**Міністерство освіти і науки України**

**Національний авіаційний університет**

**Факультет кібербезпеки та програмної інженерії**

**Кафедра інженерії програмного забезпечення**

**Дисципліна: “Основи технологій R&D”**

**Лабораторна робота №4**

**“Організація патентного пошуку по заданій темі з використанням мережі Інтернет”**

**Виконав:** студент групи ПІ-424Б

Разно О. С.

**Перевірив:** Радішевський М. Ф.

Київ-2024

**Мета роботи** – отримання навичок використання спеціальних ресурсів для проведення первинного патентного пошуку.

**Завдання:**

1. Виділити ключові слова для пошуку на обрану тематику.

2. Сформувати пошукові запити для пошуку за ключовими словами та класифікаторами.

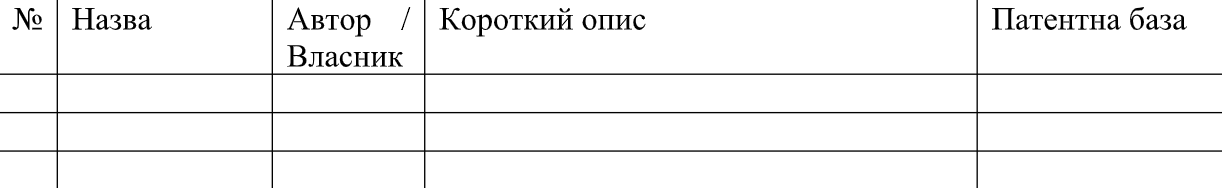
3. Використати відомі БД для пошуку патентів та свідоцтв на корисну модель.

4. Відредагувати ключові слова у випадку необхідності та переформувати пошукові запити.

5. Переглянути додаткову інформацію по знайденим патентам (зображення, схеми, креслення та ін.)

6. Визначити авторів, що найчастіше зустрічаються в знайдених матеріалах, дослідити їх патенти в суміжних областях.

7. Зберегти знайдені патенти, свідоцтва на корисну модель, результати пошукових запитів.

8. Сформувати звіт, інформацію відобразити у вигляді таблиці.

9. Обрати 1 зі знайдених патентів, скопіювати текст формули винаходу і визначити в ньому опис прототипу і позначити зеленим, а текст опису змін – світло-синім кольором.

**Виконання:**

**Знайдені патенти на тематику: “Розробка адаптивних та надійних методів захисту від кібератак на системах, що використовують технологію блокчейну”:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Назва патенту** | **Автор/ Власник** | **Короткий опис** | **Патентна база** |
| 1. | Система та метод для захисту блокчейн-систем від кібератак | IBM Corporation | Система та метод для захисту блокчейн-систем від кібератак, шляхом використання адаптивних методів аутентифікації та авторизації, а також методів моніторингу та аналізу даних. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 2. | Спосіб і система захисту блокчейн-мережі від атак типу "відмова в обслуговуванні" | Huawei Technologies Co., Ltd. | Спосіб і система захисту блокчейн-мережі від атак типу "відмова в обслуговуванні", шляхом використання методів розподіленого хешування та балансування навантаження. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 3. | Метод та система для забезпечення кібербезпеки блокчейн-мереж | Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” | Метод та система для забезпечення кібербезпеки блокчейн-мереж, шляхом використання методів криптографії та шифрування даних. | База патентів України: <https://base.uipv.org/searchINV/> |
| 4. | Система захисту блокчейн-мереж від атак типу "подвійне витрачання" | Bitfury Group Limited | Система захисту блокчейн-мереж від атак типу "подвійне витрачання", шляхом використання методів консенсусу та верифікації транзакцій. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 5. | Метод та система для аутентифікації користувачів у блокчейн-мережах | Samsung Electronics Co., Ltd. | Метод та система для аутентифікації користувачів у блокчейн-мережах, шляхом використання методів біометричної аутентифікації. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 6. | Спосіб захисту блокчейн-мережі від DDoS-атак | ТОВ "Інститут кібернетики імені В.М. Глушкова" | Спосіб передбачає використання механізму репутації для раннього виявлення та блокування DDoS-атак. | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 7. | Система та метод захисту інформації в блокчейн-мережі | АТ "Укртелеком" | Система та метод передбачають використання шифрування та аутентифікації для захисту інформації в блокчейн-мережі. | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 8. | Метод захисту блокчейн-мережі від атак типу "51%"" | ТОВ "CyberGeeks" | Метод передбачає використання алгоритму консенсусу Proof-of-Stake (PoS) для захисту блокчейн-мережі від атак типу "51%". | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 9. | Система захисту блокчейн-мережі від атак типу "Sybil" | Національний університет "Києво-Могилянська академія" | Система передбачає використання механізму репутації та алгоритму консенсусу Proof-of-Identity (PoI) для захисту блокчейн-мережі від атак типу "Sybil". | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 10. | Метод аутентифікації користувачів в блокчейн-мережі | ТОВ "BlockchainUA" | Метод передбачає використання біометричної аутентифікації для захисту блокчейн-мережі від несанкціонованого доступу. | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 11. | Система захисту смарт-контрактів від вразливостей | ТОВ "Distributed Lab" | Система передбачає використання статичного та динамічного аналізу для виявлення та усунення вразливостей смарт-контрактів. | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 12. | Метод захисту блокчейн-мережі від квантових атак | Національний технічний університет "Київський політехнічний інститут імені Ігоря Сікорського" | Метод передбачає використання квантово-стійких алгоритмів шифрування для захисту блокчейн-мережі від квантових атак. | Державний реєстр патентів України: <https://ukrpatent.org/> |
| 13. | Система та метод для захисту блокчейн-мереж від атак типу "сибірський виклик" | Symantec Corporation | Система та метод для захисту блокчейн-мереж від атак типу "сибірський виклик", шляхом використання методів моніторингу та аналізу даних, а також методів блокування транзакцій. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 14. | Метод та система для захисту смарт-контрактів від атак типу "переповнення буфера" | Chainlink Labs, Inc. | Метод та система для захисту смарт-контрактів від атак типу "переповнення буфера", шляхом використання методів статичного аналізу коду та методів верифікації смарт-контрактів. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 15. | Система та метод для анонімної аутентифікації користувачів у блокчейн-мережах | IdRamp, Inc. | Система та метод для анонімної аутентифікації користувачів у блокчейн-мережах, шляхом використання методів криптографії. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 16. | Метод та система для аудиту блокчейн-мереж | ConsenSys AG | Метод та система для аудиту блокчейн-мереж, шляхом використання методів статичного аналізу коду, динамічного аналізу та формального верифікації. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 17. | Система та метод для захисту консенсусних алгоритмів блокчейн-мереж від атак типу "51%" | Blockstream Corporation | Система та метод для захисту консенсусних алгоритмів блокчейн-мереж від атак типу "51%", шляхом використання методів економічного стимулювання та методів раннього виявлення атак. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |
| 18. | Система та метод для захисту блокчейн-мереж від атак типу "replay" | R3 LLC | Система та метод для захисту блокчейн-мереж від атак типу "replay", шляхом використання методів хешування та маркування транзакцій. | Espacenet: [https://worldwide.espacenet.com](https://worldwide.espacenet.com/)  Google Patents:  <https://patents.google.com/> |

**Обрання 1 зі знайдених патентів, наведення тексту формули винаходу і визначення в ньому опису прототипу (позначення зеленим кольором), та текст опису змін (світло-синій колір):**

**Патерн:** “Метод та система для аутентифікації користувачів у блокчейн-мережах”.

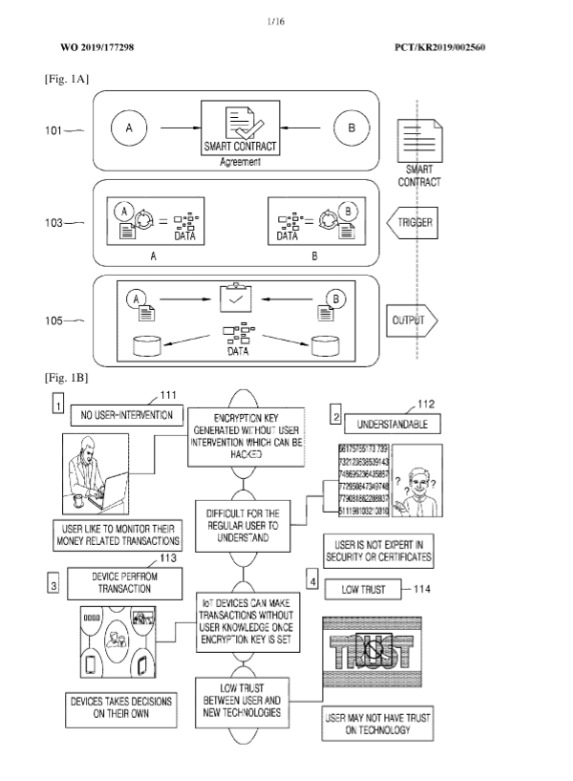
**Автор/Власник:** Samsung Electronics Co., Ltd.

**Короткий опис:** Метод та система для аутентифікації користувачів у блокчейн-мережах, шляхом використання методів біометричної аутентифікації.

**Патентна база:** Espacenet.

**Посилання на патент в патентній базі:** [https://worldwide.espacenet.com/patent/ search/family/067908436/publication/WO2019177298A1?q=pn%3DWO2019177298A1](https://worldwide.espacenet.com/patent/%20search/family/067908436/publication/WO2019177298A1?q=pn%3DWO2019177298A1)

**Формула винаходу:**

Винахід стосується методу та системи для забезпечення аутентифікації користувачів у блокчейн-мережах. Блокчейн є електронним реєстром, реалізованим як комп'ютерна децентралізована система, що включає блоки, які, в свою чергу, складаються з транзакцій. Транзакції можуть містити невеликі програми, відомі як скрипти, вбудовані в відповідні входи та виходи, і ці скрипти можуть визначати, як і ким можуть бути доступні виходи транзакцій. Додатково, наступні транзакції можуть не залежати від попередніх транзакцій.

На фігурі 1А показано приклад сценарію транзакції блокчейну, де виконується транзакція розумного контракту. У сценарії транзакції розумного контракту правила бізнесу можуть піддаватися існуючим правилам та регулюванням, редагованим постачальником послуг або однією зі сторін угоди. Виконання розумного контракту може бути викликане подією у блокчейн-мережі або за її межами. Додатково, виконання розумного контракту може створювати вихідні дані, які можуть впливати на інший блокчейн (тобто касовий реєстр) або іншу систему.

На фігурі 1Б показано приклад сценарію транзакції блокчейну, де виникає проблема безпеки. В сценарії користувач може бажати моніторити грошові транзакції. Однак генерування ключа шифрування без втручання користувача може призвести до його взлому. Крім того, звичайному користувачеві важко зрозуміти ключ шифрування. У такому випадку електронний пристрій може виконувати транзакції і приймати рішення самостійно. Також пристрій IoT може виконувати транзакції без знання користувача, якщо ключ шифрування встановлено.

Проте, ключ шифрування для транзакції блокчейну може бути недостатнім для створення дійсної транзакції. Користувач може мати низьку довіру до технології блокчейну. Втручання користувача не може бути усунено для всіх критичних транзакцій (тобто конкретних для IoT, грошових транзакцій і т. д.).

Суть винаходу: Надається пристрій для управління аутентифікацією користувача в блокчейн-мережі. Пристрій включає процесор, налаштований для передачі запиту на ідентифікатор (ID) моментального знімка з даними користувача серверу, отримання згенерованого ідентифікатора моментального знімка на основі даних користувача, ініціювання транзакції з ідентифікатором моментального знімка в блокчейн-мережі, що включає блокчейн-сервер, який аутентифікує ідентифікатор моментального знімка, та виведення даних транзакції блокчейну, що пов'язані з транзакцією, на основі аутентифікації ідентифікатора моментального знімка.

Винахід надає середовище реального часу для безпечної передачі даних та покращує довіру між користувачем і розумними системами за допомогою технології блокчейну.

**Висновок:** В ході виконання лабораторної роботи, я отримав навички використання спеціальних ресурсів для проведення первинного патентного пошуку.