

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра програмної інженерії та інтелектуальних технологій управління

ДИПЛОМНА РОБОТА

«Проектування та розробка програмних компонентів для системи токенизації із
застосуванням технологій блокчейн»

Керівник роботи:

доц. каф. ПІТУ

Шматко Олександр

Виконавець:

студент групи КН-218в

ЛЕНАРТОВИЧ Владислав

Харків – 2022

Об'єкт, предмет та ціль роботи

Об'єктом дослідження є сучасні методи збереження інформації

Предметом дослідження є системи токенизації на основі технології блокчейн

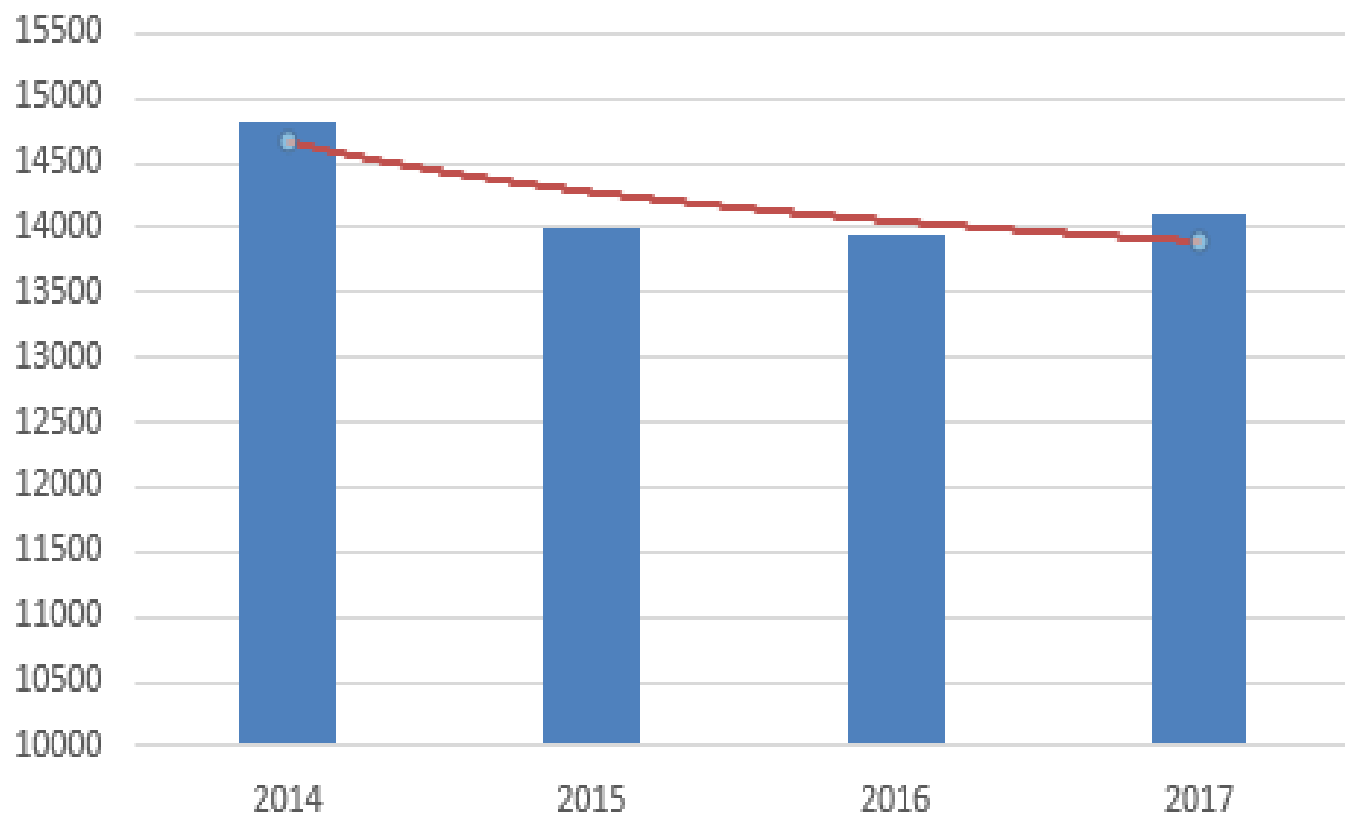
Метою роботи є підвищення безпеки даних шляхом їх токенизації на основі технологій блокчейн

Задачі роботи

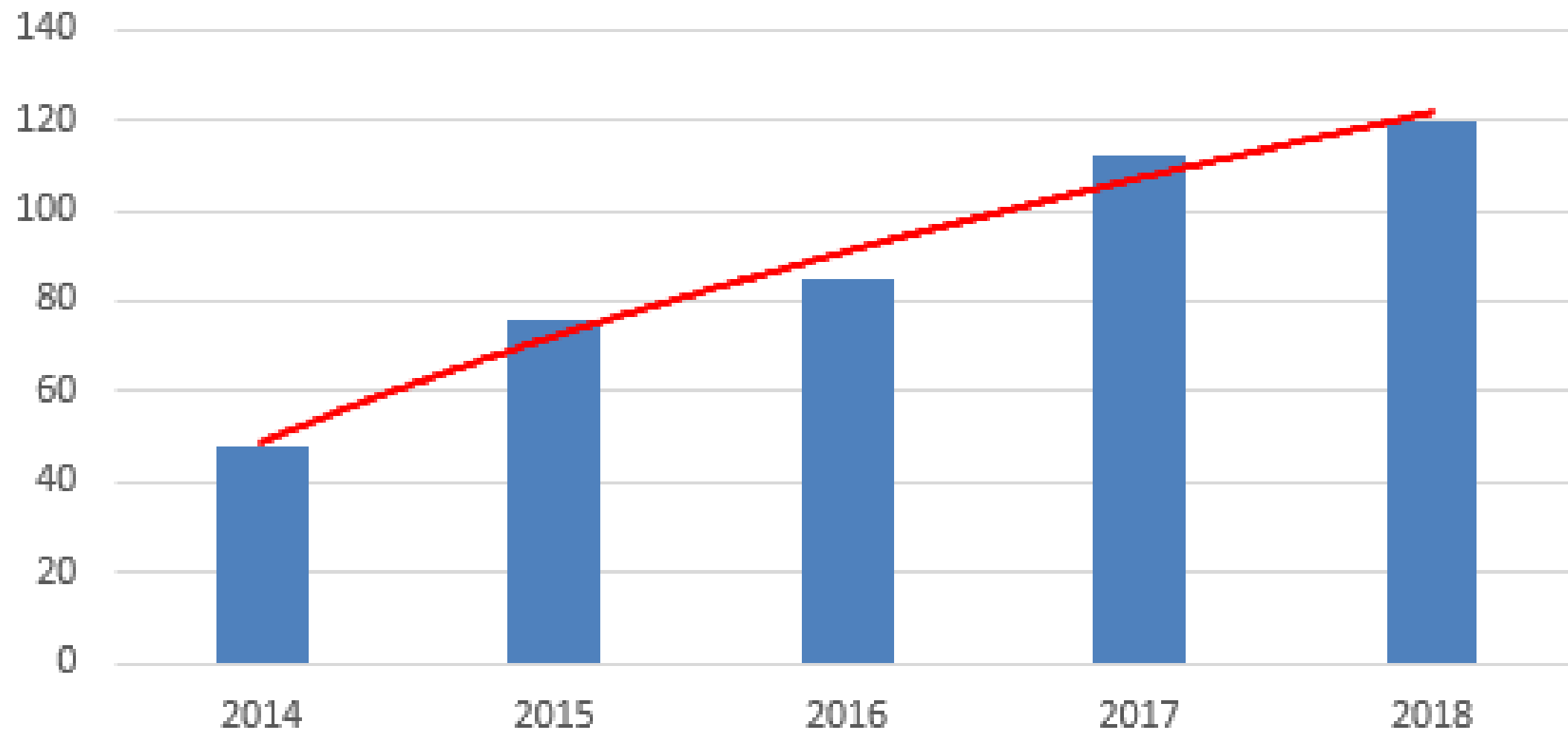
- Провести аналіз предметної області
- Проаналізувати проблеми
- Порівняти існуючі програмні рішення та виявити недоліки
- Проаналізувати методи рішення поставлених проблем
- Сформулювати вимоги до програмного забезпечення
- Виконати програмну реалізацію
- Виконати тестування системи

Виявлення сучасних проблем та актуальність теми

Згідно зі статистичними даними Генеральної прокуратури України з кожним роком випадки підроблення документів залишаються незмінно високими. Це негативно впливає на економіку, витрачає багато ресурсів спецслужб, та сприяє збільшенню кількості шахраїв та некваліфікованих людей в державі.



Статистика підроблення документів



Кількість судових справ Вінницького експертно-криміналістичного центру, що розглядали підробку документів землеволодіння

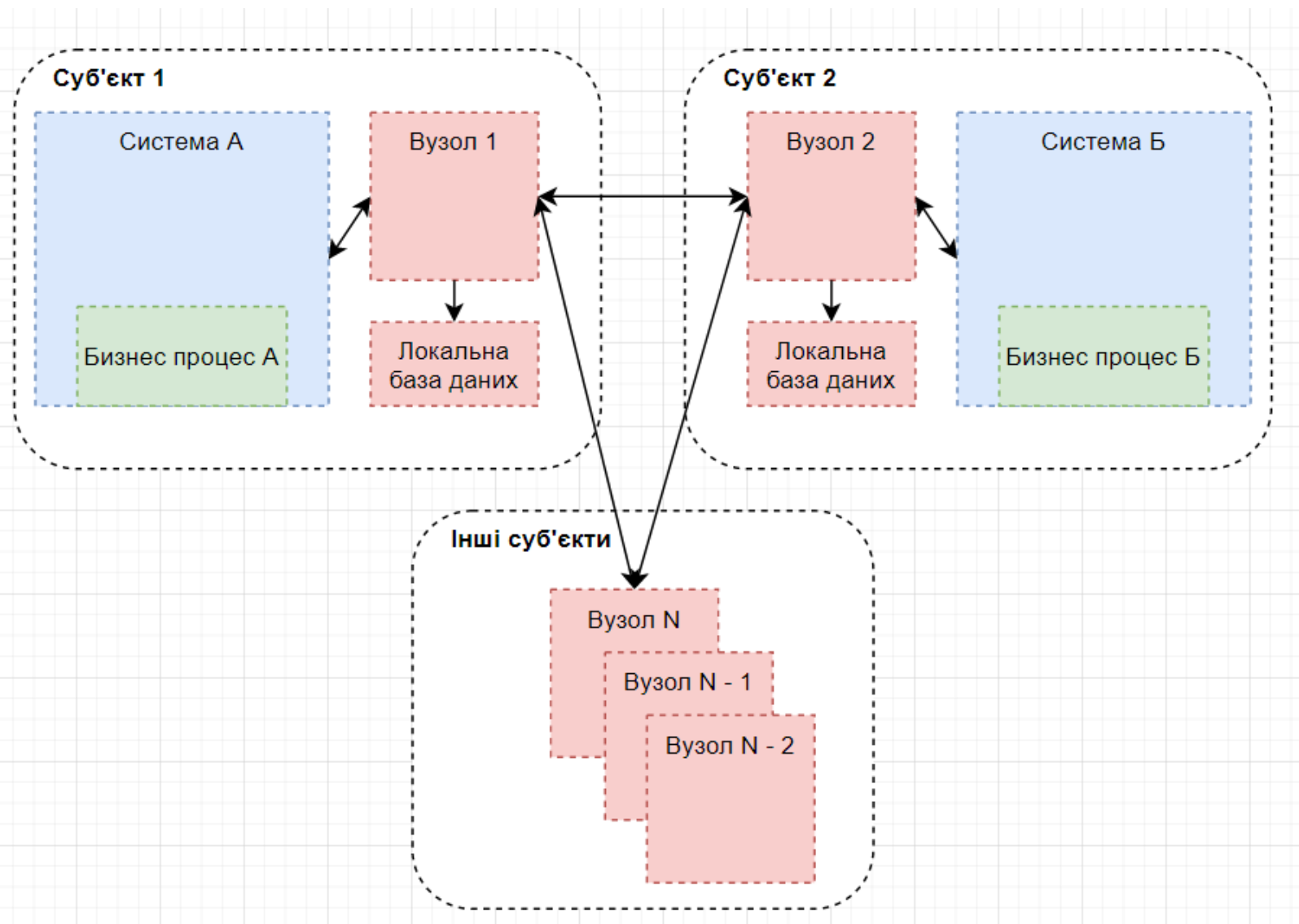
Порівняння аналогів

Порівняльна характеристика	Ethereum	Bitcoin
Надійність	Надійний, проте існує можливість похибки зі сторони розробника смарт-контрактів	Надійний
Функціональність	Має майже нескінчену кількість способів використання завдяки смарт-контрактам	Має обмежений функціонал, що націлений на керуванні активами
Швидкість обробки та внесення даних	Висока	Середня (але алгоритм хешування є надійнішим)

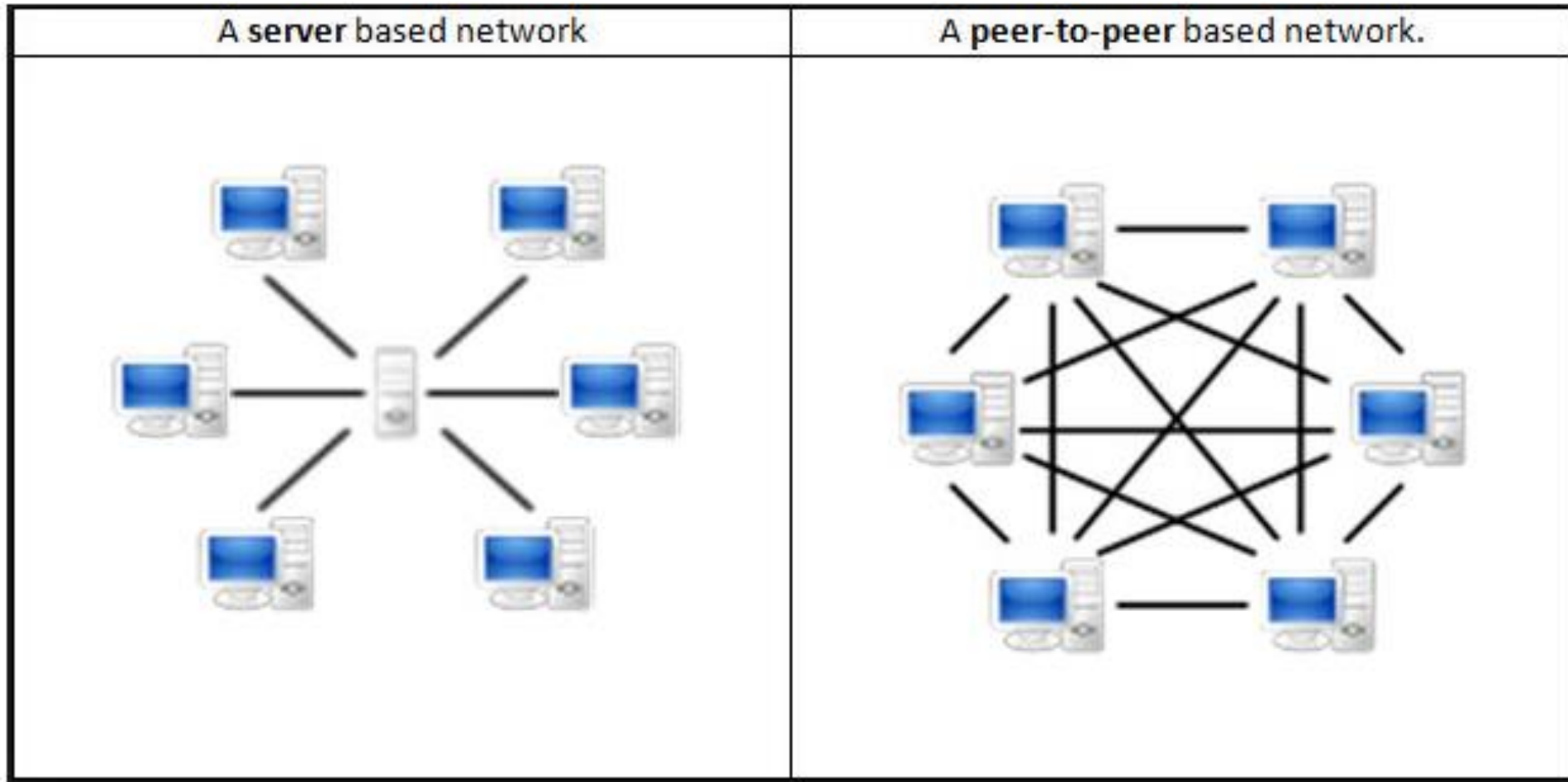
Методи рішення поставлених проблем

- 1) Використання блокчейну для збереження даних
- 2) Використання P2P для синхронізації блокчейну
- 3) Використання надійних та швидких алгоритмів хешування
- 4) Розробка простого у використанні програмного забезпечення

Технологія блокчейн



Технологія Peer-To-Peer



Функціональні вимоги до системи

- 1) Система має надавати користувачу змогу зареєструватися чи увійти.
- 2) Система має зберігати інформацію користувачів.
- 3) Система має надати можливість користувачу додавати нову інформацію до блокчейну.
- 4) Система має надавати користувачу повний доступ до інформації, що зберігається в блокчейні.
- 5) Система має захищати інформацію в блокчейні від змін.
- 6) Система має локально зберігати варіант блокчейну на пристрої користувача та синхронізуватися з мережею.

Нефункціональні вимоги до системи

Продуктивність - формування нового блоку до 30 секунд.

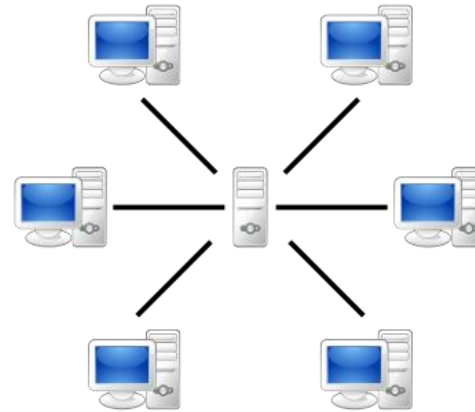
Доступність у використанні - інтерфейс простий та зрозумілий, для рядового користувача освоїтись повинно займати до 1 робочого дня.

Безпека – можливість підробити дані має бути вкрай низькою, для цього зломисникам потрібно мати більше 50% апаратної потужності мережі. Приватний ключ має бути унікальним для кожного акаунта.

Локалізація – система має бути локалізована на англійську мову.

Технічні вимоги – система має працювати на операційній системі Windows 10.

Технологій для реалізації



Peer-to-peer

SHA3-KESSAK

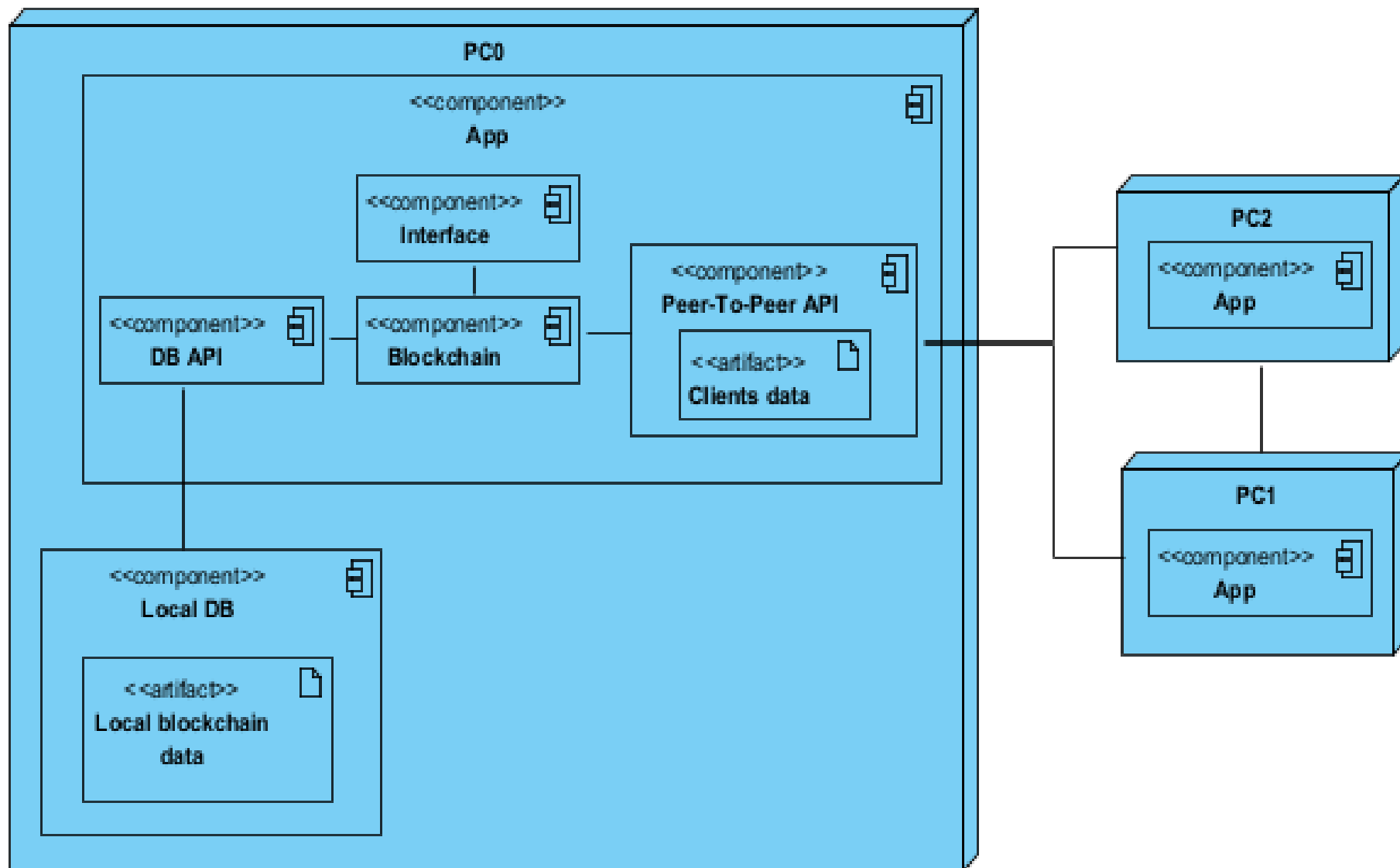
Побудова архітектури ПС

Архітектура програми має містити в собі наступні модулі:

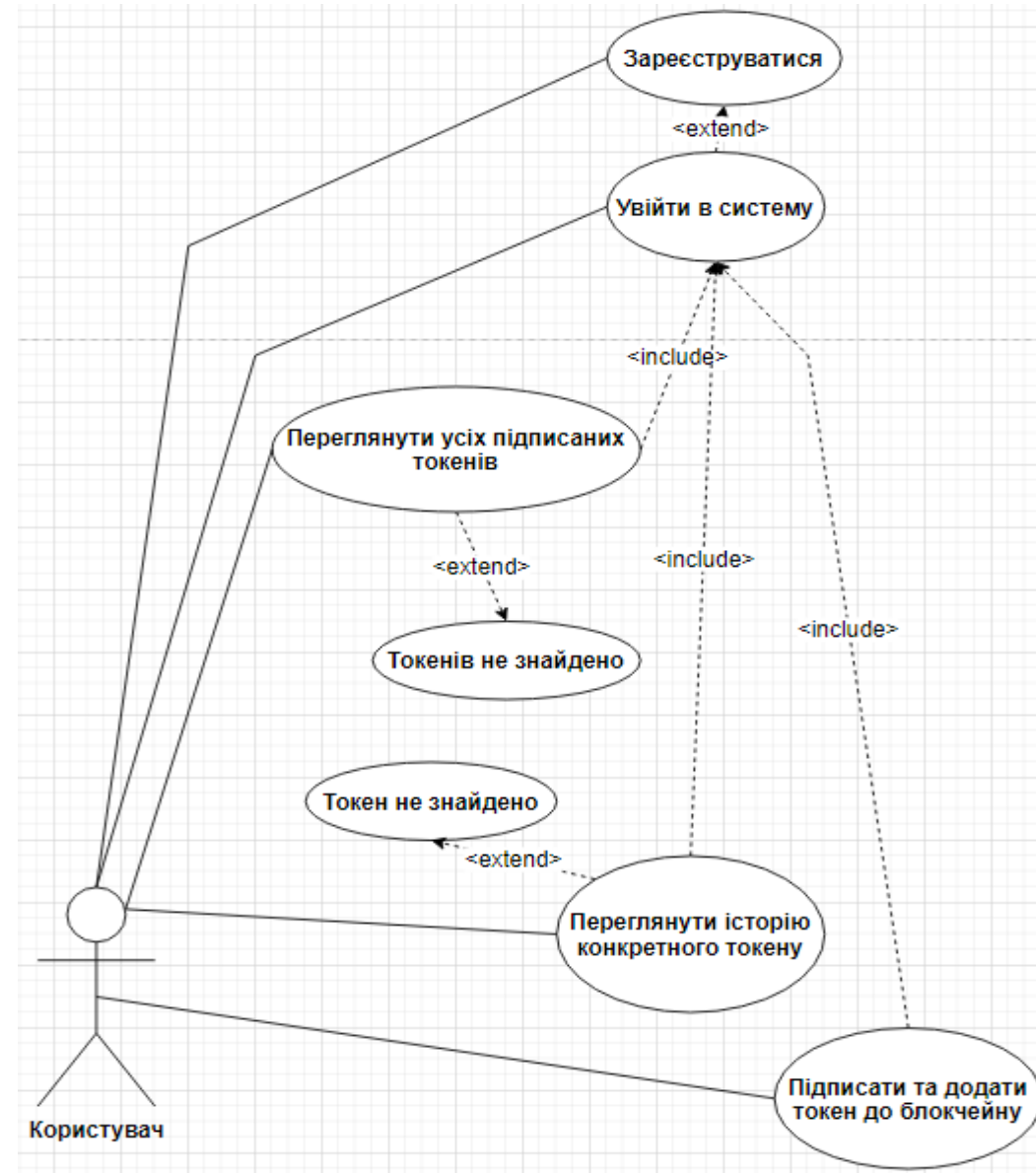
- Peer-To-Peer API
- Local blockchain store API
- Blockchain Service
- UI interface

Схематичне відображення цих модулів та їх взаємодія показано на наступному слайді у вигляді діаграми розгортання

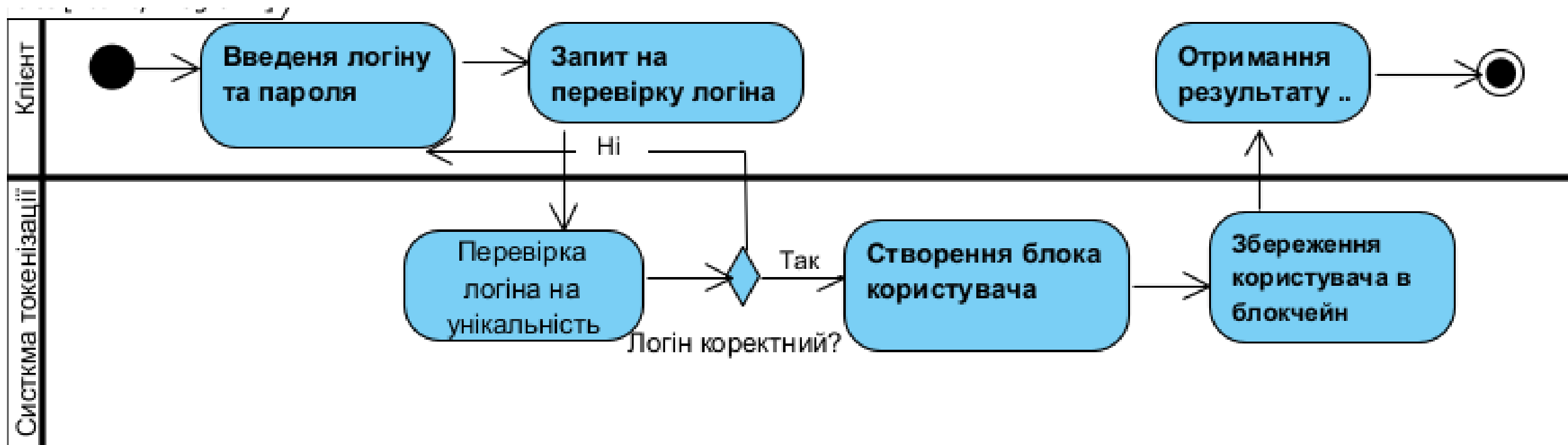
Діаграма розгортання



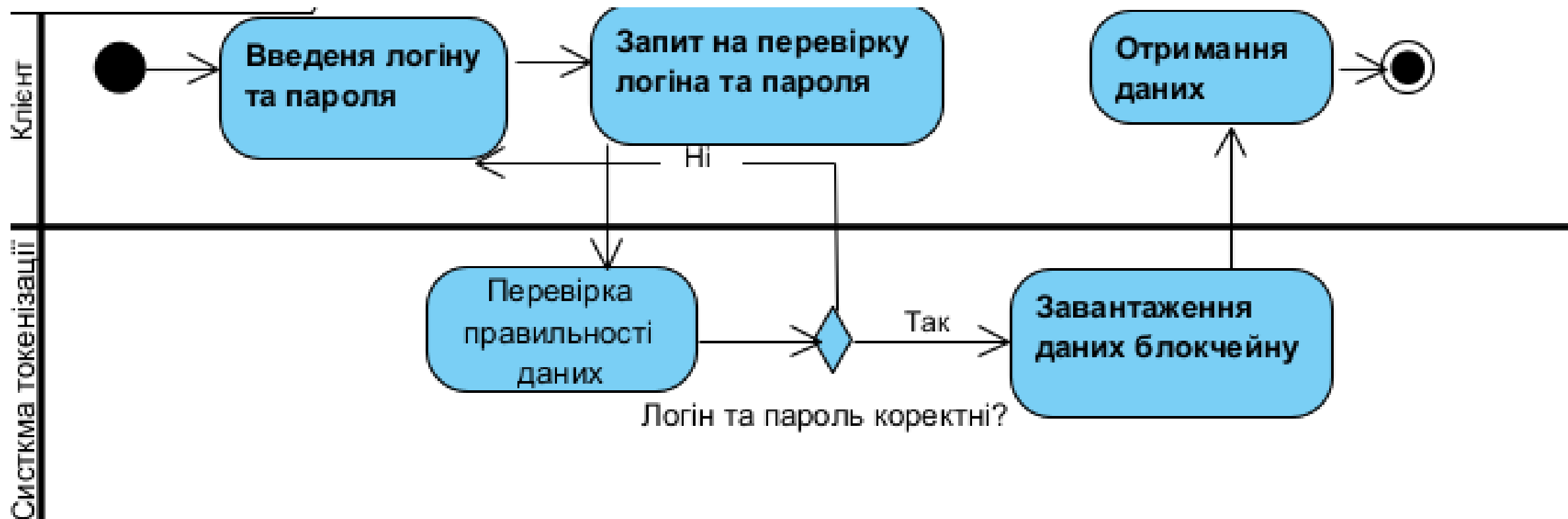
Діаграма варіантів використання



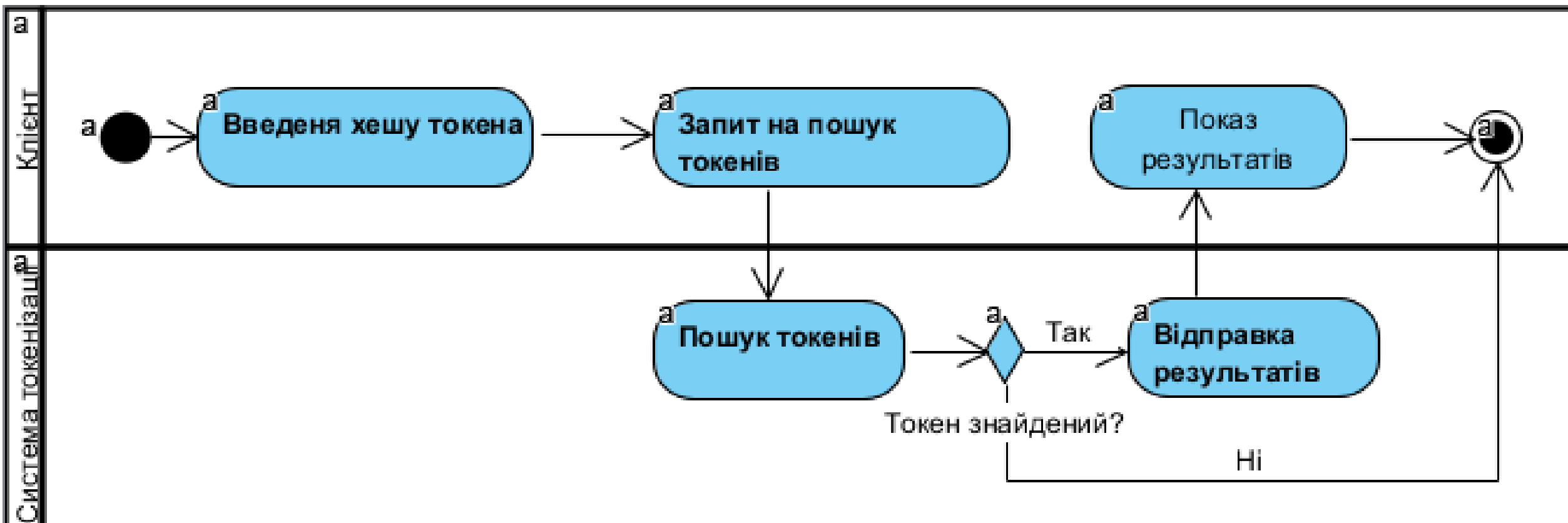
Діаграми діяльності (регістрація)



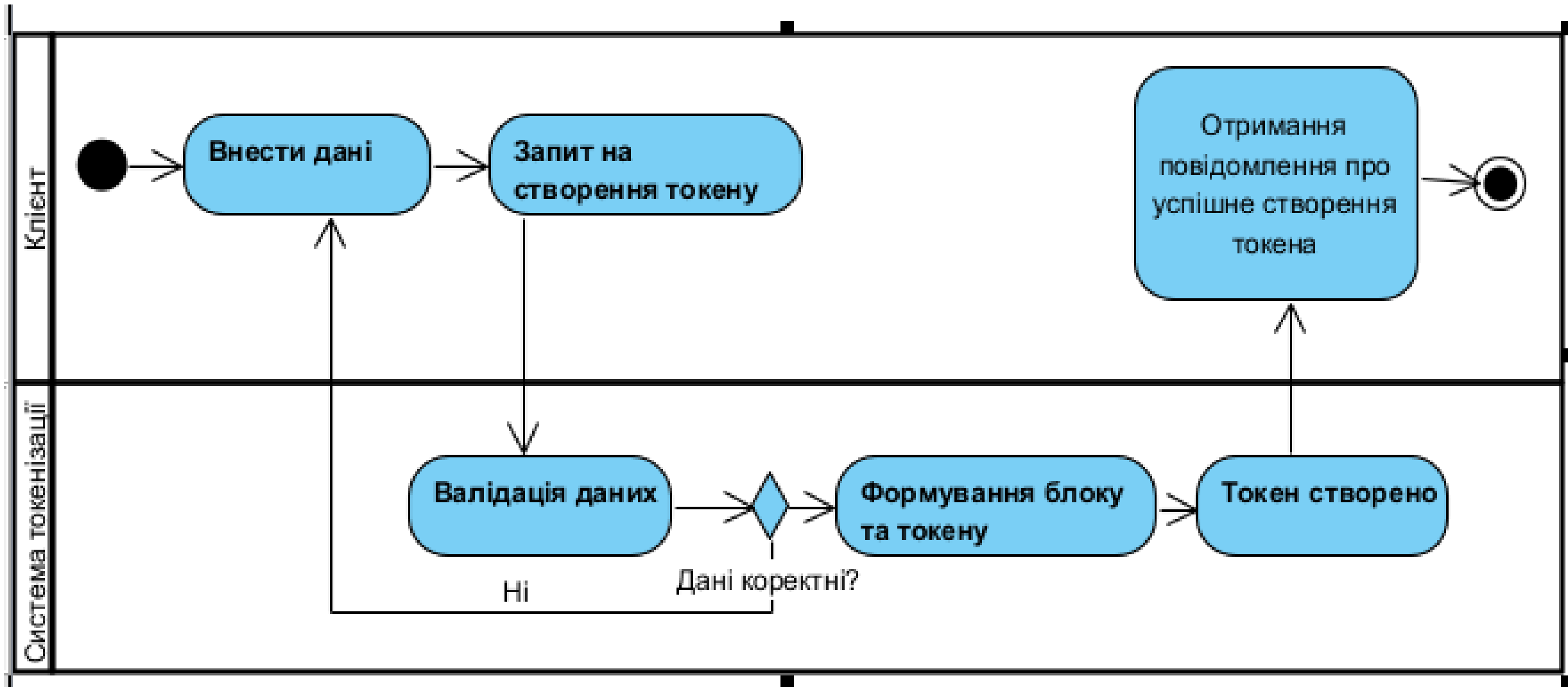
Діаграми діяльності (авторизація)



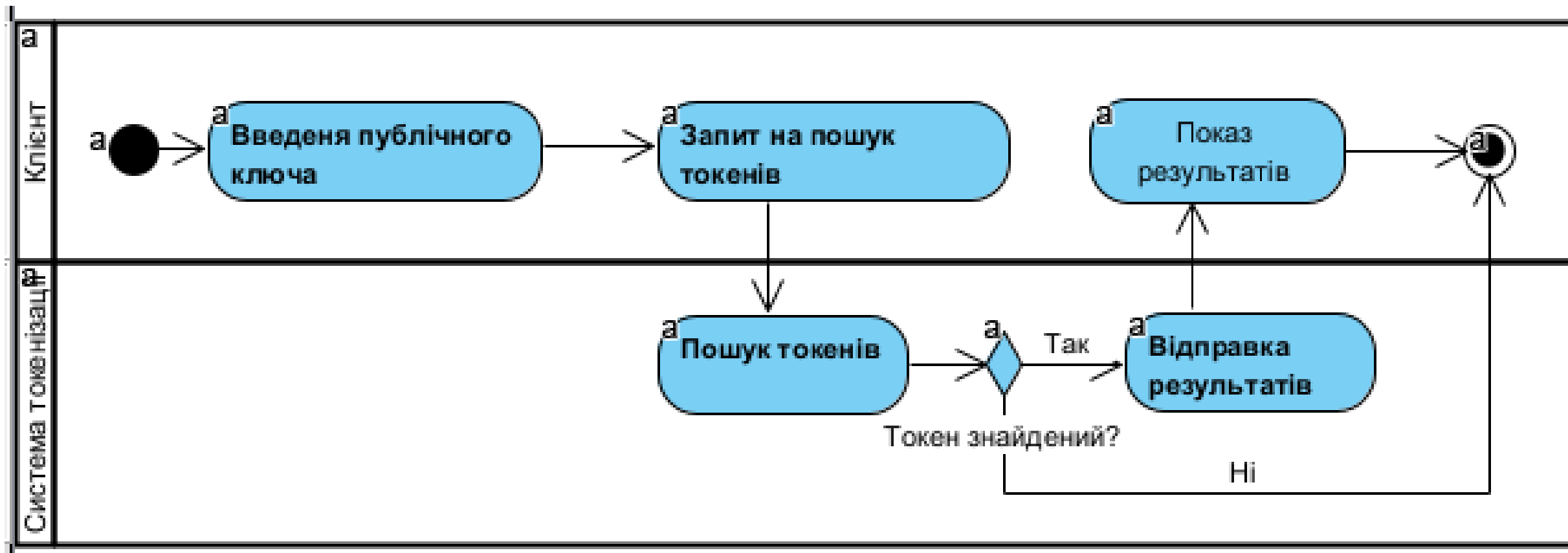
Діаграми діяльності (пошук конкретного блоку)



Діаграми діяльності (додавання блока)










Діаграми діяльності (пошук блоків користувача)

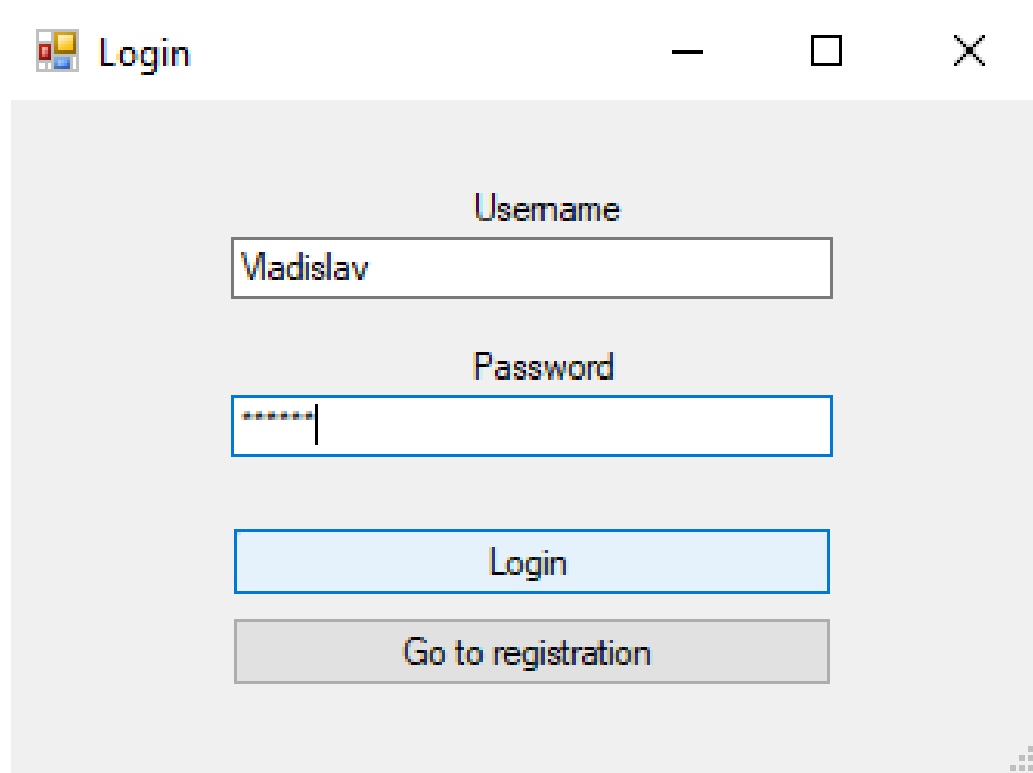


Локальне сховище

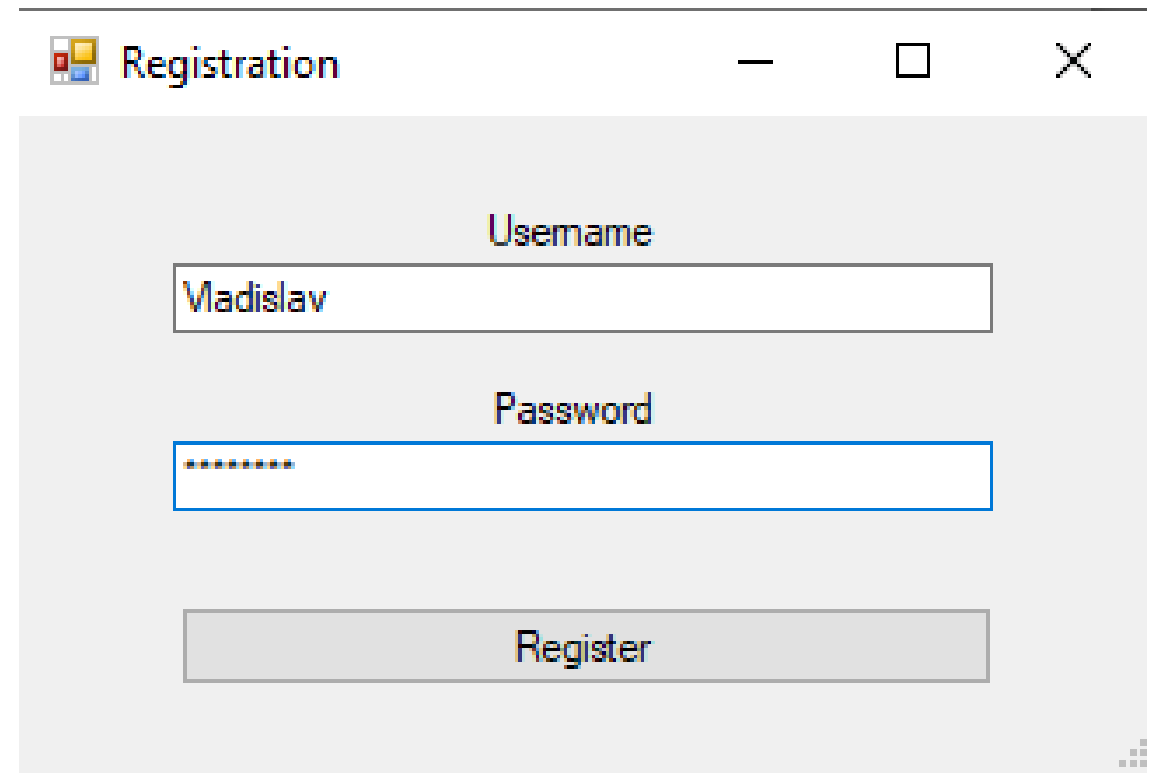
Сховище генерується автоматично за допомогою Entity Framework.
Доступ до сховища здійснюється за допомогою цього ж фрейм ворку, та спеціально створеного в ході розробки API.
Сховище містить в собі список усіх блоків.

Block		
	Owner	varchar(255)
	OwnerHash	varchar(255)
	Hash	varchar(255)
	PreviousHash	varchar(255)
	CreatedTime	timestamp
	DataType	integer(10)
	Data	varbinary(4058)

Інтерфейс взаємодії (регістрація та авторизація)



A screenshot of a 'Login' window. The window has a title bar with a standard icon, the text 'Login', and three control buttons (minimize, maximize, close). The main area is light gray. It contains two text input fields: the first is labeled 'Usemame' (misspelled) and contains the text 'Vladislav'; the second is labeled 'Password' and contains seven dots. Below the fields are two buttons: a light blue 'Login' button and a gray 'Go to registration' button. A small icon of four dots is in the bottom right corner.



A screenshot of a 'Registration' window. The window has a title bar with a standard icon, the text 'Registration', and three control buttons (minimize, maximize, close). The main area is light gray. It contains two text input fields: the first is labeled 'Usemame' (misspelled) and contains the text 'Vladislav'; the second is labeled 'Password' and contains seven dots. Below the fields is a single gray 'Register' button. A small icon of four dots is in the bottom right corner.

Інтерфейс взаємодії з блокчейном

Blockchain

— □ ×

Username

Uri

Port

Search

Search by block hash

Search by username

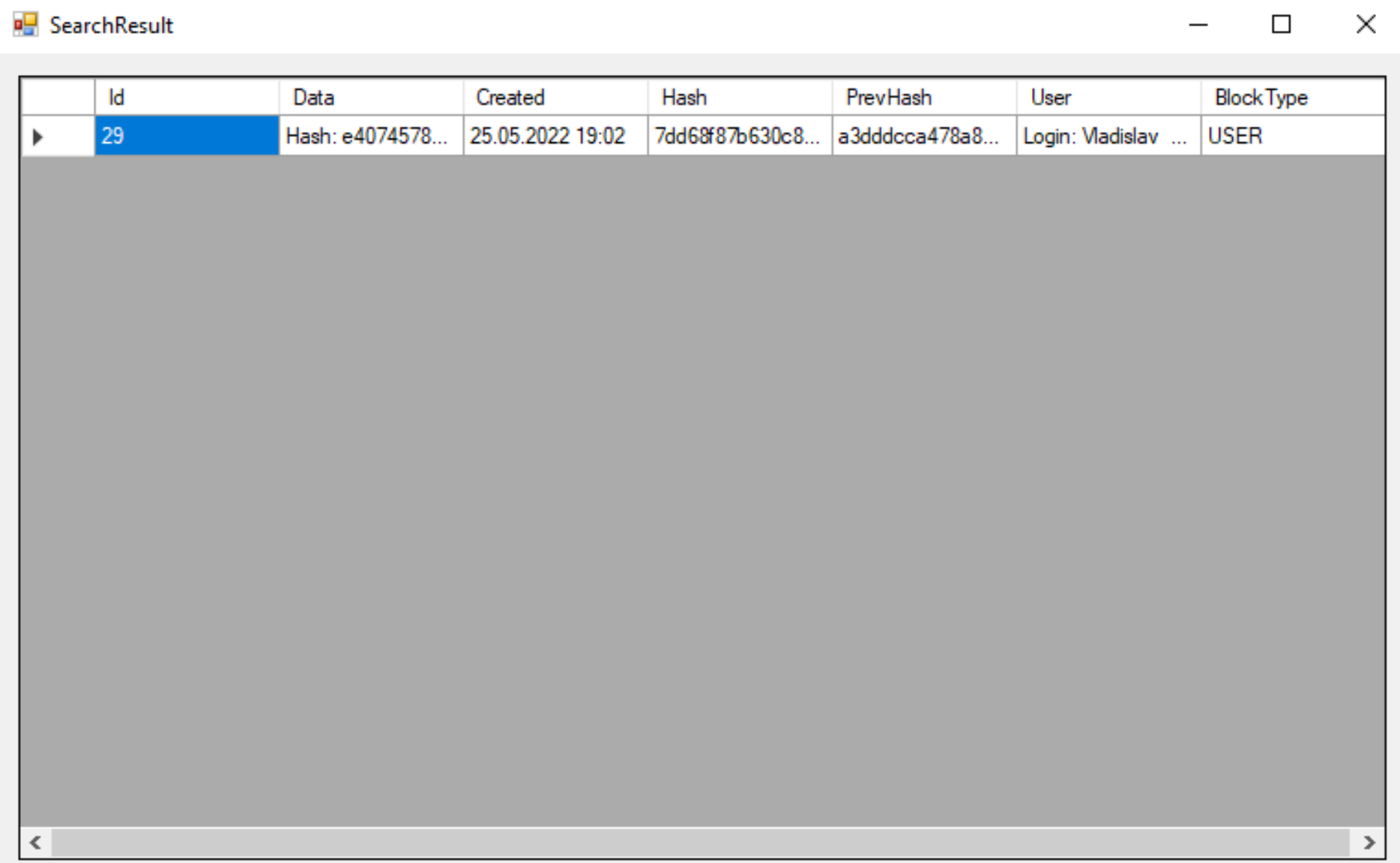
	Id	Data	Created	Hash	PrevHash	User
▶	1	Hash: d68328cf0...	11.05.2022	3a49506e44fbb9...	d9c67c4fd0e655...	Login: Penis
	2	Hash: 41fdeb63e...	24.05.2022 22:07	3f11a993522ebe...	3a49506e44fbb9...	Login: q Rc
	3	Hash: 7c2ecd07f...	24.05.2022 22:07	462ae675a14d0...	3f11a993522ebe...	Login: q Rc
	4	Hash: 5fd924625...	24.05.2022 22:08	b1e495385bd9a...	462ae675a14d0...	Login: q Rc
	5	Hash: de04d58d...	24.05.2022 22:08	13c5cf73e07a6d...	b1e495385bd9a...	Login: q Rc
	6	Hash: 53ae74be...	24.05.2022 22:19	2b2da2c6e51eb...	13c5cf73e07a6d...	Login: q Rc
	7	Hash: 1369e24b...	24.05.2022 22:19	c79741d22e35fe...	2b2da2c6e51eb...	Login: q Rc
	8	Hash: cd2eb083...	24.05.2022 22:24	7d82de75adf7...	c79741d22e35fe...	Login: q Rc
	9	Hash: cd2eb083...	24.05.2022 22:24	ce4187aeecdd8...	7d82de75adf7...	Login: q Rc
	10	Hash: 489cd5db...	24.05.2022 22:26	09e6b325ffc8ef4...	ce4187aeecdd8...	Login: q Rc
	11	Hash: 489cd5db...	24.05.2022 22:26	43ea730be066a...	09e6b325ffc8ef4...	Login: q Rc
	12	Hash: 489cd5db...	24.05.2022 22:27	9d3a109feabc9a...	43ea730be066a...	Login: q Rc
	13	Hash: e602cbd0...	24.05.2022 22:27	f32bf815fa8638c...	9d3a109feabc9a...	Login: q Rc
	14	Hash: 7ca12506...	24.05.2022 22:33	2df29ef5397eb3...	f32bf815fa8638c...	Login: q Rc
	15	Hash: 2a084937...	24.05.2022 22:34	740f0c9b7b09f...	2df29ef5397eb3...	Login: q Rc

< >

Add text to block

Add file to block

Інтерфейс взаємодії з результатами пошуку



The screenshot shows a window titled "SearchResult" with a table of search results. The table has 8 columns: Id, Data, Created, Hash, PrevHash, User, and BlockType. The first row is highlighted in blue.

	Id	Data	Created	Hash	PrevHash	User	BlockType
▶	29	Hash: e4074578...	25.05.2022 19:02	7dd68f87b630c8...	a3dddcca478a8...	Login: Vladislav ...	USER

Тестування

При тестуванні були проведені модульні тести.
Також було проведено функціональні та нефункціональні тести,
що мають на меті перевірити чи відповідає ПЗ на вимоги.

▲	✓ BlockchainTests1 (34)	97 мс
▲	✓ Blockchain.Tests (25)	93 мс
▸	✓ BlockTests (9)	93 мс
▸	✓ ChainTests (12)	< 1 мс
▸	✓ PeerServiceHostTests (4)	< 1 мс
▲	✓ FileShare.Tests (9)	4 мс
▸	✓ PingServiceTests (9)	4 мс

Приклади використання

Розроблену систему можна використовувати наприклад в системах, що мають на меті медичний облік історій хвороб пацієнтів. Або звичайне збереження документів, наприклад про закінчення вищої освіти чи проходження якогось курсу. Також, можна зберігати невеликі програми, що можна використовувати як спрощену альтернативу смарт-контрактів Ethereum.

Усе це можна досягти не змінюючи саму систему, а лиш змінюючи найвищий шар взаємодії з системою та інтерфейс користувача.

Приклад медичного обліку

Doctoral accounting

Doctor Pepper

	PatientName	PatientSurName	CurrentDate	Date
	Иван	Полубоков	28.05.2022 0:32	28.0
▶	Владислав	Роксоланов	28.05.2022 0:34	29.0

Patient Name

Владислав

Patient Sumame

Diagnos

Рак

Coment

Рак на початковому рівні розвитку, є шанс на одужання

Analyzes

Опухоль лобної долі мрзку

Treatment

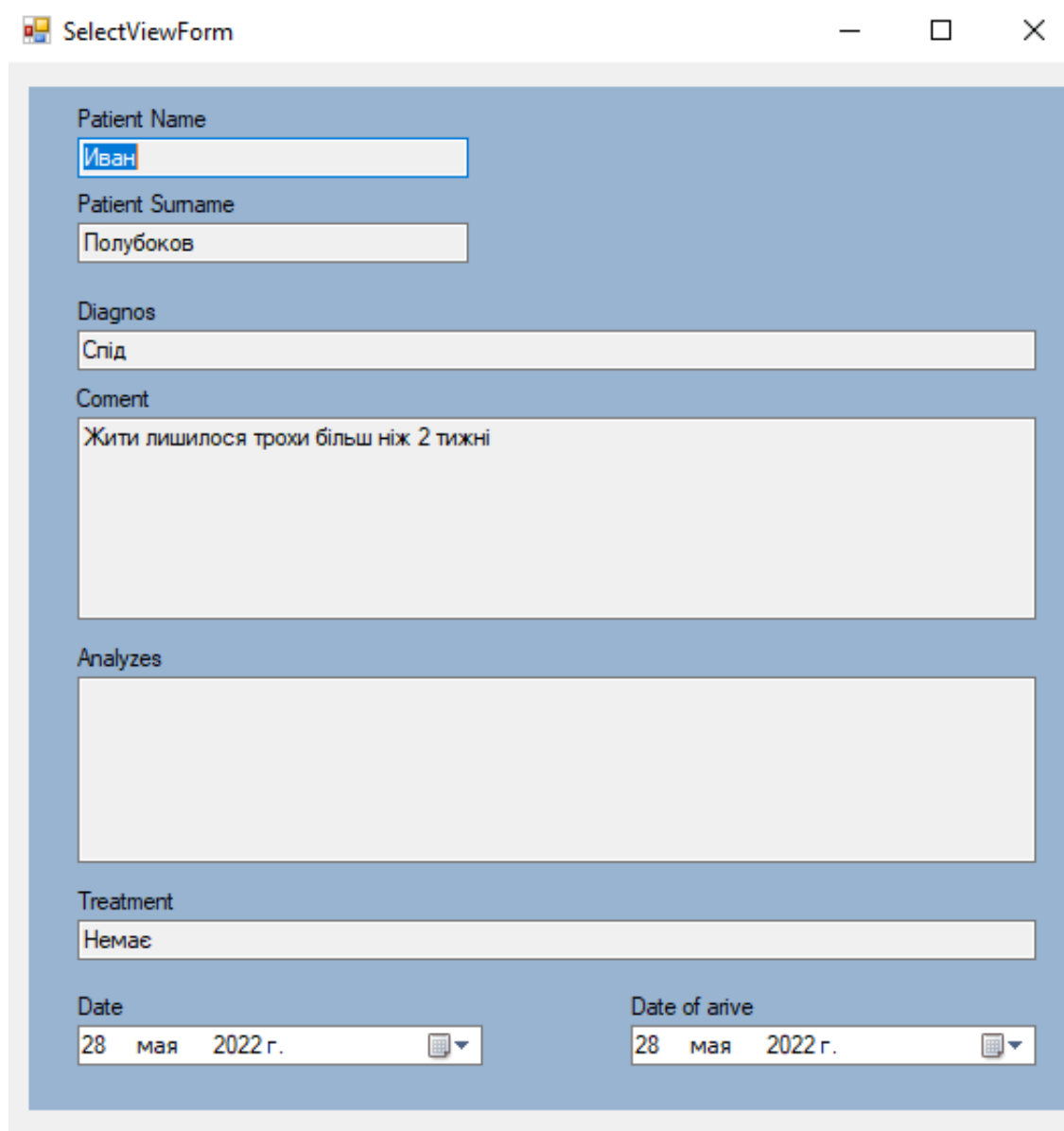
Хіміо терапія 2 тижні

Date

29 мая 2022 г.

Save new

Приклад перегляду історії хворого



The image shows a screenshot of a software window titled "SelectViewForm". The window contains a form for viewing patient history. The form is divided into several sections, each with a label and a corresponding input field or text area. The background of the form is light blue, and the input fields are white with blue borders.

The form contains the following fields:

- Patient Name:** Input field containing "Иван".
- Patient Sumame:** Input field containing "Полубоков".
- Diagnos:** Input field containing "Спід".
- Coment:** Text area containing "Жити лишилося трохи більш ніж 2 тижні".
- Analyzes:** Text area (empty).
- Treatment:** Input field containing "Немає".
- Date:** Date picker showing "28 мая 2022 г.". (Note: The text in the image is "28 мая 2022 г.", which is Russian for May 28, 2022).
- Date of arive:** Date picker showing "28 мая 2022 г.". (Note: The text in the image is "28 мая 2022 г.", which is Russian for May 28, 2022).

Можливі вдосконалення

При розробці ПЗ були виявлені недоліки в архітектурі взаємодій між системою токенизації та системою Peer-To-Peer передачі даних. Ці проблеми слід виправити для більшої надійності, та покращенню гнучкості системи для подальших модифікацій.

Також слід провести оптимізацію збережень даних при першому запуску застосунка, тому що, час входу буде значно збільшуватися з кількістю інформації, що знаходиться в блокчейні.

Висновки

В ході дипломної роботи було:

- Проведено аналіз предметної області;
- Проаналізовано проблеми;
- Виявлені недоліки та переваги сучасних систем;
- Проведений аналіз методів рішення поставлених проблем;
- Сформовані вимоги до програмної системи
- Виконано реалізацію системи
- Виконано тестування розробленої системи

Дякую за увагу!