платежі, у яких помилок немає)	Якщо в платіжному повідомленні pacs.008, pacs.009 наявні платіжні інструкції без помилок, то вони приймаються, а помилкові відхиляються. Проте якщо виявлено помилку в трансакції pacs.004, то повідомлення відхиляється в цілому без прийняття до обробки хороших трансакцій (так само, як і файл $A в СЕП-3) Платіжне повідомлення pacs.010 містить тільки одну трансакцію, тому воно завжди відхиляється в цілому незалежно від рівня (у повідомленні в цілому чи в трансакції), на якому виявлено помилку.
Для приймання файлу $A необхідно, щоб на технічному рахунку була сума коштів на повну суму файлу $A	У платіжному повідомленні pacs.008, pacs.009 приймається стільки платіжних інструкцій, на скільки вистачило коштів, решта – відхиляються. Проте повідомлення pacs.004, pacs.010 приймається тільки тоді, коли є кошти на його повну суму

Продовження таблиці 2.4.

Дебетове списання виконується незалежно від наявності коштів на технічному рахунку банка (запобіжні методи, щоб в результаті примусового списання, стягнення коррахунок не став від'ємним, – суто організаційні)	Списання (pacs.010) за результатами клірингу НПС «ПРОСТІР» виконується незалежно від наявності коштів на технічному рахунку банка. Примусове списання, стягнення виконується тільки тоді, коли на технічному рахунку достатньо коштів (інакше ЦОСЕП відхиляє pacs.010)
Для дебетового списання, стягнення, яке виконує НБУ, не існує програмних	Для дебетового списання, стягнення, яке виконує НБУ, Платником (і отримувачем

обмежень щодо того, який учасник СЕП може бути отримувачем цього електронного розрахункового документу	повідомлення pacs.010) може бути тільки банкюридична особа і не може бути філія
У структурах даних наявні елементи, що визначають банківський день, до якого «прив'язано» платіж, і ЦОСЕП не приймає платежі, дата в яких не збігається з поточним банк.днем	У структурах платежів не задано дату виконання. ЦОСЕП приймає всі платежі і в момент їх виконання визначає дату, до якої фактично віднесено виконаний платіж, за своїм годинником
За регламентом роботи	
СЕП-3 працює в псевдо-цілодобовому режимі 23/7 (з технологічною перервою в 1 годину з 00:00 до 01:00)	СЕП-4 працює цілодобово без перерв (24/7)
У вихідні та святкові дні СЕП-3 працює з датою банківського дня,	Поняття "банківський день" в СЕП-4 скасовано. СЕП-4 завжди працює з
Продовження таблиці 2.4.	
що дорівнює даті першого робочого дня за святковими/вихідними. Відповідно відображення платежу в балансі учасника-відправника, ЦОСЕП і учасникаотримувача здійснюється датою зазначеного банківського дня	датою поточного календарного дня. Відповідно відображення платежу в балансі учасника-відправника, ЦОСЕП і учасникаотримувача здійснюється датою зазначеного календарного дня (тобто кожний вихідний / святковий день розглядається як окремий календарний день, за який формується окремий баланс)
Розсилання виписок ($V.0, $V.G/$V.F) здійснюється 1 раз на день, при закритті банківського дня	Розсилання виписок (camt.053) здійснюється кілька разів на день з інтервалом, визначеним регламентом
За технічною реалізацією взаємодії учасника з ЦОСЕП	
НБУ постачає шлюзове робоче місце для взаємодії з СЕП – АРМ-СЕП	НБУ не постачає учасникам робочих місць для взаємодії з СЕП. Взаємодію з ЦОСЕП здійснює безпосередньо САБ / ВМПС учасника
Використання бібліотек криптозахисту НБУ є обов'язковим: – в САБ учасника на етапі підготовки файлів/пакетів (ключі	Захист інформації в САБ при підготовці/обробці документів учасник організовує самостійно, власними

операціоністів, бухгалтерів); – при взаємодії з ЦОСЕП (у складі АРМСЕП)	засобами з дотриманням вимог. НБУ регулює тільки ланку обміну САБ банку – ЦОСЕП. Безпосередню взаємодію з ЦОСЕП учасник здійснює з використанням:

Продовження таблиці 2.4.

	- самостійно вибраних засобів (апаратних, програмних), що відповідають специфікаціям та погоджені з Департаментом безпеки НБУ; - або бібліотек, наданих Департаментом безпеки НБУ
Засоби генерації ключів надаються Національним банком. На робочих місцях використовуються ТВК (таблиці відкритих ключів)	Засоби генерації ключів надаються Національним банком. Для перевірки статусу сертифікатів використовуються сервіси OCSP / CRL ЦСК НБУ. (ТВК не використовуються)
Документ «Система електронних платежів Національного банку України (шифр СЕП3.х). Опис інтерфейсу між САБ банку і СЕП НБУ» відігравав подвійну роль: 1) опис номенклатури файлів/пакетів, їх змістовного призначення, структури, реквізитів і правил заповнення та рекомендацій з оброблення в САБ; 2) опис технології обміну з ЦОСЕП.	Окремого документу «Опис інтерфейсу між САБ банку і СЕП НБУ» не передбачено. Загальні поняття про номенклатуру повідомлень та їх змістовне призначення наведені у верхнерівневих документах групи "Імплементація стандарту ISO 20022 в Україні". Детальний опис повідомлень, їх змістовного призначення, структури, реквізитів і правил заповнення подається в документах типу «Функціональні вимоги», специфікаціях і додатках до них.

Продовження таблиці 2.4.

	Опис технології обміну з ЦОСЕП надається в окремому документі «Система

	електронних платежів Національного банку України (шифр СЕП-4). Технологія і формати обміну повідомленнями між учасниками і ЦОСЕП»
Якщо учаснику потрібно ще раз отримати файл СЕП, то він звертається до служби експлуатації СЕП для повторного надсилання	Учаснику надаються засоби автоматизованого запиту повторного надсилання повідомлення (camt.060 та інші, про які буде повідомлено окремо по мірі розроблення)

2.2.5. Файли СЕП-3 і повідомлення СЕП-4

Функціональна відповідність між файлами/пакетами режиму реального часу СЕП-3 та повідомленнями СЕП-4, призначеними для виконання таких самих або аналогічних функцій показана у таблиці 2.5.

СЕП-3		СЕП-4
Файловий режим	**Режим реального часу**	
$A –початкові платежі	1.08	pacs.008
$B –платежі у відповідь	3.08	pacs.009
$C – платежі режиму реального часу у відповідь		pacs.004 pacs.010 camt.056 pain.013 повідомлення

Продовження таблиці 2.5.

		інструменту «Exceptions and Investigations”
$T – квитанція на файл $A		pacs.002
$S – квитанція на файл $B		camt.029 pain.014
$K – динамічний стан технічного		camt.054

рахунку		
$V.0 – – виписка з технічного рахунку за платежами файлового режиму		camt.053
$V.G / $V.F – за платежами режиму реального часу		
$U – коригування довідника учасників СЕП		-
S_UCH.DBF / S_UCH_WI.DBF – повний зміст довідника учасників СЕП	4.04 , 3.04	admi.998 (тип даних SUch)
$V.B – перелік файлів B, заквитованих автоматично в кінці банківського дня		-
$F.L – встановлення лімітів	2.06	camt.011 camt.012
$F.T – стан технічних рахунків філій	3.06 – інформація про ТРФ	camt.003/camt.004

Продовження таблиці 2.5.

	3.05 – інформація про ТКР	camt.003/camt.004
$O – квитанція від АРМ-СЕП		-

Таблиця 2.5. Файли пакети СЕП-3 та СЕП-4

2.2.6. Принцип роботи СЕП-3 та СЕП-4

До переходу на нове покоління СЕП-4 з інтеграцією блокчейну, Національний банк України використовував СЕП-3, процес транзакцій в якій включав декілька ключових етапів:

1. Ініціювання транзакції: Клієнт подає інструкцію своєму банку на переказ коштів, використовуючи різні методи, такі як банківський переказ, чек, платіжна карта або інтернет-банкінг.
2. Перевірка даних та авторизація: Банк клієнта перевіряє дані транзакції, включаючи доступність коштів та достовірність інформації про одержувача. У разі необхідності банк може запросити додаткову авторизацію від клієнта.
3. Обробка через систему платежів: Після авторизації банк відправника вносить транзакцію до внутрішньої системи обробки платежів або зовнішній платіжній системі, такій як СЕП НБУ.
4. Міжбанківська обробка: Транзакція передається від банку відправника до НБУ, де вона обробляється та перенаправляється до банку одержувача через міжбанківські системи.
5. Пост-процесинг та підтвердження: Після отримання транзакції, банк одержувача обробляє її та зараховує кошти на рахунок одержувача. Обидва банки - відправника та одержувача - оновлюють свої внутрішні рахунки та звітність.
6. Інформування клієнтів: Після завершення транзакції клієнти обох сторін інформуються про її статус через відповідні канали (наприклад, SMS-повідомлення, електронна пошта, інтернет-банкінг).

Приклад роботи СЕП показаний на рисунку 2.5

Рисунок 2.5. Приклад роботи системи електронних платежів

З 1 квітня 2023 року був зроблений перехід на нове покоління СЕП

(СЕП-4)і тепер транзакція мала наступний вигляд:

1. Ініціювання транзакції: Клієнт або інша банківська установа ініціює транзакцію через інтерфейс, сумісний з Stellar. Це може бути переказ коштів, платіж або інша фінансова операція.
2. Створення транзакції в блокчейні: Інформація про транзакцію, така як сума, відправник, одержувач та інші необхідні дані, заноситься у формат транзакції блокчейну Stellar.
3. Перевірка і автентифікація: Транзакція проходить автентифікацію за допомогою криптографічних ключів. Відправник підписує транзакцію своїм приватним ключем, що забезпечує її безпеку та автентичність.
4. Розповсюдження транзакції: Після створення та підпису транзакція відправляється в мережу Stellar. Вона розповсюджується серед вузлів мережі для подальшої обробки.
5. Консенсус в мережі: Вузли мережі Stellar використовують унікальний механізм консенсусу для перевірки транзакції. Цей процес забезпечує, що транзакція є дійсною і не містить подвійних витрат.
6. Запис у блокчейн: Після досягнення консенсусу транзакція записується у відповідний блок у блокчейні Stellar. Це забезпечує незмінність і прозорість запису.
7. Підтвердження та завершення транзакції: Після запису транзакції в блокчейн, вона вважається підтвердженою. Одержувач та інші учасники мережі можуть перевірити статус транзакції. На цьому етапі кошти вважаються переданими, і транзакція завершується.

Цей процес забезпечує безпеку, швидкість та прозорість транзакцій, а також знижує ризики та витрати, пов'язані з традиційними платіжними системами.

2.3. Аналіз загроз системи електронних платежів

Інтеграція блокчейн технології від компанії Stellar у систему СЕП-4 вирішує ряд проблем, які були притаманні системі СЕП-3. Вразливості

системи електронних платежів без технології блокчейн та їх вирішення у СЕП-4 показані у таблиці 2.6.

Таблиця 2.6. Загрози СЕП-3 та рішення СЕП-4

№	Вразливість СЕП – 3	Рішення СЕП – 4
1	Застарілі технології: Системи, які використовують застаріле програмне забезпечення або архітектуру, вразливі до новітніх видів кібератак. Застарілі технології часто не підтримують новіші заходи безпеки, що підвищує ризик зломів та втрати даних.	Використання сучасних блокчейн технологій забезпечує оновлену та безпечнішу платформу. Це включає використання останніх протоколів безпеки та алгоритмів шифрування. Блокчейн пропонує сучасні криптографічні механізми, які підвищують безпеку транзакцій.

Продовження таблиці 2.6.

2	Централізація системи: Централізовані системи створюють одну точку відмови, що може призвести до великих перебоїв у роботі в разі атаки або технічних проблем. Вони також можуть бути вразливими до DDoS-атак, оскільки атака на центральний сервер може паралізувати всю систему.	Блокчейн технологія працює на децентралізованій основі, що зменшує ризики, пов'язані з централізованими системами, такі як вразливість до DDoS-атак. Відсутність єдиної точки відмови в децентралізованих системах робить їх більш стійкими до різних видів кібератак.
3	Проблеми з ідентифікацією та автентифікацією: Недостатньо сильні або застарілі методи ідентифікації користувачів та автентифікації можуть відкривати шлях для несанкціонованого доступу. Це може призвести до шахрайства, крадіжки ідентичності та несанкціонованих фінансових	Впровадження розширених механізмів ідентифікації та автентифікації, таких як біометричні дані, цифрові підписи, розширені криптографічні протоколи та двофакторна аутентифікація, для забезпечення безпеки користувачів, що значно ускладнює несанкціонований доступ.

	транзакцій.	
4	Відсутність прозорості: Брак прозорості у фінансових транзакціях може сприяти шахрайству та корупції. Відсутність засобів для ефективного відстеження транзакцій ускладнює виявлення та запобігання	Блокчейн забезпечує високий рівень прозорості транзакцій, дозволяючи всім учасникам мережі перевіряти та відстежувати транзакції в реальному часі, що сприяє виявленню шахрайства, корупцій або помилок.

Продовження таблиці 2.6.

	неправомірним діям.	
5	Ризик внутрішнього зловживання: Централізовані системи можуть бути більш вразливими до внутрішнього зловживання або шахрайства з боку співробітників. Це стосується особливо тих, хто має доступ до важливих системних компонентів або конфіденційної інформації.	Незмінність та прозорість блокчейна зменшує можливості для внутрішнього зловживання, оскільки будь-які спроби несанкціонованих змін відразу стають помітними. Децентралізована структура блокчейну знижує можливості для внутрішнього зловживання, оскільки не існує одинокої точки контролю над усіма транзакціями.
6	Обмежена швидкість реагування на інциденти: У великих, централізованих системах може бути складно швидко ідентифікувати та вирішити проблеми кібербезпеки. Це може призвести до тривалого часу відновлення після атак та великих фінансових втрат.	Використання технологій блокчейну може допомогти в автоматизації виявлення та реагування на інциденти, забезпечуючи швидке вирішення проблем, через автоматизовані механізми та простішу структуру відстеження.
7	Залежність від зовнішніх постачальників: Системи, які залежать від сторонніх постачальників або сервісів, несуть додаткові ризики, пов'язані з	Блокчейн дозволяє зменшити залежність від зовнішніх постачальників завдяки своїй децентралізованій та розподіленій природі, забезпечуючи більшу незалежність та контроль над

безпекою та

Продовження таблиці 2.6.

надійністю цих зовнішніх систем. Витоки даних або збої у роботі зовнішніх постачальників можуть безпосередньо вплинути на безпеку та ефективність СЕП-3.	системою.

2.4. Платформа Anchor

2.4.1. Архітектура платформи Anchor

Anchor - це специфічний для Stellar термін для позначення входів і виходів, які з'єднують мережу Stellar з традиційними фінансовими рейками, такими як фінансові установи або фінтех-компанії. Anchor приймають депозити у фіатній валюті (наприклад, долар США, аргентинське песо або нігерійська найра) через існуючі канали (наприклад, банківські депозити або пункти видачі готівки), а потім надсилають користувачеві еквівалент цифрових токенів у мережі Stellar. Еквівалентні цифрові токени можуть представляти ту саму фіатну валюту або інший цифровий токен. Крім того, Anchor дозволяють власникам токенів обмінювати свої токени на реальні активи, які вони представляють.

Загальна архітектура платформи Anchor показана на рисунку 2.6.

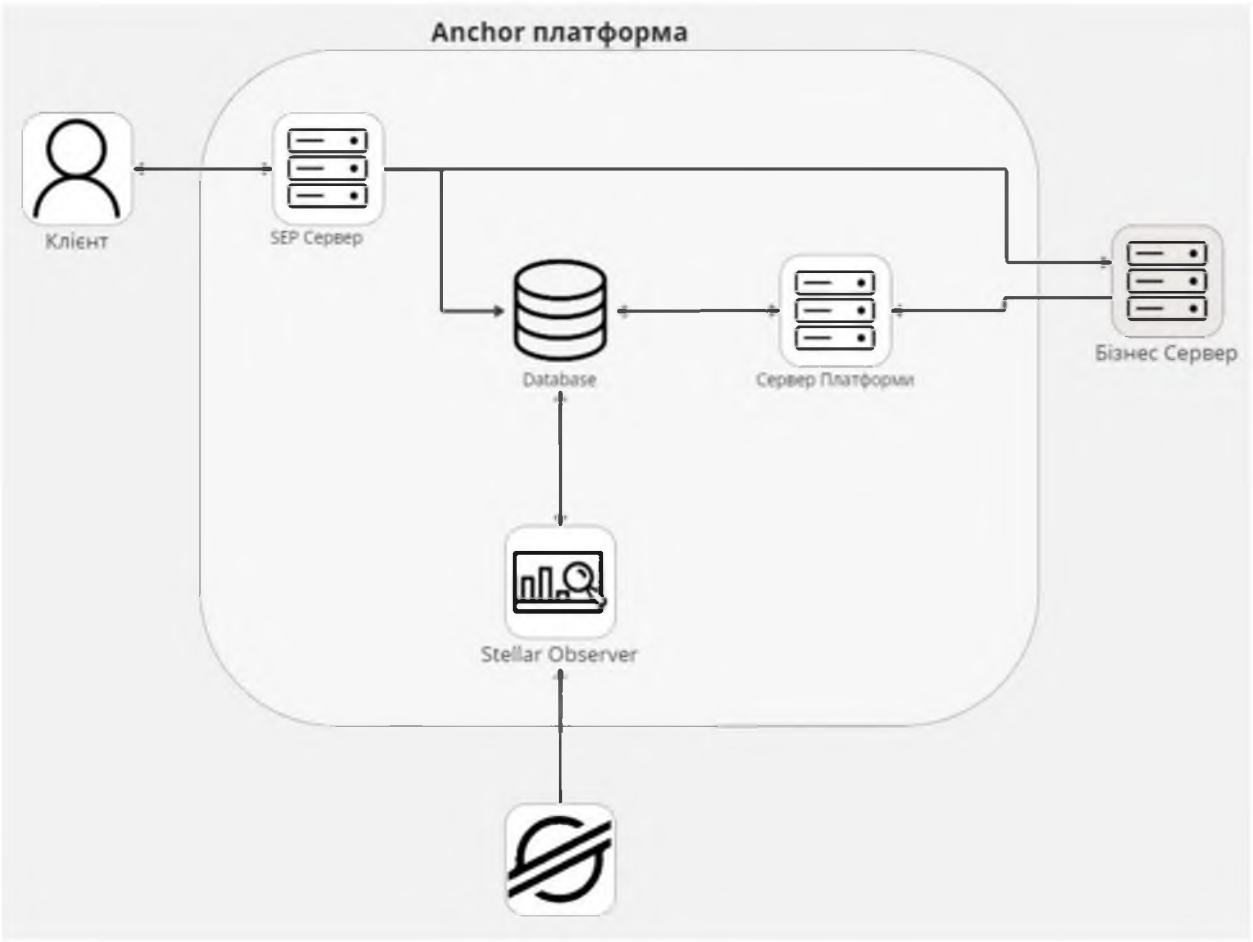

Рисунок 2.6. Схема архітектури платформи Anchor

Де:

Клієнт

Клієнт - це програма, наприклад, гаманець або відправник грошових переказів, яка діє від імені користувача і робить запити до системи. Клієнти надсилають запити до SEP-сервера Anchor Platform, використовуючи набори стандартів, які називаються SEP (Stellar Ecosystem Proposals).

SEP-сервер

SEP-сервер - це клієнтський сервер, тому він повинен бути доступний із зовнішньої мережі. SEP-сервер обробляє запити користувачів і керує станом транзакцій, які вони ініціюють. Коли SEP-серверу потрібно надати клієнту інформацію, якої він не має, наприклад, курс обміну для пари активів, він робить синхронні запити на бізнес-сервер.

Деякі запити SEP призначені для отримання клієнтом даних, пов'язаних з бізнесом, таких як котирування або комісійні. Оскільки це бізнес-запити, SEP-сервер створить запит до вашого сервера і передасть інформацію назад клієнту. Він також перетворить відповідь у SEP-сумісний формат. Сервер SEP ніколи не зберігає в базі даних конфіденційну інформацію, таку як KYC (PII).

Database

Платформа Anchor використовує базу даних PostgreSQL для зберігання подій та сутностей Stellar. Її основне використання - зберігання транзакцій SEP (24 і 31).

Сервер платформи

Сервер платформи є внутрішнім компонентом. Він повинен бути розміщений у приватній мережі і не повинен бути доступним з Інтернету. Цей сервер дозволяє бізнесу отримувати та оновлювати стан транзакцій, використовуючи його API.

Stellar Observer

Спостерігач Stellar контролює блокчейн Stellar, автоматично виявляє користувацькі платежі, надіслані бізнесу, та оновлює відповідні статуси SEP-транзакцій. Цей компонент не є обов'язковим і може бути замінений власним спостерігачем.

Business Server

Бізнес-сервер - це сервер, який бізнес повинні впровадити, щоб повністю підтримувати більшість SEP, пропонованих Anchor платформою. Бізнес-сервер відповідає на запити зворотного дзвінка, надіслані Anchor платформою (наприклад, запит на отримання котирування для SEP-38), і надає оновлення Anchor платформі, коли відбуваються позамережеві події (наприклад, завершення банківського переказу). Запланована архітекрута, взята з офіційної документації Stellar показана на рисунку 2.7.

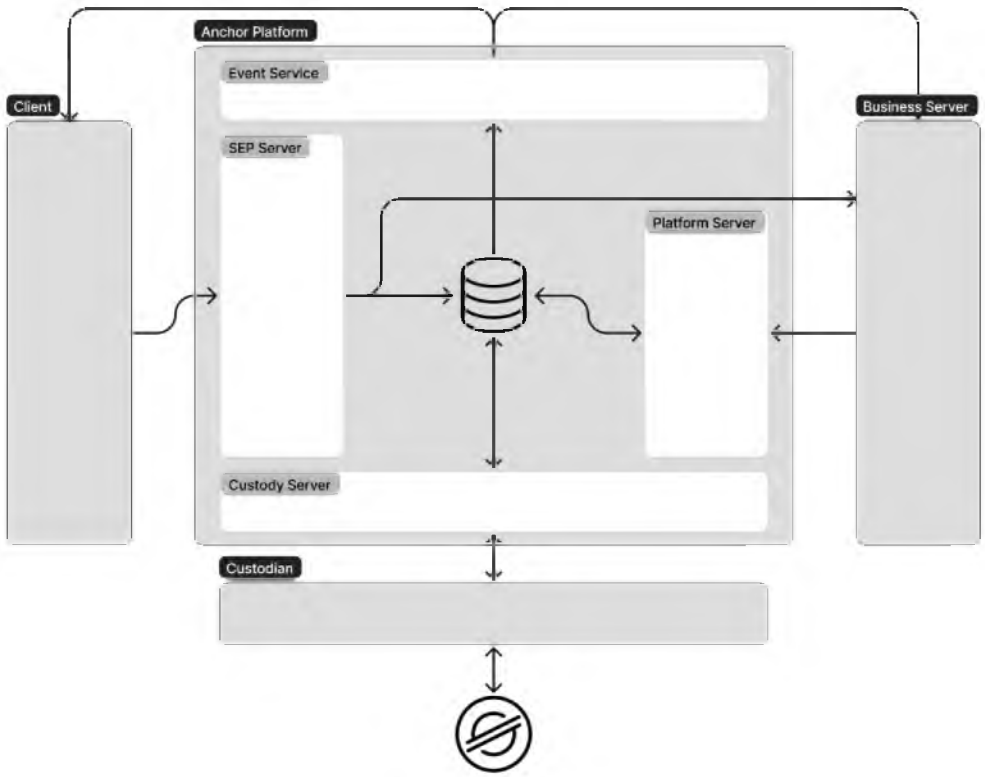

Рисунок 2.7. Запланована архітекрута платформи Anchor

Нові компоненти

Event Service

Сервіс подій - це новий компонент, який надсилає події як клієнту, так і бізнесу за допомогою HTTP-хуків.

Custody Server

Custody сервер - це новий компонент, який дозволяє компаніям підключатися до кастодіального сервісу (наприклад, Fireblocks) для відправлення та отримання платежів у мережі Stellar. При використанні в режимі самостійного зберігання цей сервіс є наступним поколінням існуючого Stellar Observer.

2.4.2. Встановлення

Найпростіший спосіб встановити Anchor платформу - витягнути образ докера.

Приклад bash

```
docker pull stellar/anchor-platform:latest
```

Налаштування середовища розробки

Використовуеться docker compose для простоти, але можна запустити Anchor Platform за допомогою інших інструментів, які також підтримують docker, наприклад, minikube або повноцінний кластер kubernetes.

Мінімальний файл compose для початку.

YAML

```
# docker-compose.yml
services:
  sep-server:
    image: stellar/anchor-platform:latest
    command: --sep-server
    ports:
      - "8080:8080"
    env_file:
      - ./dev.env
    volumes:
      - ./config:/home
  platform-server:
    image: stellar/anchor-platform:latest
    command: --platform-server
    ports:
      - "8085:8085"
    env_file:
```

```
    - ./dev.env
  volumes:
    - ./config:/home
```

Параметр --sep-server вказує платформі Anchor зробити доступними на порту 8080 кінцеві точки API, визначені SEP, які користувач ввімкнув в конфігурації.

Параметр --platform-sever робить доступним API платформи, який є внутрішнім API, що використовуватиметься вашим сервісом(ами) для зв'язку з платформою Anchor. Він буде доступний на порту 8085

Конфігурація

Платформа Anchor підтримує два підходи до конфігурації:

- за допомогою змінних оточення
- за допомогою конфігураційного файлу YAML

Можна використовувати один або комбінацію обох підходів. Вкладені змінні в YAML-файлі виражаються за допомогою символів підкреслення або крапок (_, .) при використанні змінних оточення. На прикладі продемонструємо обидва підходи. Повний набір параметрів конфігурації можна знайти у файлі значень за замовчуванням Anchor Platform.

Платформа Anchor не дозволяє використовувати секрети додатків у файлі конфігурації YAML. Замість цього, секрети додатків, які всі мають префікс SECRET_, повинні бути вказані в середовищі.

bash

```
touch dev.env
```

Якщо використовується файл конфігурації YAML, створимо і його.

```
mkdir config
touch config/dev.services.yaml
```

Додамо змінну оточення. Тому що потрібно буде повідомити платформі, де вона може знайти конфігураційний файл.

```
# dev.env
STELLAR_ANCHOR_CONFIG=/home/dev.services.yaml
```

Вкажіть версію схеми конфігурації у вашому YAML-файлі.
YAML

```
# dev.services.yaml
version: 1
```

Зміна порту сервера платформи
Наприклад, змінимо порт сервера платформи.
bash

```
# dev.env
PLATFORM_SERVER_PORT=8085
```

Або якщо використовується конфігурація YAML:
YAML

```
# dev.services.yaml
platform_server:
  port: 8085
```

Створимо anchor сервіси для USDC Circle у тестовій мережі Stellar. Оновити наведені вище значення відповідно до активів, які ви будете випускати. Не забудьте вказати емітента тестової мережі у вашому файлі розробки та створіть власний distribution_account за

допомогою такого інструменту, як Stellar Lab. Рахунок distribution_account буде використовуватися вашими клієнтами як рахунок призначення для платежів на ваш сервіс.

```
# dev.assets.yaml
assets:
  - schema: stellar
    code: USDC
    issuer:
GBBD47IF6LWK7P7MDEVSCWR7DPUWV3NY3DTQEVFL4NAT4AQH3ZLLFLA5
    distribution_account:
GBLSAHONJRODSFTLOV225NZR4LHICH63RIFQTQN37L5CRTR2IMQ5UEK7
    significant_decimals: 2
```

Додати збереження даних

Anchor Platform підтримує PostgreSQL та Aurora PostgreSQL для використання у виробництві, але також підтримує H2 або SQLite для використання у розробці. Для керування міграціями Anchor Platform використовує Flyway. Остання версія PostgreSQL, яку підтримує Flyway - PostgreSQL 14.

```
# docker-compose.yml
version: "3.8"
services:
  sep-server:
    image: stellar/anchor-platform:latest
    command: --sep-server
    env_file:
      - ./dev.env
    volumes:
      - ./config:/home
```

```
    ports:
      - "8080:8080"
    depends_on:
      - db
  platform-server:
    image: stellar/anchor-platform:latest
    command: --platform-server
    env_file:
      - ./dev.env
    volumes:
      - ./config:/home
    ports:
      - "8085:8085"
    depends_on:
      - db
  db:
    image: postgres:14
    ports:
      - "5432:5432"
    env_file:
      - ./dev.env
    volumes:
      - ./init.sql:/docker-entrypoint-initdb.d/init.sql
```

Оновимо наше середовище, щоб сервер платформи міг з'єднатися з сервером бази даних.

```
# dev.env
DATA_TYPE=postgres
DATA_SERVER=db
```

```
DATA_DATABASE=platform
DATA_FLYWAY_ENABLED=true

SECRET_DATA_USERNAME=postgres
SECRET_DATA_PASSWORD=password

POSTGRES_USER=postgres
POSTGRES_PASSWORD=password
```

Подробиці запуску вказані на офіційній документації Stellar [20]

2.5. Платформа Stellar Disbursement Platform (SDP)

2.5.1. Огляд платформи

Платформа Stellar Disbursement Platform (SDP) - це інструмент, створений для того, щоб організації могли здійснювати масові платежі групі одержувачів через мережу Stellar. Повний покроковий процес після розгортання SDP та налаштування користувачів в організації зазвичай виглядає приблизно так, як показано нижче:

1) Організація фінансує розподільчий рахунок ПДР за допомогою активу на основі Stellar (наприклад, USDC)
2) Адміністратор заходить на інформаційну панель SDP та завантажує CSV-файл, що містить платіжну інформацію, щоб ініціювати нову виплату.
3) SDP надсилає текстове повідомлення кожному першому одержувачу в CSV-файлі із запрошенням завантажити додаток гаманця з підтримкою Stellar
4) Тим часом, SDP негайно починає здійснювати виплати кожному реципієнту, який вже зареєстрував гаманець за допомогою попереднього платежу
5) Кожен реципієнт, який вперше отримує кошти, переходить за посиланням для завантаження додатку для гаманця з підтримкою

Stellar, обраного організацією для цієї виплати, завантажує додаток і проходить процедуру реєстрації гаманця.

6) Після того, як одержувач зареєструвався і його обліковий запис Stellar створено, гаманець негайно проходить автентифікацію в SDP, використовуючи параметри з глибокого посилання, і відкриває веб-сторінку реєстрації в SDP для завершення верифікації одержувачем.
7) Користувач підтверджує свою особу, надаючи OTP-код, надісланий на його номер телефону, та додаткову інформацію для перевірки з метою безпеки. SDP підтримує три різні типи верифікаційної інформації: Дата народження, персональний PIN-код та національне посвідчення особи. Ця інформація вводиться одержувачем у веб-потоці і передається безпосередньо до SDP, тобто гаманцю не потрібно обробляти або зберігати цю інформацію.
8) SDP перевіряє інформацію одержувача. Якщо вона збігається з інформацією з CSV, SDP автоматично здійснює платіж на акаунт Stellar одержувача

Графічне зображення руху коштів показано на рисунку 2.8.

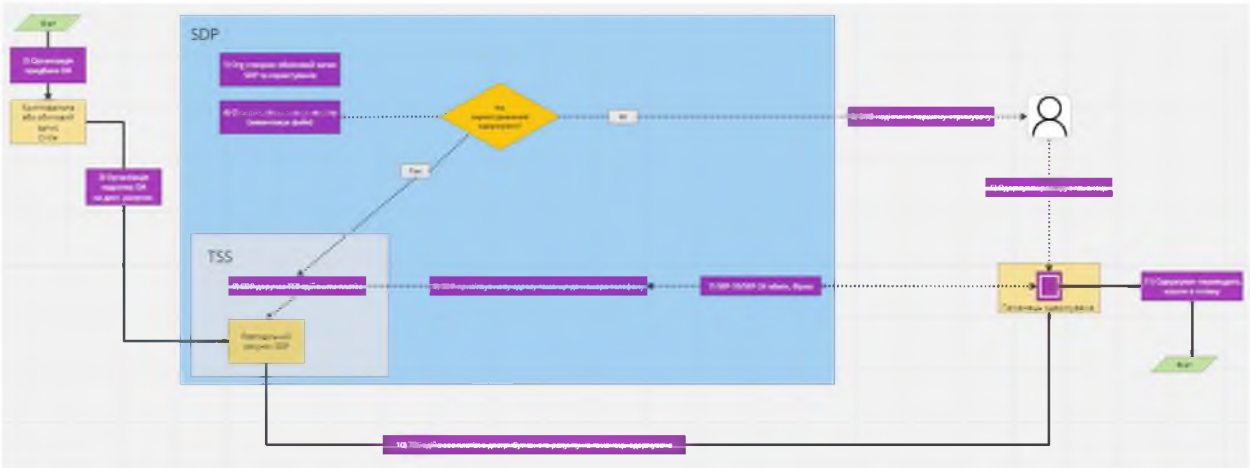

Рисунок 2.8. Рух коштів у блокчейні

Org. = гравець (благодійна організація, компанія, уряд тощо)

DA = цифровий актив (USDC, EUROC тощо)

Dist.acct. = розподільчий рахунок, вбудований гаманець SDP (технічно в TSS)

⟶ = потік грошей/вартості -------- = потік даних

2.6. Запуск та інтеграція Stellar

2.6.1. Основи та концепції

2.6.1.1. Stellar Consensus Protocol (SCP)

Консенсус надзвичайно важливий у децентралізованій платіжній системі. Вона розподіляє моніторинг і затвердження транзакцій між багатьма окремими вузлами (комп'ютерами) замість того, щоб покладатися на одну закриту, центральну систему. Вузли управляються організаціями або приватними особами, і мета полягає в тому, щоб всі вузли оновлювали реєстр однаково, гарантуючи, що кожен реєстр досягне однакового стану. Консенсус є життєво важливим для безпеки блокчейну, дозволяючи вузлам безпечно домовлятися про щось і запобігаючи атакам подвійних витрат.

Мережа Stellar досягає консенсусу за допомогою протоколу консенсусу Stellar (SCP), який є конструкцією Федеративної Візантійської Угоди (FBA). FBA відрізняється від інших відомих механізмів консенсусу, таких як Proof of Work (який покладається на обчислювальну потужність вузла) і Proof of Stake (який покладається на потужність стейкінга вузла), тим, що замість цього він покладається на згоду довірених вузлів.

У SCP кожен вузол Stellar Core (який також називається валідатором або вузлом-валідатором) вирішує, якому набору інших вузлів він хоче довіряти. Гнучкість довіри, визначеної користувачем, забезпечує відкрите членство в мережі (тобто будь-хто може стати вузлом ядра) і децентралізований контроль (тобто жоден центральний орган не диктує, чий голос необхідний для досягнення консенсусу).

За роботу валідатора в мережі Stellar не передбачено грошової винагороди. Натомість, користувачів заохочують ставати валідаторами, оскільки вони роблять свій внесок у безпеку та відмовостійкість мережі, що приносить користь продуктам і сервісам, побудованим на Stellar.

Існує три бажані властивості механізмів консенсусу: відмовостійкість, безпека і життєздатність.

- Відмовостійкість - система може продовжувати працювати, незважаючи на збої або несправності вузлів
- Безпека - жодні два вузли ніколи не погоджуються з різними значеннями, що гарантує, що вузли будуть виробляти один і той же блок
- Життєздатність - вузол може виводити значення без участі будь-яких вузлів, що поводяться неправильно.

Механізми консенсусу, як правило, можуть надавати пріоритет лише двом з трьох цих властивостей. SCP надає пріоритет відмовостійкості та безпеці, а не життєздатності. Через пріоритет безпеки блоки іноді можуть застрягати в очікуванні згоди вузлів. [20]

2.6.1.2. Stellar Stack

Стек Stellar складається з чотирьох програмних компонентів (Stellar Core, Horizon API, SDK, testnet та pubnet), кожен з яких відіграє певну роль у створенні фінансової інфраструктури, стійкої до збоїв, доступної для будь-кого, достатньо швидкої та дешевої для обслуговування реальних випадків використання. Подробиці роботи показані на рисунку 2.9.

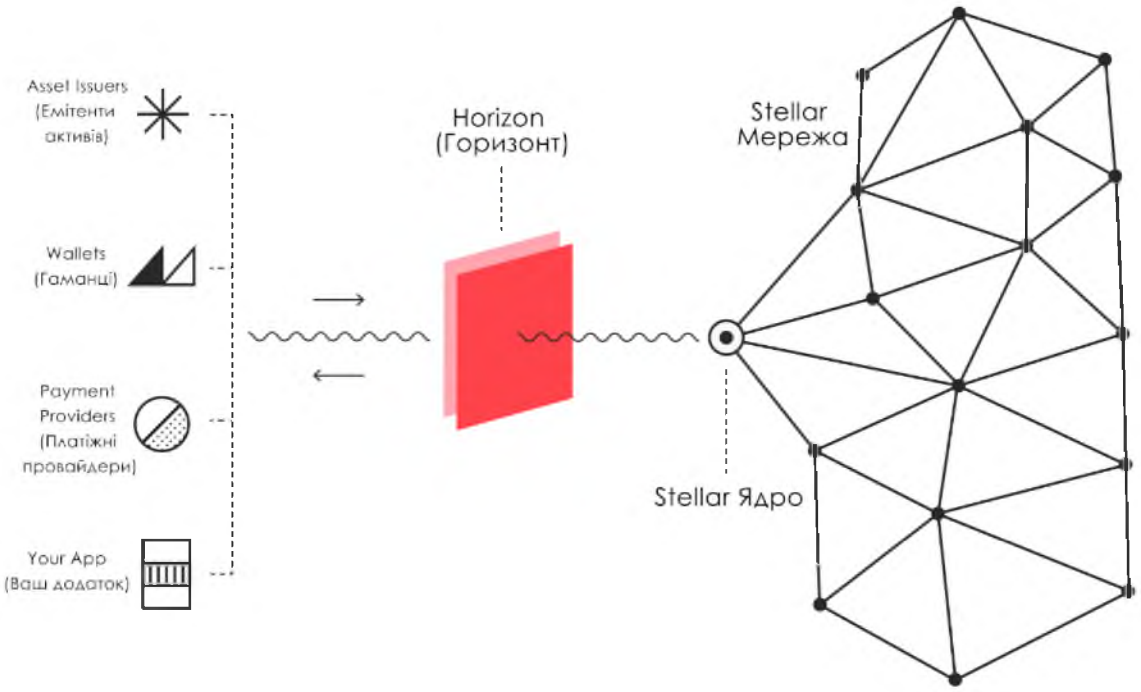

Рисунок 2.9. Схема роботи Stellar Stack

Stellar Core (Stellar ядро) - це програма, яка використовується окремими вузлами (або комп'ютерами), що складають мережу. Stellar Core веде спільний розподілений реєстр і бере участь у консенсусі для перевірки та обробки транзакцій. Зазвичай, вузли досягають консенсусу, застосовують набір транзакцій і оновлюють реєстр кожні 5-7 секунд. Ноди досягають консенсусу за допомогою протоколу Stellar Consensus Protocol.

Horizon - це клієнтський сервер RESTful HTTP API, який дозволяє програмному доступу надсилати транзакції та запитувати історію даних мережі. Він виступає в якості інтерфейсу для додатків, які хочуть отримати доступ до мережі Stellar. З Horizon взаємодіють за допомогою SDK, веб-браузера або за допомогою простих командних інструментів, таких як cURL.

Запускати власний екземпляр Horizon не потрібно, на початковому етапі можна використовувати безкоштовний екземпляр SDF Horizon для доступу до мережі, але рекомендується зробити це, коли буде повна готовність запустити продукт. SDK спрощують частину роботи з доступом до Horizon, перетворюючи дані в більш зручні формати і дозволяючи вам програмувати на обраній користувачем мові. За допомогою SDK від Stellar можна дізнатися, як запитувати дані, створювати та надсилати транзакції.

Рівні безпеки блокчейну. Блокчейн, як технологія, може бути розділений на кілька рівнів які показані у таблиці 2.7.

Таблиця 2.7. Рівні блокчейн технології

Рівень	Назва	Опис
Рівень 0	Інфраструктурний (Network Layer)	- Цей рівень складається з фізичної та програмної інфраструктури, необхідної для функціонування блокчейна. - Включає сервери, мережеве обладнання, протоколи зв'язку та інші основні технології, які забезпечують підключення і взаємодію між вузлами мережі.
Рівень 1	Блокчейн Протокол (Protocol Layer)	- Це серце блокчейну, яке включає основні алгоритми консенсусу (наприклад, Proof of Work, Proof of Stake), криптографічні механізми та протоколи. - На цьому рівні визначаються правила створення блоків, валідації транзакцій та ведення реєстру.
Рівень 2	Логіка Транзакцій (Transaction Layer)	- Рівень, на якому відбуваються транзакції. Включає механізми для виконання та запису транзакцій в блокчейн. - Також може включати реалізацію смарт-контрактів, які дозволяють виконувати складніші операції на основі попередньо визначених умов.
Рівень 3	Додатковий	- Цей рівень включає додатки та сервіси,

	Функціонал (Application Layer)	побудовані на базі блокчейну. - Тут розміщуються різноманітні блокчейн-додатки (DApps), які можуть бути використані для різних цілей, від фінансових операцій до ведення реєстрів та голосувань.
Рівень 4	Інтерфейс Користувача (User Interface Layer)	- Це рівень, на якому користувачі взаємодіють з блокчейн-системами. - Включає веб-інтерфейси, мобільні додатки, клієнтське програмне забезпечення тощо, що дозволяють користувачам використовувати функціонал блокчейну в зручній та інтуїтивно зрозумілій формі.

Разом ці рівні створюють комплексну екосистему блокчейну, кожен рівень якої відіграє важливу роль у загальному функціонуванні та використанні технології.

2.4.1.3. Testnet та Pubnet

Stellar має дві мережі: публічну мережу (Pubnet, яку також називають Mainnet) та тестову мережу (Testnet).

Pubnet - це основна мережа, яка використовується додатками у виробництві. Вона підключається до реальних рейок і вимагає від XLM покриття мінімальних балансів і комісій за транзакції.

Testnet - це менша, безкоштовна мережа, що підтримується SDF, яка функціонує як Pubnet, але не підключена до реальних грошей. Вона має вбудований кран Testnet XLM, що використовується розробниками для тестування своїх додатків.

Статистика: Testnet у порівнянні з Pubnet показана у таблиці 2.8.

Таблиця 2.8. Порівняння Testnet та Pubnet

Testnet	Pubnet
SDF працює з трьома основними вузлами валідатора	Вузли валідаторів знаходяться у відкритому доступі
SDF пропонує безкоштовний екземпляр Horizon, який може використовуватись для взаємодії з Testnet	SDF пропонує безкоштовний екземпляр Horizon для взаємодії з Pubnet, або можна запустити свій власний
Friendbot - це кран, який може використовуватись для безкоштовного Testnet XLM	Потрібно поповнити свій рахунок в XLM з іншого облікового запису
Testnet обмежений 100 операціями на одну книгу	Pubnet обмежений до 1,000 операцій на одну книгу

Friendbot - це бот, який поповнює акаунти фальшивими XLM на Testnet. Можна запросити XLM у friendbot за допомогою Stellar Laboratory або різних SDK. Кількість запитів до friendbot обмежена. Friendbot надає 10 000 фальшивих XLM при фінансуванні нового акаунта Testnet.

Подробиці з додаковою інформацією перед встановленням ядра блокчейну Stellar можна подивитись на офіційній сторінці документації вказаній у переліку посилань. [20]

2.6.2. Запуск основного вузла

Stellar - це однорангова мережа, що складається з вузлів - комп'ютерів, які ведуть спільний розподілений реєстр і взаємодіють для перевірки та додавання транзакцій до нього. Ноди використовують програму Stellar Core - реалізацію протоколу консенсусу Stellar - для синхронізації під час роботи над узгодженням дійсності наборів транзакцій і внесенням їх до реєстру. Як правило, вузли досягають консенсусу, застосовують набір транзакцій і оновлюють реєстр кожні 3-5 секунд.

Щоб будувати на Stellar не потрібно запускати вузол: можна почати розробку з обраного SDK і використовувати загальнодоступні екземпляри Horizon для запитів до реєстру і негайного відправлення транзакцій.

Насправді, Stellar Development Foundation пропонує два публічних екземпляри Horizon - один для публічної мережі і один для тестової мережі.

Якщо запустити свій власний екземпляр Horizon, він включає в себе власну версію Core і повністю керує своїм життям, тому немає необхідності запускати окремий екземпляр.

2.6.2.1. Передумови

Можна встановити Stellar Core кількома різними способами, і після цього налаштувати його для участі в мережі на декількох різних рівнях: це може бути як базовий валідатор, так і повний валідатор. Незалежно від того, як встановлений Stellar Core або який тип вузла використовується, потрібно налаштувати підключення до однорангової мережі та зберігання стану книги в базі даних SQL.

Вимоги до обчислень

Було проведено опитування операторів Stellar Core про їхні налаштування. На початку 2018 року Stellar Core з PostgreSQL на одній машині добре працювали на m5.large в AWS (двоядерний Intel Xeon 2,5 ГГц, 8 ГБ оперативної пам'яті, 20 ГБ основної).

Перед встановленням Stellar Core на тій самій машині, що й Horizon, потрібно додатково буде переконатися, що установка також відповідає обчислювальним вимогам Horizon.

Доступ до мережі

Stellar Core взаємодіє з одноранговою мережею для синхронізації розподіленого реєстру, а це означає, що вузол повинен зробити певні TCP-порти доступними для вхідного та вихідного зв'язку.

- Вхідний: вузол Stellar Core повинен дозволити всім IP-адресам підключатися до його PEER_PORT через TCP. Можна вказати порт під час налаштування Stellar Core, але частіше за все використовують порт за замовчуванням, який дорівнює 11625.

- Вихідний: Stellar Core має з'єднуватися з іншими вузлами через їхні PEER_PORTs TCP. Можна знайти інформацію про PEER_PORTs інших вузлів у мережевому провіднику, такому як Stellarbeat, але частіше за все використовує порт за замовчуванням, який дорівнює 11625.

Внутрішній доступ до системи

Вихідні дані:

- Stellar Core потребує доступу до бази даних PostgreSQL. Якщо ця база даних знаходиться на іншому комп'ютері у мережі, потрібно дозволити це з'єднання. Користувач вказує базу даних під час налаштування Stellar Core.
- Користувач можете заблокувати всі інші з'єднання.

Вхідні дані:

- Stellar Core виявляє неавторизовану кінцеву точку HTTP на своєму HTTP_PORT. Користувач може вказати порт під час налаштування Stellar Core, але частіше за все використовують значення за замовчуванням 11626.
- HTTP_PORT використовується Horizon для відправки транзакцій, тому може бути відкритий для решти внутрішніх IP-адрес користувача.
- Також використовується для запиту інформації Stellar Core і надання метрик
- Для виконання адміністративних команд, таких як планування оновлень і зміна рівнів журналів

Подробиці вказані у документації на офіційній сторінці Stellar [20]

2.6.2.2. Встановлення

Існує три способи встановлення Stellar Core: Користувач може використати образ Docker, pre-built packages або зібрати з коду. Використання образу Docker - це найшвидший і найпростіший спосіб, тому він підходить для багатьох розробників.

Встановлення на основі докера

Середовища розробки

SDF підтримує образ швидкого запуску, який об'єднує Stellar Core з базами даних Horizon і postgreSQL. Це швидкий спосіб встановити конфігурацію за замовчуванням, яка не перевіряється і має працювати для більшості розробників.

На додаток до SDF-образів, Satoshipay підтримує окремі Docker-образи для Stellar Core та Horizon. Образ Satoshipay Stellar Core Docker поставляється в декількох варіантах, в тому числі зі встановленим AWS CLI і зі встановленим Google Cloud SDK. Образ Horizon підтримує всі змінні середовища Horizon.

Виробничі середовища

SDF також підтримує автономне зображення лише для Stellar Core: stellar/stellar-core.

Приклад використання:

```
docker run stellar/stellar-core:latest help
docker run stellar/stellar-core:latest gen-seed
```

Для запуску потрібно надати конфігураційний файл:

```
# Initialize postgres DB (see DATABASE config option)
docker run -v "/path/to/config/dir:/etc/stellar/" stellar/stellar-core:latest new-db
# Run stellar-core daemon in the background
docker run -d -v "/path/to/config/dir:/etc/stellar/" stellar/stellar-core:latest run
```

Образ використовує deb packages, тому можна перевірити відповідність контрольної суми двійкового коду Stellar Core в образі докера контрольній сумі у криптографічно підписаному пакунку deb. Настанови щодо встановлення пакунків Ubuntu наведено у документації до пакунків. Для обчислення контрольної суми в образі докера можна запустити програму:

```
docker run --entrypoint=/bin/sha256sum stellar/stellar-core:latest /usr/bin/stellar-core
```

Встановлення з пакунків

При використанні Ubuntu 18.04 LTS або новішу версію, будут надані останні версії stellar-core і stellar-horizon у форматі двійкових пакетів Debian.

Користувач може встановити ці пакунки окремо, що забезпечує найбільшу гнучкість, але вимагає ручного створення відповідних конфігураційних файлів і налаштування бази даних PostgreSQL.

Подробиці вказані на сайті Github у переліку посилань [21]

2.6.2.3. Налаштування

Після встановлення Stellar Core наступним кроком буде заповнення конфігураційного файлу, в якому будуть вказані важливі дані про вузол - наприклад, чи підключається він до тестової мережі, чи до загальнодоступної, до якої бази даних він пише, і які інші вузли входять до його кворуму. Користувач може це зробити за допомогою TOML, і за замовчуванням Stellar Core завантажує цей файл з ./stellar-core.cfg. Можна вказати інший файл для завантаження за допомогою командного рядка:

```
$ stellar-core --conf betterfile.cfg <COMMAND>
```

База даних

Stellar Core зберігає дві копії реєстру: одну в базі даних SQL і одну в XDR-файлах на локальному диску, які називаються buckets. База даних консультується під час консенсусу і модифікується атомарно, коли набір транзакцій застосовується до реєстру. Це випадковий доступ, дрібнозернистий і швидкий.

Хоча база даних SQLite працює зі Stellar Core, але рекомендується використовувати окремий сервер PostgreSQL. База даних Postgres є основою Stellar Core.

Користувач вказує базу даних потрібного вузла у відповідному полі DATABASE конфігураційного файлу, про який можна прочитати більше у повному прикладі конфігурації. За замовчуванням це база даних у пам'яті, але можна вказати шлях до неї, як показано у прикладі.

Якщо використовується Postgresql, рекомендується налаштувати доступ до локальної бази даних через сокет домену Unix, а також оновити наведені нижче параметри конфігурації Postgresql:

```
# !!! DB connection should be over a Unix domain socket !!!
# shared_buffers = 25% of available system ram
# effective_cache_size = 50% of available system ram
# max_wal_size = 5GB
# max_connections = 150
```

Buckets

Stellar-core також зберігає дублікат книги у вигляді пласких XDR-файлів, які називаються "buckets". Ці файли розміщуються в каталозі, вказаному в конфігураційному файлі як BUCKET_DIR_PATH, який за замовчуванням дорівнює buckets. Файли-buckets використовуються для хешування і передачі різниць у журналах до архівів історії.

Buckets слід зберігати на швидкому локальному диску з достатнім простором для зберігання файлів, розмір яких у кілька разів перевищує розмір поточного журналу.

Здебільшого вміст як бази даних, так і каталогів buckets можна ігнорувати, оскільки ними керує Stellar Core. Однак, при першому запуску Stellar Core повинні ініціалізувати обидва каталоги за допомогою наступної команди:

$ stellar-core new-db

Ця команда ініціалізує базу даних і директорії buckets, а потім завершує роботу. Користувач також може використовувати цю команду, якщо база даних пошкоджена і потрібно перезапустити її з нуля.

Мережева парольна фраза

Використовуйте поле NETWORK_PASSPHRASE, щоб вказати, до якої мережі підключається вузол - тестової чи загальнодоступної:

```
- NETWORK_PASSPHRASE="Test SDF Network ; September 2015"
- NETWORK_PASSPHRASE="Public Global Stellar Network ; September 2015"
```

Валідація

За замовчуванням Stellar Core не налаштовано на валідацію. Якщо потрібно, щоб вузол був базовим валідатором або повним валідатором, потрібно налаштувати його для цього, тобто підготувати його до участі в SCP і підписання повідомлень, які підтверджують, що мережа погоджується з певним набором транзакцій.

Налаштування вузла для участі в SCP і підписання повідомлень складається з трьох кроків:

- Create a keypair stellar-core gen-seed
- Add NODE_SEED="SD7DN..." to your configuration file,
  where SD7DN... is the secret key from the keypair
- Add NODE_IS_VALIDATOR=true to your configuration file

Якщо потрібно, щоб інші валідатори додали ваш вузол до своїх наборів кворуму, потрібно поділитися своїм відкритим ключем (GDMTUTQ...), опублікувавши файл stellar.toml на своєму домашньому домені відповідно до специфікацій, викладених в SEP-20.

Важливо зберігати і захищати секретний ключ вашого вузла: якщо хтось інший має доступ до нього, він може надсилати повідомлення в мережу, і буде здаватися, що вони походять з вашого вузла. Кожен вузол, який ви запускаєте, повинен мати свій власний секретний ключ.

Якщо використовується більше одного вузла, потрібно встановити HOME_DOMAIN, спільний для цих вузлів, за допомогою властивості NODE_HOME_DOMAIN. Це дозволить правильно згрупувати вузли під час генерації кворуму.

Вибір набору кворуму

Незалежно від того, який вузол використовується - базовий валідатор, повний валідатор або архіватор - потрібно вибрати набір кворуму, який складається з валідаторів (згрупованих за організаціями), з якими вузол звіряється, щоб визначити, чи застосовувати набір транзакцій до книги.

Хороший набір кворуму:

- відповідає пріоритетам потрібної організації
- має достатню надлишковість для обробки довільних відмов вузлів
- підтримує хороший перетин кворуму

Оскільки створити хороший набір кворуму досить складно, stellar core автоматично генерує його на основі структурованої інформації, яку надає користувач у своєму конфігураційному файлі. Користувач обирає валідаторів, яким хоче довіряти, а stellar core конфігурує їх в оптимальний набір кворуму.

Щоб згенерувати кворум, stellar core:

- Об'єднує валідаторів від однієї організації в підкворум
- Встановлює поріг для кожного з цих підкворумів
- Надає вагу цим підкворумам на основі якості

Виявлення валідатора

Коли додають валідатор до свого набору кворуму, це зазвичай відбувається тому, що довіряють організації, яка керує цим вузлом:

користувач довіряють SDF, а не якомусь анонімному відкритому ключу Stellar.

Щоб створити самоперевірений зв'язок між вузлом і організацією, яка ним керує, валідатор оголошує домашній домен в ланцюжку за допомогою операції set_options і публікує інформацію про організацію у файлі stellar.toml, розміщеному на цьому домені.

Важливо зазначити, що для правильної роботи автоматичного визначення кворуму вам потрібно або залежати лише від одного вузла, або мати принаймні 4 вузли для автоматичного визначення кворуму. Щонайменше 4 - кращий варіант.

Масив домашніх доменів

Для створення набору кворуму Stellar Core використовує два масиви таблиць: [[HOME_DOMAINS]] і [[VALIDATORS]].

Приклад показаний у офіційній документації [20]

[[HOME_DOMAINS]] визначає підмножину валідаторів: коли користувач додає до конфігурації вузли, розміщені в одній організації, вони мають спільний домашній домен, і інформація в таблиці [[HOME_DOMAINS]], а саме рейтинг якості, автоматично застосовується до кожного з цих валідаторів.

Для кожної організації, яку потрібно додати, є окрема таблиця 2.9.

[[HOME_DOMAINS]]

Поле (Field)	**Вимоги (Requirements)**	**Опис (Description)**
HOME_DOMAIN	string	URL домашнього домену, пов'язаний з групою валідаторів
QUALITY	string	Рейтинг для вузлів організації: HIGH, MEDIUM або LOW

Таблиця 2.9. Домени

Приклад:

[[HOME_DOMAINS]]

```
HOME_DOMAIN="testnet.stellar.org"
QUALITY="HIGH"
[[HOME_DOMAINS]]
HOME_DOMAIN="some-other-domain"
QUALITY="LOW"
```

Масив валідаторів

Для кожного вузла до набору кворуму є таблиця 2.10.

Таблиця 2.10. [[VALIDATORS]]

Поле (Field)	**Вимоги (Requirements)**	**Опис (Description)**
NAME	string	Унікальний псевдонім для вузла
QUALITY	string	Рейтинг для вузла (обов'язковий, якщо не вказано в [[HOME_DOMAINS]]): HIGH, MEDIUM, або LOW.
HOME_DOMAIN	string	URL домашнього домену, пов'язаний з валідатором.
PUBLIC_KEY	string	Stellar відкритий ключ, пов'язаний з валідатором.
ADDRESS	string	Peer:порт, пов'язаний з валідатором (необов'язково)
HISTORY	string	архів GET-команди, пов'язаної з валідатором (необов'язково)

Якщо HOME_DOMAIN вузла збігається з організацією, визначеною в масиві [[HOME_DOMAINS]], до вузла буде застосовано вказаний там рейтинг якості.

Приклад:

```
[[VALIDATORS]]
NAME="sdftest1"
HOME_DOMAIN="testnet.stellar.org"
```

```
PUBLIC_KEY="GDKXE2OZMJIPOSLNA6N6F2BVCI3O777I2OOC4BV7VOYUEH
YX7RTRYA7Y"
ADDRESS="core-testnet1.stellar.org"
HISTORY="curl -sf http://history.stellar.org/prd/core-testnet/core_testnet_001/{0} -o
{1}"

[[VALIDATORS]]
NAME="sdftest2"
HOME_DOMAIN="testnet.stellar.org"
PUBLIC_KEY="GCUCJTIYXSOXKBSNFGNFWW5MUQ54HKRPGJUTQFJ5RQXZ
XNOLNXYDHRAP"
ADDRESS="core-testnet2.stellar.org"
HISTORY="curl -sf http://history.stellar.org/prd/core-testnet/core_testnet_002/{0} -o
{1}"

[[VALIDATORS]]
NAME="rando-node"
QUALITY="LOW"
HOME_DOMAIN="rando.com"
PUBLIC_KEY="GC2V2EFSXN6SQTWVYA5EPJPBWWIMSD2XQNKUOHGEKB53
5AQE2I6IXV2Z"
ADDRESS="core.rando.com"
```

Валідатор якості

QUALITY є обов'язковим полем для кожного вузла, який додається до набору кворуму. Незалежно від того, чи вказують його для набору вузлів у [[HOME_DOMAINS]], чи для одного вузла у [[VALIDATORS]], воно означає три варіанти оцінки: HIGH, MEDIUM або LOW.

Валідатори високої якості (HIGH) мають найбільшу вагу при автоматичному налаштуванні набору кворуму. Перш ніж присвоїти вузлу високий рейтинг якості, потрібно переконатись, що він має низьку затримку і хороший час безвідмовної роботи, а також, що організація, яка керує вузлом, є надійною і заслуговує на довіру.

Валідатор високої якості:

- публікує архів
- належить до набору вузлів, які забезпечують надмірність

Вибір надлишкових вузлів є доброю практикою. Вимога щодо наявності архіву забезпечується програмно.

Валідатори з середньою якістю (MEDIUM) вкладені під валідаторами з високою якістю, а їхня сукупна вага еквівалентна одній високоякісній сутності. Якщо вузол не публікує архів, він вважається надійним або має організаційний інтерес включити його до свого кворуму, потрібно надати йому оцінку середньої якості.

Валідатори низької якості (LOW) вкладені під валідаторами середньої якості, а їхня сукупна вага еквівалентна одній сутності середньої якості. Якщо з часом вони доведуть свою надійність, можна підвищити їхній рейтинг до середнього, щоб надати їм більшу роль у конфігурації набору для визначення кворуму.

2.6.2.4. Публікація архівів історії

Якщо потрібно запустити повний валідатор або архіватор, потрібно налаштувати вузол для публікації архіву історії. Для цього можна розмістити архів за допомогою блоб-сховища, такого як Amazon's S3, простору Digital Ocean, або просто завантажити локальний архів безпосередньо через HTTP-сервер, такий як Nginx або Apache. Якщо налаштовується базовий валідатор, можна пропустити цей розділ. Незалежно від того, який тип вузла планується запустити, важливо переконатись, що він налаштований на отримання історії, що описано в розділі Конфігурація.

Архів з використанням nginx

Публікація локального архіву історії за допомогою nginx:

Потрібно додати рядок конфігурації історії до файлу

/etc/stellar/stellar-core.cfg

Приклад:

```
[HISTORY.local]
get="cp /mnt/xvdf/stellar-core-archive/node_001/{0} {1}"
put="cp {0} /mnt/xvdf/stellar-core-archive/node_001/{1}"
mkdir="mkdir -p /mnt/xvdf/stellar-core-archive/node_001/{0}"
```

Запускаємо new-hist, щоб створити локальний архів

```
# sudo -u stellar stellar-core --conf /etc/stellar/stellar-core.cfg new-hist local
```

Ця команда створює структуру архіву історії:

```
# tree -a /mnt/xvdf/stellar-core-archive/
/mnt/xvdf/stellar-core-archive
└── node_001
    ├── history
    │   └── 00
    │       └── 00
    │           └── 00
    │               └── history-00000000.json
    └── .well-known
        └── stellar-history.json

6 directories, 2 files
```

Налаштування віртуального хосту для обслуговування локального архіву (Nginx)

```
server {
  listen 80;
  root /mnt/xvdf/stellar-core-archive/node_001/;
```

```
  server_name history.example.com;

  # default is to deny all
  location / { deny all; }

  # do not cache 404 errors
  error_page 404 /404.html;
  location = /404.html {
    add_header Cache-Control "no-cache" always;
  }

  # do not cache history state file
  location ~ ^/.well-known/stellar-history.json$ {
    add_header Cache-Control "no-cache" always;
    try_files $uri;
  }

  # cache entire history archive for 1 day
  location / {
    add_header Cache-Control "max-age=86400";
    try_files $uri;
  }
}
```

Complete History Archive

Якщо потрібно опублікувати повний архів - що дозволить іншим користувачам приєднатися до мережі з книги генезису - можна використовувати stellar-archivist для додавання всіх відсутніх даних історії до

вашого часткового архіву, а також для перевірки стану і цілісності вашого архіву.

Наприклад:

```
# stellar-archivist scan file:///mnt/xvdf/stellar-core-archive/node_001
2019/04/25 11:42:51 Scanning checkpoint files in range: [0x0000003f, 0x0000417f]
2019/04/25 11:42:51 Checkpoint files scanned with 324 errors
2019/04/25 11:42:51 Archive: 3 history, 2 ledger, 2 transactions, 2 results, 2 scp
2019/04/25 11:42:51 Scanning all buckets, and those referenced by range
2019/04/25 11:42:51 Archive: 30 buckets total, 30 referenced
2019/04/25 11:42:51 Examining checkpoint files for gaps
2019/04/25 11:42:51 Examining buckets referenced by checkpoints
2019/04/25 11:42:51 Missing history (260): [0x0000003f-0x000040ff]
2019/04/25 11:42:51 Missing ledger (260): [0x0000003f-0x000040ff]
2019/04/25 11:42:51 Missing transactions (260): [0x0000003f-0x000040ff]
2019/04/25 11:42:51 Missing results (260): [0x0000003f-0x000040ff]
2019/04/25 11:42:51 No missing buckets referenced in range [0x0000003f, 0x0000417f]
2019/04/25 11:42:51 324 errors scanning checkpoints
```

З результатів виконання команди scan, в краєзнавчому архіві бракує певної історії, книги, транзакцій та результатів.

Можна відновити відсутні дані за допомогою команди stellar-archivist's repair у поєднанні з відомим повним архівом - наприклад, публічним історичним архівом SDF:

stellar-archivist repair http://history.stellar.org/prd/core-testnet/core_testnet_001/ file:///mnt/xvdf/stellar-core-archive/node_001/

Приклад:

```
2019/04/25 11:50:15 repairing http://history.stellar.org/prd/core-testnet/core_testnet_001/
-> file:///mnt/xvdf/stellar-core-archive/node_001/
2019/04/25 11:50:15 Starting scan for repair
2019/04/25 11:50:15 Scanning checkpoint files in range: [0x0000003f, 0x000041bf]
2019/04/25 11:50:15 Checkpoint files scanned with 244 errors
```

2019/04/25 11:50:15 Archive: 4 history, 3 ledger, 263 transactions, 61 results, 3 scp

2019/04/25 11:50:15 Error: 244 errors scanning checkpoints

2019/04/25 11:50:15 Examining checkpoint files for gaps

2019/04/25 11:50:15 Repairing history/00/00/00/history-0000003f.json

2019/04/25 11:50:15 Repairing history/00/00/00/history-0000007f.json

2019/04/25 11:50:15 Repairing history/00/00/00/history-000000bf.json

...

2019/04/25 11:50:22 Repairing ledger/00/00/00/ledger-0000003f.xdr.gz

2019/04/25 11:50:23 Repairing ledger/00/00/00/ledger-0000007f.xdr.gz

2019/04/25 11:50:23 Repairing ledger/00/00/00/ledger-000000bf.xdr.gz

...

2019/04/25 11:51:18 Repairing results/00/00/0e/results-00000ebf.xdr.gz

2019/04/25 11:51:18 Repairing results/00/00/0e/results-00000eff.xdr.gz

2019/04/25 11:51:19 Repairing results/00/00/0f/results-00000f3f.xdr.gz

...

2019/04/25 11:51:39 Repairing scp/00/00/00/scp-0000003f.xdr.gz

2019/04/25 11:51:39 Repairing scp/00/00/00/scp-0000007f.xdr.gz

2019/04/25 11:51:39 Repairing scp/00/00/00/scp-000000bf.xdr.gz

...

2019/04/25 11:51:50 Re-running checkpoing-file scan, for bucket repair

2019/04/25 11:51:50 Scanning checkpoint files in range: [0x0000003f, 0x000041bf]

2019/04/25 11:51:50 Checkpoint files scanned with 5 errors

2019/04/25 11:51:50 Archive: 264 history, 263 ledger, 263 transactions, 263 results, 241 scp

2019/04/25 11:51:50 Error: 5 errors scanning checkpoints

2019/04/25 11:51:50 Scanning all buckets, and those referenced by range

2019/04/25 11:51:50 Archive: 40 buckets total, 2478 referenced

2019/04/25 11:51:50 Examining buckets referenced by checkpoints

2019/04/25 11:51:50 Repairing bucket/57/18/d4/bucket-5718d412bdc19084dafeb7e1852cf06f454392df627e1ec056c8b756263a47f1.xdr.gz

2019/04/25 11:51:50 Repairing bucket/8a/a1/62/bucket-8aa1624cc44aa02609366fe6038ffc5309698d4ba8212ef9c0d89dc1f2c73033.xdr.gz

2019/04/25 11:51:50 Repairing bucket/30/82/6a/bucket-30826a8569cb6b178526ddba71b995c612128439f090f371b6bf70fe8cf7ec24.xdr.gz

...

Фінальне сканування місцевого архіву підтверджує, що його успішно відремонтовано

stellar-archivist scan `file:///mnt/xvdf/stellar-core-archive/node_001`

Приклад:

2019/04/25 12:15:41 Scanning checkpoint files in range: [0x0000003f, 0x000041bf]

2019/04/25 12:15:41 Archive: 264 history, 263 ledger, 263 transactions, 263 results, 241 scp

2019/04/25 12:15:41 Scanning all buckets, and those referenced by range

2019/04/25 12:15:41 Archive: 2478 buckets total, 2478 referenced

2019/04/25 12:15:41 Examining checkpoint files for gaps

2019/04/25 12:15:41 Examining buckets referenced by checkpoints

2019/04/25 12:15:41 No checkpoint files missing in range [0x0000003f, 0x000041bf]

2019/04/25 12:15:41 No missing buckets referenced in range [0x0000003f, 0x000041bf]

Запустити екземпляр stellar-core (systemctl start stellar-core), і повинен з'явитися повний архів історії, до якого буде записуватися повний валідатор.

Подробиці запуску вказані на офіційній сторінці з документацією Stellar [20]

2.6.2.5. Запуск

Запуск Stellar Core

Після того, як налаштували середовище, конфігурували вузол, встановили кворум і вибрали архіви для отримання історії, можна запускати Stellar Core.

Використаємо команду:

$ stellar-core run

На цьому етапі можна спостерігати за активністю вузла під час приєднання до мережі.

Взаємодія з екземпляром

Коли вузол працює, можна взаємодіяти зі Stellar Core через адміністративну кінцеву точку HTTP. Команди можна надсилати за допомогою HTTP-інструментів командного рядка, таких як curl, або за допомогою команди типу

$ stellar-core http-command <http-command>

Ця кінцева точка HTTP не призначена для публічного доступу до інтернету. Зазвичай до неї отримують доступ адміністратори або програми середнього рівня для відправки транзакцій в мережу Stellar.

Приєднання до мережі

Під час приєднання до мережі вузол пройде наступні етапи:

Встановлення з'єднання з іншими одноранговими вузлами.

Можна побачити, що authenticated_count збільшується.

JSON:

```
"peers" : {
  "authenticated_count" : 3,
  "pending_count" : 4
},
```

Observing Consensus

Поки вузол не побачить кворум, він буде видавати:

JSON:

```
"state" : "Joining SCP"
```

Після дотримання консенсусу, новий польовий кворум відобразить інформацію про рішення мережі. У цей момент вузол перейде в режим "Catching up":

JSON

```
"quorum" : {
  "qset" : {
    "ledger" : 22267866,
    "agree" : 5,
    "delayed" : 0,
    "disagree" : 0,
    "fail_at" : 3,
    "hash" : "980a24",
    "missing" : 0,
    "phase" : "EXTERNALIZE"
  },
  "transitive" : {
    "intersection" : true,
    "last_check_ledger" : 22267866,
    "node_count" : 21
  }
},
"state" : "Catching up",
```


Catching up

Це фаза, на якій вузол завантажує дані з архівів.


```
"state" : "Catching up",
"status" : [ "Catching up: Awaiting checkpoint (ETA: 35 seconds)" ]
```


Ведення журналу

За замовчуванням Stellar Core надсилає журнали на стандартний вивід і до файлу stellar-core.log, який налаштовується як LOG_FILE_PATH.

Повідомлення журналу класифікуються за прогресивними рівнями пріоритету: TRACE, DEBUG, INFO, WARNING, ERROR і FATAL. Система журналювання видає лише ті повідомлення, рівень яких не нижчий за налаштований рівень журналювання.

Рівень журналу можна контролювати за допомогою конфігурації, прапорця командного рядка -ll або динамічно змінювати за допомогою адміністративних (HTTP) команд. Для цього виконайте

$ stellar-core http-command "ll?level=debug"

під час роботи системи.

Рівні журналів також можна налаштувати для кожного розділу за допомогою адміністративного інтерфейсу. Наприклад, систему журналювання історії можна налаштувати на рівень DEBUG під час запуску:

$ stellar-core http-command "ll?level=debug&partition=history"

Проти працюючої системи.

Типовий рівень журналу - INFO, який є помірно багатослівним і має виводити повідомлення про хід виконання кожні кілька секунд за нормальної роботи.

2.6.2.6. Моніторинг

Після того, як вузол запущений і працює, важливо стежити за ним, щоб переконатися, що він залишається на плаву і продовжує робити свій внесок у здоров'я всієї мережі. Для цього Stellar Core надає життєво важливу інформацію, яку можна використовувати для моніторингу вузла та діагностики потенційних проблем.

Загальна інформація про вузол

Якщо виконати $ stellar-core http-command 'info', вивід буде виглядати так:

JSON

```
{
    "build" : "v11.1.0",
    "history_failure_rate" : "0",
    "ledger" : {
      "age" : 3,
      "baseFee" : 100,
      "baseReserve" : 5000000,
      "closeTime" : 1560350852,
      "hash" :
"40d884f6eb105da56bea518513ba9c5cda9a4e45ac824e5eac8f7262c713cc60",
      "maxTxSetSize" : 1000,
      "num" : 24311579,
      "version" : 11
    },
    "network" : "Public Global Stellar Network ; September 2015",
    "peers" : {
      "authenticated_count" : 5,
      "pending_count" : 0
    },
    "protocol_version" : 10,
    "quorum" : {
      "qset" : {
        "agree" : 6,
        "delayed" : 0,
        "disagree" : 0,
        "fail_at" : 2,
        "hash" : "d5c247",
        "ledger" : 24311579,
        "missing" : 1,
        "phase" : "EXTERNALIZE"
      },
      "transitive" : {
        "critical" : null,
        "intersection" : true,
        "last_check_ledger" : 24311536,
```

```
        "node_count" : 21
      }
    },
    "startedOn" : "2019-06-10T17:40:29Z",
    "state" : "Catching up",
    "status" : [ "Catching up: downloading and verifying buckets: 30/30 (100%)" ]
  }
}
```


Де:

Build - номер збірки для цього екземпляра Stellar Core

Ledger - локальний стан вашого вузла, який може відрізнятися від мережевого, якщо ваш вузол було від'єднано від мережі. Кілька важливих підполів:

Age - час, що минув з моменту закриття цього реєстру (при нормальній роботі менше 10 секунд)

Num - номер книги

Version - версія протоколу, яку підтримує цей журнал

network - мережева ключова фраза, яку використовує цей основний екземпляр, щоб вирішити, чи підключатися до тестової мережі, чи до загальнодоступної мережі

peers - інформація про підключення до мережі

authenticated_count - кількість активних підключень

pending_count - кількість з'єднань, які ще не повністю встановлено

protocol_version - максимальна версія протоколу, яку розпізнає даний екземпляр

state - стан синхронізації вузла відносно мережі

quorum - підсумовує стан учасників протоколу SCP, аналогічно інформації, що повертається командою quorum

Інформація про накладання

Команда peers повертає інформацію про однорангові вузли, до яких підключено ваш вузол.

Цей список є результатом як вхідних з'єднань від інших вузлів, так і вихідних з'єднань від цього вузла до інших вузлів.

$ stellar-core http-command 'peers'

JSON


```
{
 "authenticated_peers": {
  "inbound": [
   {
    "address": "54.161.82.181:11625",
    "elapsed": 6,
    "id": "sdf1",
    "olver": 5,
    "ver": "v9.1.0"
   }
  ],
  "outbound": [
   {
    "address": "54.211.174.177:11625",
    "elapsed": 2303,
    "id": "sdf2",
    "olver": 5,
    "ver": "v9.1.0"
   },
   {
    "address": "54.160.175.7:11625",
    "elapsed": 14082,
    "id": "sdf3",
    "olver": 5,
```

```
      "ver": "v9.1.0"
     }
    ]
   },
   "pending_peers": {
    "inbound": ["211.249.63.74:11625", "45.77.5.118:11625"],
    "outbound": ["178.21.47.226:11625", "178.131.109.241:11625"]
   }
}
```


Подробиці з моніторингу мережі вказані на офіційній технічній документації Stellar [20]

2.7. Висновок

У цьому розділі була детально розглянута взаємодія Національного Банку України та його користувачів з блокчейн технологією Stellar, що відіграє ключову роль у сучасній системі електронних платежів.

Спочатку було висвітлено процес транзакції користувача в системі СЕП-4, де зазначено попередні умови, деталізований процес транзакції та особливості системи. Це допомогло виявити, як блокчейн Stellar може забезпечити більш ефективне, прозоре та безпечне проведення фінансових операцій.

Далі, було розглянуто взаємодію НБУ з Stellar, де наголошено на важливості інтеграції блокчейн технологій у діяльність центральних банків для підвищення ефективності та забезпечення безпеки платіжних систем. Також були запропоновані рекомендації для НБУ щодо взаємодії з Stellar, включаючи аспекти безпеки, технологічної інфраструктури та управління ризиками.

У підрозділах присвячених системі електронних платежів, було викладено термінологію, опис системи СЕП, її розвиток, а також порівняльну характеристику СЕП-3 та СЕП-4. Це дозволило глибше зрозуміти принципи роботи та ключові відмінності між старими та новими версіями систем.

Аналіз загроз системи електронних платежів показав потенційні ризики та вразливі місця, які необхідно враховувати при розробці та впровадженні нових технологічних рішень.

Окрему увагу було приділено платформі Anchor, її архітектурі, встановленню та інтеграції, а також платформі Stellar Disbursement Platform (SDP), що забезпечує додаткові можливості для ефективного управління фінансовими активами.

Заключна частина розділу описує основи та концепції Stellar, включаючи Stellar Consensus Protocol (SCP), Stellar Stack, а також процес запуску основного вузла, його встановлення, налаштування та моніторингу, що є фундаментальним для забезпечення стабільної та надійної роботи системи.

У цілому, цей розділ надає цінний внесок у розуміння можливостей та викликів, пов'язаних з інтеграцією блокчейн технологій у системи електронних платежів, з особливим акцентом на ролі Stellar у цьому процесі.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1. Обґрунтування економічної проблематики системи СЕП-3

3.1.1. Аналіз недоліків системи СЕП-3 з економічної точки зору

Аналіз недоліків системи електронних платежів третього покоління (СЕП-3) показаний у таблиці 3.1. Система електронних платежів мала достатню швидкість але була дуже вразливою, тому система була оновлена на четверте покоління яке мало вищу швидкість та підвищений рівень безпеки.

Назва недоліку СЕП-3	Опис
Час обробки транзакції	Час на кожну транзакцію користувача становив 15 секунд. У порівнянні з новою системою електронних платежів де швидкість становила від 1 секунди до 10 секунд
Безпека та прозорість транзакцій	Через відсутність нормальної прозорості ускладняється контроль за рухом коштів, особливо у великих обсягах, що може сприяти незаконним фінансовим операціям, таким як відмивання грошей або інші корупційні схеми.
Масштабованість	Можливі обмеження у здатності системи масштабуватися для задоволення зростаючих потреб.
Коефіцієнт обігу коштів	Коефіцієнт обігу коштів у СЕП у 2022 році становив 6,64, що вказує на високий оборот коштів у системі. Це може бути позитивним аспектом, але також вказує на необхідність високої ефективності та надійності системи.

Таблиця 3.1. Недоліки системи СЕП-3

3.1.2. Економічні наслідки недоліків СЕП-3

Централізована система: централізовані системи, як СЕП-3, можуть бути більш вразливими до кібератак, що збільшує ризики безпеки для банків та їх клієнтів.

Затримки та висока вартість: комбінація вищих витрат та повільної обробки може негативно вплинути на ефективність фінансових операцій, знижуючи конкурентоспроможність банків.

Вплив на клієнтів: високі витрати та неефективність можуть відбитися на рівні задоволення клієнтів, зменшуючи їх лояльність та довіру до фінансових установ.

Повільний обіг коштів: через повільну обробку транзакцій та високі витрати, обіг коштів у економіці може уповільнюватися. Це, в свою чергу, може впливати на здатність бізнесу швидко реагувати на ринкові зміни, а також на загальну ліквідність у фінансовій системі.

Обмеження для малого та середнього бізнесу: високі витрати на транзакції та недоліки у швидкості обробки можуть створювати бар'єри для малих та середніх підприємств, які залежать від швидких і доступних платіжних послуг.

Відставання від глобальних тенденцій: у світі, де фінансові технології швидко розвиваються, застарілі системи, як СЕП-3, можуть зменшити конкурентоспроможність країни на міжнародному рівні, особливо у галузях, пов'язаних з цифровими платежами та фінансовими інноваціями.

3.2. Важливість оновлення до системи СЕП-4

3.2.1. Переваги системи СЕП-4 з економічної перспективи

Зниження операційних витрат.

Ефективність витрат: використання блокчейн технології в СЕП-4 може суттєво зменшити витрати на обслуговування та утримання системи. Автоматизація та вдосконалення процесів можуть зменшити потребу в ресурсах для технічного обслуговування.

Зниження комісійних витрат: блокчейн може забезпечити більшу ефективність транзакцій, потенційно знижуючи комісійні збори.

Підвищення швидкості та ефективності обробки транзакцій.

Швидкість транзакцій: СЕП-4 може забезпечити значно швидшу обробку платежів завдяки автоматизації та ефективності блокчейн технологій.

Зменшення затримок: це приведе до більш швидкого грошового обороту, що позитивно позначиться на загальній економічній активності.

Підвищення безпеки та надійності.

Зменшення ризиків безпеки: блокчейн пропонує покращену безпеку через свою децентралізовану структуру, зменшуючи ризики пов'язані з централізованими системами.

Прозорість транзакцій: блокчейн забезпечує більшу прозорість, що може допомогти виявленню та запобіганню шахрайству.

Поліпшена Масштабованість

Гнучкість та адаптивність: система СЕП-4, побудована на блокчейні, може бути легше масштабована для задоволення зростаючих потреб ринку.

Можливість інтеграції з іншими системами: блокчейн може бути легше інтегрований з іншими фінансовими системами та технологіями.

Сприяння економічному розвитку

Покращення ліквідності: швидші та більш ефективні транзакції можуть сприяти кращій ліквідності в економіці.

Підтримка малого та середнього бізнесу: зниження вартості та поліпшення доступу до фінансових послуг для малого та середнього бізнесу.

Відповідність міжнародним стандартам

Глобальна конкурентоспроможність: оновлення до технологічно просунутої системи, як СЕП-4, може підвищити міжнародну конкурентоспроможність фінансового сектору країни.

Оновлення до СЕП-4 може вирішити багато із зазначених недоліків СЕП-3, пропонуючи більш ефективну, безпечну, та масштабовану систему.

Це може привести не тільки до зниження витрат та підвищення ефективності для банків та їх клієнтів, але йсприяти позитивному економічному розвитку.

3.2.2. Прогнозований економічний вплив оновлення

Прогнозований економічний вплив оновлення системи платежів з СЕП-3 на СЕП-4 може бути оцінений у декількох ключових областях: економії витрат, зменшенні ризиків, та поліпшенні загальної продуктивності.

Економія витрат

Зниження операційних витрат: завдяки ефективності блокчейн технологій, СЕП-4 може значно знизити витрати на обслуговування та утримання системи. Автоматизація та поліпшення процесів обробки транзакцій зменшують потребу в ручній роботі та технічному обслуговуванні.

Зниження вартості транзакцій: перехід на блокчейн може дозволити знизити комісії за транзакції, що прямо впливає на витрати банків та їх клієнтів.

Зменшення ризиків

Безпека транзакцій: використання блокчейн технології підвищує безпеку транзакцій, зменшуючи ризик шахрайства та кібератак. Це знижує потенційні фінансові втрати від таких інцидентів.

Прозорість і відстежуваність: блокчейн надає більшу прозорість у проведенні транзакцій, що допомагає запобігти неправомірним діям та забезпечує легший аудит.

Поліпшення продуктивності

Швидкість обробки: СЕП-4 може забезпечити значно більшу швидкість обробки транзакцій, зменшуючи час очікування для клієнтів та підвищуючи загальну продуктивність системи.

Підтримка економічного розвитку: швидкі та ефективні платіжні системи сприяють загальному економічному розвитку, оскільки вони підтримують бізнес-операції та споживчі транзакції.

3.3. Оцінка капітальних витрат

3.3.1. Аналіз вартості інтеграції блокчейн технології

У зв'язку з відсутністю конкретних даних про витрати на розробку, інтеграцію, підтримку та інші аспекти впровадження блокчейн технології в систему СЕП-4, цей аналіз базується на приблизних оцінках. Ці оцінки формуються на основі загальноприйнятих стандартів витрат у сфері IT-проектів та блокчейн-інтеграції, а також аналізі аналогічних проектів у галузі фінансових технологій.

Однією з ключових переваг використання блокчейн платформи Stellar у системі СЕП-4 є те, що Stellar є технологією з відкритим кодом. Це означає, що витрати на ліцензування для використання технології Stellar, швидше за все, відсутні.

Основні характеристики та переваги використання технології з відкритим кодом показані у таблиці 3.2.

Перевага	Опис
Відсутність ліцензійних платежів	Оскільки Stellar є відкритою платформою, вона доступна для використання без необхідності сплачувати ліцензійні збори.
Гнучкість та модифікація	Відкритий код дозволяє адаптувати та модифікувати платформу для специфічних потреб системи СЕП-4.
Спільнота та підтримка	Можливість користуватися знаннями та підтримкою широкої спільноти розробників Stellar.

Таблиця 3.2. Характеристики та переваги використання технології з відкритим кодом

3.3.2. Витрати на придбання обладнання

У зв'язку з відсутністю конкретної інформації в відкритих джерелах щодо специфікацій серверного обладнання, яке використовується Національним банком України (НБУ) для інтеграції блокчейн технології Stellar, будуть наведені приклади які мають потрібні характеристики для роботи. Ці рекомендації базуються на загальних стандартах для обладнання, яке зазвичай використовується в подібних блокчейн-проектах та забезпечує високий рівень продуктивності, безпеки та надійності.

Приклади обладнання показані у таблиці 3.3.

Назва обладнання	**Характеристика**
Високопродуктивні сервери	
HPE ProLiant DL380 Gen10	Процесор: Intel Xeon 2x5120 2.2GHz 14-Core 105W Пам'ять: Підтримка до 3 ТБ оперативної пам'яті DDR4 2933 МГц. Зберігання: Гнучкі опції для використання SSD, SAS або SATA дисків. Порти: 2 x RJ-45 10Gbit/s, 1 x USB 3.0/3.1 Gen 1 Type-A, 1 x DisplayPort Блок живлення: 800 Вт Вартість: 217 232,00 грн
Dell PowerEdge R740	Процесор: Intel Xeon Gold 2x5218 2.3GHz 16-Core 105W Пам'ять: До 6 ТБ оперативної пам'яті DDR4-2666 ECC. Зберігання: Висока ємність зберігання з підтримкою різних конфігурацій. Порти: 1 x External Serial Port, 1 x

Продовження таблиці 3.3.

	VGA, 2 x USB 3.0, 4 x RJ-45 GbE LAN ports, 1 x Dedicated iDRAC network port Блок живлення: 1000 Вт Вартість: 182 202 грн
Cisco UCS C240 M5	Процесор: Двовісникові опції процесора Intel Xeon Scalable з підтримкою до 28 ядер на процесор. Пам'ять: Підтримка до 3 ТБ оперативної пам'яті DDR4 2666 МГц. Зберігання: Підтримка до 24 SFF SAS/SATA HDD або SSD та до 6 M.2 SATA SSD. Порти: 2 x 10GbE LAN, 1 x VGA, 2 x USB 3.0, 1 x RJ-45 для менеджменту. Блок живлення: Двовісниковий блок живлення з опціями 1050 Вт, 1600 Вт, або 2400 Вт. Вартість: 105 480,00 грн
IBM Power System S922	Процесор: 1 або 2 процесори POWER9, кожен з яких може мати від 4 до 12 ядер, залежно від моделі. Пам'ять: Підтримка до 4 ТБ оперативної пам'яті DDR4. Зберігання: Підтримка різних варіантів зберігання внутрішніх дисків, включаючи SFF і LFF SAS диски, а також NVMe SSD. Порти: Множина портів, включаючи

Продовження таблиці 3.3.

	USB 3.0, HMC, LAN та інші опції для розширення. Блок живлення: Опції блоку живлення залежать від моделі, але зазвичай включають високоефективні блоки живлення. Вартість: 81 170,00 грн
Засоби захисту мережі	
Cisco Firepower 2100 Series	Архітектура: Використовує архітектуру подвійної обробки даних. Інтерфейси: 10/100/1000 Ethernet, 1G/10G/40G оптичні інтерфейси. Підтримка VPN: IPsec, SSL VPN. Пропускна здатність: від 1.9 Gbps до 8.5 Gbps. Захист від загроз: IPS (система попередження про вторгнення), захист від вірусів, фільтрацію веб-трафіку. Інтеграція з іншими рішеннями Cisco: Інтеграція з Cisco ASA, Cisco ISE для поліпшеного управління доступом та політиками безпеки. Засоби управління безпекою: Centralized management using Cisco Firepower Management Center. Вартість: 154 159,50 грн
Системи зберігання даних	
Synology DiskStation DS1621+	Модель: Synology DiskStation

Продовження таблиці 3.3.

	DS1621+. Процесор: AMD Ryzen V1500B 4-ядерний 2.2 GHz. Оперативна Пам'ять: 4GB DDR4 ECC SODIMM, розширювана до 32GB (2 x 16GB). Кількість Відсіків для Дисків: 6 відсіків для HDD або SSD. Максимальна Ємність Зберігання: Залежить від розміру встановлених дисків, підтримка дисків до 16TB кожен. Підтримка RAID: RAID 0, 1, 5, 6, 10, Basic, Hybrid RAID (SHR). Розширення: Підтримка двох Synology DX517 для розширення до 16 відсіків для дисків. Мережеві Порти: 4 x Gigabit Ethernet LAN. Підтримка Link Aggregation та Failover. USB Порти: 3 x USB 3.0. eSATA Порт: 2 x eSATA. M.2 NVMe SSD Slots: 2 (для кешування). Операційна Система: DiskStation Manager (DSM) Блок Живлення: 250W. Система Охолодження: Активне охолодження з вентиляторами. Вартість: 105 000,00 грн

Продовження таблиці 3.3.

Cisco Catalyst 9000 Series	Робота в стеку (опціонально) Робота на 2 і 3 рівні; продуктивність до 160 Гбіт/с; підтримка PoE +; наявність 24-х або 48 портів Гбіт/с, і аплінків 1/10 Гбіт/с. Блок живлення: 125 W. Вартість: 142 210,60 грн

Таблиця 3.3. Приклади обладнання, характеристика та вартість

У таблиці 3.3. вказані приклади обладнання яці можуть бути використані при роботі з інтеграцією блокчейн мережі.

Візьмемо для прикладу

x4 сервера для аналізу трафіку Dell PowerEdge R740 – 728 808,00 грн

x1 сервер який їх буде об'єднувати Cisco UCS C240 M5 – 105 408,00 грн

x1 маршрутизатор Cisco Catalyst 9000 Series – 142 210,60 грн

x1 система зберігання даних Synology DiskStation DS1621 – 105 000,00 грн

x1 засіб захисту мережі Cisco Firepower 2100 Series – 154 159,50 грн

Суммарно: 1 235 586,10 грн

Це вартість базового обладнання для інтеграції блокчейн технології у СЕП для НБУ. Вартість програмного забезпечення буде вказана у додаткових витратах.

3.4. Розрахунок операційних витрат

3.4.1. Експлуатаційні витрати на систему

Експлуатаційні витрати на систему включають широкий спектр компонентів, від енергоспоживання до зарплати персоналу. Для точного розрахунку потрібно зібрати дані про споживання енергії кожним компонентом системи, вартість електроенергії, план обслуговування обладнання та вартість робочої сили. Також важливо враховувати періодичні

та непередбачувані витрати, а також забезпечити адекватний резервний бюджет для неочікуваних випадків.

Інформація з споживанням електроенергії кожного з компонентів системи вказано у таблиці 3.4.

Споживач	Кількість споживачів	Споживання кВт/год
Dell PowerEdge R740	4	4
Cisco UCS C240 M5	1	1,6
Cisco Catalyst 9000 Series	1	0,15
Synology DiskStation DS1621	1	0,25
Cisco Firepower 2100 Series	1	0,2
Сумарно	8	6,2

Таблиця 3.4. Споживання електроенергії системи

4 кВт (Dell PowerEdge R740) + 1.6 кВт (Cisco UCS C240 M5) + 0.15 кВт (Cisco Catalyst 9000) + 0.25 кВт (Synology DS1621) + 0.2 кВт (Cisco Firepower 2100) = 6.2 кВт на годину. (2,64 грн/кВт-год) Вся система споживає приблизно 6.2 кіловат-годин електроенергії за одну годину роботи.

У зв'язку з відсутністю повної інформації про зарплатні всіх фахівців, задіяних у проекті, та розмір резервного бюджету, наведена оцінка витрат базується на особистій зарплатні як спеціаліста з інформаційної безпеки та приблизних стандартах для подібних ролей і задач. Приблизна інформація з кількістю співробітників, їх спеціалізацією та зарплатнею за заданим прикладом показано у таблиці 3.5.

Таблиця 3.5. Інформація з кількістю співробітників та зарплатнею

Посада	Кількість	Зарплатня грн/міс.
Системний адміністратор	2	25 000
Мережевий інженер	1	22 500
Спеціаліст з кібербезпеки	1	30 000
Технічна підтримка	2	20 000
Суммарно:	6	142 500

Також буде задіяний резервний бюджет у розмірі 30% від вартості проекту Для ефективної роботи описаної інфраструктури рекомендується мати команду з 6 до 10 IT-фахівців, залежно від конкретних обов'язків, обсягу роботи та рівня автоматизації. Важливо також враховувати потребу в неперервному професійному розвитку та навчанні команди, оскільки технології та загрози постійно еволюціонують.

Загальна вартість обладнання: 1 235 586,10 грн;

Вся система споживає приблизно 6.2 кВт·год електроенергії за годину;

Вартість електроенергії за місяць: 11 784,96 грн (при ціні 2,64 грн/кВт·год);

Сумарна заробітна плата на місяць: 142 500 грн

Загальні Експлуатаційні Витрати (на Місяць) включаючи заробітні плати та витрати на електроенергію: 154 284,96 грн

3.4.2. Оцінка витрат на технічне обслуговування та підтримку

Оцінка витрат на технічне обслуговування показано у таблиці 3.6.

Таблиця 3.6. Оцінка витрат на технічне обслуговування

Технічне обслуговування обладнання	Періодичне сервісне обслуговування	Включає перевірку, чищення, оновлення ПЗ та заміну компонентів, які зношуються. Оскільки обладнання працює цілодобово то процедура проводиться кожні 3-6 місяців залежно від умов гарантії та рекомендацій виробника.
	Заміна комплектуючих	Потенційна заміна або модернізація комплектуючих, таких як жорсткі диски, пам'ять, блоки живлення.
	Ліцензії та оновлення ПЗ	Витрати на ліцензії для серверного програмного

Продовження таблиці 3.6.

Підтримка програмного забезпечення		забезпечення, а також на регулярні оновлення та патчі безпеки.
	Антивірусне та захисне ПЗ	Регулярні витрати на антивірусне програмне забезпечення та інші інструменти кібербезпеки.
Підтримка персоналу	Заробітна плата	Витрати на заробітну плату IT-персоналу, який займається обслуговуванням та підтримкою інфраструктури.
	Навчання та сертифікація	Витрати на навчання та професійний розвиток співробітників, включно з участю в семінарах, курсах та сертифікаціях.
Екстрені ремонти та непередбачені витрати	Резервний фонд	Важливо мати резервний фонд для покриття екстрених ремонтів або непередбачених проблем, які можуть виникнути.

Вартість обладнання: 1 235 586,10 грн

Річні витрати на обслуговування:

15% від вартості обладнання = 185 337,92 грн

Ці витрати приблизні з збільшенням відсотку для непередбачуваних обставин, можуть бути розділені на місяці для отримання місячної оцінки витрат.

3.4.3. Витрати на оновлення та модернізацію системи

Для розрахунку витрат на оновлення та модернізацію системи, що включає ваше обладнання, потрібно врахувати кілька ключових аспектів які вказані у таблиці 3.7.

Таблиця 3.7. Витрати на оновлення і модернізацію системи

Плановані оновлення обладнання	Заміна комплектуючих	Включає заміну застарілих або зношених компонентів, таких як жорсткі диски, оперативна пам'ять, процесори.
	Орієнтовна вартість	Приблизно: 20-30% від первісної вартості обладнання за період у 3-5 років.
Модернізація Інфраструктури	Заміна застарілого обладнання	Інвестиції в нове обладнання для підвищення продуктивності та ефективності системи.
	Орієнтовна вартість	Приблизно: 40% від первісної вартості обладнання за період у 4-5 років.

Загальна первісна вартість обладнання: 1 235 586,10 грн

Оновлення та модернізація на період 4 роки:

25% від загальної вартості = 308 896,53 грн

Задані витрати є орієнтовними і можуть змінюватися в залежності від конкретних потреб у модернізації, технологічних змін на ринку, та вартості нового обладнання та програмного забезпечення. Ринок обладнання кожен

рік змінюється як і його вартість, тому важливо регулярно слідкувати за оновленням обладнання та програмного забезпечення щоб план модернізації відповідав актуальним потребам та технологічним трендам.

3.5. Визначення економічного ефекту

3.5.1. Оцінка збільшення ефективності та зниження витрат

Для визначення економічного ефекту від інвестицій у IT-інфраструктуру, важливо оцінити, як впровадження нового обладнання та систем зможе збільшити ефективність та знизити загальні витрати.

Для заданого прикладу на сьогоднішній день вже стоїть досить швидке та ефективне обладнання і в заміні на більш швидкі та ефективні не має потреби, але навіть з надійним та ефективним обладнанням, є кілька стратегій, які можна використовувати для подальшого підвищення продуктивності. Дана стратегія описана у таблиці 3.8.

Таблиця 3.8. Стратегія для збільшення ефективності та зниженню витрат

Підвищення продуктивності обладнання	
Оптимізація конфігурації	Перевірка та оптимізація налаштування обладнання для максимальної ефективності. Розглянути можливість використання спеціалізованого програмного забезпечення для керування ресурсами та моніторингу продуктивності.
Оновлення програмного забезпечення	Регулярно оновлення операційної системи та програмного забезпечення для використання останніх поліпшень у продуктивності та безпеці.
Використання Технологій Віртуалізації	Розглянути віртуалізацію серверів для оптимізації використання апаратних ресурсів.
Ефективність ресурсів	
Автоматизація	Впровадження інструментів та процесів для

Продовження таблиці 3.8.

рутинних задач	автоматизації стандартних задач, звільняючи час співробітників для більш складних завдань.
Перенавчання та розвиток навичок персоналу	Інвестиції в навчання та розвиток навичок персоналу для ефективнішого використання технологій.
Енергоефективність	
Оптимізація використання енергії	Розгляд можливості для оптимізації використання енергії. Наприклад: використання лічильників день/ніч для економії електроенергії під час нічних годин.
Моніторинг та управління енергоспоживанням	Встановлення систем моніторингу та управління енергоспоживанням для відстеження та оптимізації використання енергії.

Навіть із сучасним обладнанням, є значний потенціал для підвищення ефективності та оптимізації використання ресурсів. Це може включати технічні налаштування, автоматизацію, перенавчання персоналу та управління енергоспоживанням.

3.5.2. Аналіз впливу на підвищення безпеки та прозорості платежів

Аналіз впливу оновлення IT-інфраструктури на підвищення безпеки та прозорості платежів включає розгляд того, як технічні оновлення та вдосконалення можуть покращити ці аспекти у організації. Подробиці аналізу показані у таблиці 3.9.

Таблиця 3.9. Аналіз впливу оновлення IT-інфраструктури на підвищення безпеки та забезпечення прозорості платежів

Підвищення безпеки платежів	
Застосування Сучасних Засобів Захисту	Впровадження найновіших технологій кібербезпеки, таких як надійне шифрування та аутентифікація, для захисту платіжних транзакцій.

Продовження таблиці 3.9.

	Оновлене обладнання Cisco Firepower 2100 Series, забезпечує кращий захист від зовнішніх загроз.
Моніторинг та виявлення аномалій	Використання систем виявлення вторгнень та моніторингу трафіку для раннього виявлення потенційних загроз.
	Автоматизація процесів моніторингу для постійного відстеження підозрілої активності.
Поліпшення протоколів внутрішньої безпеки	Оновлення внутрішніх політик безпеки та процедур для забезпечення суворого контролю за доступом до платіжних систем.
Забезпечення прозорості платежів	
Покращення слідкуваності транзакцій	Використання систем, що дозволяють детально відстежувати та звітувати про всі платіжні транзакції.
	Застосування технологій блокчейну або схожих технологій для забезпечення незмінності та прозорості платіжних записів.
Аудит та звітність	Покращення можливостей збору даних та звітності для спрощення процесу аудиту та забезпечення відповідності нормативним вимогам.
Інтеграція з іншими системами	Забезпечення сумісності та ефективної інтеграції з іншими фінансовими системами та платформами.

3.5.3. Розрахунок економічного ефекту

Розрахунок економічного ефекту від впровадження оновлень в IT-інфраструктуру, таких як підвищення безпеки та прозорості платежів, зазвичай включає оцінку витрат, пов'язаних з реалізацією цих оновлень, та порівняння їх з отриманими вигодами.

Капітальні витрати включають всі витрати на придбання нового обладнання та витрати на навчання персоналу, які є одноразовими на початкове встановлення системи. Капітальні витрати показані у таблиці 3.10

Таблиця 3.10. Капітальні витрати

Оцінка витрат	Сума, грн.
Вартість обладнання	1 235 586,10
Витрати на навчання за рік	171 000,00

Сумарні капітальні витрати отже становлять:

1 235 586,10 грн (обладнання) + 171 000 грн (навчання) = 1 406 586,10 грн

Операційні витрати включають щорічні повторювані витрати, які необхідні для підтримки та експлуатації обладнання. Для цього розрахунку використовуємо наступні дані показані у таблиці 3.11.

Таблиця 3.11. Операційні витрати

Оцінка витрат	Сума, грн.
Щомісячна вартість електроенергії	11 784,96
Щомісячна заробітна плата	142 500,00
Щорічні витрати на технічне обслуговування:	185 337,92
Частка витрат на оновлення та модернізацію системи розрахована на рік:	77 224,13

Частка витрат на оновлення та модернізацію системи розрахована на рік: 308 896,53 грн поділити на 4 роки = 77 224,13 грн щорічно.

Розрахунок щорічних операційних витрат:

Електроенергія щорічно: 11 784,96 грн * 12 місяців = 141 419,52 грн

Заробітна плата щорічно: 142 500 грн * 12 місяців = 1 710 000 грн

Технічне обслуговування + оновлення/модернізація: 185 337,92 грн + 77 224,13 грн = 262 562,05 грн

Сумарні операційні витрати за рік:

141 419,52 грн (електроенергія) + 1 710 000 грн (зарплата) + 262 562,05 грн (обслуговування і модернізація) = 2 113 981,57 грн

Капітальні витрати = 1 406 586,10 грн.

Операційні витрати за рік = 2 113 981,57 грн.

Операційні витрати за місяць = 176 165,13 грн

Оцінка отриманих вигод охоплює економію на електроенергії за рахунок використання лічильника день/ніч, зменшення втрат від простоїв та збоїв (приблизно в 30% від операційних витрат), та підвищення продуктивності (приблизно в 25% від операційних витрат). Подробиці показані у таблиці 3.12.

Таблиця 3.12. Оцінка отриманих вигод

Оцінка вигод	Сума, грн
Річна економія на електроенергії	35 354,88
Зменшення втрат від простоїв та збоїв	634 194,47
Підвищення Продуктивності	528 495,39

$$\text{Економічний ефект} = \text{отримані вигоди} - \text{операційні витрати}$$

$$= 35\,354{,}88 + 634\,194{,}47 + 528\,495{,}39 - 2\,113\,981{,}57 = -915\,936{,}83$$

$$\text{Економічний ефект} = -915\,936{,}83 \text{ грн}$$

Зазначений вище економічний ефект розраховано без врахування комісій, які Національний банк України (НБУ) стягує за проведення транзакцій, у зв'язку з недоступністю цієї інформації через Закон України «Про банки та банківську діяльність» Глава 10 Стаття 60. Банківська таємниця.

Наведемо приклад з приблизними даними комісій банку, щоб детальніше оцінити потенційний економічний ефект від оновлення нашої платіжної системи. Важливо розуміти, як комісійні збори, стягувані фінансовими установами за обробку транзакцій, можуть вплинути на загальну вигоду від наших інвестицій у технологічні оновлення. Ці комісійні збори часто є значною частиною операційних витрат у фінансовому секторі, тому їх аналіз є ключовим для повного розуміння фінансових наслідків наших рішень.

Якщо припустити, що обладнання здатне в повній мірі використовувати потенціал мережі Stellar:

Максимальна пропускна здатність Stellar: 1 000 транзакцій/секунду.

Транзакцій за хвилину:

$$1000 \text{ транзакцій/секунду} \times 60 \text{ секунд} = 60\,000 \text{ транзакцій/хвилину}$$

Транзакцій за годину:

$$60000 \text{ транзакцій/хвилину} \times 60 \text{ хвилин} = 3\,600\,000 \text{ транзакцій/годину}$$

Транзакцій за добу

$$3\,600\,000 \text{ транзакцій/год.} \times 24 \text{ год.} = 86\,400\,000 \text{ транзакцій/добу}$$

Транзакцій за місяць

$$86\,400\,000 \text{ транзакцій/добу} \times 30 \text{ днів.} = 2\,592\,000\,000 \text{ транзакцій/міс.}$$

При ідеальних умовах пропускної здатності та безперервної роботи за місяць система може виконати 2,592 млрд. транзакцій

Станом на 2023 рік при обміні з е-гривня на XLM(Stellar Lumens) стягується комісія у розмірі 0.00001 XLM = 0,0000448 UAH. Ця сума є стандартною та застосовується до кожної операції в мережі Stellar, незалежно від її розміру чи складності.

За даними від НБУ розподіл транзакцій у Системі Електронних Платежів (СЕП) за 2022 рік був таким:

Транзакції до 1 тис. грн: Становили приблизно 45% від загальної кількості транзакцій.

Транзакції від 1 тис. грн до 100 тис. грн: Складали близько 51% від загальної кількості транзакцій.

Транзакції від 100 тис. грн і більше: Становили близько 4% від загальної кількості транзакцій.

Візьмемо середній чек у 30 000 грн

Додатково банк стягує комісію 0,001% з кожної транзакції

Розрахунок:

Комісійні витрати за день

Щомісячна кількість транзакцій (2 592 000 000) ділимо на кількість днів у місяці (30), отримуємо 86 400 000 транзакцій за день.

Комісія за конвертацію в XLM та назад у гривні:

Комісія становить 0.00001 XLM за кожну конвертацію, тобто 0.00002 XLM за повний цикл (в XLM і назад). Множимо це на кількість транзакцій, отримуємо 1 728 000 XLM.

Комісія у гривнях:

За кожну транзакцію стягується 0.0000448 UAH. Множимо це на кількість транзакцій, отримуємо 3 870 720 UAH.

Банківська комісія:

Стягується 0.001% з кожної транзакції. З урахуванням середнього чеку у 30 000 UAH, загальна сума комісії становить 86 400 000 * 30 000 UAH * 0.001% = 25 920 000 UAH.

Загальні комісійні витрати за день:

1 728 000 XLM + 3 870 720 UAH + 25 920 000 UAH = 25 925 598,72 UAH.

Комісійні витрати за місяць

Транзакцій за місяць: 2 592 000 000 (без змін).

Комісії за конвертацію та банківські комісії за місяць:

Множимо денні витрати на кількість днів у місяці (30), отримуємо 777 767 961,60 UAH.

Комісійні витрати за рік

Транзакцій за рік: Множимо щомісячну кількість транзакцій на 12 місяців, отримуємо 31 104 000 000 транзакцій.

Комісії за конвертацію та банківські комісії за рік:

Множимо місячні витрати на 12, отримуємо 9 333 215 539,20 UAH.

Ці розрахунки демонструють, що комісійні витрати мають значний вплив на загальну економіку платіжної системи, особливо при великій кількості транзакцій.

З урахуванням прибутку від комісійних витрат, економічний ефект за рік складає:

Економічний ефект за рік = Загальні вигоди - (Сумарні капітальні + Операційні витрати)

Економічний ефект за рік = 9 334 413 584,94 - (1 406 586,10 + 2 113 981,57) = 9 330 893 016,27 грн.

Це позитивний економічний ефект, що вказує на те, що заробіток від комісій значно перевищує сумарні капітальні та операційні витрати, а також забезпечує велику вигоду порівняно з витратами на енергію, технічне обслуговування та підвищення продуктивності, показуючи значний фінансовий потенціал платіжної системи на базі блокчейн технології Stellar.

3.6. Аналіз показників економічної ефективності

3.6.1. Розрахунок показників окупності інвестицій (ROI)

Дані для розрахунку показників окупності показані у таблиці 3.13.

Таблиця 3.13. Показники для розрахунку окупності інвестицій

Показник	Сума, грн.
Витрати на оновлення системи	
Капітальні витрати	1 406 586,10
Операційні витрати за рік:	2 113 981,57
Щорічні економії	
Економія на електроенергії	35 354,88
Зменшення втрат від простоїв та збоїв	634 194,47
Підвищення продуктивності	528 495,39
Дохід від Комісій	
Заробіток від комісійних витрат за рік	9 333 215 539,20
Економічний ефект	
Економічний ефект за рік	9 330 893 016,27

Рентабельність Інвестицій (ROI):

ROI = (Загальні Вигоди - Всі Витрати) / Всі Витрати.

ROI = (9 334 413 584,94 - 3 520 567,67) / 3 520 567,67 ≈ 2650.39.

Це означає, що на кожну гривню, вкладену у проект, отримується приблизно 2650 гривень назад у вигляді чистого доходу. Такий високий показник ROI є індикатором надзвичайно ефективної інвестиції.

Дані розрахунки показані у якості прикладу при ідеальних умовах роботи обладнання, без непередбачуваних обставин, максимальну завантаженість обладнання та максимальну пропускну здатність через блокчейн Stellar при середньому чеку (середньої вартості на кожну транзакцію) у 30 000 грн. На практиці дані показники можуть бути значно меншими.

3.6.2. Оцінка терміну окупності проекту

Розрахунок терміну окупності проекту (Payback Period) зазвичай виконується за допомогою формули, яка дозволяє визначити, скільки часу знадобиться інвестиціям для повернення своєї первісної вартості.

Термін окупності = Початкові інвестиції / Щорічний чистий дохід

Початкові інвестиції – це сума ваших капітальних витрат та операційних витрат за перший рік .

1 406 586,10 грн (Капітальні витрати) + 2 113 981,57 грн (Операційні витрати) = 3 520 567,67 грн.

Щорічний чистий дохід – це ваші загальні вигоди за рік мінус операційні витрати.

9 334 413 584,94 грн (Загальні вигоди) - 2 113 981,57 грн (Операційні витрати) = 9 332 299 603,37 грн.

Термін окупності = 3 520 567,67 грн / 9 332 299 603,37 грн = 0.000377 років.

0.000377 років × 365 днів/рік ≈ 0.138 дня.

Даний результат лише приклад у ідеальних умовах та максимальному навантаженню обладнання з максимальною пропускною здатністю через блокчейн Stellar.

3.6.3. Аналіз ризиків та невизначеностей проекту

Аналіз ризиків та невизначеностей проекту допоможе зрозуміти потенційні виклики та підготувати відповідні стратегії щодо їх мінімізації або управління. Приклади таких ризиків вказані у таблиці 3.14.

Таблиця 3.14. Аналіз ризиків

Назва	Опис
Технічні ризики	Збої в обладнанні або програмному забезпеченні: потенційні технічні збої можуть призвести до простоїв у системі. Безпека даних: ризики, пов'язані з кібербезпекою, включаючи можливі зломи та витоки даних. Сумісність та інтеграція: виклики, пов'язані з інтеграцією блокчейн технології з існуючими системами.
Ринкові ризики	Зміна ринкових умов: ризики, пов'язані зі змінами у фінансових ринках та поведінці споживачів. Конкуренція: зростання конкуренції у сфері блокчейн технологій та платіжних систем.
Регуляторні ризики	Законодавчі зміни: ризики, що виникають через зміни у законодавстві, які можуть вплинути на використання блокчейн технологій. Комплаєнс і ліцензування: вимоги до відповідності нормативним актам та ліцензіям.
Фінансові ризики	Зміни в комісійних ставках: ризики зміни доходів від комісій у зв'язку з коливаннями ринкових ставок. Непередбачувані витрати: можливість виникнення додаткових непланованих витрат.
Операційні ризики	Залучення та збереження персоналу: виклики у підборі кваліфікованих співробітників та утриманні персоналу. Управління проектом: ризики, пов'язані з управлінням проекту, включаючи дотримання термінів та бюджету.

Продовження таблиці 3.14.

Стратегічні ризики	Залежність від технологій: ризик втрати конкурентоспроможності при застаріванні технології.
	Репутаційні ризики: можливість негативного сприйняття компанії у випадку збоїв або інших проблем.
Стратегії мінімізації ризиків	Регулярний моніторинг та оцінка ризиків: постійне відстеження та аналіз ризиків для своєчасного реагування. Планування надзвичайних ситуацій: розробка планів на випадок технічних збоїв, кібератак, та інших кризових ситуацій. Страхування та геджування: використання фінансових інструментів для мінімізації потенційних збитків. Підтримка якості та надійності: інвестиції в якість обладнання та програмного забезпечення. Диверсифікація портфеля: зменшення залежності від одного виду активів або ринку.

Дотримуючись стретегії мінімізації ризиків можна підвищити ймовірність успішного виконання проекту та зменшити потенційні негативні наслідки.

3.7. Висновки щодо економічної доцільності

3.7.1. Загальна оцінка економічної вигоди проекту

Даний приклад базується на припущенні, що обладнання працює при максимальній пропускній здатності, забезпечуючи оптимальну обробку транзакцій. Цей проект в умовах ідеальної пропускної здатності, здатен обробляти значний обсяг транзакцій, що підвищує потенціал заробітку від комісій. Розрахунки засновані на середньому чеку у 30 000 грн за транзакцію, що є одним з ключових факторів високого доходу від комісій.

За результатами розрахунку проект демонструє високий економічний ефект, що свідчить про його економічну доцільність.

Високий показник ROI та надзвичайно короткий термін окупності підтверджують фінансову вигоду проекту.

Стратегічна перевага через впровадження передових технологій, таких як блокчейн, відкриває нові можливості для зростання та покращення конкурентоспроможності.

З огляду на ідеальні умови роботи обладнання та високий середній чек, проект є економічно доцільним із великим потенціалом для забезпечення стабільного доходу та розвитку. Важливо продовжувати моніторинг зовнішніх умов та адаптуватися до змін у ринковому середовищі для підтримки цього успіху на тривалий термін.

3.7.2. Рекомендації щодо подальшої оптимізації та розвитку

У таблиці 3.15. описані у подробицях рекомендації щодо оптимізації

Таблиця 3.15. Рекомендації щодо оптимізації та розвитку

Рекомендації	Опис
Покращення технічної інфраструктури	Регулярно оновлювати та модернізувати обладнання та програмне забезпечення для підтримання високої продуктивності та надійності системи. Зосередження на підвищенні масштабованості системи для обробки збільшеного обсягу транзакцій у майбутньому.
Забезпечення високої рівня безпеки	Впровадження передих методів кібербезпеки, регулярно проводити аудити безпеки для забезпечення захисту від кібератак. Організовувати навчання для персоналу з питань кібербезпеки.
Аналіз ринкових тенденцій	Слідкувати за ринковими тенденціями та адаптуватись до змін у поведінці споживачів та технологічних інноваціях. Розглянути можливість розширення послуг або впровадження нових на основі ринкових досліджень.

Продовження таблиці 3.15.

Управління ризиками	Постійно оцінювати та управляти потенційними ризиками, включаючи технічні, фінансові та регуляторні аспекти. Розробляти стратегії мінімізації ризиків та плани дій на випадок непередбачуваних ситуацій.
Розширення партнерських відносин	Працювати над створенням та розвитком партнерських відносин із іншими організаціями та технологічними постачальниками для розширення можливостей системи.
Інновації та дослідження	Інвестувати у дослідження та розробку для впровадження нових технологічних рішень, які можуть підвищити ефективність та конкурентоспроможність системи. Розглядати можливості застосування штучного інтелекту, машинного навчання та інших інноваційних технологій.
Фокус на клієнтському сервісі	Впровадження покращення у сфері обслуговування клієнтів, щоб підвищити задоволеність та лояльність користувачів. Забезпечити наявність зручних та інтуїтивно зрозумілих інтерфейсів для кінцевих користувачів.
Прозорість та відповідальність	Підтримувати високий рівень прозорості у фінансових операціях та взаємодії з регуляторними органами. Бути відповідальним перед своїми клієнтами та партнерами, підтримуючи відкритий діалог та вчасне інформування про важливі зміни.

Подальша оптимізація та розвиток проекту повинні зосереджуватися на технічному вдосконаленні, ринковій адаптації, ризик-менеджменті, інноваціях та покращенні взаємодії з клієнтами.

ВИСНОВКИ

У цій кваліфікаційній роботі роботі було проведено повний аналіз та дослідження застосування блокчейн технології в системах електронних платежів, з порівнянням СЕП-3 між СЕП-4. Де остання використовувалась з інтеграцією технології від компанії Stellar Lumens за міжнародним стандартом ISO 20022.

Детально розглянуто основи технології блокчейн, її ключові компоненти, такі як блоки транзакцій, ланцюжок блоків, механізми підтвердження транзакцій, та їх складність. Також розглянуто особливості впровадження стандарту ISO 20022 у платіжній інфраструктурі України та його вплив на розвиток платіжної системи

Проаналізовано інноваційні рішення компанії Stellar у контексті міжнародних платежів і роль цієї технології у фінансовій індустрії. Особливу увагу приділено порівняльному аналізу між Stellar та іншими провідними блокчейн компаніями, з акцентом на переваги для НБУ.

В третьому розділі роботи проведено глибокий аналіз економічної доцільності переходу на систему СЕП-4, включаючи оцінку капітальних та операційних витрат, розрахунок економічного ефекту від оновлення та аналіз показників економічної ефективності, таких як ROI і термін окупності проекту.

Надано конкретні рекомендації щодо подальшої оптимізації та розвитку системи, включаючи технічні вдосконалення, забезпечення безпеки, аналіз ринкових тенденцій, управління ризиками, а також стратегії для покращення взаємодії з користувачами.

Результати дослідження підкреслюють значний потенціал та економічну доцільність впровадження блокчейн технології в системи електронних платежів, зокрема оновлення системи НБУ до СЕП-4.

ПЕРЕЛІК ПОСИЛАНЬ

1. SWIFT. About ISO 20022 [Електронний ресурс] /– Режим доступу до ресурсу: https://www.swift.com/standards/iso-20022.
2. ISO20022 [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso20022.org.
3. Stellar Lumens [Електронний ресурс] – Режим доступу до ресурсу: https://stellar.org.
4. Національний Банк України та ISO20022 [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/ua/payments/project-iso20022.
5. Огляд ISO20022 [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/Review_ISO20022.pdf
6. Концепція реформи платіжного законодавства [Електронний ресурс] – Режим доступу до ресурсу: 6. https://bank.gov.ua/files/ISO20022/Concept_reform_payment_legislation.pdf.
7. СТ кредитований переказ НБУ.версії.3.1_22.02.2022 [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/CT_cred_perekaz.NBU.ver.3.1_22.02.2022.pdf.
8. СЕП НБУ.версії.1.2_0107 [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/SEP-4.1.ICT.FR.NBU.ver.1.2_01072023.pdf.
9. СЕП 4 Загальна ідентифікація [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/SEP4_zagalne_2_Identifikacia_ver.2.4_16.03.23.pdf
10. СЕП 4. Загальне. Управління рахунками [Електронний ресурс] – Режим доступу до ресурсу:

https://bank.gov.ua/files/ISO20022/Sep4_zagalne_6_dodMP_Upravlinna_rahunkami_15.09.2023.pdf.

11. ISO 20022 Інформування про стан технічних рахунків [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/camt.003.camt.004_MP.NBU.ver.2.5_15.09.2023.pdf.
12. Вікіпедія UA Stellar [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Stellar.
13. Накамото, С. (2008). "Біткойн: система електронних грошей з одноранговою комунікацією."
14. Система електронних платежів Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Система_електронних_платежів_Національного_банку_України.
15. Кейсі, М. Дж., & Вігна, П. (2018). "Машина правди: блокчейн та майбутнє всього." St. Martin's Press.
16. Антонопулос, А. М. (2014). "Освоєння біткойну: розблокування цифрових криптовалют." O'Reilly Media.
17. Мугайар, В. (2016). "Бізнес-блокчейн: обіцянка, практика та застосування нової інтернет-технології." John Wiley & Sons.
18. Порівняння СЕП-3 та СЕП-4 НБУ [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/files/ISO20022/SEP4_porivnanna_SEP3_SEP4.NBU.ver.1.0_02.11.21.pdf.
19. Відкритий код на GITHUB Stellar [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/stellar/stellar-core/blob/master/INSTALL.md.
20. Офіційна документація блокчейну Stellar [Електронний ресурс] – Режим доступу до ресурсу: https://developers.stellar.org/docs/category/basic-tutorials.

21. Бутерін, В. (2013). "Ethereum: платформа для розумних контрактів та децентралізованих додатків нового покоління."
22. Stellar Development Foundation. (2022). "Stellar Documentation." [Офіційна документація] - https://www.stellar.org/developers/docs/
23. Нараянан, А., Бонно, Дж., Фелтен, Е., Міллер, А., та Голдфедер, С. (2016). "Біткойн та технології криптовалют: всеосяжний підручник." Princeton University Press.
24. Тапскотт, Д., & Тапскотт, А. (2016). "Блокчейн-революція: як технологія за біткойном змінює світ." Penguin.
25. Сван, М. (2015). "Блокчейн: проект нової економіки." O'Reilly Media.
26. Меркл, Р. К. (1987). "Цифровий підпис, заснований на конвенційній функції шифрування." Advances in Cryptology—CRYPTO'87.
27. Забо, Н. (1997). "Формалізація та забезпечення відносин у публічних мережах." First Monday.
28. Вуд, Г. (2014). "Ethereum: безпечний децентралізований універсальний реєстр транзакцій."
29. ISO 20022. (2022). "Фінансові послуги – Універсальна схема взаємодії у фінансовій галузі."

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Титульний аркуш	1	
2	А4	Завдання	2	
3	А4	Реферат	2	
4	А4	Список умовних скорочень	2	
5	А4	Зміст	4	
6	А4	Вступ	5	
7	А4	1 Розділ	34	
8	А4	2 Розділ	73	
9	А4	3 Розділ	27	
10	А4	Висновки	1	
11	А4	Перелік посилань	3	
12	А4	Додаток А	1	
13	А4	Додаток Б	1	
14	А4	Додаток В	1	
15	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

01 Титульна сторінка.docx

02 Завдання.docx

03 Реферат.docx

04 Список умовних скорочень.docx

05 Зміст.docx

06 Вступ.docx

07 Розділ 1.docx

08 Розділ 2.docx

09 Розділ 3.docx

10 Висновки.docx

11 Перелік посилань.docx

12 Додаток А.docx

13 Додаток Б.docx

14 Додаток В.docx

15 Додаток Г.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:
Розробка рекомендацій щодо застосування blockchain технології в системах електронних платежів

ст. гр. 125м-22-1
Чорного Дмитра Віталійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 154 сторінках та містить 16 рисунків, 34 таблиці, 29 джерел та 4 додатка.

Методи дослідження які були використані у роботі: спостереження, порівняння, аналіз та опис.

У першому розділі роботи проведено аналіз нормативно-правової бази та стандартів у сфері кібербезпеки, досліджено організаційне забезпечення ідентифікації інформаційних активів та визначено актуальність проведення ідентифікації інформаційних активів у контексті сучасних загроз кібербезпеці.

У другому розділі надано визначення основних характеристик інформаційних активів, упорядковано класифікацію інформаційних активів та розроблено методику проведення ідентифікації інформаційних активів.

У третьому розділі роботи досліджено економічний аспект ідентифікації інформаційних активів, проведено розрахунки капітальних та поточних витрат, загального збитку від атак на інформаційну та загального ефекту від впровадження рекомендацій.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник спец. частини
ст. викл. кафедри БІТ Вадим МЄШКОВ