Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації____
(повна назва)

Кафедра Радіотехнологій інформаційно-комунікаційних систем_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
ГЮІК.467750.009 ПЗ

Дослідження розподілених систем на базі блочейн технологій та протоколу Open VAS
(тема)

Виконав: студент 2 курсу, групи РПСКм-19-1_
_____Галкіна А. О._____
(прізвище, ініціали)
спеціальності _172_Телекомунікації та_____
радіотехніка_____
(код і повна назва спеціальності)
Тип програми___освітньо-професійна _____
(освітньо-професійна або освітньо-наукова)
Освітня програма Радіолектронні пристрої,__
системи та_комплекси_____
(повна назва освітньої програми)

Керівник ___Цопа О.І._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ____Цопа О. І.__
(підпис) (прізвище, ініціали)

2020 р.

Не містить відомостей заборонених для відкритого публікування

Керівник Цопа О.І.

Студент Галкіна А.О.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації

Кафедра Радіотехнологій інформаційно-комунікаційних систем _____

Рівень вищої освіти_____другий (магістерський)_____

Спеціальність _____172__Телекомунікації та радіотехніка_____

(код і повна назва)

Тип програми _____освітньо-професійна_____

(освітньо-професійна або освітньо-наукова)

Освітня програма Радіоелектронні пристрої, системи та комплекси_____

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Галкіній Анастасії Олегівні

(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження розподілених систем на базі блокчейн технологій та протоколу OpenVASP

затверджена наказом по університету від 21 11 2020 р. № 1729 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 12 грудня 2020р.

3. Вихідні дані до роботи

3.1 Дослідити принцип роботи блокчейн систем

3.2 Розглянути методи тестування систем на базі блокчейн

4. Перелік питань, що потрібно опрацювати в роботі

4.1. Принцип роботи блокчейн систем

4.2. Методи тестування систем на базі блокчейн

4.3. Дослідження розвитку блокчейн систем в Україні

4.4. Дослідження додатку на базі OpenVAS протоколу

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п. 5 включається до завдання за рішенням випускової кафедри)
Слайди презентацій

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім’я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Блокчейн в Україні та потенціал OpenVAS протоколу	Цопа О.І.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Вступ	05.09-10.09	Виконано
2	Постановка проблеми	21.09-14.10	Виконано
3	Аналіз останніх досліджень і публікацій	15.10-29.10	Виконано
4	Дослідження методів тесування Blockchain систем	30.10-11.11	Виконано
5	Дослідження OpenVAS протоколу	12.11-01.12	Виконано
6	Висновки	02.12-03.12	Виконано
7	Оформлення пояснювальної записки	04.12-06.12	Виконано
8	Оформлення графічного матеріалу	07.12-08.12	Виконано
9	Подання роботи на кафедру	09.12.2020	Виконано

Дата видачі завдання _4___вересня_____2020 р.

Студент _____
(підпис)

Керівник роботи _____ _____ Цопа О.І._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 70 с., 9 рис., 2 додатки, 15 джерел.

БЛОКЧЕЙН, OPENVASP, СМАРТ-КОНТРАКТ, ТЕСТУВАННЯ, БЛОК, ТРАНЗАКЦІЯ

Об’єктом дослідження є розподілені системи на базі блокчейн та протоколу Open VAS .

Метою даної роботи є дослідження розподілених систем на базі блокчейн та протоколу Open VAS, та методи тестування систем на базі протоколу Open VAS.

З метою вирішення поставлених задач в роботі проведений аналіз різновидів та технологій на базі блокчейн, а також дослідження існуючого досвіду застосування технологій блокчейн у світі .

ABSTRACT

Explanatory note: 70 p., 9 Fig., 2 Appendix, 15 sources.

BLOCKCHAIN, OPENVASP, SMART-CONTRACT, TESTING, BLOCK, TRANSACTION

The object of the development is the software for the remote voice remote control device.

The purpose of this work is to develop a device for voice remote object management, a remote server to synchronize the mobile application and objects and the mobile application to display the status of objects and voice control.

In order to solve these problems, the analysis of similar devices and technologies, methods of wireless information transfer, the device based on Arduino and mobile application were carried out.

The object of the investigating is distributed systems based on blockchain and Open VAS protocol.

The purpose of this work is to explore distributed systems based on blockchain and Open VAS protocol, and methods of testing systems based on Open VAS protocol.

In order to solve this topic, the analysis of varieties and technologies based on blockchain, as well as the investigation of existing experience in the use of blockchain technologies in the world.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

DAO – децентралізована автономна организация

OpenVASP – протокол відкритого віртуального артефакту

DB – база даних

ЄС – Європейский Союз

ВСТУП

Протягом десятиліття, технології, які узагальнюються як технології блокчейн, отримують все більше уваги та інтересу з боку громадськості.

Основні інгредієнти - це асиметрична ключова криптографія та використання криптографічних хеш-функцій, які були винайдені між сімдесятими роками та кінцем минулого століття.

На сьогодні ми маємо велике різноманіття галузей, в яких застосовують блокчейн технології..

Як зазначив Заступник Міністра юстиції України Денис Чернишов, у майбутньому Україна переведе всю цифрову державну інформацію на блокчейн-платформу. У зв'язку з цим активно обговорюється переведення на систему блокчейну: державних реєстрів (зокрема, державної реєстрації прав на нерухоме майно), нотаріальної діяльності, зберігання державних даних, проведення земельних аукціонів, електронного майданчика торгівлі арештованим майном (СЕТАМ), Державного земельного кадастру, банківської сфери, проведення голосування та ін. Наразі серед галузей, де в першу чергу планується використання системи блокчейн, – держреєстри, ЖКГ, соціальне страхування, охорона здоров'я та енергетика..

Метою даної роботи є дослідження технологій на базі блокчейн, а також застосування та користь цих технологій для України.

Для досягнення поставленої мети сформульовані наступні задачі:

- зробити огляд та аналіз технології в цілому, в чому її унікальність;
- розглянути види застосування технології блокчейн;
- аналіз можливості застосування сьогодні технології блокчейн в Україні та перспективи її використання;
- розгляд протоколу OpenVAS.

1 ОГЛЯД НА ПОНЯТТЯ БЛОКЧЕЙН

1.1 Історія появи технології та застосування у країнах світу

Блокчейн, тобто ланцюжок блоків транзакцій (англ. Blockchain, Block chain від block — блок, chain — ланцюг) — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Кожен блок містить часову позначку, хеш попереднього блока та дані транзакцій, подані як хеш-дерево. Таку розподілену базу даних закладено в основу криптовалюти Bitcoin (вона була описана 2008 і реалізована 2009 року), де слугує бухгалтерською книгою для всіх операцій. Таку базу називають Блокчейн[1].

Перша робота над криптографічно захищеним ланцюгом блоків була описана 1991-го року Стюартом Хабером (англ. Stuart Haber) та У. Скоттом Сторнеттою (англ. W. Scott Stornetta). Вони хотіли запровадити систему, де часові позначки документів неможливо спотворити чи пошкодити. 1992-го року Байєр, Хабер і Сторнетта використали в проекті дерево Меркла, що покращило ефективність, дозволяючи включати в один блок декілька документів.

Задум першого блокчейну було розроблено людиною (або гуртком людей), відомою як Сатоші Накамото 2008-го року. Цей задум Накамото втілив наступного року, розробивши основний складник криптовалюти Bitcoin, де він служить відкритою книгою обліку для всіх транзакцій в мережі. Завдяки блокчейну, Bitcoin став першою цифровою валютою, де проблему подвійних витрат було вирішено без залучення довірених вузлів або централізованого сервера. Відтак устрій Bitcoin став взірцем для багатьох інших застосувань.

У серпні 2014 р. розмір блокчейн-файлу Bitcoin, що містить відомості про всі транзакції мережі, сягнув 20 Гб (гігабайтів). У січні 2015 року розмір зріс до

майже 30 Гб, а з січня 2016 року по січень 2017 року Bitcoin блокчейн виріс з 50 ГБ до 100 ГБ.

Слова «блок» і «ланцюг» використовувались окремо в первинній роботі Сатоші Накамото, але потім, з 2016 року, вони стали вживатись як одне слово — блокчейн. Термін блокчейн 2.0 належить до нових застосувань розподіленої блокчейн бази даних, яка вперше виникла 2014 року. The Economist описав одну з реалізацій цього блокчейну другого покоління як «мову програмування, що дозволяє користувачам писати більш складні та витончені угоди, створюючи таким чином рахунки-фактури, які сплачують себе після доставки товару, або сертифікати, що самі надсилають своїм власникам дивіденди, щойно прибуток сягає певного рівня». Очікується, що вони допоможуть людям інтегруватись у світову економіку, захистять конфіденційність учасників, дозволять людям «монетизувати свою власну інформацію» та забезпечать творцям компенсацію за їхню інтелектуальну власність. Технологія блокчейн другого покоління дозволяє зберігати «стійкий цифровий ідентифікатор та особу» індивідуума та надає просунутий шлях вирішення проблеми суспільної нерівності шляхом «потенційної зміни способів розподілу багатства».

У травні 2018 року Gartner з'ясував, що лише 1 % IT-директорів з інформаційних технологій заявляли про будь-яке використання блокчейнів у своїх компаніях, а лише 8 % директорів «планували або розглядають можливість спробувати використання блокчейну» найближчим часом.

Безліч організацій в різних країнах світу сміливо користуються перевагами блокчейн-технологій для вирішення найрізноманітніших завдань, наближаючи той день, коли їх застосування стане повсюдним.

Проблематика застосування циф- рових технологій в галузі державного управління стала об'єктом наукових досліджень зарубіжних вчених, так, на мою думку, серед багатьох публікацій особливу увагу привертають праці таких канадійських дослідників як Д. Браун , Дж. Вільямс, П. Джонс , П. Дютіл, Д. Каргнелло, А. Кларк, Дж. Крафт, Е. Лінквіст, Д. Ма- рандо, Дж. Рой, С. Тоз, М.

Флуміан, які розглядали різні технологічні аспекти реалізації практичного впровадження концепції «Ера цифрового врядування» (Digital Era Governance, DEG).

1.2 Блок транзакцій

Блок транзакцій — спеціальна структура для запису нових транзакцій в системі Біткоїн та аналогічних їй (рисунок 1.1).

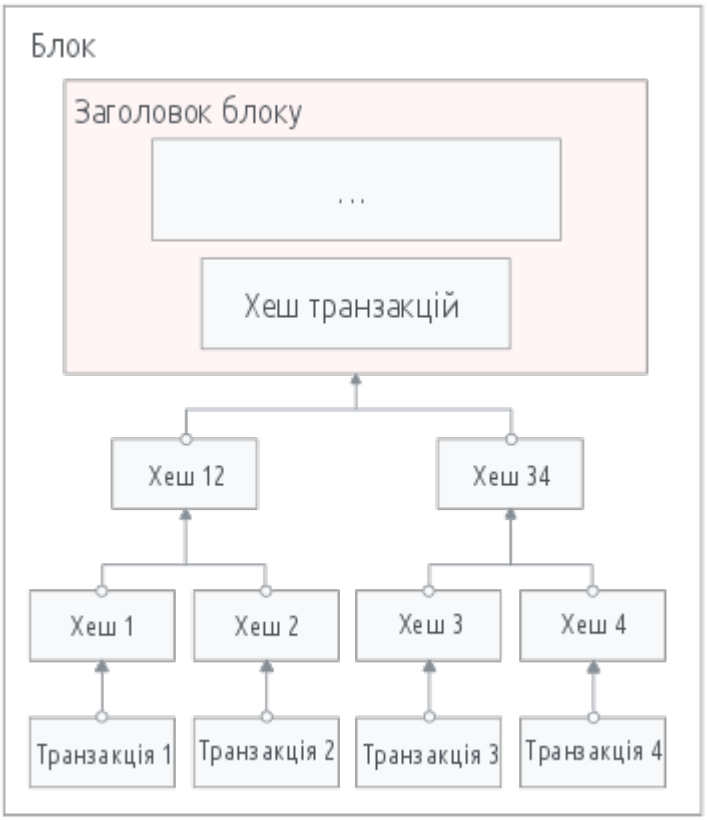

Рисунок 1.1 - Схема блоку транзакцій

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[2]. 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 блоці 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 блоці використовується деревисте гешування, аналогічне формуванню геш-суми файлу в протоколі BitTorrent (рисунок 1.2). 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.

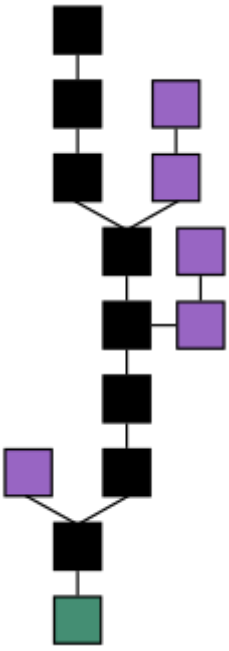

Рисунок 1.2 - Схема блоку транзакцій

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 геш 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.

1.3. 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.

1.4 Підтвердження транзакції

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[21]. 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.

1.5 Поняття смарт-контракту

Смарт-контракт (англ. Smart contract — “розумний контракт”) — Різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання і розірвання яких можливо лише з використанням комп'ютерних програм (блокчейн платформ) в рамках мережі Інтернет.

В реальному світі панівне охоплення в реалізації смарт-контрактів здобула DAO, розподілена автономна організація для венчурного фінансування, яка була запущена у травні 2016 року[3].

Словосполучення «смарт-контракт» було створено вченим у галузі інформатики, криптографії, а також в області права, Ніком Сабо в 1996 році, для підкреслення того, що він називає «високорозвинені практики» договірного права і пов'язаних з діловою практикою в розробці електронних протоколів торгівлі, між незнайомими людьми в Інтернеті. Можна сказати, що йдеться про врегулювання відносин сторін шляхом закріплення їх вираженої волі у формі певного коду, який придатний для зчитування комп'ютером.

У 1996 році Сабо описував його так: «Нові інституції і нові способи формалізації відносин цих інституцій сталі можливі завдяки цифровій революції. Я називаю ці контракти «розумними» тому що вони набагато більш функціональні, ніж їхні неживі паперові предки. Не передбачається використання штучного інтелекту. Смарт-контракти це набір обіцянок у цифровому форматі, включно з протоколами за якими сторони виконують ці обіцянки.»

Сабо, натхненний дослідником Девід Чаумом, також мав широке очікування того, що специфікації на основі чіткої логіки і перевірки, або виконання через криптографічні протоколи та інші механізми цифрової безпеки, може являти собою різке поліпшення в порівнянні з традиційним

контрактом, навіть для деяких традиційних видів договірних положень, які можуть бути передані під владу комп'ютерних протоколів.

У документі 2013 року, Марк Міллер та інші підкреслювали можливості як основи безпеки розумних контрактів, на відміну від Чаума та інших дослідників в криптографічної фінансової спільноти, які використовують сучасні криптографічні протоколи, щоб забезпечити безпеку і конфіденційність цифрових грошей, облікових даних, підписання контракту, аукціонів, а також інших комерційних механізмів.

Кілька формальних мов були розроблені та запропоновані для визначення договірних положень. IEEE провів два семінари з електронним укладенням договорів.

Останнім часом галас навколо блокчейну, смарт-контрактів використовується в основному в сенсі загального розуміння цілі, що відбувається на блокчейні. У цій інтерпретації смарт-контракт не обов'язково має відношення до класичної концепції договору, але може бути будь-якою комп'ютерною програмою.

1.5.6 Питання безпеки

Смарт-контракт як «комп'ютеризований протокол транзакцій, який виконує умови контракту, то не по своїй природі "розумний", а як окремий атрибут типу контракту. Блок ланцюг, на основі смарт-контракта, видно всім користувачам зазначеного блоку. Проте, це призводить до помилок, в тому числі дірок в системі безпеки, які видно всім, але не може бути швидко виправлено. Таким чином, була успішно виконана атака на DAO в червні 2016 року вартістю 50 млн USD у Ethereum, в той час, як розробники намагалися прийти до вирішення цієї проблеми. Обробка задачі на блокчейні вимагала часу, за який хакер може отримати доступ до ресурсів, і зняти кошти з DAO контракту.

1.5.7 Винагорода та виконання

Сабо передбачає, що смарт-контракт це інфраструктура, яка може бути реалізована шляхом тиражованих реєстрів активів та виконання контрактів з

використанням криптографічного хеш-ланцюга і Візантійської відмовостійкої винагороди. Кожен вузол у мережі рівноправних вузлів виступає як заголовок реєстру і умовна порука, що виконує зміни права власності та автоматично відзначає правила, що регулюють ці операції, і перевіряє ту ж роботу інших вузлів. Аскемос реалізував цей підхід в 2002 році, використовуючи схему як мову сценаріїв контракту.

Криптовалюти, такі як bitcoin впровадили спеціальні випадки таких реєстрів, де майно гроші. Bitcoin і багато з його спін-оффів містять механізми для того, щоб мати більше можливостей спільної власності і виконання контрактів. Код підтримки це прихована частина протоколу Bitcoin, на основі імовірної та анонімної (за рахунок доказу роботи на основі візантійського) винагороди.

Одна з пропозицій для використання Bitcoin для реєстрації активів і виконання контракту називається «кольорові монети». Реєстрація доменного імені реєстру здійснюється в Namecoin; реєструємо назви для потенційно довільних форм власності, поряд з виконанням контракту, реалізовані в Crypti, Ripple, Mastercoin і Ethereum. NXT реалізує право власності на доказі власності, частки в базовій валюті.

Смарт-контракти можуть бути реалізовані за допомогою рікардіанському шаблону проектування контракту[4].

Додатки можуть включати в себе фінансові інструменти, такі як облігації, акції та похідні, договорів по забезпеченню, а також інші документи і угоди, де вузли можуть стежити за розвитком подій, на яких зумовлені розумні правила контракту. Переваги смарт-контракту як еквіваленту звичайного фінансового інструменту гіпотетично включають зведення до мінімуму ризику контрагента, скорочення термінів розрахунків, а також підвищення прозорості. UBS експериментував з "розумними" облігаціями, які використовують блокчейн, в якому платіжні потоки гіпотетично могли б бути повністю автоматизовані, створюючи самостійно оплачуваний інструмент.

1.6 Висновки за розділом

Розглянувши історію появи поняття блокчейн, а також основні поняття, такі як, блок та ланцюжок блоків ми можемо зробити висновок, що блокчейн – це передусім технологія. Технологія на ранній стадії розвитку, і, тут дуже важко говорити про переваги та перспективи розвитку, не заглиблюючись в технічні деталі, яких немало. Але спробуємо максимально об'єктивно висвітлити загальну ситуацію.

Можна назвати як переваги блокчейну, так і проблеми, що виникають у зв'язку з його використанням. До переваг використання системи блокчейн можна віднести: 1) децентралізацію, тобто використовується вся мережа, а не один комп'ютер (організація, людина тощо). У такому випадку, навіть якщо один або декілька комп'ютерів (осіб) не може виконувати ніяких функцій (ліквідований, арештований тощо), – інші зберігають цю інформацію, що ускладнює хакерські атаки та підробку інформації (хоча від цього і ніхто не застрахований); 2) доказовість кожної трансакції: є криптографічне підтвердження кожної трансакції, запису тощо. Зокрема, ключі є приватні (що належать конкретній особі) і публічні (які можуть бути використані всіма користувачами цієї мережі), тобто якщо є одна особа чи один комп'ютер; 3) прозорість (загальний доступ): будь-хто і будь-коли може побачити, які саме операції проводилися; 4) безпека: інформація зберігається із застосуванням криптографії; 5) неможливість внесення змін у «підписаний» блок: інформація, яка попала в блокчейн, проходить перевірку і якщо перевірку пройдено – ставиться своєрідна «печатка» і ці дані синхронізуються між всіма учасниками, з цього моменту інформацію змінити не можна; 6) обчислювальна логіка: цифрова природа реєстру працює таким чином, що трансакції у блокчейні можуть бути прив'язані до обчислювальної логіки і фактично їх можна програмувати, що дає можливість користувачам налаштовувати алгоритми і правила автоматичного виконання трансакцій між вузлами.

Підсумовуючи викладене, можна констатувати, що блокчейн є дійсно революційною технологією, він дає змогу в розподіленому світі прийти до свого роду «консенсусу», обійтися без посередників, що може бути використано у всіх сферах суспільного життя (охорона здоров’я, фінанси, медіа тощо), а тому: «народжуються» нові бізнес-моделі; знижується рівень шахрайства; спрощуються процеси (робота) між бізнес-агентами.

2 МЕТОДИ ТЕСТУВАННЯ ТЕХНОЛОГІЙ НА БАЗІ БЛОКЧЕЙН

2.1 Загальні відомості

Обсяги даних вибухають, за останні два роки було створено більше даних, ніж за всю попередню історію людського роду. За такої швидкості ми всі будемо оточені лише даними. Для зберігання та аналізу таких даних було запроваджено кілька технологій / інструментів. Хоча для обробки таких величезних даних запроваджено безліч інструментів, захист даних стає ключовим фактором у цьому світі Інтернету. Блокчейн - це одна з таких технологій, яка використовується для зберігання таких величезних даних, маючи на увазі безпеку. Сам по собі блокчейн приносить величезні випробування у світі тесутвання завдяки своїм концепціям і обсягу даних, які він повинен обробляти. Зупинимось на деяких основних викликах, з якими, ймовірно, доведеться зіткнутися під час тестування програми Blockchain.

Також, викликом для розробників є програмування та тестування системи, яка буде дійсно надійною. Розглянемо два відомих випадки блокчейн атак.

Найвідомішим проектом DAO був DAO, створений Slock.it, який розпочав свою діяльність 30 квітня 2016 року. Це був віртуальний фонд венчурного капіталу, яким керували інвестори DAO. Ідея полягала в наступному: кошти, залучені від інвесторів, власників токенів, об’єднуються. Власники жетонів можуть стати підрядниками, подаючи пропозиції щодо фінансування свого проекту за допомогою коштів DAO. Був проведений іспит куратора, який був просто перевіркою особи, проведеним одним із кураторів, які були обрані серед поважних членів спільноти Ethereum. Як тільки пропозиція пройде перевірку куратора, інвестори проголосують за неї. Якщо пропозиція схвалена кворумом у 20% усіх токенів, DAO автоматично передає Ether до смарт-контракту, який

представляє пропозицію. Будь-який ефір, отриманий із пропозицій, що фінансуються DAO, буде повернутий інвесторам як винагороду.

Під час первинної пропозиції, яка відбулась у травні 2016 року, єдиною вимогою для інвестування було інвестування ефіру в систему. В обмін на це учасникам були надані токени DAO, 100 токенів DAO за 1 ефір, які дають право голосу для використання під час відбору проектів, що фінансуються. DAO зібрав 12,7 млн. Ефірів, що дорівнювало понад 150 млн. Доларів США тоді і став найбільшим проектом краудфандингу до свого часу. Однак 16 червня 2016 року DAO було зламано.

Механізм управління, прийнятий DAO, був подібним до управління державними акціонерними корпораціями. Не дивно, що існувала ймовірність того, що меншість буде придушена більшістю. Творці DAO хотіли запровадити захист для меншості. Ідея полягала в тому, щоб меншість могла отримати свої кошти, коли пропозиція, в якій вони не хочуть брати участь, буде схвалена, незважаючи на їхні заперечення, що насправді було еквівалент DAO права на оцінку, який ми бачимо відповідно до корпоративного законодавства в деяких юрисдикціях.

Творці застосували це рішення як здатність DAO розділитися навпіл. Подаючи спеціальну форму пропозиції, меншість, разом з іншими власниками жетонів, які проголосували за цю другу спеціальну пропозицію, можуть взяти свій Ефір в новий DAO, який називається дочірнім DAO, але має ті самі здібності, і він піддається таким же обмеження, обмежені DAO, від якого вона розділена. Процедуру розділення може ініціювати будь-який власник токена в будь-який час щодо власного ефіру. Однак після ініціювання існує графік, якого слід чітко кодувати в кодексі DAO, згідно з яким роздільна пропозиція повинна мати принаймні 1 тиждень (7 днів) часу обговорення. Після цього 1 тижня можна викликати функцію розбиття, і Ether ініціатора можна перенести до нового дочірнього DAO, але тоді існує 27 днів періоду створення розбиття, протягом якого жодна пропозиція не може бути висунута. І навіть після цього, якщо ви намагаєтесь надіслати кошти в дочірньому DAO на рахунок, який знаходиться під

вашим власним контролем, вам потрібно подати пропозицію та почекати 2 тижні (14 днів), що є регулярним періодом обговорення пропозиції. Підводячи підсумок, як тільки ви вирішите розділити DAO, вам знадобиться принаймні 48 днів, перш ніж отримати його в контрольованому вами обліковому записі.

Кодер виявив лазівку в цій процедурі. Після виклику функції розділення код був написаний таким чином, щоб спочатку отримати ефір, а пізніше оновити баланс. Крім того, він не перевіряв, чи був рекурсивний виклик, який є виразом, що використовується для позначення функції, яка викликає себе. Зловмисникам вдалося рекурсивно викликати функцію розбиття та кілька разів отримувати свої кошти, перш ніж дійти до кроку, де код перевіряв баланс. 16 червня 2016 року зловмисникові вдалося отримати приблизно 3,6 мільйона ефіру з фонду DAO, зловживаючи цією лазівкою, яка відома як "експлуатування рекурсивного виклику".

2.1.1 Інцидент із переповненням вартості

15 серпня 2010 року було виявлено, що блок 74638 містив транзакцію, яка створила 184 467 440 737,09 551616 біткойнів для трьох різних адрес[5]. Дві адреси отримали по 92,2 мільярда біткойнів кожна, і той, хто вирішив блок, отримав додаткові 0,01 BTC, яких не було до транзакції. Це стало можливим, оскільки код, який використовувався для перевірки транзакцій перед включенням їх у блок, не враховував випадки настільки великих результатів, що вони переповнювались під час підсумовування.

Нова версія клієнта була опублікована протягом п’яти годин після відкриття, що містила зміну правил консенсусу, що відхиляло транзакції з перевищенням вихідної вартості (а також будь-яку транзакцію, яка з будь-якої причини виплатила понад 21 мільйон біткойнів за вихід). Блок ланцюга був роздвоєний. Хоча багато незв'язаних вузлів продовжували будувати на "поганому" ланцюжку блоків, "хороший" ланцюг блоків обігнав його на висоті блоку 74691, тоді всі вузли прийняли "хороший" блокчейн як авторитетне джерело транзакцій біткойнів.

Погана транзакція більше не існує для людей, які використовують найдовший ланцюг. Тому створені ним біткойни теж не існують. Хоча транзакція вже не існує, 0,5 BTC, яку вона спожила, існує.

Основне випробування при тестуванні блокчейну - розуміння технології: Blockchain - це відносно нова технологія, яку потрібно глибоко зрозуміти, перш ніж застосовувати Blockchain як технологію для створення додатків. Тестування та знання доменів дуже важливі при тестуванні блокчейн додатку.

Інструменти тестування: На ринку існує чимало інструментів тестування, які можна використовувати для тестування програми Blockchain. Однак підібрати правильний інструмент відповідно до програми є вирішальним рішенням. Це знову залежить від знання плюсів і мінусів кожного інструменту. Truffle, Ethereum Tester, BitcoinJ і Embark - це деякі з популярних інструментів, що використовуються для тестування програми Blockchain

Відсутність досвіду / навичок: Технологія блокчейн була вперше представлена в 2008 році Сатоші Накамото у формі біткойнів. Однак він не отримав широкого поширення в галузі через брак досвіду та навичок. Це робить тестування складним завданням.

Визначення тестової стратегії: Визначення тестової стратегії для блокчейну подібно до будь-якого іншого додатку, який враховує кілька параметрів. Як і будь-який інший додаток, розробка стратегії тестування технології Blockchain вимагає глибокого розуміння програми, її використання та самої технології[6].

2.1.1Додавання блоків

Технологія Blockchain призначена для використання для зберігання та обробки величезних обсягів даних, і в міру збільшення блоків блоки продовжують додаватися. Опрацювання такого сценарію тестування призводить до розгляду багатьох тестових випадків. Оскільки такі величезні дані додаються щосекунди, додавання блоків, швидше за все, відбуватиметься з однаковим темпом. Ну, складність додавання блоків можна зрозуміти само собою.

2.1.2 Розмір блоку та ланцюга

Тестування розміру блоку та ланцюжка є важливим аспектом для застосування блокчейну. Це вимагає належної перевірки доданих даних. Передача криптографічних даних: Головна суть технології Blockchain - це передача зашифрованих даних. Існує високий ризик збою у випадку, якщо передача даних не перевірена належним чином.

2.1.3 Інтеграційне тестування

Це зрозуміло. Оскільки в розробці програми Blockchain бере участь декілька компонентів, потрібно переконатися, що всі вони інтегровані належним чином. Отже, інтеграційне тестування слід проводити часто, щоб уникнути будь-яких збоїв(див. рисунок 2.1 – Традиційна V-модель тестування майже будь-якого додатку).

Тестування безпеки: Ну, тестування безпеки - це ще один аспект тестування програми Blockchain. Як уже згадувалося раніше, захист даних повинен бути найвищим пріоритетом. Технологію блокчейн можна використовувати в різних секторах, таких як охорона здоров'я, банківська справа, фінанси, освіта тощо, і будь-яке порушення безпеки в підсумку призведе до величезних втрат. Тестування продуктивності та навантаження: Тестування продуктивності та навантаження для програми Blockchain по суті означало б обсяг даних, які можна додати в блок, розмір ланцюжка, наскільки швидко і точно майнер може перевірити транзакцію за допомогою алгоритму «Доказ роботи» .

На закінчення, як і будь-яка інша програма для тестування додатків Blockchain, також потрібен відповідний набір навичок та розуміння, щоб розробити стратегію тестування. Найголовніше, що нефункціональне тестування стає тут ключовим викликом.

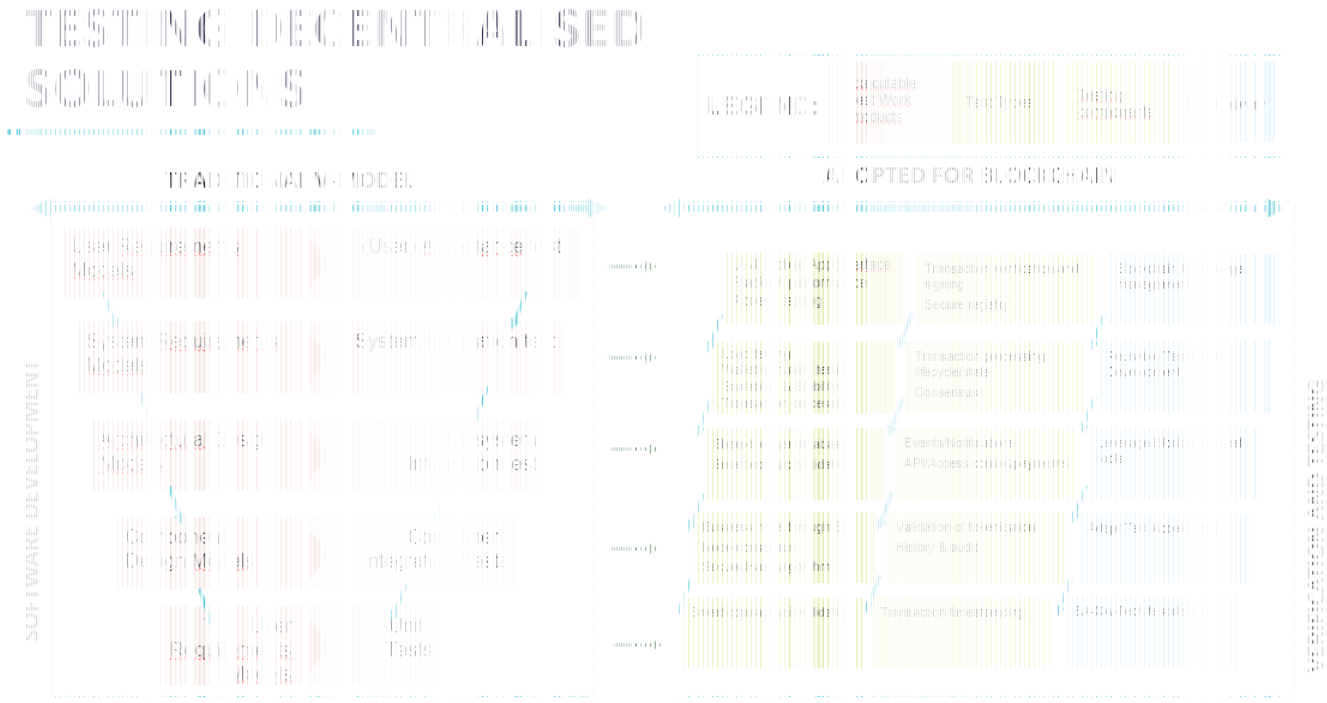

Рисунок 2.1 – Традиційна V-модель тестування майже будь-якого додатку

2.2 Функціональне тестування

Функціональне тестування відіграє вирішальну роль у тестуванні блокчейн технологій, оскільки воно допомагає оцінити ділові обставини, процеси та ефективність сценаріїв використання[7]. Деякі важливі компоненти, які тестувались як частина функціонального тестування, це:

2.2.1 Розмір блоку

Як уже зазначалося, блок містить запис книги реального часу із шифруванням та міткою часу. Це групи транзакцій, які підтверджуються, а потім розподіляються в публічній книзі біткойнів (це блокчейн). Існує багато суперечок щодо розміру блоку, оскільки чим більше розміру / транзакцій приєднується до блоку, тим складніше тестування зростає. Більшість майнерів хотіли б мати більші розміри блоків (зі зрозумілих причин), тоді як користувачі та розробники, з іншого боку, шукають кращих алгоритмів стиснення, щоб вмістити вміст у визначений розмір блоку. Традиційно блоки можуть містити до 36 МБ (кожен) даних транзакцій, але незабаром це спричинило загрози спаму та інші проблеми

відмови в послугах в Інтернеті. Таким чином, розмір блоку був зменшений і зафіксований (мабуть, одноголосно) до 1 Мб за штуку. Зі зміною складності, основні технології та можливість мати кілька транзакцій всередині одного блоку збільшують цю межу до максимуму. Зараз тестувальники зосереджуються на кількох питаннях, таких як - що, якщо розмір транзакції перевищує 1 МБ, які тести слід враховувати, якщо в блоці є кілька транзакцій, які правила шифрування пов'язані та багато інших таких складних сценаріїв. - Розмір ланцюга практично може складати багато блоків, оскільки ланцюг подовжується. Тестери гарантують, що під час тестування ланцюги не розриваються, а повна реєстрація кожного перенесення вартості тестується за можливими сценаріями.

2.2.2 Передача даних

На цьому етапі проводиться тестування втрат даних під час передачі, оскільки однорангова архітектура блокчейну стосується шифрування даних у джерела та дешифрування на приймальному кінці. Тестування на передачу забезпечує мінімальну втрату даних, покращення робочих процесів між однолітками та забезпечує можливість виявлення можливостей інтеграції.

2.2.3 Додавання блоку

Тестери перевіряють усі блоки, які додаються до ланцюжкової автентифікації кожної транзакції. Оскільки ланцюг не може бути змінений, а доданий блок ніколи не може бути змінений, тестування на цьому етапі є дуже важливим.

2.3 Нефункціональне тестування

Нефункціональне тестування описує тести, необхідні для визначення характеристик програмного забезпечення, які можуть бути виміряні різними величинами. У цілому, це тестування того, «як» система працює. Далі перераховані основні види нефукнціональних тестів.

2.3.1 Нефункціональне тестування (продуктивність).

Тестування продуктивності в блокчейні важливо з точки зору кількості транзакцій та розміру транзакції, що перевіряється на продуктивність блоку або програми, яка готується до розгортання на виробництві. Команда тестування

також фокусується на інших важливих та залежних параметрах, таких як затримка мережі, вузькі місця продуктивності, послідовність транзакцій на кожному вузлі, залежність від виробничого середовища, швидкість обробки транзакцій, клієнт / користувач та системний інтерфейс, а також відповіді, що вимагаються від смарт-контрактів. Оскільки при складеному тестуванні може бути кілька кінцевих точок, наскрізні сценарії розглядаються для загальної продуктивності, що в більшості випадків призводить до автоматизованого тестування продуктивності для загальної масштабованості екосистеми блокчейну[8].

2.3.2 Нефункціональне тестування (безпека).

Основна увага тут полягає в тому, щоб забезпечити ретельне тестування програм блокчейну, щоб перевірити, чи є вони вразливими до атак (шкідливі, вірусні тощо), чи надійні системи авторизації та чи автентифікація (включаючи доступу) є справжніми. Тестування безпеки також розглядає інші важливі аспекти, такі як конфіденційність, цілісність, не відмова в послугах, узгодженість/доступність та колізії. Тестування безпеки стає важливим у випадку злому рівня ідентичності, що може призвести до викриття переходів. Транзакція, яка триває, не може бути негайно зупинена, отже, тестування безпеки має бути ефективним, щоб розкрити всі такі потенційні злами рівня ідентичності. Деякі інші проблеми, пов'язані з тестуванням безпеки, включають - методи підпису гаманця, приватні ключі, захищений хеш, алгоритм консенсусу, залежності платформи додатків тощо. Визначений підхід перевірки та перевірки допомагає вирішити більшість таких невідповідностей.

2.4 Тестування інтерфейсу прикладного програмування

Тестування інтерфейсу прикладного програмування (API): Цей тип тестування повідомляє про зв’язок та взаємодію програм, які відбуваються в системі. Тут тестувальники перевіряють зовнішні відповіді, які отримує додаток, гарантують, що формати запиту API є правильними та дійсними. У рамках блокчейну також існує технологія, схожа на API, яка дозволяє використовувати

подібний підхід для тестування API; називаються смарт-контрактами. Деякі з найпопулярніших засобів тестування API - Postman та SoapUI[9].

2.5 Peer/node тестування

Спільна книга є абсолютно однаковою на кожному вузлі з однаковим набором і послідовністю транзакцій. Це досягається шляхом консенсусу між усіма вузлами в порядку, в якому транзакції додаються до мережі.

Тестування консенсусного протоколу для забезпечення збереження транзакцій у належній послідовності в звичайних умовах, а також у випадках, коли вузли виходять з ладу одночасно або достатня кількість вузлів не бере участі в мережі протягом певного періоду, включаючи тестування, що вузли в мережі синхронізуються з іншими перевірками нод.

2.6 Тестування смарт контракту

Тестування смарт контрактів передбачає моделювання всіх можливих очікуваних і несподіваних умов для кожного контракту, тестування всіх комбінацій бізнес-логіки та належного запуску та правильного виконання транзакцій.

Враховуючи кількість вузлів і комбінацій, які можливі, автоматизація тестів та оптимізація тестів є важливою частиною цього.

Три критичні кроки при тестуванні смарт-контракту:

- перевірка методів;
- перевірка шифрування та передачі;
- перевірка обробки.

2.7 Висновки за розділом

У цьому розділі були розглянуті найпоширеніші види тестування додатків, які використовуються як для тестування звичайних додатків, так і для систем на базі блокчейн.

В одній із розмов Білла Гейтса (співзасновника Microsoft), Чарлі Мангера (заступника голови Berkshire Hathaway) та Уорена Баффетта (американський бізнес-магнат, інвестор та голова та генеральний директор Berkshire Hathaway), глядачі отримали поєднання невизначеності, популярність та потенціал щодо біткойнів та блокчейну в одному реченні кожним із трьох ветеранів. Ось як це пройшло. Білл Гейтс: "Біткойн - це техно tour de force". Чарлі Мангер: "Я думаю, що це отрута для щурів". Уоррен Баффет: "Я думаю, що Чарлі або Білл мають рацію".

Розуміння поточного застосування та реалізації Blockchain є важливим, оскільки це допоможе визначити шлях зростання та ймовірні проблеми з технологією.

3 БЛОКЧЕЙН В УКРАЇНІ ТА ПОТЕНЦІАЛ OpenVAS ПРОТОКОЛУ

3.1 Блокчейн в Україні

До 2014 - незалежні експерти та розробники[10].

2014 - Сатоші сквер, перше Біткоїн посольство в СНД, Bitcoin Foundation Ukraine, перша конференція, перші публічні компанії.

2015 - нові публічні компанії, розпочалася дискусія із державою.

2016 - меморандум з державними органами (e-Auction 3.0), діалог із державою, великі конференції та хакатони.

2017 - поява більшості публічних компаній, ICO, продовження діалогу з держорганами.

2018 - заснована Асоціація Блокчейн України, запропонований законопроект з регулювання криптовалют, етап хаотичного розвитку ринку завершився.

32% компаній були засновані в 2017 році, 20% у 2016, 14% у 2018, 12% у 2015, по 8% - ті, що були засновані у 2014 та раніше. Більшість засновників представлених компаній прийшли до сфери блокчейну із програмування та розробки (38%); фінансів, інвестицій та трейдингу (38%); криптографії та криптовалют (32%); маркетингу та реклами (12%). Деякі компанії мають кількох фаундерів із різних сфер.

78% орієнтуються на ринок України та глобальний ринок, 16% - тільки на зовнішні ринки і лише одна компанія виключно на Український ринок.

26% компаній залучили венчурний капітал. Із них 37% - від українських інвесторів, та 63% - від іноземних.

56% компаній дуже тісно комунікують зі всіма учасниками блокчейн/крипто спільноти в Україні, 34% знають більшість, але із багатьма хотіли б познайомитись. Активна спільнота, до якої входять засновники

компаній, приватні підприємці, експерти та ентузіасти галузі налічує більше 350 учасників. Один захід в середньому відбувається на тиждень із теми блокчейну та криптовалют в Україні. Системні ініціативи, спрямовані на розвиток індустрії, вважають необхідними 60% представників ринку, фінансову підтримку та інвестиції - 48%, розширені освітні можливості - 44%, заходи та нетворкінг - 31% респонденти могли обрати декілька варіантів.

Україна потрапила в список 14 країн-лідерів по впровадженню блокчейна. У квітні минулого року уряд уклав угоду з американською компанією BitFury про переведення державних реєстрів на блокчейн-платформу. А в жовтні Міністерство аграрної політики і Агентство з питань електронного уряду запустили оновлений Державний земельний кадастр, який буде працювати на технології блокчейн.

Крім того, у вересні 2017 го Державне агентство з питань електронного урядування перевело на блокчейн систему держзакупівель «сетах», яка займається реалізацією арештованого, конфіскованого та заставного майна банкрутів.

Аналізуючи зарубіжну та вітчизняну джерельну базу дослідження визначимо пріоритетні сфери застосування блокчейн-систем в сучасних умовах цифровізації публічного врядування України.

3.1.1 Виборчий процес (блокчейн-системи стаціонарного та дистанційного голосування).

Існуючі системи так званого «електронного» голосування мають ряд недоліків, головним з яких є централізоване розміщення баз результатів, звідки здійснюється управління й застосовується контроль (виробляються методи/ форми) збирання даних, що унеможливлює перевірку коректності обробки результатів та підрахунок голосів ззовні. Непрозорість процедури забезпечення виборчого процесу не сприяє підвищенню рівня довіри результатів голосування. Такі системи недостатньо захищені як від маніпулятивного втручання з боку влади, так і від зовнішніх кібератак, тому й результати плебісциту можуть бути сфальсифіковані. Так, наприклад, через вразливість програмного забезпечення

«електронного» голосування, чисельних комп'ютерних помилок в Казахстані (2012 р.) та Нідерландах (2008, 2017 р.) організатори виборчого процесу були вимушені відмовитись від національних систем «електронного» голосування «Sailau» й «EVM» (Electronic Voting Machines), повертаючись до традиційного волевиявлення із застосуванням паперових бюлетенів та їх «ручного» досліджен-генеза підрахунку[11]. Зазначимо, що основними завданнями забезпечення ефективної організації процесу волевиявлення громадян є транспарентність, доступність та неможливість фальсифікувати його результати, які услішно розв'язує системи стаціонарного та дистанційного голосування, які побудовані на основі блокчейн-технологій які здатні стати ефективною альтернативою системам так званого «електронного» голосування. У більшості блокчейн-систем дистанційного голосування використовується розподілений публічний реєстр, який формує «цифрову скриньку (урну)» для бюлетенів, скористатись нею можуть громадяни незалежно від їх місця знаходження у будь-якій країні світу. В країнах ЄС та США блокчейн-системи вже активно використовуються в організації політичних процесах, так, наприклад у 2014 році за ініціативою датської партії «Ліберальний Альянс» технологія розподіленого реєстру використовувалась в процесі троведення внутрішнього голосування на партійних зборах в Копенгагені, що дозволило забезпечити належну прозорість процесу голосування . Натомість, у США в штаті Те- хас у 2016 на эїзді Лібертаріанської партї під час виборів кандидатів на ряд внутрішньопартійних посад. підрахунок голосів здійснювався за допомогою блок-чейн-системи голосування «Blockchain Technologies Corp». В Україні у 2016 році на базі відкритого програмного забезпечення платформи E-VOX (без- коштовна ліцензія Open Source) розроблено першу вітчизняну стаціонарну блокчейн-систему голосування «NaRada», яку успішно впроваджено у Одеській області місцевими радами Овідіополя, Крижанівки та Балти для проведення голосування депутатів на пленарних засіданнях, а також систему (портал) оприлюднення його результатів.

3.1.2 Блокчейн-системи розподіленого документообігу.

У грудні 2015 року урядом Естонії спільно в рамках проекту «BitNation» було впроваджено блок- чейн-система державного нотаріату «BitNation Public Notary» з надання послуг в режимі он-лайн, завдяки якій, громадяни мають можливість дистанційно одер- жувати нотаріальні послуги, візувати та ідентифікувати документи за допомогою цифрового підпису, користу- ватися сервісами інтернет-банкінгу. Сервіс «BitNation Public Notary» працює наступним чином: резидент завантажує PDF-документ, зміст якого «хешується» (шифрується для побудови унікальних ідентифікаторів вхідних наборів даних), після чого генерується ключ, користувач одержує нотаріально завірений документ. Таким чином, складовими транзакції блокчейн-систе- ми є хеш-функція, відкритий ключ і цифровий підпис. У 2017 році в США (штат Делавар) за ініціативою юридичної фірми Pilsbury Winthrop Shaw Pittman LLP спільно із стартапом «Symbiont» було презентовано подібну блокчейн-систему розподіленого документообігу для процесу реєстрації компаній, відстеження руху акцій, комунікацій та управління[12].

3.1.3 Захист персональних данник в сфері охорони здоров'я (блокчейн-системи реєстрації медичних даних).

В сучасних «електронних» системах які застосовуються у сфері охорони здоров'я, актуальною є проблема достовірності, надійності та належного зберігання медичних даних пацієнтів. Зазначимо, що з метою унеможливлення несанкціонованого доступу та внесення змін щодо інформації про пацієнтів державних та приватних закладах країн ЄС застосо- вуються блокчейн-системи реєстрації медичних даних, оскільки саме технологія розподіленого реєстру може дозволити накопичувати інформацію за все життя пацієнта. Такі блокчейн-системи дозволяють формувати клінічне резюме (історію хвороб) пацієнтів: результати лабораторних досліджень, діагнози, лікування. Причому, одержати доступ до такої інформації можливо лише за умови використання певного переліку довірених цифрових підписів лікаря та пацієнта. Окрім лікаря, доступ до медичної картки в таких блокчейн-системах можуть, з дозволу пацієнта, мати й представники страхової компанії, але тільки шляхом надання їм відповідного

сертифікату за допомогою технології смарт-контракту. В світовій практиці, починаючи з 2016 року, застосування блокчейн-систем в сфері охорони здоров'я набуло потужного розвитку. Наприклад, естонська блокчейн-система реєстрації медичних даних, яку впроваджено фондом «eHealth Foundatioп» в рамках проекту «Guardtime», забезпечує збереження, прозорість і цілісність медичної інформації, захищаючи її від несанкціонованої зміни або видалення, в тому числі в наслідок зовнішніх кібератак, системних збоїв, а також від наслідків комп'ютерних вірусів та шкідливого програмного забезпечення. Так, у разі зміни даних, система автоматично створює оновлений запис, дозволяючи відновити історію записів у разі неправомірного втручання. Таким чином, самі записи не зберігаються на блокчейні, а фіксуються лише серії їх хеш-значень, в яких і відображається інформація про зміни. Ціллю програми «Guardtime» є забезпечення захисту понад 1 млн цифрових записів в медичних картах пацієнтів.

Наприклад, у США Міністерство охорони здоров'я та соціальних служб (HHS) залучає науково-дослідницькі роботи, пов'язані з застосуванням блокчейн-систем в галузі охорони здоров'я[13]. Так, стартап «BitHealth» почав використання блокчейн-технології для того, щоб дати пацієнтам додаткові платіжні можливості при роботі з страховими компаніями. В Великобританії для Національної служби охорони здоров'я (NHS) на основі сервісів корпорації «Google» розроблено блок- чейн-систему реєстрації медичних даних «Verifiable Data Audit», яка регулює роботу з опрацювання інформації про пацієнтів закладами охорони здоров'я. Для захисту цього реєстру використана система «деревоподібного хешування» (дерево Меркле). В Нідерландах інноваційною корпорацією «REshape Center» у співпраці з банком «SNS Bank NV» та аудиторською компанією «Deloitte» розроблено блокчейн-систему, основою якої є банківський-додаток «PreScrypt» (аналог інтернет-банкінгу) на основі iDIN-Сервісу онлайн-автентифікації, яким користуються хронічно хворі пацієнти для придбання «повторюваних» ліків за цифровими рецептами.

3.1.4 Облік земельних ресурсів (блокчейн-системи земельного кадастру). Нагальні проблеми функціонування сучасних «електронних» систем обліку

земельних ресурсів вирішуються завдяки застосуванню блокчейн-технологій, які дозволяють суттево зменшити тривалість здійснення операцій, пов'язаних з набуттям (або припиненням) прав власності або користуванням земельними ділянками, зниження ризиків шахрайства, виникнення помилок при оформленні документів та здійсненні транзакцій, а також підвищення рівня надійності системи в цілому.

Світовий досвід застосування блокчейн-систем ведення земельних кадастрів налічує чимало успішних проектів, так, зокрема: Національною земельною службою Швеції запроваджено блокчейн-платформу «Chroma Way», в Гондурасі компанівєю «Factom» -розподілений рєєстр для реєстрації прав на землю, а у Гані -на платформі «Graphene» урядом дозволено реалізацію блокчейн-системи «Bitland», яка функціонує на основі базових маркерів «Bitshares» та «CADASTRAL» [14]. Зазначимо, що й в Україні з метою забезпечення надійної синхронізації даних, що унеможливить їх підміну в результаті зовнішнього втручання, а також для здійснення суспільного контролю за системою обліку земельних ресурсів Міністерством аграрної політики та продовольства України спільно з Державним агентством електронного урядування України та Transparency International презентовано оновлений Державний земельний кадастр, який відтепер працюватиме на цифровій технології «блокчейн».

3.1.5 Державні блокчейн-системи електронних торгів (аукціонів). Основним завданням використання блокчейн технологій в системах державних закупівель та аукціонів (електронних торгів), які ініціюються органами публічної влади, є необхідність забезпечити прозорість будь-яких транзакцій та захищеність від спотворення даних. Україна є новатором з проведення державних аукціонів, оскільки вперше у світовій практиці на основі сервісу «Open Market» державним підприємством "СЕТАМ за сприянням Державного агентства з питань електронного урядування України та компанії «BitFury Group» проведено електронні торги арештованим майном із застосуванням блокчейн-системи. Ще одним вітчизняним проектом з проведення електронних торгів є e-Auction 3.0- система електронних аукціонів, за якою органи публічної влади зможуть продавати

або здавати в оренду активи (землю, ліцензії, нерухомість). Державні аукціони на цій платформі на рівні місцевих ініціатив вже проведено в декількох регіонах України.

3.1.6 Потенціал Open VAS протоколу

Для вирішення постановленої задачі, тобто дослідження блокчейну та системи на базі OpenVASP, слід більш детально розглянути принцип роботи цієї системи.

VA (Virtual Asset) - це цифрове представлення вартості, якою можна торгувати або передавати в цифровому вигляді та використовувати для платежів чи інвестицій. Віртуальні активи не включають цифрові подання фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені в інших місцях рекомендацій FATF. Приклади: BTC, ETH.

VASP (Virtual Asset Service Provider) – це будь-яка фізична або юридична особа, на яку не поширюються дії інших рекомендацій, і як бізнес здійснює одну або декілька з наступних видів діяльності або операцій для або від імені іншої фізичної або юридичної особи: обмін між віртуальними активами та фіатними валютами; обмін між однією або кількома формами віртуальних активів; передача віртуальних активів; зберігання та / або адміністрування віртуальних активів або інструментів, що дозволяють контролювати віртуальні активи; участь та надання фінансових послуг, пов'язаних з пропозицією емітента та / або продажем віртуального активу[15]. Приклади: Coinbase, Bitfinex

Відповідно до Правила подорожей Рекомендації 16, організатори та бенефіціари всіх переказів цифрових коштів повинні обмінюватися ідентифікаційною інформацією. Правило застосовуватиметься до всіх VASP, фінансових установ та зобов’язаних осіб. Крім того, ініціатори та бенефіціари, які беруть участь у передачі, повинні мати можливість гарантувати точність інформації, яку вони надсилають іншому (див. рисунок 3.1 – VA транфер – перед «подорожжю»).

.

Рисунок 3.1 – VA транфер – перед «подорожжю»

В червні 2019 року Група розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ) випустила оновлене керівництво з «Віртуальні активи та постачальники послуг віртуальних активів», в якому містяться додаткові роз'яснення щодо того, як слід розуміти її рекомендації в контексті операцій з віртуальними активами. Впровадження новітніх рекомендацій в даний час розробляються в деяких країнах, але для більшості членів ФАТФ обізнаність про цю вимогу все ще перебуває на дуже ранній стадії. ФАТФ відстежує і надає рекомендації щодо запобігання відмивання грошей і фінансування тероризму з 2014 року. У 2018 році міжнародне суспільство прийняло зміни в свої рекомендації по визначенню «віртуальних активів» і ввів термін «постачальник послуг віртуальних активів» (VASP). Однак, впровадження деяких останніх вказівок є викликом для криптофінансової галузі, яка все ще зароджується. Рекомендація 16, яку часто називають "Правилом подорожей", представляє особливі виклики, вимагаючи від учасників галузі узгодити загальні стандарти. Вона вимагає, щоб будь-який VASP отримував, зберігав і передав інформацію про ініціатора та бенефіціара під час проведення віртуальних операцій з активами із зобов’язаними суб’єктами, як це визначено FATF (іншими VASPS, банками та фінансовими посередниками). Ця довідка окреслює відкритий протокол між VASPS щодо взаємного обміну інформацією про джерела та бенефіціара. Він

робить це повністю децентралізовано, використовуючи криптографічно безпечний одноранговий зв’язок та можливості чорного ланцюжка Ethereum для аутентифікації. Протокол Thes працює з будь-якою технологією блокчейну або розподіленої книги (DLT), яка використовується для базової передачі віртуальних активів. Це ставить конфіденційність переданих даних в центр дизайну (див. Рисунок 3.2 - VA транфер – після «подорожі»).

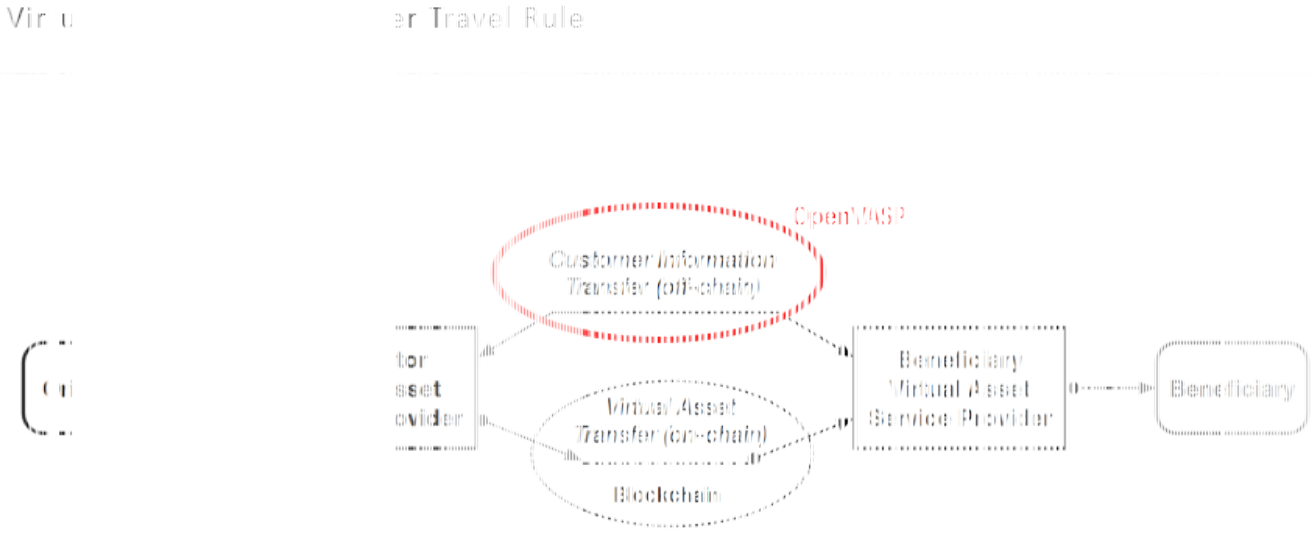

Рисунок 3.2 - VA транфер – після «подорожі»

При розробці цієї пропозиції щодо відкритого протоколу для полегшення дотримання правила подорожей FATF щодо віртуальних активів розробники керувалися наступними трьома принципами.

1) Дотримання правил подорожей

Встановіть спільний протокол зв'язку для VASPS для обміну інформацією про передачу віртуальних активів, як зазначено у вимогах FATF. Цей принцип включає:

а) загальний стандарт передачі даних для необхідної інформації про джерела та бенефіціара;

б) відповідний набір правил для полегшення обміну даними між VASPS.

2) Децентралізований підхід

Дотримуйтесь децентралізованого підходу, який дозволяє будь-яким двом VASPS використовувати протокол без згода або навіть знання будь-якої третьої сторони. Цей принцип включає, що протокол:

а) не вимагає VASP для отримання будь-якої форми членства або реєстрації в будь-якій третій сторони;

б) не вимагає використання центрального компонента в будь-який час;

В) ми припускаємо, що кожен VASP не має обов'язку ретельно відбирати інші VASPS, з якими він хоче працювати, дотримуючись підходу, заснованого на оцінці ризику.

3) Технологічний агностик

Переконайтесь, що протокол працює з будь-якою технологією блокчейну або розподіленої книги (DLT), яка використовується для базової передачі віртуального активу. Цей принцип включає в себе, що протокол:

а) не вимагає змін в базовому блокчейні / DLT;

б) не передбачає конкретних характеристик базового блокчейну / DLT (наприклад, існування унікального ідентифікатора або поля коментарів у транзакціях).

4) Дизайн

Переконайтеся, що протокол ставить конфіденційність переданих даних в центр свого дизайну. Цей принцип включає, що протокол:

а) вимагає надійної аутентифікації задіяного VASPS; вимагає надійного наскрізного шифрування між VASPS;

б) застосовує ідеальну пряму таємницю (захищаючи передані раніше дані від майбутніх компрометацій приватних ключів);

в) дозволяє двом VASPS передавати дані без відома третьої сторони. 3.1.7 Звернення до ідентифікації VASP та коду VASP

Протокол використовує блокчейн Ethereum як децентралізовану інфраструктуру відкритого ключа. Кожен учасник VASP повинен розгорнути стандартизований інтелектуальний контракт, який представляє його ідентичність на блокчейні, подібно до того, як би функціонував традиційний сертифікат відкритого ключа. Адреса Ethereum стандартизованого розгорнутого VASP визначається як ідентифікатор VASP, а останні 32 біти називаються кодом VASP. Обидва значення - це числа, кодовані як шістнадцяткові числа, які легко обробляти та читати людиною. Однак радіус "0x", який зазвичай використовується для позначення шістнадцяткового формату (див. рисунок 3.1 - Ідентифікатор
VASP).

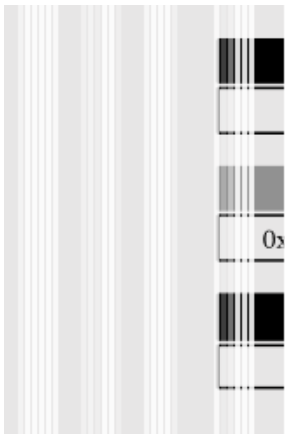

Рисунок 3.1 - Ідентифікатор VASP

3.1.8 Номер рахунку віртуальних активів (VAAN)

Спочатку бенефіціар хоче отримати віртуальні активи на гаманці, розміщеному VASP, і тому надає ініціатору інформацію про маршрутизацію, куди їх відправити. Потім ініціатор доручає своєму VASP передати віртуальні активи на основі інформації про маршрутизацію. У традиційних платіжних системах банківський рахунок з номером (наприклад, BIC / SWIFT, IBAN) використовується як інформація про маршрутизацію. У поєднанні з ідентифікаторами банку (наприклад, ми пропонуємо подібний, але децентралізований підхід у формі номера рахунку віртуальних активів (VAAN), який являє собою 24-символьний шістнадцятковий код, що включає 2-знакову

контрольну суму. Перші вісім символів відповідають VASP код, тоді як решта символів стосуються замовника. VAAN не повинен містити пробілів при електронній передачі. При друку його можна виразити групами з чотирьох символів, розділених одним пробілом для читабельності (див . рисунок 3.2 – Структура VAAN).

Рисунок 3.2 – Структура VAAN

Кожен VASP на власний розсуд визначає деталі того, як VAANS призначаються та використовуються їхніми клієнтами. Запропонована довжина 14 шістнадцяткових символів (56 біт) для конкретного клієнта номера VAAN надає кожному VASP досить великий адресний простір з 7,2 x 101 ідентифікаторами, дозволяючи достатньо місця, включаючи суєтні номери. VASP може за замовчуванням призначити кожному клієнту єдиний фіксований VAAN, подібно до того, як використовується традиційний номер банківського рахунку. Інший VASP може надавати кілька VAANS за запитом або обмежувати термін їх дії. Клієнти, які орієнтуються на конфіденційність, можуть навіть воліти використовувати VAAN лише один раз. Хоча VASP повністю вільно призначають VAANS своїм клієнтам у форматі, вони повинні гарантувати, що кожен VAAN однозначно присвоєний саме одному із своїх клієнтів. Цим забезпечується нормативна вимога щодо унікальної ідентифікації. Запропонований формат дозволяє легко обмінюватись VAAN (наприклад, електронною поштою) між

бенефіціаром та ініціатором, а також полегшує передачу віртуальних активів між VASP-VASP за межі відповідності FATF.

3.1.8 Контракт VASP

У цьому розділі викладена високорівнева специфікація контракту VASP, в якій основна увага приділяється найбільш важливим аспектам, необхідним для функціонування протоколу. Як згадувалося раніше, кожен VASP розгортає свій власний примірник контракту та приймає адреса розгортання контракту в якості ідентифікатора особистості і останні 32 біта в якості коду VASP (див. таблицю 3.1). Контракт включає відповідну інформацію про VASP (див. рисунок 3.3 – Смарт контракт) . Для більшої безпеки і полегшення поділу обов'язків повинні бути реалізовані різні ролі (наприклад, власник, адміністратор). Адреси, призначені цим ролям, можуть знову вказувати на смарт-контракти з кількома підписами для більшої безпеки. Однак сам контракт VASP повинен бути максимально простим і делегувати управління доступом і управління викликає контрактами і системам.

Рисунок 3.3 – Смарт контракт

Таблиця 3.1 - Атрибути контракту VASP

name	Юридична назва VASP
code	Остання 32-бітна адреса контракту VASP, що використовується як абревіатура для ідентифікації VASP
channels	Канали зв'язку, які VASP приймає для повідомлень(наприклад, Whisper, Email)

handshakeKey	Асиметричний відкритий ключ, що використовується для безпечно встановлювати сеанси
singingKey	Асиметричний відкритий ключ, що використовується для перевірки підписів повідомлень
owner	Адреса, призначена власником контракту VASP
administrator	Адреса, призначена для зміни атрибутів смарт-контракту
postal address	Атрибути поштової адреси VASP
email, website	Контактна інформація
trustedPeer	Довірений одноранговий VASPS
identityClaims	Ідентифікаційні вимоги

3.1.9 Потік протоколу

Протокол надає набір запитів та відповідей для полегшення структурованого спілкування між ініціатором VASP та бенефіціаром VASP, передаючи віртуальні активи від імені своїх відповідних клієнтів. Спочатку бенефіціар хоче отримати віртуальні активи на гаманці, розміщеному VASP бенефіціара, і тому надає ініціатору інформацію про маршрутизацію про те, куди їх відправити. Потім ініціатор доручає ініціатору VASP передати віртуальні активи. На етапі ініціації залучений VASP8 встановлює зв'язок та взаємно аутентифікує та авторизує один одного. На етапі передачі обмінюється інформацією про ініціатора / бенефіціара, передача отримує взаємне схвалення, а виконання на блокчейні повідомляється та підтверджується (див. рисунок 3.4 - Потік протоколу).

Рисунок 3.4 – Потік протоколу

Як приклад OpenVAS протоколу, розглянемо приклад додатку на базі blockchain. Існує три ноди: originator, beneficiary та administrator. За допомогою originator та beneficiary нод, клієнти моють змогу пересилати одне одному інформацію або кошти. Адміністратор, може або схвалити або відмінити їїх транзакції, у випадку, якщо VAAN не є дійсним або сумма переказу занатто велика та є підозрілою.

Рисунок 3.5 – Приклад додавку на базі OpenVAS протоколу

Поточна реалізація включає просте управління сеансами. В режимі асинхронізації сеанси ініціатора та бенефіціара створюються автоматично. У режимі синхронізації сеанси ініціатора створюються кодом хоста, а сеанси бенефіціарів – бібліотекою. Дані сеансу включають лише список отриманих повідомлень, але є можливість включити будь-який тип даних користувача в об’єкт сеансу. Дані сеансу зберігаються в пам'яті. Поточна реалізація забезпечує доступ до служби повідомлень низького рівня, яка дозволяє надсилати та прослуховувати нові повідомлення. Це дозволяє реалізувати інший механізм управління сеансом (наприклад, якщо ми хочемо зберігати дані сеансу в БД).

Розглянемо синхроний режим. Він дозволяє надіслати повідомлення VASP, а потім або дочекайтеся відповіді, або періодично опитуйте нові повідомлення. Кожен крок обробки повідомлень може включати деякі взаємодії з користувальницьким інтерфейсом для показу нових повідомлень користувачеві та очікування його рішення про наступні кроки обробки. Обробка повідомлення може бути відкладена на деякий час, поки користувач не визначиться з деталями. Він підходить для певної ручної обробки повідомлень, що включає користувача.

Асинхроний режим дозволяє реєструвати зворотний дзвінок для обробки кожного типу повідомлень VASP. Вся обробка повідомлень, крім початкового повідомлення-ініціатора, розміщується у зворотному дзвінку. Повідомлення

обробляється негайно, як тільки воно надійшло. Він підходить для певної обробки, коли нам не потрібні будь-які рішення користувача, і є деякі правила, як автоматично відповідати на кожен тип повідомлення.

Як бачимо, тестування данної блокчейн технології досить слкладне випробування, так як це досить нова система. Але на базі знань про функціональне, нефункціональне та специфічне для блокчену тесування, ми створили тестові сценарії. Для початку треба переірити, що ініціатор може створити транзакію за допомогою додатка (див. лістинг 3.1 - Сценарій для тестування додатку на базі OpenVAS протоколу – Створення транферу).

Scenario: Create transfeк with Request Session
GIVEN: The Originator landed on the Transfer screen (VASP-1)
AND The Beneficiary landed on the Transfer screen (VASP-2)
WHEN The Originator clicks on the "Create transfer" button
THEN The Originator sees the "Create transfer" pop-up displayed on "Transfer" screen
WHEN The Originator enters values to fields on the "Create transfer" pop-up on "Transfer" screen
field	value
originator	string
beneficiary	string
asset	string
anount	int
sender address	string
destination address	string
hash	int
AND The Originator clicks on the "Create" button
THEN The "Create transfer" pop-up is closed
WHEN The Originator refreshes the page
THEN The Originator sees the newly created record at the end of the transfer list
field	value

type	OUTGOING
id	int
updated	date
status	CREATED
session id	null

WHEN The Originator cliks on the record

THEN The Originator sees the advanced information about transfer

field	value
transaction ID	int
transaction type	OUTGOING
date	dd/mm/yyyy
session id	null
originatory name	string
originator vasp vaan	string
beneficiary name	string
beneficiary vasp vaan	string
asset	string
amount	int

WHEN The Originator selects "REQUEST_SESSION" from the "Transfer commands" drop-down list on the Transfer screen

THEN The Originator sees the confirmation pop-up with question and two buttoms "Confirm" and "Cancel"

WHEN The Originator clicks on the "Confirm" button

THEN The confirmation pop-up is closed

AND The Originator sees the updated transfer record on "Transfer" screen

field	value
type	OUTGOING
id	int
updated	date
status	SESSION_REQUESTED

| session id | 0x..ea1 |

AND The Beneficiary sees the newly received transfer record on the "Transfer" screen (VASP-2)

field	value
type	INCOMING
id	int
updated	date
status	SESSION_REQUESTED
session id	0x..ea1

WHEN The Beneficiary clicks on the appropriate record on the "Transfer" screen (VASP-2)

THEN The Beneficiary sees the advanced information about transfer

field	value
transaction ID	int
transaction type	INCOMING
date	dd/mm/yyyy
session id	null
originatory name	string
originator vasp vaan	string
beneficiary name	string
beneficiary vasp vaan	string
asset	string
amount	int

Лістинг 3.1 – Сценарій для тестування додатку на базі OpenVAS протоколу – Створення транферу

Також слід переірити, що отримувач може прийняти транзакію за допомогою додатка (див. лістинг 3.2 - Сценарій для тестування додатку на базі OpenVAS протоколу – Підтвердження транзакції отримувачем).

Scenario: Accept_session by Beneficiary

GIVEN: The Beneficiary landed on the Transfer screen (VASP-2)

AND The Beneficiary has the newly received transfer with Session_Requested status

AND The Originator landed on the Transfer screen (VASP-1)

WHEN The Beneficiary clicks on the appropriate record on the "Transfer" screen (VASP-2)

AND The Beneficiary selects "ACCEPT_SESSION" from the "Transfer commands" drop-down list on the Transfer screen

THEN The Beneficiary sees the confirmation pop-up with question and two buttoms "Confirm" and "Cancel"

WHEN The Beneficiary clicks on the "Confirm" button

THEN The confirmation pop-up is closed

AND The System displays the confirmation message "ACCEPT_SESSION was sent" with the option "Close" on the bottom of the screen

AND The Beneficiary sees the updated transfer record on "Transfer" screen with following details

field	value
type	INCOMING
id	int
updated	date
status	SESSION_CONFIRMED
session id	0x..ea1

AND The Originator sees the updated transfer record on "Transfer" screen (VASP-1) with following details

field	value
type	INCOMING
id	int
updated	date
status	SESSION_CONFIRMED
session id	0x..ea1

Лістинг 3.2 – Сценарій для тестування додатку на базі OpenVAS протоколу – Підтвердження транзакції отримувачем

3.1 Висновки за розділом

У данному розділі ми дослідили метод роботи Open VAS протоколу. З самого початку ви бачите, більш-менш, у назві - “OpenVASP” - це “відкрито”. Це означає відсутність захисту інтелектуальної власності (ІВ) - кожен може брати участь. І цією справою керують люди, які хочуть дотримуватися загального, але «відкритого» стандарту.

Оскільки данна система має відкритий код - це безкоштовно, щоб різні постачальники могли використовувати власні рішення. Все, що їм потрібно зробити, це узгодити базовий протокол. І вже ми бачимо, що багато хто стрибнув на "перемогу".

Асоціація (OpenVASP Association), фінансує впровадження з відкритим кодом, які не є конкурентами комерційним рішенням, але забезпечують ядро для тих, хто будує власні системи.

Важливо зазначити, що ці системи для крипто-транзакцій повинні бути прив’язані до системних систем постачальників послуг віртуальних активів (VASP). Вони повинні бути повністю вбудовані в існуючий системний ландшафт - особливо тому, що великі VASP мають настільки багато взаємодій і вимагають "прямої обробки". Так багато з них захочуть рішення, розроблені на замовлення. Ці “довідкові” реалізації з відкритим кодом можуть бути великою підмогою для тих, хто не просто хоче мати систему “під ключ”.

Тож “відкритість” дуже важлива. Деякі з перших систем дотримання правил подорожей були закритими та є приватними. Це протилежне тому, до чого націлений OpenVASP. Ми створили спільну мову, але без централізованого центру в середині. Таким чином, речі можуть залишатися якомога більше p2p. Не використовуючи своєрідний концентратор, забезпечується краща безпека. Децентралізована система набагато міцніша, і є набагато більше можливостей для інновацій. Протокол все ще застосовується до всіх, але кожен постачальник або VASP може вдосконалювати нові технології.

Зрештою, наявність різних конкуруючих постачальників призведе до більш привабливих пропозицій. Оскільки можуть існувати різні конкретні реалізації для різних випадків використання, це також буде стимулювати розробку вперед - підтримувати їх у всьому спектрі.

Треба пам’ятати - для VASP існує не лише один, єдиний випадок використання. Роздрібна торгівля значно відрізняється від рішень щодо зберігання для інституційних клієнтів. Ми очікуємо, що випадки використання будуть дуже різними - з різними повідомленнями для різних випадків.

ВИСНОВКИ

В результаті проведеного дослідження було виявлено основні проблеми та недоліки існуючих «електронних» систем в різних сферах публічного врядування, які пов'язані з їх технологічною недосконалістю, непрозорістю операцій (транзакцій), недостатньою захищеністю даних і процесів як від внутрішнього, так і від зовнішнього маніпулятивного втручання. Здійснено фактологічний аналіз зарубіжного та вітчизняного досвіду застосування блокчейн-технологій органами публічної влади з метою прогнозування подальших перспектив їх впровадження, врахування переваг та недоліків, визначення ефективних управлінських та технологічних рішень в умовах цифровізації публічного врядування. На основі аналізу світових тенденцій обгрунтовано пріоритетність впровадження в Україні державних блокчейн-систем стаціонарного та дистанційного голосування, розподіленого документообігу, реєстрації медичних даних в сфері охорони здоров'я, обліку земельних ресурсів, електронних торгів (аукціонів). Визначено основні переваги застосування блокчейн-систем органами публічної влади, що сприятиме підвищенню рівня довіри громадян до використання цифрових технологій в цілому, а саме: достовірність та надійність зберігання (одночасна синхронізація різних місцях розташування) даних, прозорість транзакцій та практично абсолютна захищеність інформації від спотворення й несанкціонованого вилучення (переміщення). У подальших наукових дослідженнях пропонується розглянути перспективні сфери застосування цифрової технології блокчейн: сервісна діяльність органів публічної влади, судочинство, управління правами власності, здійснення міграційного контролю, верифікація товарів й послуг, реєстрація даних щодо проходження кваліфікаційних випробувань, патентування, інтелектуальна власність, цифрова ідентифікація, логістика, оподаткування, облік руху бюджетних коштів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. OpenVASP: An Open Protocol to Implement FATF's Travel Rule for Virtual Assets - David Riegelnig, Bitcoin Suisse [Електронный ресурс]. - Режим доступу: https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf (Дата звернення 08.09.2020)

2. Challenges in Testing Blockchain Application [Електронный ресурс]. - Режим доступу: https://medium.com/@LipikaDugar/challenges-in-testing-blockchain-application-ca8103f6fc81 (Дата звернення 10.09.2020)

3. Overview of the Blockchain Industry in Ukraine [Електронный ресурс]. - Режим доступу: https://www.slideshare.net/DarinaMatkovska/overview-of-the-blockchain-industry-in-ukraine-145284361 (Дата звернення 11.09.2020)

4. Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets. [Електронный ресурс]. - Режим доступу: www.fon.hum.uva.nl. (Дата звернення 11.09.2020)

5. Smart contract slow [Електронный ресурс]. - Режим доступу: http://www.multichain.com/blog/2015/11/smart-contracts-slow-blockchains/ (Дата звернення 09.09.2020)

6. Використання блокчейн-систем органами публічної влади: український та зарубіжний досвід [Електронный ресурс]. - Режим доступу: http://academy.gov.ua/infpol/pages/dop/2/files/66072efa-2c85-4464-bee2-da0f3d79bef4.pdf (Дата звернення 14.09.2020)

7. Control smart home devices - iPhone & iPad - Google Assistant Help [Електронный ресурс]. - Режим доступу: https://support.google.com/assistant/answer/7540702?co=GENIE.Platform%3DAndroid&oco=0 (Дата звернення 15.09.2019)

8. Меморандум про взаєморозуміння та співробітництво між міністерством юстиції України, Міністерством аграрної політики та продовольства України, Державним агенством з питань електронного урядування Україниб громадською організаціюTransparency International Україна та Бітфурі Холдінг [Електронный

ресурс]. - Режим доступу: https://ti-ukraine.org/wp-content/uploads/2017/06/MEMO-SIGNED_2017_06_16.pdf (Дата звернення 15.09.2020)

9. Державний земельний кадастр перейшов на технологію Blockchain [Електронный ресурс]. - Режим доступу: https://land.gov.ua/dezhavnyi-zemelnyi-kadastr-pereishov-na-tekhnolohiiu-blockchain (Дата звернення 15.09.2020)

10. Google's DeerMindplans bitcoin-style health record tracking for hospitals. [Електронный ресурс]. - Режим доступу: htps: //www.theguardian. com / fechnology / 2017 / mar / 09 / google-deepmind-health- records-tracking-blockchain-nhs-hospitals. (Дата звернення 29.09.2019)

11. Blockchain for health care and your banking card. [Електронный ресурс]. - Режим доступу: http://radboudreshapecenter.com/blog/blockchain/. (Дата звернення 02.10.2020)

12. TheLandRegistryintheblockchain-testbed. [Електронный ресурс]. - Режим доступу: https://chromaway.com/papers/Blockchain_Landregistry_ Report_2017.pdf. (Дата звернення 02.10.2020)

13. Honduras to build land title registru using bitcoin article technology. [Електронный ресурс]. - Режим доступу: https://in.reuters.com/ (Дата звернення 06.10.2020)

14. . Белая Церковь переходит на e-Auction 3.0. - Режим доступу: : http://gesellberg.com/ru/біла-церква-переходить-на-e-auction-3-0 (Дата звернення 04.11.2020)

15. Екатерина Ядова. Блокчейн в образовании. Выступление на международной образовательной конференции %#EdCrunch 2016. [Електронный ресурс]. - Режим доступу: https://fte-st.ru/ reports/edcrunch-2016-results. (Дата звернення 04.11.2020)