ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Вдосконалення процесу обліку нерухомості за допомогою технології блокчейн»

на здобуття освітнього ступеня магістра
зі спеціальності 121 Інженерія програмного забезпечення
(код, найменування спеціальності)
освітньо-професійної програми «Інженерія програмного забезпечення»
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Євген ЄРМОЛЕНКО
(підпис)

Виконав: здобувач вищої освіти групи ПДМ-62
Євген ЄРМОЛЕНКО

Керівник: Олена НЕГОДЕНКО
к.т.н., доцент

Рецензент: _____
науковий ступінь, вчене звання *Ім'я, ПРІЗВИЩЕ*

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення

Ступінь вищої освіти Магістр

Спеціальність 121 Інженерія програмного забезпечення

Освітньо-професійна програма «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____ Ірина ЗАМРІЙ
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Єрмоленко Євгену Михайловичу

1. Тема кваліфікаційної роботи: «Вдосконалення процесу обліку нерухомості за допомогою технології блокчейн»

керівник кваліфікаційної роботи Олена НЕГОДЕНКО, к.т.н., доцент,

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023 р. № 145.

2. Строк подання кваліфікаційної роботи «29» грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, переваги технології блокчейн, вдосконалення процесу обліку нерухомості

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Проаналізувати проблематику процесів обліку нерухомості в Україні та світі.

2. Дослідити переваги та недоліки технології блокчейн при роботі з інформаційними системами.

3. Розробити інформаційну систему, що усуває можливість недобросовісного запису в реєстр у розглянутих сценаріях.

5. Перелік ілюстративного матеріалу: *презентація*

1. Аналіз існуючих рішень обліку нерухомості та їх моделей.
2. Алгоритм внесення запису в реєстр.
3. Приклад отримання прав доступу на запис.
4. Діаграма розгортання мережі блокчейн.
5. Діаграма компонентів системи обліку нерухомості.

6. Дата видачі завдання «19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	19.10-04.11.23	
2	Аналіз проблематики процесів обліку нерухомості	05.11-13.11.23	
3	Дослідження переваг та недоліків технології блокчейн	14.11-26.11.23	
4	Розробка інформаційної системи	27.11-03.12.23	
5	Оформлення роботи	04.12-20.12.23	
6	Розробка демонстраційних матеріалів	21.12-29.12.23	

Здобувач вищої освіти _____ Євген ЄРМОЛЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Олена НЕГОДЕНКО
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 63 стор., 1 табл., 11 рис., 33 джерел.

Мета роботи – підвищення рівня безпеки системи обліку нерухомості шляхом автоматизації процесів за допомогою технології блокчейн.

Об'єкт дослідження – автоматизація процесів обліку нерухомості.

Предмет дослідження – технології блокчейн.

Короткий зміст роботи: У роботі проведено дослідження переваг та недоліків технології блокчейн при роботі з інформаційними системами. Проаналізовано проблематику обліку нерухомості в Україні та світі. Розроблено інформаційну систему, що усуває можливість недобросовісного запису в реєстр у розглянутих сценаріях.

КЛЮЧОВІ СЛОВА: РЕЄСТР НЕРУХОМОСТІ, БЛОКЧЕЙН, РОЗУМНІ КОНТРАКТИ, HYPERLEDGER FABRIC.

ABSTRACT

Text part of the master's qualification work: 63 pages, 11 pictures, 1 table, 33 sources.

The purpose of the work – to improve the security level of the real estate accounting system by automating processes using blockchain technology.

Object of research – automation of real estate accounting processes.

Subject of research – blockchain technology.

Summary of the work: the work investigates the advantages and disadvantages of blockchain technology when working with information systems. The problems of real estate accounting in Ukraine and the world are analyzed. An information system has been developed that eliminates the possibility of unfair entry into the register in the scenarios considered.

KEYWORDS: REAL ESTATE ACCOUNTING, BLOCKCHAIN, SMART CONTRACTS, HYPERLEDGER FABRIC.

ЗМІСТ

ВСТУП……..…….. 09
РОЗДІЛ 1 АНАЛІЗ ПРОЦЕСІВ ОБЛІКУ НЕРУХОМОСТІ ……..... 13
1.1 Проблематика обліку нерухомості в Україні ……... 13
1.2 Проблематика обліку нерухомості в зарубіжних країнах ……... 15
1.3 Рішення обліку нерухомості на технології блокчейн ……. 18
РОЗДІЛ 2 АНАЛІЗ ТЕХНОЛОГІЇ БЛОКЧЕЙН…….…… 22
2.1 Аналіз основних концепцій технології блокчейн……. 22
2.2 Аналіз основних концепцій розумних контрактів .……. 29
2.3 Аналіз блокчейн платформи Hyperledger Fabric ….……. 31
2.3.1 Блокчейн мережі Hyperledger Fabric…….…. 33
2.3.2 Розумні контракти Hyperledger Fabric ……..….. 34
2.3.3 Особливості розподіленого реєстру Hyperledger Fabric…... 35
2.3.4 Безпека Hyperledger Fabric……..…… 38
2.4 Аналіз існуючих математичних методів для покращення безпеки обліку нерухомості за допомогою технології блокчейн …….. 43
РОЗДІЛ 3 РОЗРОБКА СИСТЕМИ ОБЛІКУ НЕРУХОМОСТІ НА ТЕХНОЛОГІЇ БЛОКЧЕЙН ……..… 46
3.1 Проєктування архітектури інформаційної системи ……...…. 46
3.2 Розгортання інформаційної системи…….……. 47
3.3 Сценарії доступу до реєстру …….……. 52
ВИСНОВКИ…….. 57
ПЕРЕЛІК ПОСИЛАНЬ…….. 58
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) …… 62

ВСТУП

Стрімкий розвиток інформаційних технологій та діджиталізація країн робить актуальним питання покращення процесів роботи з інформацією, зокрема заміни паперової документації на цифрову. Переведення публічних реєстрів у цифровий формат дозволяє не тільки більш ефективно отримувати інформацію, а й зменшувати вплив людського фактору, насамперед бюрократизацію процесів та ймовірність помилок.

Процес цифровізації тісно пов’язаний з інформаційною безпекою. Внесення змін в реєстри особами, які не мають на це право, може призвести до порушення основних прав громадян, зокрема права власності.

Проблемою процесу реєстру нерухомості в Україні є те, що згідно з законодавством, право власності настає лише після реєстрації[1]. Не дивлячись на наявність укладеної угоди, набуття права власності може так і не настати. Процес реєстрації має здійснити реєстратор, на якого покладено обов’язки перевірки наданих документів та відсутності обтяжень об’єкту нерухомості. При роботі з реєстром існує ризик недобросовісного використання повноважень (наприклад реєстрації віртуального об’єкту[2]) або вчинення помилки.

Право власності на незавершене будівництво – це ще одна проблема, з якою стикаються громадяни, які вже сплатили за власну майбутню житлову площу. Доки об’єкт нерухомості не буде зареєстрований, право власності під час будівництва не може бути гарантовано в повному обсязі[1]. Здійснення записів про права до реєстру недобудованої нерухомості наразі не передбачено.

В Україні процес переведення реєстру нерухомості у цифровий формат почався ще в 2013, а з 2016 року нотаріуси отримали право безпосередньо робити запис, проте процес реєстрації та доступу громадян до реєстру не став прозорішим[3].

Метою дослідження є підвищення рівня безпеки системи обліку нерухомості шляхом автоматизації процесів за допомогою технології блокчейн. В процесі дослідження вирішувалися такі завдання:

– проаналізувати проблематику процесів обліку нерухомості;
– дослідити переваги технології блокчейн при роботі з інформаційними системами;
– підвищити безпеку процесу обліку нерухомості шляхом розробки автоматичної інформаційної системи на технології блокчейн.

Технологія блокчейн може бути розглянута як рішення для внесення записів у цифрові реєстри, які неможливо змінити. В даному контексті блокчейн можна охарактеризувати як розподілену базу даних, запис до якої можуть робити лише авторизовані та наділені відповідними правами користувачі, а сам запис повинен бути перевірений та підтверджений іншими учасниками. Якщо недобросовісний користувач матиме на меті внести хибну інформацію, такий запис не буде верифікований і не потрапить до реєстру.

Об’єктом дослідження є автоматизація процесів обліку нерухомості. Для зменшення впливу людського фактору досліджувалась можливість перенесення процесів задіяних під час реєстрації на технологію блокчейн за допомогою розумних контрактів.

Предметом дослідження є технологія блокчейн як розподілена база даних, яка гарантує незмінність інформації. Блокчейн надає різноманітні можливості для організації процесу запису даних шляхом впровадження підходящих для вирішення проблеми правил додавання записів. Розглянуто переваги і недоліки окремих видів блокчейну.

Використовувались наступні методи наукового дослідження:

– теоретичний, зокрема використовувалися теорії, гіпотези, моделювання інформаційної системи;
– емпіричний, зокрема проведено дослідження переваг технології блокчейн Hyperledger Fabric для використання в побудованій інформаційній системі управління реєстрами;

Удосконалено безпеку при роботі з реєстрами нерухомості в сценаріях можливостей вчинення неправомірних дій недобросовісними учасниками

процесів реєстрації, а також внесення реєстраційних дій щодо об’єктів, які мали обтяження та не мали прав бути об’єктами таких дій.

Побудовано інформаційну систему управління реєстрами з використанням технології блокчейну, яка дозволяє перенести або створити реєстри в середині мережі. При цьому система підтримує наявні сховища існуючих реєстрів та надає можливість змінювати технології відповідних сховищ. Також побудована система впроваджує можливість використання існуючих програмних засобів, які мають API для роботи з реєстрами, шляхом інтеграцій таких засобів за допомогою розумних контрактів.

До публікації в матеріалах наукової конференції подано наступні тези:

1. Єрмоленко Є.М. Негоденко О.В. Покращення безпеки реєстру нерухомості за допомогою технології блокчейн // Реформування економіки України як фактор забезпечення сталого розвитку : Матеріали XIII Всеукраїнської наукової студентської інтернет-конференції. –Чернівці: ЧТЕІ ДТЕУ. – 2023р. – С.130.
2. Єрмоленко Є.М. Негоденко О.В. Перспективи реєстрів на технології блокчейн // Реформування економіки України як фактор забезпечення сталого розвитку : Матеріали XIII Всеукраїнської наукової студентської інтернет-конференції. –Чернівці: ЧТЕІ ДТЕУ. – 2023р. – С.133.

Усунено можливість недобросовісного запису в реєстр у розглянутих сценаріях на відміну від інших систем завдяки автоматизації процесів з використанням розумних контрактів.

На основі побудованої інформаційної системи можливо створювати інфраструктуру не лише для реєстрів нерухомості, а і для будь-яких державних чи приватних компаній. Технологія блокчейну гарантує прозорість інформації, яка зберігається в системі, оскільки записи ініціатора змін, час та самі зміни, постійно зберігаються в системі. Процес видалення записів також залишається в історії, що надає можливість відслідкувати ланцюжок внесених змін. Дані записи зберігаються у розподіленому сховищі, що нівелює можливість фізичної втрати бази даних. Розроблена інформаційна система дозволяє доступ лише

авторизованим учасникам із гнучкою системою налаштувань, а також дозволяє забезпечувати різний рівень автономності як на рівні всієї системи, так і окремих її компонентів – від повної автономії до широкої децентралізації.

1 АНАЛІЗ ПРОЦЕСІВ ОБЛІКУ НЕРУХОМОСТІ

1.1. Проблематика обліку нерухомості в Україні

При отриманні послуг у сфері державної реєстрації речових прав на нерухоме майно громадяни України стикаються з цілою низкою проблем[4], при чому не тільки під час здійснення запису до реєстру, а й при отриманні інформації звідти[5]. Проблеми обліку під час реєстрації нерухомості в основному виникають через непрозорість процесів та людський фактор (в тому числі недобросовісність) та являються перепоною на шляху до здійснення права власності громадянами [1, 2, 6, 7].

Для отримання інформації з Державного реєстру прав, необхідно пройти цілу процедуру:

- подати заяву, яка далі зберігається у суб’єкта владних повноважень, відповідального за дії з реєстром (реєстратор);
- реєстратор повинен встановити особу заявника та внести заяву в базу даних. Якщо заявник являється представником іншої особи, реєстратор повинен перевірити обсяг повноважень такої особи, тобто взаємодіяти із іншою інформаційною системою через портал електронних сервісів ;
- реєстратор має перевірити наявність сплати адміністративного збору за відповідну дію[5].

Для отримання виписки, необхідно задіяти декілька інформаційних систем, а також працю людини, яка може незалежно від причини виконати неправомірну дію або допуститися помилки під час роботи.

Проблеми обліку нерухомості мають також і юридичний характер, оскільки, згідно з законодавством, права на нерухоме майно настають лише після державної реєстрації. Якщо контрагенти вчинили правочин купівлі-продажу, міни або дарування, права на об’єкт нерухомості ще не набуваються[1]. З моменту вчинення правочину до здійснення реєстрації може пройти тривалий час, а

наявність зовнішніх факторів, таких як наявність третіх осіб або потрапляння об’єкту нерухомості до реєстру обтяжень, може завадити реєстрації, а отже, і набуттю права власності.

Проблематика набуття права власності на новостворене нерухоме майно полягає в тому, що рішення про введення в експлуатацію приймаються вже після повної побудови об’єкту. Відповідна комісія встановлює чи належить новостворена будівля до об’єкту нерухомості та чи відповідає вона будівельним стандартам з усіма належними правами на таке будівництво. Право власності на такий об’єкт настає лише після державної реєстрації. Будівництво є складним процесом, який складається із певних етапів та може призводити до негативних економічних наслідків у випадку відмови в державній реєстрації. Підвищенню прозорості процесу прийняття об’єкту в експлуатацію та подальшій державній реєстрації міг би сприяти запис та фіксація кожного з етапів будівництва. Якщо наступний етап повинен містити попередній, який засвідчений відповідним органом, прийняття об’єкту в експлуатацію могло би відбуватися після виконання останнього етапу будівництва, а наявні недоліки виправлені на попередніх етапах, зменшуючи ризики появи цих недоліків після завершення будівництва.

Механізм реєстрації нерухомого майна має ґрунтуватися як на власних, так і на правових принципах. Серед таких принципів є справедливість, внутрішнє переконання людини, принцип захисту від недобросовісної інформації, доступності інформації, захисту інформації. Проблеми доступності і захисту інформації є найбільш обговорювані[6]. Відзначається, що разом із змінами законодавства має змінюватися й інформаційна система, яка повинна бути достатньо гнучкою в управлінні, щоб робити зміни відповідно до вимог законодавства.

Ще однією проблемою обліку нерухомості є постійна змінюваність органів, які мають право проводити дії над об’єктами нерухомості. Так, раніше реєстрацію здійснювали Бюро технічної інвентаризації, потім Державна реєстраційна служба. Під час переходу повноважень від одного органу до іншого існують проблеми при передачі реєстрів, в даному випадку проблема призвела до одночасного існування

двох реєстрів нерухомості[2].

Проблема існування двох реєстрів, які мають здійснювати дії над одним і тим об’єктом, призводить до появи віртуальних об’єктів – таких, які існують лише в документах. Недоліки законодавства або недобросовісні дії суб’єктів владних повноважень можуть сприяти реєстрації неіснуючих об’єктів та настанню економічних збитків для контрагентів. При чому притягти до відповідальності таких суб’єктів владних повноважень майже неможливо[2].

Діяльність недобросовісних учасників процесу реєстрації нерухомого майна пов’язана зокрема з наявністю таких передумов:

– відсутності покарання недобросовісних суб’єктів владних повноважень через складність доведення до обвинувального вироку в таких категоріях справ;
– відсутності чітких вимог до реєстраторів щодо приміщень, де зберігаються документи та ведеться діловодство;
– часові обмеження в здійсненні реєстрації та великий обсяг роботи з документами для перевірки відповідних прав на вчинення дії[2].

1.2. Проблематика обліку нерухомості в зарубіжних країнах

Описані проблеми обліку нерухомості характерні не лише для нашої країни. Над проблемами вірогідності корупційної складової в процесі реєстрації нерухомості, а також для мінімізації людського фактору, працювали як країни, що розвиваються, так і розвинені країни.

Окремою проблемою для Європейського союзу (далі ЄС) були труднощі громадян країн-членів союзу купувати нерухомість в інших країнах, які підривали засади відкритості кордонів між учасниками ЄС. Основні виклики стосувалися:

– недостатньої прозорості процесів між власниками нерухомості та покупцями (орендарями);
– високих комісій посередників;
– неправдивих описів об’єктів нерухомості, їх якості та інших факторів, які суттєво впливають на ціну об’єкту;

- постійною змінністю баз даних органів, які обслуговують інформаційні системи;
- високих витрат на підтримку інформаційних систем;
- високої трудомісткості процесу збору та перевірки необхідних юридичних документів. Даний процес міг займати місяці;
- непрозорістю прав власності, різноманітності податкових видатків;
- людського фактору, який призводив до недобросовісних дій та знищення інформації[8].

Операції з нерухомістю в країнах ЄС починаються з найму посередника, агента з нерухомості, який допомагає здійснювати пошук об'єкту нерухомості для укладення правочину купівлі чи оренди. Наявність посередника є обов'язковою вимогою в Бельгії, Німеччині, Ірландії та Франції[9]. Необхідність залучення посередників та їхні ролі залежить від системи, яка діє в країні:

- відповідно до Латинської нотаріальної системи, яка діє в Західній Європі, залучається нотаріус, обов'язками якого є: перевірка контрагентів та їх прав при вчиненні правочину, надання консультацій стосовно угоди та сприяння правам продавця і покупця, надання консультацій стосовно прав власності. Одним із основних обов'язків є забезпечення законності переходу права власності. Нотаріуси є обов'язковими учасниками процесу переходу права власності на нерухомість в Нідерландах, Польщі та Швейцарії. В Іспанії наявність нотаріуса не є обов'язковою за винятком певних випадків;
- в Центральній та Східній Європі до угоди мають бути долучені юристи, наприклад така умова діє в Чехії та Угорщині;
- в Англії та Ірландії діє система ліцензованих посередників. Такі особи зобов'язані надавати консультації стосовно угоди, податків, законодавства та несуть відповідальність за невиконання своїх обов'язків;
- країни Північної Європи долучають ріелторів або юристів до укладення угоди з реєстрації нерухомості[9].

Після підписання угоди вона може бути зареєстрована в земельному реєстрі відповідним суб'єктом владних повноважень. Реєстрація угоди забезпечує правомірність угоди. В різних країнах свій орган, який відповідає за реєстр. В Португалії, Іспанії, Бельгії, Нідерландах та Литві – це незалежний державний орган. В Німеччині, Польщі та Австрії – це суди. В таких країнах як Естонія, Польща та Бельгія для засвідчення права власності на нерухомість не обов'язково проводити реєстрацію, за винятком обов'язкової реєстрації іпотеки в Естонії. В Німеччині, Нідерландах та Швейцарії така реєстрація нерухомості є обов'язковою вимогою. Реєстрація угоди також не обов'язкова в Італії, Люксембурзі, Португалії, Франції та Бельгії, оскільки навіть усна угода вважається законною, але при бажанні зареєструвати, має бути заключено та посвідчено договір. У Словенії, Словаччині, Австрії та Чехії для реєстрації угоди контрагенти повинні мати сертифікат від нотаріуса або суду, який посвідчує підписи[9].

Бразилія в XIX сторіччі затвердила систему Torrens, основою якої є публічна реєстрація права власності, але на практиці її не використовувала. Більша частина нерухомості в країні лишається незареєстрованою, а відсутність сучасної системи реєстрації прав власності нерухомості є передумовою появлення корупції та шахрайства в операціях з нерухомістю[10].

Найбільш успішними в організації реєстрів нерухомості є такі країни як Кіпр, США, Великобританія, Нідерланди, Швеція, оскільки мають гарно структуровані департаменти, які відповідають за реєстрацію нерухомості. Дані країни найбільш відкриті для застосування інновацій у сфері реєстрації нерухомості. Країни з меншою структурованістю реєстрів нерухомості використовують застарілі практики або системи, є бюрократичними, мають складні процеси, корупцію та шахрайські операції з нерухомістю. До таких країн відносяться Греція, Україна та інші. Існують також і країни, які або взагалі не мають реєстру або він не ефективний. Країни цієї категорії мають ті ж проблеми, що і країни з попередньої, але рівень корупції та шахрайських операцій більш масштабні. До таких країн можна віднести Гану, де більш ніж 80 відсотків

власників нерухомості не мають офіційного підтвердження права власності на нерухомість та мають переважно усні угоди[11].

Незважаючи на те, що ринок нерухомості є найбільшим класом активів у світі та відіграє дуже важливу роль в економіці, впровадження нових технологій відчуває опір на своєму шляху розвитку. Різноманітні системи роботи з нерухомістю призводять до дуплікації даних в різних системах. Корупція та людський фактор є також проблемами країн, в яких процеси обліку нерухомості залишаються непрозорими, складними та дороговартісними[12]. Зазначене призводить до висновку, що зарубіжні країни мають таку ж проблематику обліку нерухомості як і Україна, що здебільшого виражається у непрозорості процесів та людському факторі.

1.3. Рішення обліку нерухомості на технології блокчейн

Для зменшення вірогідності корупційної складової в процесі реєстрації нерухомості, а також для мінімізації людського фактору, такі країни як Грузія, Швеція, Гана, Бразилія, Гондурас, Індія та Японія розпочали працювати над переведенням реєстру нерухомості на технологію блокчейн.

На прикладі Грузії можна відмітити, що перед застосуванням блокчейну, процес реєстрації нерухомості вже був реформований та позбавлений корупційної складової[10]. Впроваджена технологія блокчейн дозволила підвищити довіру до реєстру, а також покращити прозорість процесів реєстрації. Система була представлена як гібридний блокчейн, де записи про об’єкти зберігаються в приватному блокчейні, а потім публікуються до публічного. Адмініструється система спеціальним державним органом.

Досвід зарубіжних країн показує, що однією із найважливіших проблем реєстрів є проблема прозорості[13]. Для прикладу, в Сербії пропонується модернізувати процес реєстрації нерухомості за допомогою технології блокчейн[14]. Розглядається створення публічного реєстру на базі блокчейну Ethereum.

Цілий ряд іноземних авторів розглядає застосування блокчейну[8, 10, 11 15, 16]. Серед прикладів перших держав, які застосували блокчейн, можна виділити ОАЕ, які планують зекономити 1,2 млрд євро завдяки реєстрації транзакцій державних процесів у блокчейні. Окрім покращення процесів під час реєстрації нерухомості, також наводяться приклади покращень у сфері розрахунків між контрагентами за допомогою блокчейну, токенізації активів, використання розумних контрактів для здешевлення операцій[8].

Швеція в 2016 році розпочала проєкт з дослідження переваг застосунків, які використовують технологію блокчейн, під час здійснення транзакцій у сфері нерухомості. За оцінками, Швеція повинна зекономити 100 млн. євро щорічно після переведення реєстру нерухомості на блокчейн.[8]

Нідерланди також мають декілька тестових проєктів: проєкт відкритих даних з кадастру, урядовий проєкт покращення процесів та проєкт з логістики[8].

Бразилія запустила пілотний проєкт реєстру нерухомості на блокчейні для вирішення проблеми прозорості та безпеки під час вчинення операцій з нерухомістю. Заплановано впровадження системи на технології блокчейн, яка буде копіювати офіційно діючу систему з метою реєстрації процесів реєстрації та передачі нерухомості. Дане рішення має за метою створити сервіс для реєстрації операцій з нерухомістю від імені державних установ [8].

Уряд Японія розробляє проєкти на блокчейні для реєстрації прав, менеджменту та уніфікації процесів пов’язаних з правом власності. Головна ціль уніфікувати дані об’єктів, які не мають права власності, або власники яких невідомі[8].

Гондурас одним із першим серед країн заявляв про наміри розробити платформу для реєстрації нерухомості на технології блокчейн. Але через нетехнічні причини був скасований[8].

Гана з 2014 року працює над проєктом з використанням блокчейну, який покликаний вирішити проблему реєстрації нерухомості, оскільки більшість об’єктів нерухомості не мають належної реєстрації. Вони використовують OpenLedger для створення публічного децентралізованого блокчейну[8].

В 2017 році округ Кук, штат Іллінойс, США, брав участь у проєкті з дослідження переваг та недоліків впровадження блокчейну в реєстр нерухомості. Проєкт був успішним і наразі штат Іллінойс планує використовувати дане рішення для впровадження реєстру нерухомості на рівні держави[11].

В таблиці 1.1 список країн, які або вже використовують, або мають намір використовувати блокчейн в діяльності державних або недержавних органів.

Таблиця 1.1.

Країни, які використовують або мають намір використати блокчейн у своїх реєстрах

Країна	**Проєкт на основі технології блокчейн**
Австралія	Біржа Australian Securities Exchange (ASX)
Бразилія	Сервіс реєстрації нерухомості на блокчейні
Великобританія	Система соціальних виплат
Гана	Реєстр нерухомості
Грузія	Реєстр нерухомості
Естонія	Електронна ідентифікаційна система
Нідерланди	Пілотний проєкт у сфері нерухомості
ОАЕ	Концепція «Розумне місто Dubai»
Сінгапур	Система транскордонних міжбанківських платежів
США	Біржа медичних даних
Франція	Платформа для торгівлі цінними паперами
Швейцарія	Цифрова ідентичність
Швеція	Смарт-контракти для реєстрації нерухомості

Кожен блокчейн містить свої переваги та недоліки. Слід зважати на такі фактори: чи необхідна повна децентралізація, яка пропускна здатність має підтримуватися, наскільки легко система масштабується. Перед вибором конкретної технології, слід більш детально приділити увагу функційним та

нефункційним вимогам. Так, австралійська біржа ASX відмовилась від впровадження блокчейну після семи років розробки, оскільки система не підтримувала необхідні функційні вимоги[17]. В той же час, Естонія досягла успіхів у впровадженні власного розробленого KSI блокчейну, який веде облік усіх внесених змін до розподіленої бази даних, яка працює з системою цифрової ідентичності користувача[18].

В Україні запущено пілотний проєкт з переведення Держгеокадастру на блокчейн, але на сьогоднішній день розробка припинена через нестачу фінансування[19]. Виникають питання стосовно поставленої технічної задачі та яким чином була зроблена оцінка проєкту. Все ж таки, плани щодо подальшої розробки залишаються, а під час роботи проєкту зібрано відгуки, які будуть втілені разом з концепцією, за якою реєстр має бути максимально автоматизованим та відповідати цілям національного проєкту «Держава у смартфоні», також планується врахувати досвід зарубіжних країн[20].

В Україні окрім ініціативи з блокчейном, створено декілька інформаційних систем для реєстру нерухомого майна: Реєстр права власності на нерухоме майно, а згодом Державний реєстр речових прав на нерухоме майно, управління яким здійснює державне підприємство «Національні інформаційні системи» (далі НАІС)[6].

ДП «НАІС» складається з головного підприємства та 22 регіональних філій в обласних центрах України та обслуговує реєстри нотаріусів, нормативно-правових актів, прав на нерухоме майно, системи виконавчого провадження, розробляє програмні інтерфейси (API) до реєстрів[22].

2 АНАЛІЗ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1. Аналіз основних концепцій технології блокчейн

Основою мережі блокчейн є розподілений реєстр, до якого записується кожна підтверджена транзакція, що відбувається в цій мережі. Даний реєстр являється децентралізованим, оскільки знаходиться у кожного учасника мережі та обслуговується кожним таким учасником, тобто не існує єдиного адміністратора, який міг би вносити чи змінювати записи самостійно.

Децентралізація полягає в існуванні великої кількості учасників, які підтримують мережу. Кожен такий учасник представлений у вигляді ноди – це може як домашній комп’ютер або мобільний пристрій, так і потужний сервер. Повні ноди – це учасники, які підтримують діяльність мережі і зберігають всі дані, які коли-небуть були записані до блокчейну.

Окрім того, що інформація, яка записана в мережу блокчейн, є децентралізованою та доступною кожному учаснику, вона може бути додана лише після отримання гарантії, що така інформація не може бути змінена після додавання до реєстру. Такі гарантії надаються завдяки використанню криптографічних методів. Незмінність інформації робить реєстр прозорим та таким, який заслуговує довіру, оскільки учасники впевнені у тому, що достовірні дані не були змінені недобросовісними акторами або ж помилково.

Для вирішення різних проблем може застосовуватися різних підхід до визначення що таке блокчейн. Це може бути і розподілена база даних, і технологія, яка вирішує проблеми збереження даних, і навіть система, яка надає можливість оперувати незмінними даними. Незмінність не означає, що інформацію, яка зберігається в блокчейні неможливо змінити, це означає, що для таких змін потрібна згода інших учасників і кожна така зміна буде зберігатися в системі. Оскільки дані не можуть бути змінені якимось одним актором, або безповоротно видалені, такі дані можна вважати незмінними. Для порівняння з іншими інформаційними системами, вимоги до перевірки цілісності даних

можуть або взагалі не стосуватися учасників, або стосуватися обмеженого кола осіб, наділених повноваженнями модератора чи адміністратора. Інформаційна система на основі блокчейн сама по собі розуміє, що цілісність даних має бути перевірена та підтверджена перед кожним записом. При цьому самі дані можуть не відповідати дійсності, блокчейн не перевіряє достовірність даних, лише цілісність, тобто що ці дані не були змінені без згоди інших учасників системи. Для цього блокчейн використовує математично доведені криптографічні механізми. Скільки учасників мають підтвердити цілісність даних та яким саме чином визначає механізм згоди (консенсусу) блокчейну.

На даний момент існує велика кількість блокчейнів із своїм механізмом досягнення консенсусу.

Серед найбільш популярних алгоритмів консенсусу є:

- Proof-of-Work (далі POW);
- Proof-of-Stake (далі POS);
- Delegated POS (DPOS);
- Proof-of-Importance (POI);
- Byzantian-Fault-Tolerance (BFT);
- Federated Byzantine Agreement (FBA).

Кожен алгоритм консенсусу вирішує проблему довіри, обираючи між потребою масштабованості та децентралізації.

POW вважається одним із найбільш надійних механізмів досягнення консенсусу серед децентралізованих систем. Для створення блоку транзакцій необхідно виконати певну математичну роботу, яка потребує ресурсів. Розв’язок математичної задачі, передбаченої даним типом блокчейну, є доказом виконаної роботи і, як правило, учасник, який виконав таку роботу, отримує винагороду, передбачену системою. Такі вимоги необхідні, щоб убезпечити від запису даних, цілісність яких порушена, адже без необхідності доказів виконаної роботи і без необхідності задіяння ресурсів будь-хто може внести в блокчейн змінені дані. Чим більше учасників намагаються виконати задачу, тим більша складність задачі буде поставати перед ними. Недоліком даного типу консенсусу є значне

використання ресурсів та повільна обробка транзакцій. Прикладом може бути Біткоїн, який для своєї роботи потребує більше електроенергії ніж така велика країна як Аргентина[23]. Чим більше учасників в системі, тим більше ресурсів необхідно для отримання доказу виконаної роботи. Даний вид консенсусу найбільше підходить для публічних мереж з повною децентралізацією.

POS – це доказ володіння частиною системи. Даний алгоритм був створений для вирішення проблеми необхідності великої кількості ресурсів для POW. Даний алгоритм консенсусу схожий на голосування між акціонерами компанії. Чим більше акцій має учасник, тим більша вага його голосу під час прийняття рішень. Особливістю даного алгоритму консенсусу є процес запуску мережі блокчейн. Для підтвердження транзакцій необхідно мати частку мережі, наприклад монети, у випадку криптовалют. Але якщо мереже ще не запущена яким чином отримати монети. Дана проблема вирішується або розгортанням мережі з алгоритмом консенсусу POW, або попереднього випуску монет. Порівняно з попереднім алгоритмом, POS має такі переваги:

- відсутність значних ресурсів для виконання роботи;
- відсутність специфічного обладнання для здійснення математичних обчислень;
- більш швидкі обробки транзакцій.

Недоліком даного алгоритму є ризик зосередження більшої частки мережі в одного учасника, що перетворює децентралізовану мережу на автономну. Порівняно з POW, даний алгоритм легше атакувати, серед поширених відомих атак:

- Nothing-at-stake;
- атака попереднього обчислення;
- fake stake;
- атака накопичення віку монет;
- ближні атаки;
- дальні атаки[24, с.249].

Також рішення початкової емісії може нести свої недоліки, які можуть

призвести до зосередження основної частки мережі в одного учасника.

DPOS створений на основі переваг та недоліків алгоритмів POW та POS. Основна ідея – висування делегатів, які матимуть права підтверджувати транзакції. Кожен учасник повинен обрати свого делегата і при голосуванні певного делегата вага голосу буде відповідати частці учасника. Самі ж делегати при прийнятті рішень мають однакову вагу голосу. В даному алгоритмі делегати не є анонімними учасниками. Так само як і POS, даний алгоритм вирішує проблему необхідності великої кількості ресурсів для підтвердження транзакції. Але на відміну від алгоритму POS, діяльність делегатів можна оптимізувати, отже покращити пропускну здатність мережі. Завдяки делегатам, учасники мережі можуть не тримати повні ноди. Наприклад, станом на грудень 2023 року, для запуску повної ноди на блокчейні Ethereum, який використовує алгоритм консенсусу POS, необхідно мати 16GB оперативної пам’яті та 2TB SSD фізичної, сам блокчейн ефіріума займає більш ніж 650GB і росте зі швидкістю 14GB на тиждень[25].

DPOS як алгоритм консенсусу найкраще підходить для систем, в якій існують велика кількість користувачів, які можуть об’єднуватися у компанії або організації та надавати свого представника. Даний алгоритм консенсусу може розглядатися як кандидат для побудови інформаційної системи реєстрів, але існує недолік того, шо даний алгоритм найкраще підходить для публічних систем без необхідності авторизації учасників. Ще одним недоліком даного алгоритму є складність розгортання мережі без наявних делегатів. Як правило, для розгортання блокчейну з алгоритмом консенсусу DPOS, учасники вже повинні мати делегатів, які будуть виступати валідаторами при розгортанні системи.

POI являється видозміненим POS, де окрім володіння часткою мережі потрібно брати активну участь у роботі мережі, активно проводити транзакції, та залишатися учасником блокчейну впродовж тривалого періоду. Даний підхід схожий на програму лояльності в комерційних компаніях.

BFT відображує вирішення задачі візантійських генералів[26]. Для роботи даного алгоритму необхідно виконання умов:

– кожна нода має однакові права;
– наявність невідомих недобросовісних акторів серед учасників;
– добросовісні учасники складають більше 67 відсотків від загальної кількості;
– мережа може мати затримки в проведенні транзакцій[24].

Особливістю алгоритму є наявність п’яти етапів,:

– запит – нода-лідер отримує транзакції і формує блок;
– попередня підготовка – нода-лідер надсилає блок до інших валідаторів;
– підготовка – ноди обмінюються отриманим блоком;
– підтвердження – ноди обмінюються значенням блоку, і сповіщають про готовність підтвердження. Після підтвердження кожна нода отримує необхідну кількість підтверджень і оновлює реєстр;
– відповідь – на основі оновленого реєстру нодами-валідаторами, інші учасники системи оновлюють свій стан.

У випадку наявності недобросовісної ноди-валідатора, на етапі підтвердження можуть отримувати необхідну кількість підтверджень. Якщо недобросовісних нод буде більше, процес може перерватися на етапі підготовки. Оскільки ноди обмінюються повідомленнями і очікують певну мінімальну кількість підтверджень, така мінімальна кількість не набирається, процес припиняється і блок не створюється.

Даний алгоритм підходить до систем, які не потребують високого рівня децентралізації, валідатори можуть назначатися адміністратором, а також допускається можливість частої відмови у записі до реєстру. Даний алгоритм також може розглядатися як кандидат для інформаційної системи реєстрів.

FBA дозволяє досягати консенсусу серед великої кількості незнайомих між собою учасників. Кожен учасник має множину учасників (кворум), якому він довіряє, а сукупність таких кворумів призводить до глобальної згоди на рівні всієї мережі. Для досягнення згоди на рівні всієї мережі потрібно, щоб загальна кількість тих, хто надав підтвердження, було більше ніж 67 відсотків від кількості нод у кворумі. Для досягнення консенсусу використовується механізм

федеративного голосування, який складається з трьох етапів:

- голосування – початковий етап, коли нода обирає пропозицію за яку вона буде голосувати. Після обрання пропозиції розуміється, що добросовісна нода не буде голосувати за пропозиції, які суперечать даній пропозиції;
- ухвалення – якщо нода не ухвалювала пропозицію, яка суперечить даній, та створено кворум, пропозиція ухвалюється;
- підтвердження – нода шукає кворум, всі ноди якого ухвалили пропозицію та підтверджує пропозицію, якщо всі ноди кворуму цієї ноди також підтверджують дану пропозицію.

Перевагою даного алгоритму є більш висока масштабованість у порівнянні з попередніми, оскільки немає необхідності передавати повідомлення між усіма нодами. Недоліком даного алгоритму є можливість виходу системи із ладу. Якщо ноди будуть створювати кворуми з одними і тими ж нодами, у випадку виходу із ладу таких нод, система не зможе здійснювати свої функції. Максимальна кількість недобросовісних нод, яких підтримує алгоритм FBA не має перевищувати 33 відсотки від загальної кількості нод мережі. Ще одним недоліком є більш низький рівень децентралізації даного алгоритму, адже при формуванні кворумів ноди будуть прагнути включати до свого кворуму неанонімні ноди[24].

Система на основі блокчейну має ряд викликів, які потрібно вирішити для її реалізації. Проблематика систем на основі блокчейну включає:

- підтримку ідентифікації;
- автоматизацію процесів;
- створення правил роботи системи, які будуть єдиними для всіх учасників;
- необхідність наявності ресурсів всередині мережі;
- організація децентралізованого прийняття рішень.

При переведенні процесів у інформаційну систему постає питання отримання прав доступу до інформації та ресурсів. Для надання таких прав потрібно бути впевненим, що учасник є аутентифікованим в системі. Рішенням даної проблеми можуть бути блокчейни, які реалізують всередині себе

можливості роботи з цифровою ідентичністю.

Стабільна інформаційна система не має залежати від єдиного компоненту чи ресурсу. У випадку неавтоматизованих процесів, де потрібне підтвердження людиною, список запитів на підтвердження може накопичуватися до граничного показника, після якого система просто не буде функціонувати. При переводі процесів у цифровий світ, можна застосувати протоколи взаємодії та налаштувати обробку помилок у випадку занадто довгого очікування чи отримання неочікуваної відповіді. Блокчейни, які підтримують розумні контракти, здатні покращувати процеси шляхом переведення бізнес-логіки у розумні контракти.

Створення правил для функціонування системи характерне не лише розподіленим системам. Проте з оновленням таких правил можуть виникнути проблеми при працюючій системі. Проблема оновлення правил у блокчейнах призводить до створення альтернативної версії блокчейну. Одним із найбільш відомих прикладів такого оновлення було розподілення мережі Біткоїн на 2 частини: Біткоїн та Біткоїн класик. Під час пропозиції оновлення розміру блоку транзакцій, учасники розподіленої системи Біткоїн не досягли згоди, тому частина учасників створили свою версію, яку назвали Біткоїн класик[27]. До подібних проблем можуть приводити неактивні учасники мережі, яка мали б голосувати за пропозиції, але через відсутність, пропозиція не може бути прийнята, а оновлення відбутися. Блокчейни, які реалізовують гнучкість змін самих правил, а також внесення змін в мережу, вирішують дану проблему.

Для автономії у своїй діяльності, інформаційна система має складатися із компонентів, робота яких самодостатня для виконання функцій системи. Якщо існують зовнішні ресурси, може виникнути проблема доступу до таких ресурсів або ж довіра до них. Наразі для вирішення даної проблеми існують рішення для функціонування блокчейнів із зовнішніми системами, які називаються оракулами.

Організація децентралізованого прийняття рішення потребує виваженого вибору алгоритму консенсусу для блокчейну. Розглянуто найпоширеніші алгоритми, кожен має свою перевагу та недолік і не існує якогось універсального алгоритму консенсусу. Блокчейни, які мають підтримку декількох алгоритмів або

які можуть під час своєї діяльності змінювати алгоритми консенсусу, частково вирішують дану проблематику, адже зміна алгоритмів працюючої системи – це завжди виклик для її учасників.

Серед розглянутих алгоритмів консенсусу для інформаційної системи реєстрів, яка не має бути публічною, кандидатами можуть бути BFT та FBA, оскільки інші алгоритми розроблені для публічних блокчейнів та мають відповідні недоліки, які не підходять для розглядаємої системи.

2.2. Аналіз основних концепцій розумних контрактів

Окрім різниці в алгоритмах консенсусу блокчейни можуть відрізнятися також і за можливістю створення розумних контрактів. Першим блокчейном, який дозволив масово створювати розумні контракти, був Ethereum. Це публічний блокчейн, який характеризується високим рівнем децентралізації, але такий рівень досягається через обмеження в масштабуванні. Наразі блокчейн Ethereum має граничну пропускну спроможність, що призводить до різкого удорожчання послуг валідації транзакцій при наближенні до такої границі. Для прикладу, проведений експеримент з додавання двох чисел мільйон разів показав, що операція на блокчейні Ethereum була в 400 мільйонів разів дорожча ніж подібна операція з використанням мови програмування Python у хмарному середовищі AWS[22]. Ще одним недоліком блокчейну Ethereum є те, що для початку роботи з розумними контрактами, потрібно вивчити нову мову програмування – Solidity.

Розумні контракти (які ще називають смарт контракти) забезпечують контрольований доступ до реєстру мережі. За допомогою контрактів реєстр отримує низку функцій, таких як запит до реєстру, запис даних та виконання інших транзакцій. За допомогою розумних контрактів, учасники мережі блокчейну можуть додавати додаткову логіку при виконанні транзакції, наприклад, можна створити розумний контракт для визначення курсу валют або отримання ціни, яка постійно змінюється, в конкретний момент часу.

Для створення розумних контрактів мають бути визначені протоколи, які повинні містити правила створення, застосування та функціонування контрактів.

Система, якою управляє даний протокол, становить середовище виконання розумних контрактів. Розумні контракти, як і записи в блокчейні, мають бути незмінними в цілях безпеки. Після розгортання розумного контракту в середовищі, логіка або інші параметри залишаються незмінними протягом всього життя контракту.

Розумні контракти працюють у тісній взаємодії з нодами, які відповідальні за підтвердження транзакцій та повинні мати доступ до всіх необхідних ресурсів, з якими працюють розумні контракти. Наявність розумних контрактів у мережі дозволяє проводити аудит виконання таких контрактів. Це підвищує довіру до системи та робить її більш прозорою, оскільки незмінність і добросовісність бізнес-логіки контракту дають гарантію, що система буде працювати у передбачуваний спосіб без можливостей змін даних заднім числом. Розумні контракти здебільшого покликані автоматизувати процеси, що дозволяє оптимізувати трудові ресурси та нівелювати людську помилку при виконанні дій.

Розумні контракти не мають залежати від третіх осіб та бути ізольованими компонентами інформаційної системи. Але оскільки об’єкти сучасного світу дуже пов’язані між собою, виникає необхідність отримання інформації ззовні. Для блокчейну такі дані надають спеціальні сутності – оракули. Як правило, оракул має ідентичність з високим ступенем довіри. При передачі даних від оракула до розумного контракту створюється цифровий підпис, який засвідчує факт передачі інформації конкретним оракулом.

Платформи розумних контрактів:

– однією з найпоширеніших платформ для розгортання розумних контрактів є Ethereum. Дана платформа являється публічним децентралізованим блокчейном та підтримує власну цифрову валюту та використовує алгоритм консенсусу POS. Розумні контракти виконується на віртуальній машині Ethereum та використовують мову програмування Solidity. Недоліком даної платформи є те, що комісія за транзакцію може дуже сильно відрізнятися в залежності від завантаженості мережі. Ethereum оперує поняттями gasPrice і gasLimit, добуток яких буде максимальною

комісією, при чому комісія сплачується незалежно від того була транзакція успішна чи ні. Оскільки Ethereum є децентралізованим блокчейном, існують проблеми масштабованості. Один блок може генеруватися 10 – 20 секунд[24] та містити в собі декілька транзакцій, для прикладу платіжна система VISA підтримує більше 65000 транзакцій в секунду[28].

– Corda – платформа з відкритим кодом для виконання розумних контрактів. Розроблена фінансовим консорціумом здебільшого для зберігання, управління і синхронізації зобов'язань між фінансовими організаціями. Дана платформа характеризується можливістю конфіденційного розповсюдження інформації між різними застосунками системи, а ланцюг блоків містить не інформацію, а стан. Також за допомогою розумних контрактів можна створювати юридичні договори, які можуть використані в можливих майбутніх судових процесах. Особливості Corda: відсутність централізованого контролю транзакцій, можливість застосування різних алгоритмів консенсусу, історія у вигляді станів об'єктів, жоден учасник не має доступу до всієї історії транзакцій, відсутність анонімності.

2.3. Аналіз блокчейн платформи Hyperledger Fabric

Hyperledger Fabric – це відкрита платформа для рішень на базі розподіленого сховища, яка використовує модульну архітектуру. Дана платформа розроблена для підтримки підключення різноманітних реалізацій компонентів систем, враховуючи можливу складність і заплутаність таких систем[29].

Переваги модульної архітектури Hyperledger Fabric:

– вирішує проблеми масштабованості, які часто зустрічаються в інших блокчейнах (немає теоретичних обмежень розміру мережі);
– полегшує підтримку системи, оскільки компоненти слабко пов'язані, а зміни в одному модулі не будуть впливати на зміни в іншому;
– підвищує рівень відмовостійкості системи.

Hyperledger Fabric був заснований у 2015 році некомерційним консорціумом Linux Foundation з метою розповсюдження міжгалузевих технологій блокчейну, а також заохочення до відкритої спільної розробки технології[29]. Hyperledger Fabric, як і велика кількість блокчейнів, використовує розподілений реєстр, розумні контракти та являється системою, за допомогою якої учасники можуть керувати транзакціями.

Особливістю даної платформи є те, що вона не є публічною, а для доступу до мережі необхідно отримати відповідні права. Окрім цього, користувачі блокчейну можуть виконувати лише ті дії, якими їх наділили адміністратори системи. Це надає додатковий рівень захисту та дає можливість призначати ролі користувачам платформи. Також Hyperledger Fabric дозволяє зберігати розподілений реєстр у різних форматах, а механізми консенсусу та центри авторизації користувачів можна змінювати.

Учасниками мережі Hyperledger Fabric виступають організації, які можуть об’єднуватися в консорціуми і створювати власні блокчейн підсистеми, які будуть доступні лише учасникам консорціуму. Такий консорціум може створювати власні правила для блокчейну, при чому навіть адміністратор всієї мережі не має права втручатися в роботу такого блокчейну, якщо він не є членом консорціуму та не має відповідних прав. Кожна організація повинна мати власних представників (ноди), які будуть відповідати за життєдіяльність створеного блокчейну шляхом підтвердження транзакцій.

В залежності від налаштувань, ноди можуть мати різні функції:

- нода запису. Кожна нода в каналі є нодою запису, вона отримує блоки транзакцій, які перевіряються перед записом до реєстру на цій конкретній ноді;
- нода підтвердження. Кожна нода може стати нодою підтвердження, якщо на ній буде розгорнуто існуючий розумний контракт, який відповідає за логіку запису до реєстру. При цьому даний розумний контракт має викликатися клієнтом застосунку кінцевого користувача, щоб надати відповідь із цифровим підписом.

Політика підтвердження транзакції для розумного контракту визначає організацію, чия нода має забезпечити транзакцію цифровим підписом перед тим як транзакція потрапить до реєстру.

За правом підпису ноди поділяють на:

– нода-лідер. Якщо організація має декілька нод в каналі, нода-лідер буде відповідати за розповсюдження транзакції від сервісу черг до інших нод запису. Для визначення ноди-лідера можуть застосовуватися різні підходи, в тому числі статичні або динамічні. Дані налаштування важливі з точки зору відмовостійкості. Якщо нода-лідер відключиться від мережі, необхідно мати правила відповідно до яких в мережі з’явиться інша нода-лідер.
– нода-комунікатор. Якщо нода потребує комунікації з нодою із іншої організації, вона може використовувати ноду-комунікатор, яка задана в налаштуваннях організації. Ноди-комунікатори вирішують проблему спілкування між різними організаціями одного каналу.

В мережі Hyperledger Fabric одна і та ж нода може бути нодою-запису, нодою-підтвердженням, нодою-лідером та нодою-комунікатором одночасно.

Додавання нової ноди до каналу дозволяє підвищити пропускну здатність та стійкість системи. Чим більше нод працюють в системі, тим більше застосунків можуть підключатися до системи. Також при наявності великої кількості діючих нод в організації, планові або позапланові відключення деяких нод не будуть впливати на роботу системи, що підвищує відмовостійкість.

2.3.1. Блокчейн мережі Hyperledger Fabric

Окремо слід визначити можливість учасників системи створювати власні блокчейн мережі, які називаються канали. Такі канали можуть мати власний реєстр. За допомогою каналів інформація може бути прихована від наявних учасників мережі та бути доступною лише для учасників каналу. В середині каналу учасники можуть створювати приватні колекції, в яких будуть зберігатися дані доступні лише визначеним учасникам даного каналу. Для більшої

конфіденційності, дані можуть бути зашифровані за допомогою криптографічних алгоритмів під час проведення транзакції, а прочитані лише користувачем, який має відповідний ключ для розшифрування. Таким чином, разом із відносно відкритими мережами, Hyperledger Fabric підтримує мережі, де необхідна конфіденційність. Канали зберігають конфіденційність транзакцій від учасників усієї мережі, а колекції зберігають конфіденційність між окремими учасниками каналів.

Наявність політик мережі та політик каналів дозволяє підтримувати велику мережу. Учасники можуть додавати лише ноди, які відповідають правилам. Також політики мережі та каналів дозволяють налаштовувати рівень децентралізації мережі.

Учасники мережі об’єднуються в організації для можливості одночасної участі в різних розподілених мережах саме за допомогою каналів. Будучи членами організацій, які мають різні канали, учасники отримують доступ до мережі мереж. Канали надають можливість організаціям відокремлювати контрагентів, в той же час, підтримуючи можливість кооперації між ними.

2.3.2. Розумні контракти Hyperledger Fabric

Розумні контракти визначають логіку обробки даних, які вносять зміни до реєстру, пишуться в чейнкодах (chaincode) та викликаються зовнішніми програмами. Чейнкод можна охарактеризувати як програмне забезпечення, яке визначає об’єкт транзакції та інструкції транзакції для здійснення дій над об’єктом. Як правило, чейнкод взаємодіє лише із загальним станом реєстру мережі за допомогою транзакції. Результат виконання чейнкоду представлений у вигляді колекції записів ключ-значення, які надсилаються в мережу і вносяться до реєстру кожного учасника. Однією з переваг даної платформи є те, що вона підтримує декілька популярних мов програмування: Go, Node.js, Java[29], тому для написання розумних контрактів розробникам не потрібно вивчати специфічну мову.

Чейнкоди окрім описання логіки бізнес-процесів між організаціями також визначають системні конфігураційні правила:

– чейнкод _lifecycle – це тип чейнкоду, який запускається на всіх нодах і відповідальний за встановлення чейнкоду на ноді, затвердження визначень чейнкоду для організації та підтвердження визначень чейнкоду для каналу;
– чейнкод конфігурації запускається на всіх нодах для управління налаштуваннями каналу, наприклад оновлення політик каналу.
– чейнкод запитів запускається на всіх нодах для підтримки програмного інтерфейсу (API) реєстру;
– чейнкод підтвердження запускається лише на нодах, відповідальних за підтвердження транзакції, для криптографічного підтвердження запису;
– чейнкод погодження перевіряє транзакцію, включаючи правила підтвердження транзакцій та версію читання-запису.

Для більш гнучкого налаштування системи дані чейнкоди можуть бути змінені, але такі зміни несуть у собі ризик неправильного функціонування системи, наприклад, різниці у правилах оновлення копії реєстру для нод.

Однією з особливостей Hyperledger Fabric є те, що розумні контракти можуть викликати інші розумні контракти незалежно від того, де знаходяться контракти для виклику. Необхідно лише мати зв’язок між каналами, де знаходяться ці контракти.

2.3.3. Особливості розподіленого реєстру Hyperledger Fabric

Реєстр в мережі Hyperledger Fabric є поєднанням двох компонентів. Кожен учасник Hyperledger Fabric має копію реєстру для мережі, до якої він належить.

Реалізація реєстру в Hyperledger Fabric:

– загальний стан (world state) описує стан реєстру в певний момент часу. Даний компонент по своїй суті є базою даних, яка реалізована у форматі ключ-значення та може бути замінена іншою технологією;

– список транзакцій (transaction log) записує кожну транзакцію, яка внесла зміни до загального стану[29].

Загальний стан реєстру зберігає атрибути об’єкту системи у вигляді унікального запису в базі даних. Такий підхід надає можливість більш швидкого доступу до значень об’єкту порівняно з пошуком по всьому блокчейну. Оскільки база даних представлена у вигляді NoSQL типу ключ-значення, кожен об’єкт може мати свої індивідуальні атрибути. Загальний стан реєстру не потребує загальної схеми. Перевагою такої реалізації є можливість використання API, які надає обрана база даних, наприклад виклик методів:

–get – як правило, запит для отримання інформації про теперішній стан об’єкту в реєстрі;

– put – створення нового об’єкту або зміна існуючого;

–delete – видалення об’єкту із загального стану, але при цьому історія про всі зміни залишається в історії, включаючи і видалення цього об’єкту.

Для вирішення проблем одночасного оновлення даних (т.з. конкурентний доступ), Hyperledger Fabric використовує атрибут version, який перевіряється перед оновленням запису[29]. Такий підхід відомий під назвою «оптимістичне блокування» і дозволяє уникати фізичного блокування бази даних під час оновлення запису, оскільки, якщо версія об’єкту не співпадає із версією, яка була прочитана і є збереженою в базі даних (тобто була оновлена паралельно), оновлення даних не відбудеться, а клієнт зможе зробити повторний запит. У випадку фізичної втрати носія бази даних або виходу елементів із даних, завжди можна згенерувати загальний стан реєстру із списку транзакцій. У випадку планового або позапланового перезапуску ноди, загальний стан реєстру можна згенерувати заново перед тим як нода буде готова отримувати нові транзакції. При розгортанні мережі Hyperledger Fabric є можливість обрати між двома існуючими в налаштуваннях базами даних: LevelDB та CouchDB, а також підключити своє сховище, включаючи реляційну базу даних.

Список транзакцій представлений у вигляді блокчейну, в якому записується історія змін об’єктів. Даний блокчейн представлений у вигляді послідовних

записів пов'язаних блоків. Кожен блок містить послідовність транзакцій, а кожна транзакція представлена як запит до реєстру загального стану. Кожен блок має заголовок, основну інформацію та метадані (рис. 2.1). Заголовок містить криптографічно створений хешкод заголовка попереднього блока, таким чином блоки поєднані у послідовність. На відміну від загального стану реєстру, список транзакцій зберігається у вигляді файлів.

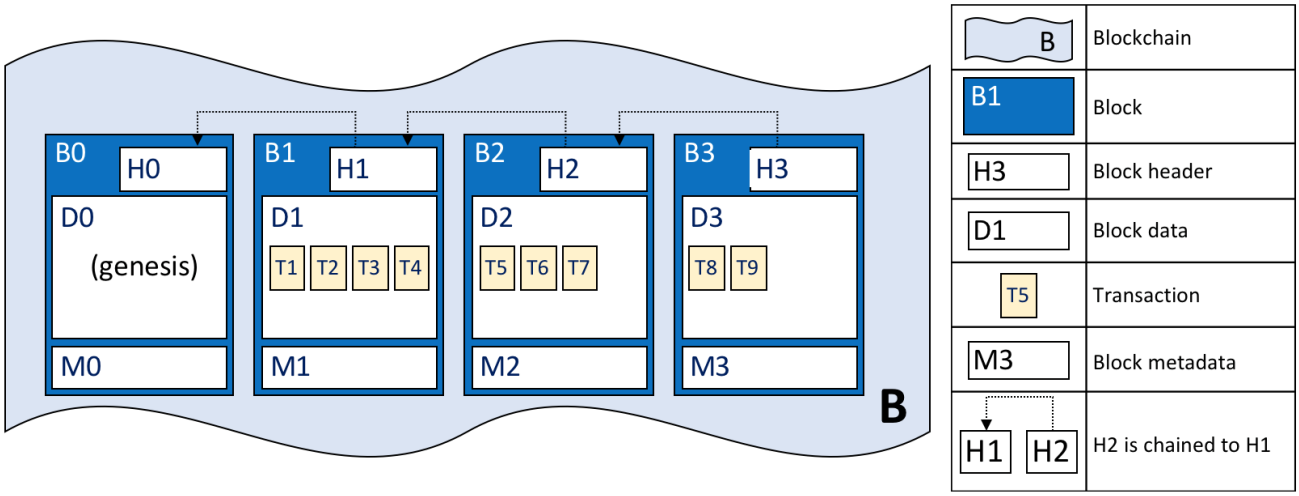


Рис. 2.1. Блокчейн Hyperledger Fabric[29]

Структура блоку:

а) заголовок:

1) номер блоку – число типу integer, яке починається з цифри 0 та зростає на одиницю при додаванні наступного блоку;

2) криптографічний хеш блоку – це хеш усіх транзакцій, які містяться в блоці;

3) криптографічний хеш заголовку попереднього блоку;

б) основна інформація – черга списку транзакцій, який створюється при створенні блоку сервісом керування чергами;

в) метадані блоку містять сертифікат і підпис сутності, яка створила блок, для можливості верифікації блоку нодами. Кожна транзакція має помітку коректності, що зберігається в бітовій мапі (bitmap), що зберігається в метаданих

блоку. Також до метаданих додається хеш всіх попередніх оновлень станів, включаючи даний блок, це дає можливість побачити, якщо блокчейн отримає альтернативне розгалуження, коли записи наступних блоків розходяться в інші ланцюги. Метадані не включаються до створення криптографічного хешу блоку.

Структура транзакції:

– заголовок – як і кожен блок, транзакція повинна мати свій власний заголовок, який містить метадані щодо транзакції, наприклад версію чейнкоду;

– криптографічний підпис, створений клієнтським застосунком, який підтверджує, що транзакція не була змінена чи підроблена;

– пропозиція транзакції – вхідні параметри застосунку в закодованому вигляді, які передаються до розумного контракту для створення пропозиції запису в реєстр;

– відповідь – вихідні дані розумного контракту після обробки транзакції;

– підтвердження – список підписаних вихідних даних організацій, які відповідали за підтвердження транзакції.

Можливості, які надає реєстр:

– пошук та оновлення реєстру за ключем, можливість використовувати композитні ключі під час запитів, а також використовувати діапазони в запитах;
– запити читання з використанням можливостей запитів, які надає реалізоване сховище;
– запити історії змін даних;
– робота з транзакціями, які містять підпис кожного учасника, який підтвердив таку транзакцію;

2.3.4. Безпека Hyperledger Fabric

Досліджувана платформа містить в собі ряд політик – правила, які визначають як будуть прийматися рішення та яким чином системою будуть досягатися бажані результати. Зокрема, хто та яким чином має права та які саме всередині системи. Прикладом політик можуть бути правила підтвердження змін

до мережі, каналу або розумного контракту. Правилами можна встановити яким чином будуть формуватися блоки та які учасники системи повинні поставити криптографічний підпис для розумного контракту.

Гнучкість у налаштуванні політик – це особливість платформи Hyperledger Fabric та одна із властивостей, які відрізняють дану платформа від блокчейнів Ethereum та Bitcoin, в яких кожна нода може генерувати і підтверджувати транзакції. Правила обслуговування мережі жорстко закріплені в системі і можуть бути змінені лише таким же процесом який управляє кодом системи. Користувачі Hyperledger Fabric можуть змінювати правила обслуговування мережі незалежно від правил підтвердження транзакцій. Платформа дозволяє створювати правила не тільки перед створенням мережі (каналу), а й під час її функціонування. За допомогою політик, учасники мережі можуть вирішувати хто може приєднуватися до них та з якими правами. Також політики можуть визначати яким має бути консенсус всередині мережі або чи мають транзакції відповідні підписи перед тим як внести їх до реєстру.

Ієрархія політик в мережі Hyperledger Fabric:

1. Політики каналу системи. Канал системи – це початкова сутність для кожної мережі, вона забезпечує роботу одного з головних елементів Hyperledger Fabric – Сервісу черг. Учасниками каналу системи є організації, які є учасниками сервісу черг, а також консорціуми (об’єднання організацій), які створили власні мережі. Дані політики визначають структуру блокчейну, алгоритми консенсусу, правила створення, адміністрування та участі в консорціумах.
2. Політики каналу мережі. Дані канали існують для приватної комунікації між учасниками організацій консорціуму. Політики даного каналу визначають процедури додавання та видалення учасників, описують які організації мають право підтверджувати чейнкоди перед застосуванням. При створенні каналу, він успадковує всі налаштування Каналу системи, які можуть бути змінені під власні потреби каналу.

3. Політики списків доступу та розумних контрактів надають можливість адміністратору мережі налаштовувати можливість доступу до ресурсів мережі, наприклад до системних функцій чейнкодів, повідомлень про наявність нових блоків тощо. Розумні контракти мають свої політики всередині чейнкодів, які визначають яка кількість нод, що належать до учасників каналу, має виконати і підтвердити транзакцію, щоб вважати транзакцію успішною.
4. Політики змін є правилами, які визначають як політики мають оновлюватися. Ці правила визначають групу учасників мережі, які повинні підписати запропоновані зміни перед їх застосуванням. Кожен канал має містити посилання на правила, які визначають порядок змін каналу.

Кожен учасник мережі блокчейну Hyperledger Fabric має бути авторизованим в системі. Кожен елемент системи також має засвідчувати свої права та ідентифікувати себе за допомогою цифрової ідентичності всередині мережі. Для взаємодії з цифровою ідентичністю елемента системи застосовується цифровий сертифікат стандарту X.509[29]. Даний стандарт був розроблений в кінці 80х років XIX століття і широко використовується у роботі із сертифікатами публічних ключів. Наявність сертифікатів такого стандарту забезпечують дозволи на доступ до ресурсів та інформації системи.

В мережі Hyperledger Fabric цифрова ідентичність наповнюється властивостями, необхідними для функціонування в мережі, і називається провідним об’єктом (principal). Такі об’єкти можуть мати різноманітні властивості для ідентифікації та розуміються як властивості, які визначають дозволи.

Для того, щоб сутність системи мала можливість бути задіяна в мережі Hyperledger Fabric, вона повинна мати узгодження для роботи. Сервіс надання прав участі в мережі являється довіреним елементом Hyperledger Fabric, який має право узгоджувати участь інших елементів системи. Стандартна реалізація досліджуваної платформи використовує X.509 сертифікати, застосовуючи традиційну ієрархічну Модель відкритих ключів[29]. Дана модель може надавати

різноманітні дані для ідентифікації, а Сервіс надання прав участі визначає які дані необхідні для права реєстрації в мережі. За допомогою моделі відкрити ключів сервіс узгоджує елементи мережі. Блокчейн користується моделями відкритих ключів для безпечної комунікації між учасниками мережі. Головними елементами зазначеної моделі є:

– цифрові сертифікати;
– публічні та приватні ключі;
– центри сертифікації;
– списки анульованих сертифікатів.

Hyperledger Fabric особливу роль надає центрам сертифікації, пропонуючи вбудований компонент Fabric CA, що дозволяє створювати такі центри в мережі при її побудові. Fabric CA являється приватним кореневим центром сертифікації, який здійснює управління цифровою ідентифікацією в мережі на основі сертифікатів X.509.

Сервіс надання прав участі дозволяє елементам системи використовувати публічні ключі, отримані центрами сертифікації, для ідентифікації та тримати приватні ключі у повній конфіденційності.

Приклад роботи сервісу надання прав участі в мережі:

1. Нода підписує транзакцію за допомогою приватного ключа.
2. Сервіс надання прав участі Сервісу черг має публічний ключ ноди, за допомогою якого підтверджує, що підпис транзакції здійснений відповідною нодою.

Особливістю платформи Hyperledger Fabric є можливість встановлювати сервіс надання прав участі на рівні організації, ноди, каналу та керувати таким чином правами доступу на своєму рівні.

Приклад роботи Сервісу надання прав участі при приєднанні нового компоненту до мережі:

1. Новий компонент має отримати цифрову ідентичність у центрі сертифікації, якому довіряє мережа.

2. Компонент має бути включеним до організації, яка визнана і затверджена мережею, шляхом додавання публічного ключа до Сервісу надання прав участі організації.
3. Сервіс надання прав участі організації має бути наявним або в консорціумі, або в каналі мережі.
4. Сервіс надання прав участі також має бути включений в політики мережі.

Реалізація сервісу полягає у сукупності списків із авторизованими елементами системи, відповідно до якого встановлюються які права має елемент (компонент зареєстрований як нода доданий до списку нод та має права ноди).

Виділяють два види сервісів надання прав участі:

– локального рівня – для роботи з клієнтами і нодами. Визначають списки адміністраторів нод, авторизують клієнтів для участі в транзакціях чейнкодів або для надання ролей (наприклад адміністратор організації);
– рівня каналу – визначають ролі на рівні каналу.

Досліджувана платформа вирішує основні проблеми, які виникають при виборі блокчейну для інформаційної системи:

– підтримку ідентифікації – Hyperledger Fabric реалізовує взаємодію сертифікатів X.509 для створення цифрової ідентичності в системі;
– автоматизацію процесів – підтримка розумних контрактів, які можуть взаємодіяти між собою, включаючи взаємодію між різними блокчейнами дозволяє переводити процеси в цифрову площину;
– створення правил роботи системи, які будуть єдиними для всіх учасників – Hyperledger Fabric підтримує гнучку систему керування політиками;
– необхідність наявності ресурсів всередині мережі – Hyperledger Fabric може взаємодіяти як із зовнішніми застосунками так і з оракулами за допомогою розумних контрактів;
– організація децентралізованого прийняття рішень –Hyperledger Fabric надає гнучкість у виборі алгоритму консенсусу для кожного блокчейну всередині мережі.

2.4. Аналіз існуючих математичних методів для покращення безпеки обліку нерухомості за допомогою технології блокчейн

Для покращення рівня безпеки реєстру слід визначити математичні моделі, які застосовуються для побудови інформаційних систем (рис. 2.2).

Дискреційне розмежування являється найпершою та найбільш популярною розробленою моделлю. Доступ до системи за такою моделлю назначається дискретним набором «Суб'єкт – операція – об'єкт».

Модель мандатного доступу більш зосереджена на вирішенні проблем «троянських коней» та покликана покращити контроль над інформаційними потоками.

Для досліджуваної системи найбільш підходящою вбачається система рольового контролю доступу, відомого як RBAC. Для отримання права на запис до реєстру можна застосувати підхід керування доступом на основі ролей. При такому підході, як правило, використовується матриця повноважень, яка має зберігатися в системі. Для нівелювання можливості внесення хибних даних в матрицю, пропонується надавати права на кожну сесію, починаючи з найменших прав для реєстратора (початкове право – лише здійснювати читання з реєстру). Для отримання права на запис, реєстратор повинен мати роль, яка дозволяє цей запис та бути авторизований через інтегрований в систему сертифікаційний центр. Також реєстратор повинен отримати право на запис. Такі права надають розумні контракти, які можуть робити виклики до інших реєстрів.

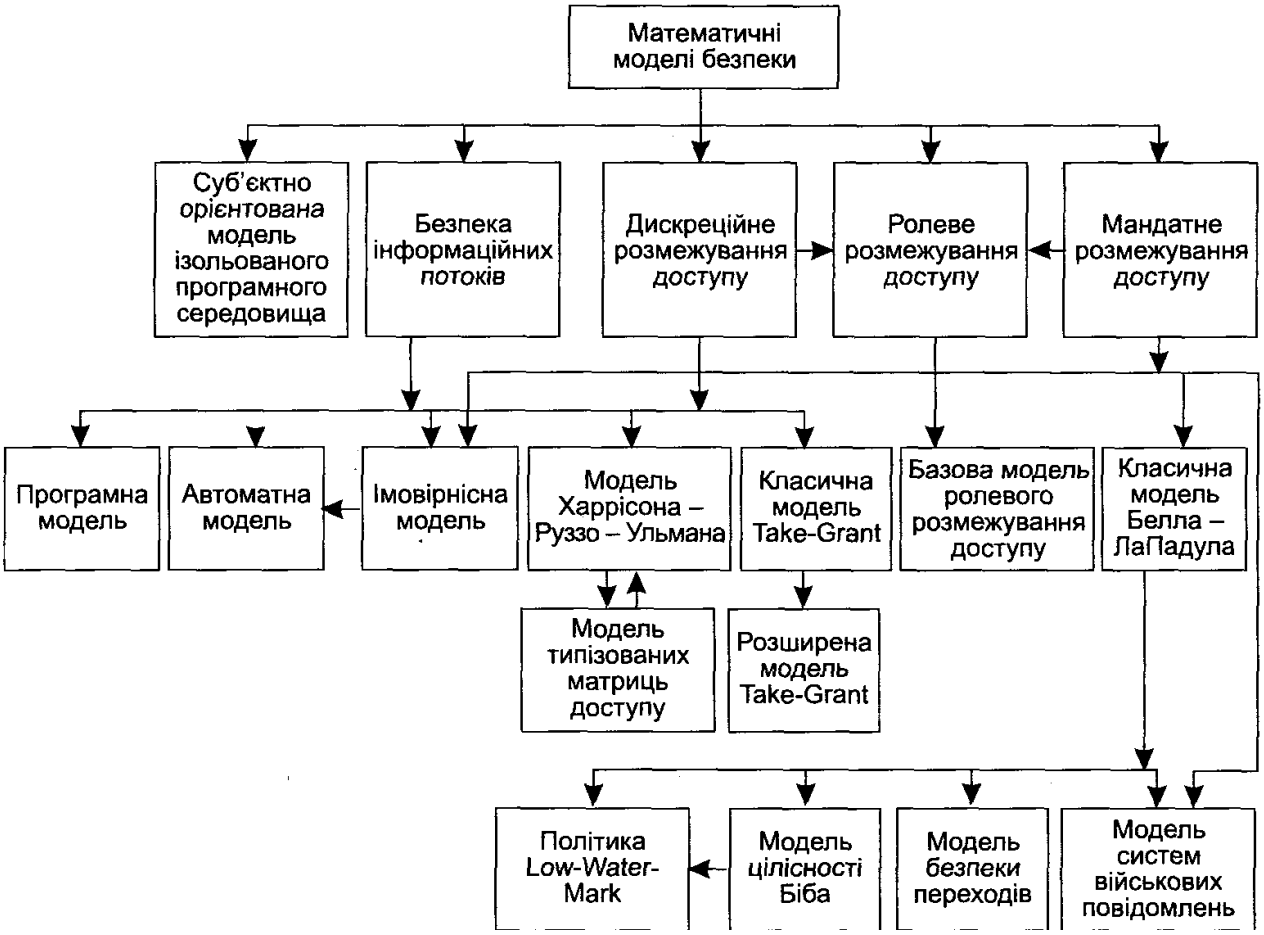


Рис. 2.2. Основні види математичних моделей безпеки[31]

Для визначення базової моделі ролевого розмежування доступу визначаються умови:

- S – суб'єкт (множина користувачів),
- R – роль (множина ролей),
- P – дозволи (множина прав доступу на об'єкти системи),
- SE – сесія (відповідність між S, R, P),
- SA – призначення суб'єкта,
- PA: R → 2p – функція, що визначає для кожної ролі множину прав доступу. При цьому для кожного $p \in P$ існує $r \in R$ така, що
- $p \in PA(r)$,
- RH – частково впорядкована ієрархія ролей. RH може бути ще записана так:
    a) один суб'єкт може мати кілька ролей;

б) одну роль можуть мати декілька суб'єктів;

в) одна роль може мати кілька дозволів;

г) один дозвіл може належати кільком ролям.

Для виконання умови доступу необхідно, щоб виконувались три умови:

– наявна роль – суб’єкт може виконати транзакцію лише якщо має відповідну роль;
– авторизована роль – активна роль суб’єкта має бути авторизована для суб’єкта;
– авторизація транзакції – суб’єкт може виконати транзакцію лише якщо транзакція авторизована для активної ролі суб’єкта[32].

Використовуючи нотацію теорії множин[33]:

а) $PA \subseteq P \times R$, при цьому дозволи призначаються зв’язкам ролей у відношенні «багато до багатьох»;

б) $SA \subseteq S \times R$, при цьому суб’єкти призначаються зв’язкам ролей і суб’єктів у відношенні «багато до багатьох»;

в) $RH \subseteq R \times R$

Перевагою технології керування доступом на основі ролей є можливість гнучкого налаштування. Hyperledger Fabric містить Сервіс надання прав участі, який в свою чергу керує списками контролю доступу. Також дана технологія може використовувати саму себе для сприяння децентралізованому управлінню керуванням доступом на основі ролей[33].

Технологія керування доступом на основі ролей може додатково надавати права на складні операції із складовими даними, а не тільки на атомарні операції з низькорівневими об’єктами даних[33], чим відрізняється від звичайних списків контролю доступу. В досліджуваній системі бізнес-логіка розумного контракту може назначати додаткову роль учаснику системи, що не можна описати у простому списку контролю доступом, яким керує Сервіс надання прав участі.

3 РОЗРОБКА СИСТЕМИ ОБЛІКУ НЕРУХОМОСТІ НА ТЕХНОЛОГІЇ БЛОКЧЕЙН

3.1. Проєктування архітектури інформаційної системи

При проєктуванні архітектури інформаційної системи використовувалась модель C4[200]. Перевагами даної моделі є:

– можливість застосування архітектурних абстракцій (систем, контейнерів, компонентів та коду);
– можливість застосування ієрархічних діаграм (контекст системи, контейнерів, компонентів та коду);
– можливість використання неформальних елементів при побудові діаграми;
– відсутність прив’язки до програмних застосунків.

Контекст системи представлено у вигляді UML діаграми (рис.3.1).

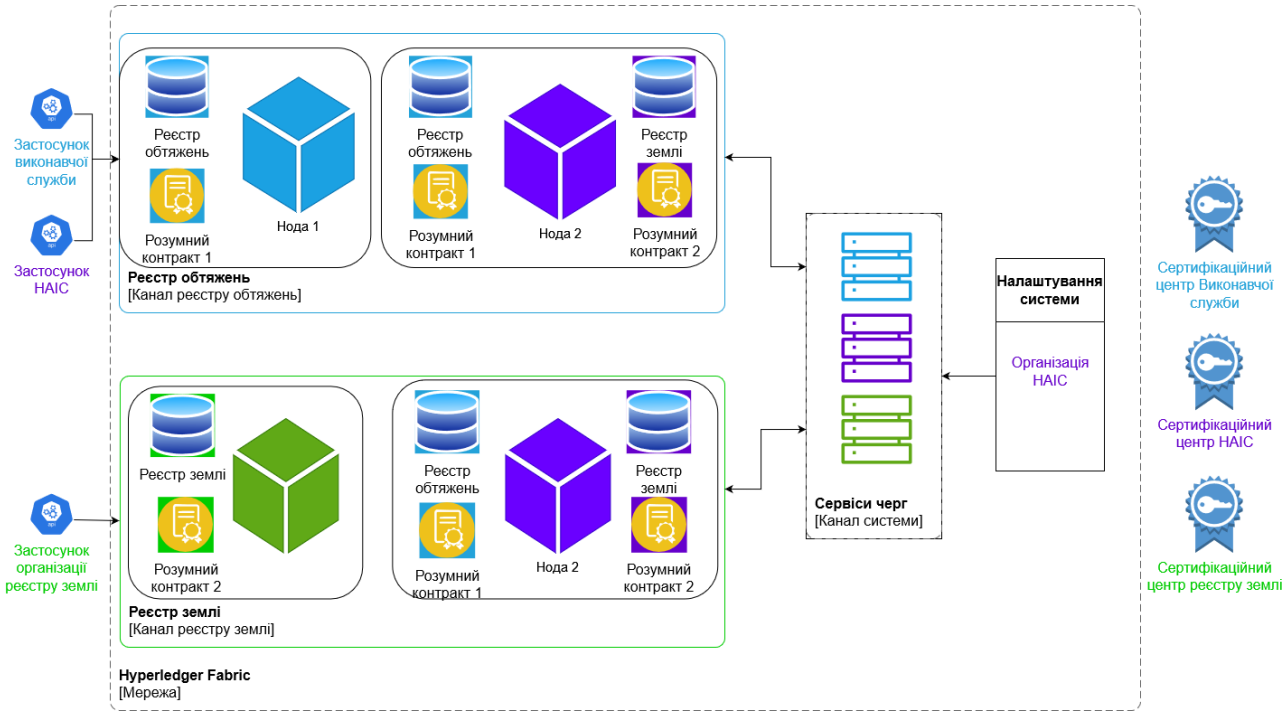


Рис. 3.1. Діаграма контексту інформаційної системи

На діаграмі зазначено контекст інформаційної системи на основі блокчейну Hyperledger Fabric.

Пропонується використовувати приватну мережу блокчейну. Завдяки вбудованій підтримці існуючих сертифікаційних центрів, авторизація учасників може відбуватися на основі існуючої системи авторизації. Сертифікаційні центри зображені як зовнішні ресурси системи (рис. 3.1).

Розглянуто сценарій побудови системи, яка підтримує реєстр землі і реєстр обтяжень та адмініструється однією організацією. Для побудови мережі необхідні адміністратори. Оскільки в Україні існує державне підприємство «Національні інформаційні системи» (НАІС), яке є розгалужене по більш ніж 22х регіонах та здійснює обслуговування існуючих державних реєстрів[21], побудова та адміністрування мережі може бути покладено на дане підприємство.

3.2. Розгортання інформаційної системи

Створення мережі Hyperledger Fabric починається із створення налаштувань мережі та запуску першої ноди – Сервісу черг. Згідно з початкових налаштувань, НАІС наділяється правами адміністратора та виступає в системі як перша організація, на ресурсах якої розгортається система.

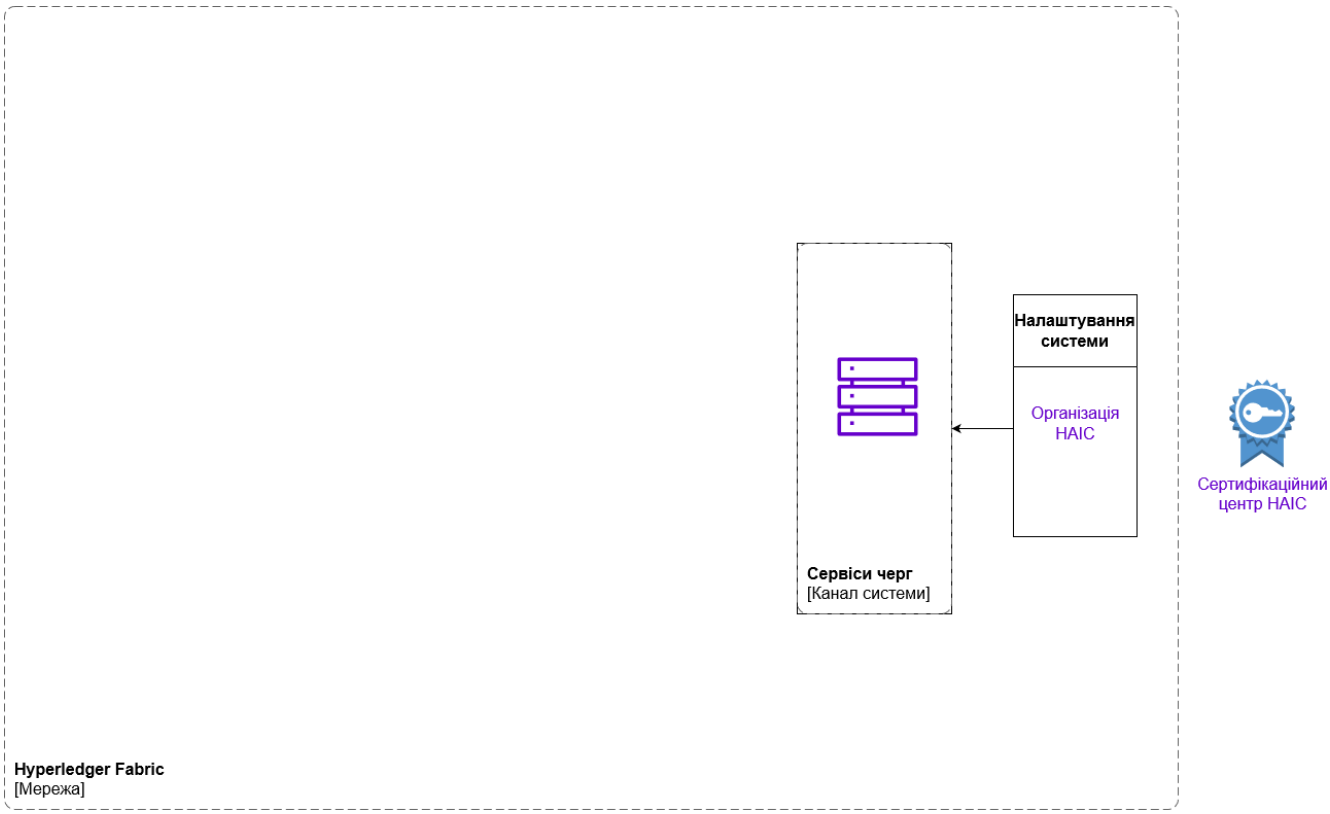


Рис. 3.2. Діаграма розгортання інформаційної системи

На рисунку 3.2 зображено процес розгортання інформаційної системи. Адміністратором являється НАІС та створено основний канал мережі, в якому працює єдина нода адміністратора, яка відповідальна за роботу Сервіса черг.

У випадку необхідності приєднання іншої організації в якості адміністратора для підвищення рівня децентралізації управління системою, діючий адміністратор оновлює налаштування мережі, куди додає нову організацію з правами адміністратора. Після приєднання нового адміністратора, права щодо адміністрування системи залишаються однаковими для обох адміністраторів. Кожна із організацій продовжує використовувати свій сертифікаційний центр. При цьому створюється нода Сервісу черг на боці нового адміністратора.

Сукупність організацій здійснюють управління власними каналами мережі Hyperledger Fabric через об’єднання у консорціуми. При створенні Організації реєстру землі, НАІС на правах адміністратора формує консорціум із двох організацій: Організація реєстру землі, та сам НАІС. Таке об’єднання

пояснюється тим, що Організація реєстру землі буде впроваджувати дії безпосередньо з реєстром, а НАІС як обслуговуюча організація реєстрів, виконуватиме консультативні та адміністративні функції в даному консорціумі. Запис про створений консорціум зберігається в компоненті Налаштувань системи. Організація реєстру землі або додає новий сертифікаційний центр для своєї діяльності, або приєднує існуючий. (рисунок 3.3). Консорціум № 1 відображено як логічну сутність. При створенні нової організації, адміністратор наділяє правами таку організацію на створення власної ноди в сервісі черг. Як правило, для підвищення відмовостійкості, кожна організація буде додавати власні ноди до сервісу черг системи.

Ідея даного консорціуму полягає у створенні записів до розподіленого реєстру землі та визначення правил, які будуть діяти під час запису до блокчейну. Для виконання цієї мети необхідно створити Канал.

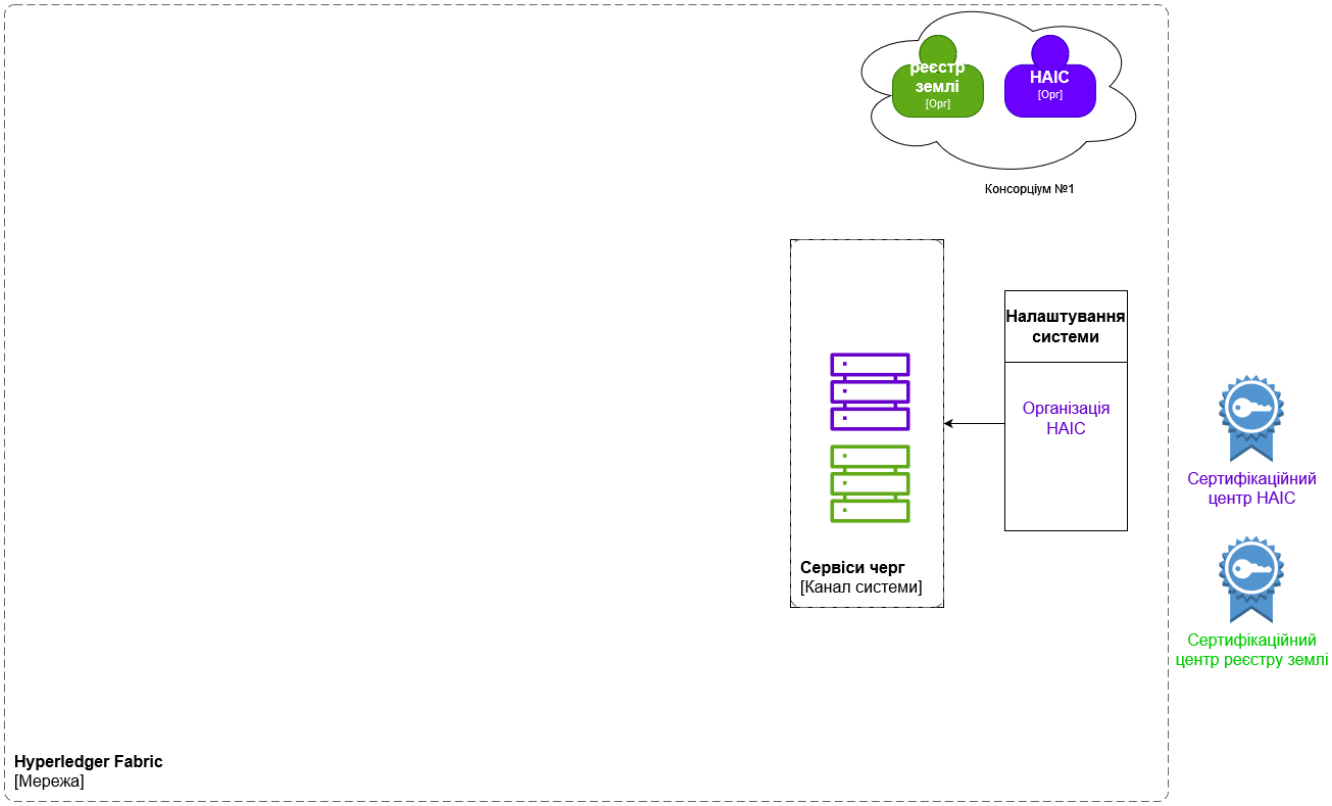


Рис. 3.3. Діаграма створення Консорціуму №1 інформаційної системи

Учасники консорціуму можуть спілкуватися через створений канал і мати гарантію, що транзакції всередині каналу не доступні до інших учасників

загальної мережі. Навіть адміністратори мережі не можуть мати доступу до каналу да впливати на його налаштування, якщо вони не є учасниками консорціуму. Під час створення каналу створюються налаштування, які визначають політики додавання нової організації до каналу та інші необхідні умови функціонування каналу. Налаштування каналу визначають адміністративні функції та являються ізольованими від налаштувань всієї мережі. Таким чином, зміни консорціуму на рівні мережі, не вплинуть на налаштування самого каналу.

Після створення каналу НАІС та Організація реєстру землі можуть підключати власні ноди. По замовчуванню, всі ноди являються нодами-запису. Оскільки НАІС адмініструє різноманітні реєстри, виглядає логічним мати ноди-комунікатори саме в цій організації. Дані ноди-комунікатори дозволять спілкуватися компонентам каналу з іншими каналами у разі необхідності отримати інформацію ззовні. По замовчуванню в системі, яка розробляється, кожна нода має право на читання із блокчейну. Hyperledger Fabric надає можливість учасникам консорціуму самостійно вирішувати який ступінь децентралізації матиме їх канал. Таким чином, організації можуть динамічно визначати кількість нод у своїй організації та визначати які ноди будуть нодами-лідерами та яким чином обирати нового лідера в разі відмови існуючого. На рисунку 3.4 зображено створення Каналу реєстру землі та встановлення однієї ноди Організацією реєстру землі, а другої ноди Організацією НАІС. База даних та список транзакцій у вигляді блокчейну можуть бути запущені, але взаємодіяти з ним немає можливості доки не встановлено і налаштовано розумний контракт.

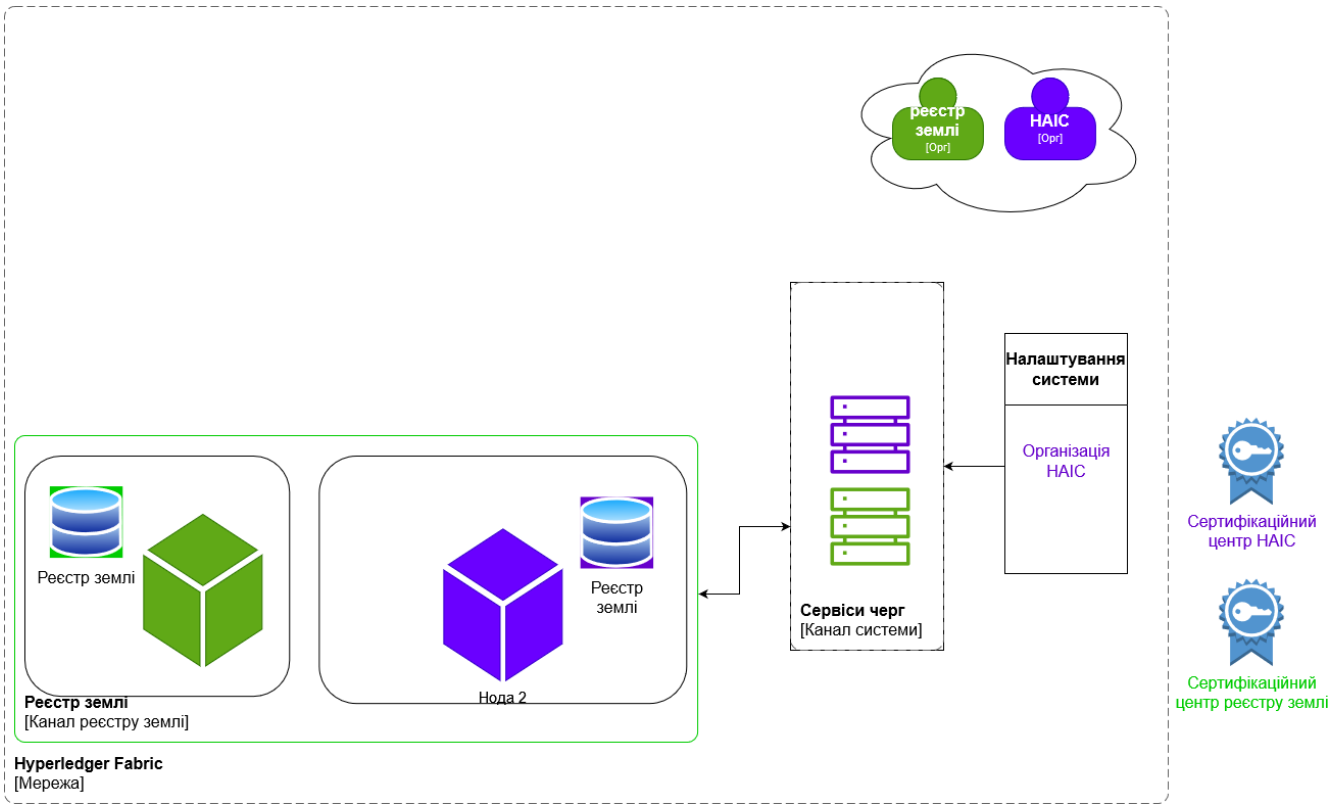


Рис. 3.4. Діаграма створення нод в каналі інформаційної системи

На визначені ноди, які відповідають за підтвердження транзакцій, встановлюються розумні контракти за допомогою чейнкодів. Розумний контракт визначатиме правила доступу до запису до реєстру. Після розгортання контрактів, застосунки-клієнти можуть запитувати інформацію із розподіленого сховища каналу, а також робити записи до сховища при отриманні відповідних прав (рисунок 3.5). Після розгортання розумного контракту, зовнішній застосунок організації реєстру землі може взаємодіяти з реєстром.

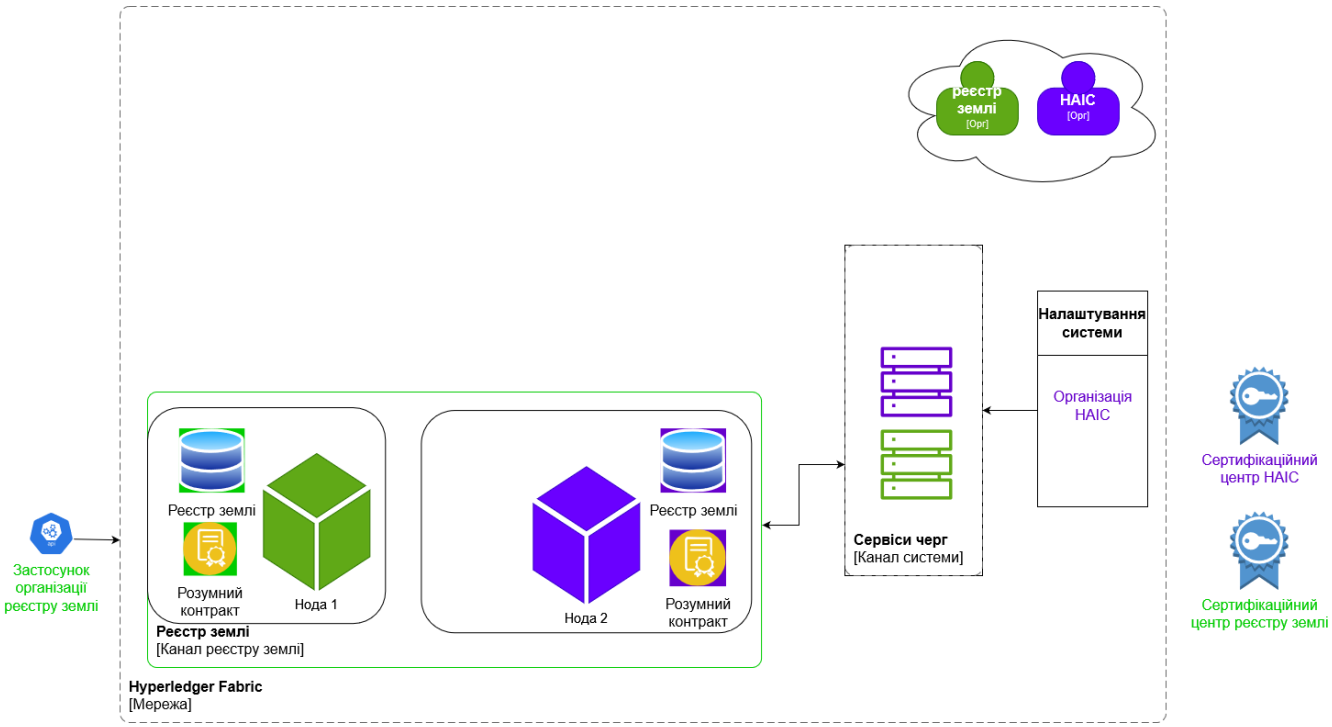


Рис. 3.5. Діаграма розгортання розумного контракту інформаційної системи

Для створення реєстру обтяжень виконуються такі ж процедури, які були виконані при створенні розглянутого реєстру. Створюється Організація виконавчої служби з новим або наявним сертифікаційним центром, встановлюється відповідна нода Сервісу черг. Разом із HAIC утворюється новий консорціум та новий канал, визначаються налаштування каналу. В новоствореному каналі розгортаються ноди, визначаються ті, на яких будуть розгорнуті розумні контракти (рис. 3.1).

3.3. Сценарії доступу до реєстру

На рис. 3.6 наведено приклад алгоритму запису до розподіленого реєстру.

На рис. 3.7 наведено діаграму успішного виконання запису до реєстру. Застосунок реєстратора робить пропозицію транзакції, яка викликає серію розумних контрактів, які надають додаткові права для виконання дії і після набуття всіх прав, розумний контракт, який відповідає за запис до блокчейну, робить такий запис і повертає відповідь клієнту. В даному випадку виконуються всі три умови доступу: наявна роль, авторизована роль, авторизація транзакції. Роль наділяється за допомогою розумних контрактів, а права для даної ролі

зберігаються у Сервісі надання участі. При цьому роль реєстратора має дозволи на запис, а реєстратор являється підтвердженою особою.

– PA ⊆ P × R,
– SA ⊆ S × R,
– RH ⊆ R × R

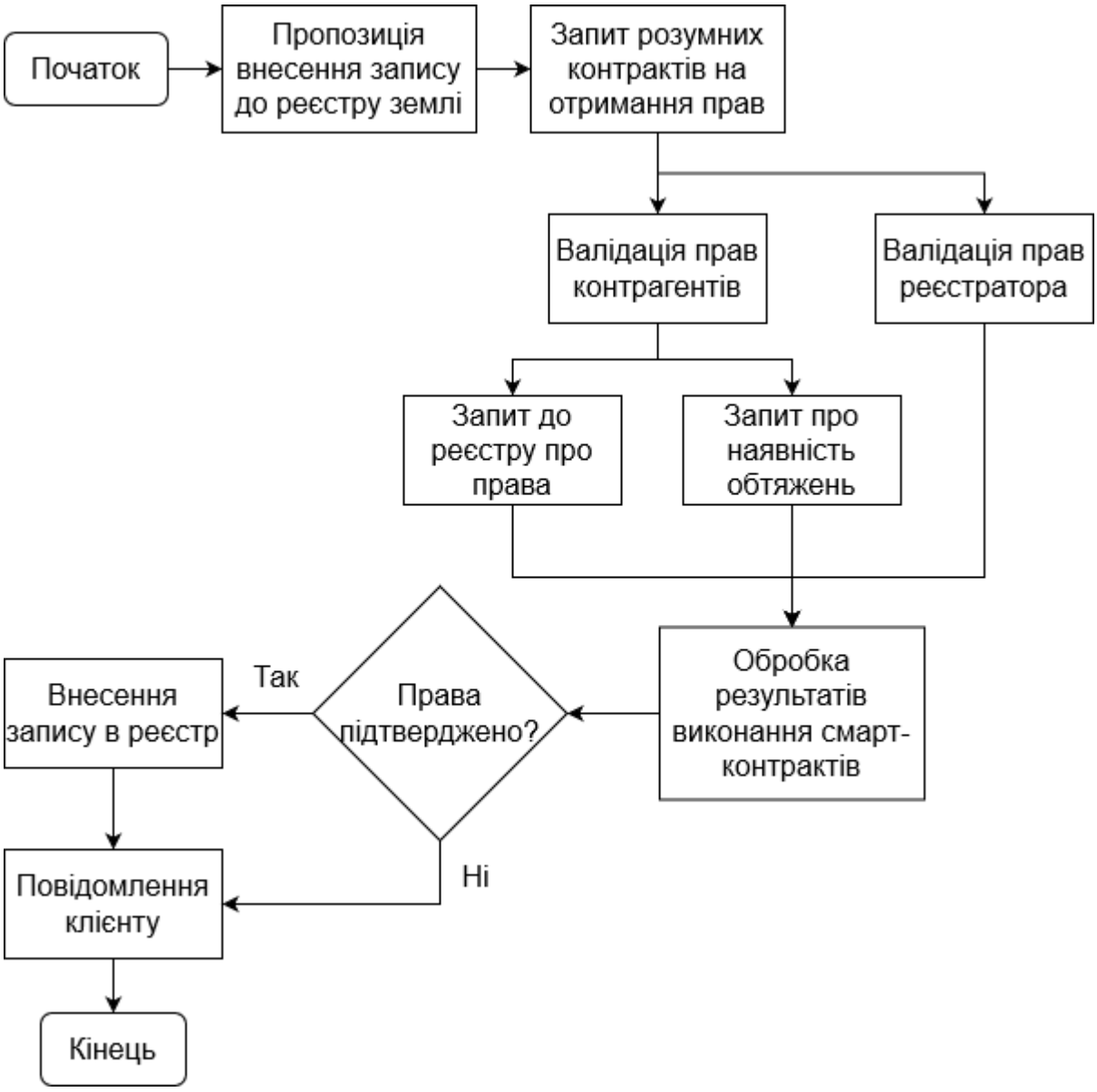


Рис. 3.6. Алгоритм внесення запису до реєстру

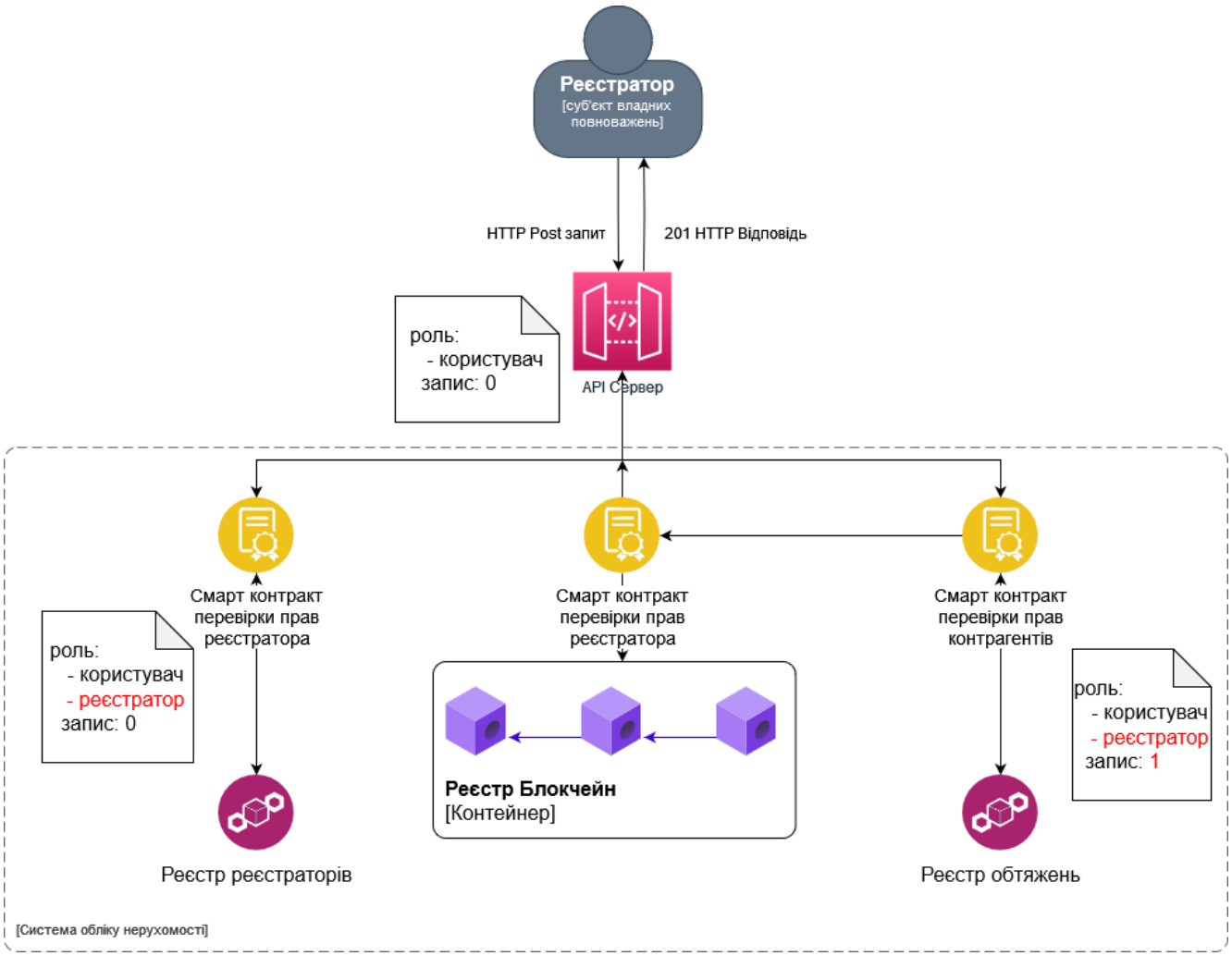


Рис. 3.7. Діаграма успішного запису до реєстру

Інформаційні системи мають ризик втручання в роботу з боку недобросовісних акторів. У звичайній інформаційній системі доступ до API сервісів або до особистого комп'ютера працівника може відкрити доступ до всієї системи. В сценарії, де був зламаний комп'ютер реєстратора недобросовісний актор отримує доступ до зовнішнього застосунку, але для пропозиції транзакції на неправомірний запис до реєстру зловмиснику необхідно також заволодіти приватним ключем реєстратора, який може бути або сховано, або зашифровано, або взагалі знаходитися на іншому пристрої. Оскільки не виконуються умови доступу і зловмисник не отримує роль реєстратора, призначення суб'єкта не відбувається, тому і запис в блокчейн не відбувається (рис. 3.8).

В існуючій системі реєстратор зобов'язаний перевірити чи існує обтяження на об'єкті нерухомості. Людська помилка або недобросовісні дії можуть привести

до відповідного неправомірного реєстраційного запису в реєстр нерухомості. В розглянутому сценарії недобросовісної дії з боку реєстратора запис в реєстр не відбувається через невиконання умови розумного контракту (рис.3.9). В даному випадку авторизація транзакції не відбувається завдяки відповіді розумного контракту, який не дозволяє вчинити запис до блокчейну.

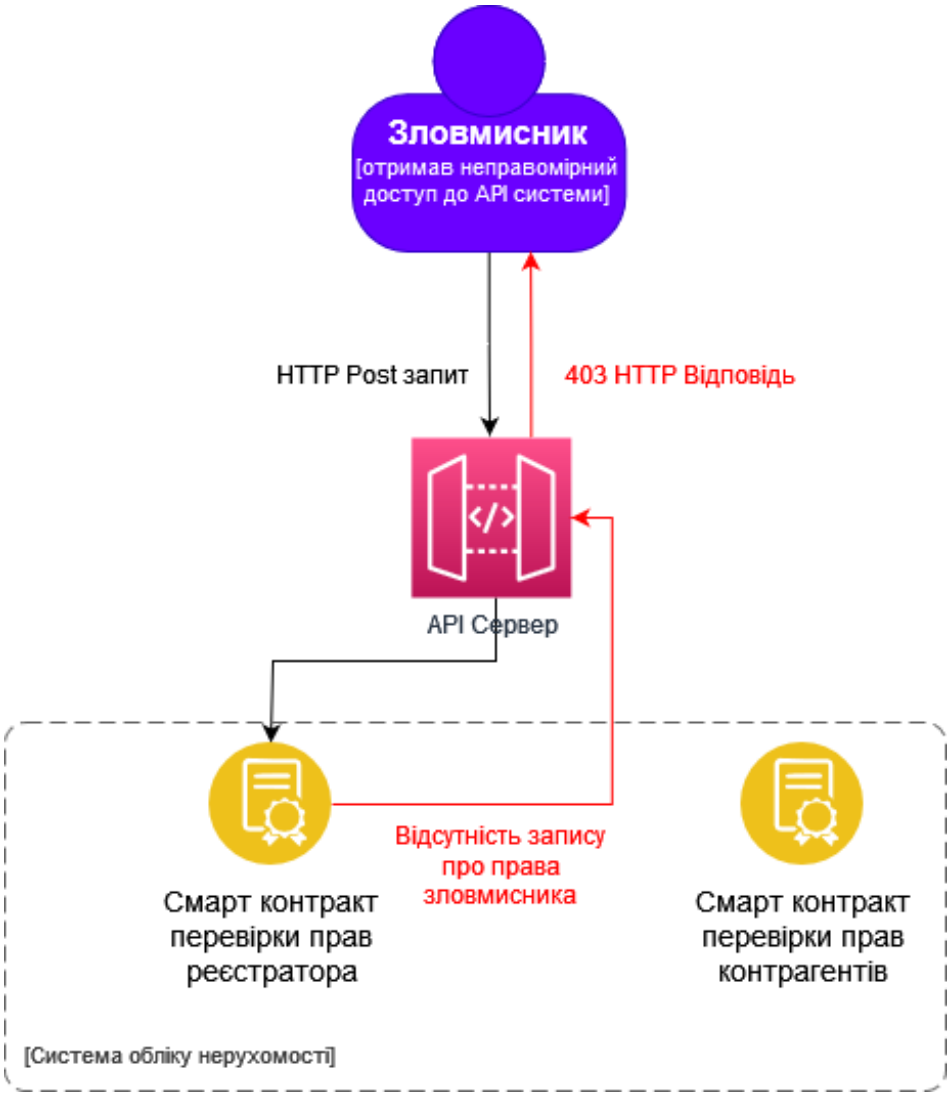


Рис. 3.8. Діаграма неуспішного запису через відсутність ролі

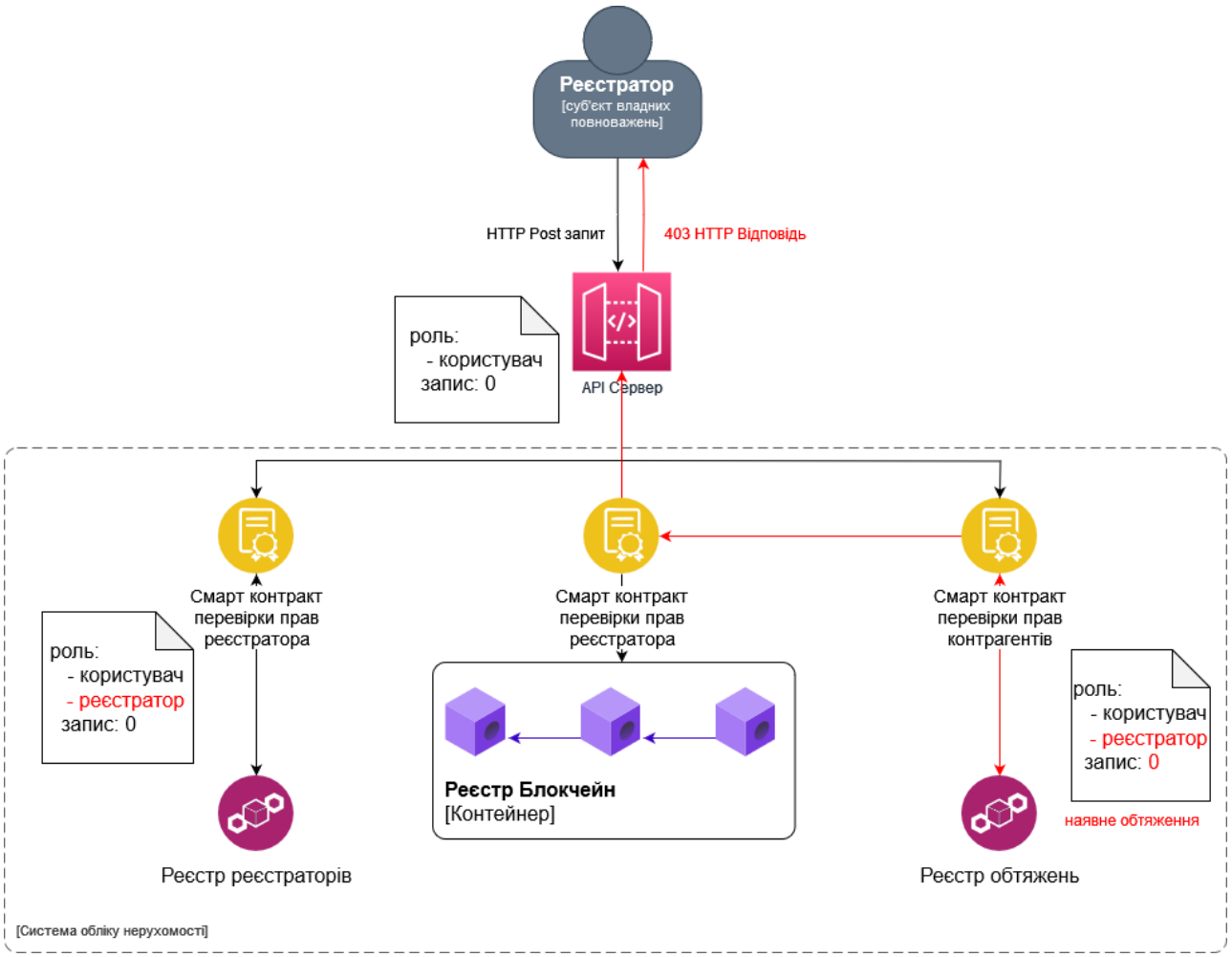


Рис. 3.9. Діаграма неуспішного запису через відсутність авторизації транзакції

ВИСНОВКИ

1. Проаналізовано проблематику процесів обліку нерухомості в Україні та світі.
2. Досліджено переваги та недоліки технології блокчейн при роботі з інформаційними системами.
3. Розроблено інформаційну систему, що усуває можливість недобросовісного запису в реєстр у розглянутих сценаріях.

ПЕРЕЛІК ПОСИЛАНЬ

1. Яроцький В. Л. Сучасні виклики та проблеми цивільно-правового забезпечення державної реєстрації речових прав на нерухоме майно в україні. // Матеріали XVIII міжнародної науково-практичної конференції, присвяченої 98-й річниці з дня народження доктора юридичних наук, професора, члена-кореспондента АН УРСР В. П. Маслова. – 2020. – С. 66-75.
2. Таранова О. О. Проблемні аспекти діяльності реєстру речових прав на нерухоме майно в Україні / Ольга Олександрівна Таранова. // 3. Дніпровський науковий часопис публічного управління, психології, права. – 2021. – №1. – С. 141.
3. Turchyn V. The use of blockchain technology for registration of property rights to real estate in Ukraine /. Visegrad journal on human rights // 3 (vol.2). – 2020. – С. 179.
4. Мачуський О. Зміст надання послуг у сфері державної реєстрації речових прав на нерухоме майно. / Law. State. Technology // 2. – 2022. – С. 43–48, doi:10.32782/LST/2022-2-7
5. О.О. Торбас. Особливості отримання та використання інформації з державного реєстру речових прав на нерухоме майно. / Суспільство, економіка, право: теорія, методологія, концепції розвитку: Матеріали III Міжнародної науково-практичної конференції (м. Київ, 12–13 лютого 2021 р.) / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. – Київ : ГО «Інститут інноваційної освіти». – 2021. – С.69-71.
6. Томчук Г. Принципи механізму державної реєстрації речових прав на нерухоме майно. // Актуальні проблеми вітчизняної юриспруденції. – 2021. – №6. – С. 88.
7. Селіванова К. В. Позасудовий (адміністративний) порядок оскарження рішень, дій чи бездіяльності державних реєстраторів прав на нерухоме майно в контексті реформування системи органів державної реєстрації / Адміністративне право і адміністративний процес, інформаційне право. – 2020. – №4. – DOI

https://doi.org/10.32842/2078-3736/2020.4.28

8. Francisco Ferreira Santana. Blockchain for Real Estate: A Systematic Literature Review / 29th international conference on information systems development (isd2021 valencia, spain).

9. Garcia-Teruel R. Legal challenges and opportunities of blockchain technology in the real estate sector / Rosa M. Garcia-Teruel. // Journal of Property, Planning and Environmental Law. – 2020. – №12/2. – С. 129–145.

10. Kaczorowska M. Blockchain-based Land Registration: Possibilities and Challenges / Maria Kaczorowska. // Masaryk University Journal of Law and Technology. – 2019. – №2. – С. 339–360.

11. Themistocleous M. Blockchain Technology and Land Registry / Marinos Themistocleous. // The Cyprus Review. – 2018. – №30. – С. 195–202.

12. Mira da Silva M. A Systematic Literature Review on Blockchain for Real Estate Transactions: Benets, Challenges, Enablers, and Inhibitors / M. Mira da Silva, F. Galvão Cunha // International Journal of System Assurance Engineering and Management. (попередня версія). – 2023. – Режим доступу до ресурсу: https://www.researchsquare.com/article/rs-2823844/v1, doi: https://doi.org/10.21203/rs.3.rs-2823844/v1.

13. Карнаушенко А.С. Міжнародний досвід застосування технології блокчейн в системі державного управління / Публічне управління та адміністрування у процесах економічних рефор. – 2018. – С.171-175.

14. Goran Sladi´c. A Blockchain Solution for Securing Real Property Transactions: A Case Study for Serbia. / SPRS Int. J. Geo-Inf. –2021. – №10. – С.35. – https://doi.org/10.3390/ijgi10010035

15. Karthika Veeramani. Land Registration: Use-case of e-Governance using Blockchain Technology. / KSII Transactions on internet and information systems. – 2020. – №14(9). – С.3693.

16. Bell Bitjoka G. Blockchain Study and Analysis with a View to Optimizing Security on the Aspects of Land Registry / G. Bell Bitjoka, S. Yves Wono Emvudu, B. Bete Mbezele. // American Journal of Computer Science and Technology. – 2020. –

№3/2. – С. 27–37.

17. Australian stock exchange officially abandons blockchain plans: Report [Електронний ресурс] // Cointelegraph.com. – 2023. – Режим доступу до ресурсу: https://cointelegraph.com/news/australian-stock-exchange-officially-abandons-blockchain-plans-report.

18. KSI Blockchain [Електронний ресурс] // e-estonia.com. – 2023. – Режим доступу до ресурсу: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

19. Інтерв'ю голови Держгеокадастру [Електронний ресурс] // AgroPolit.com. – 2020. – Режим доступу до ресурсу: https://agropolit.com/interview/731-denis-bashlik-tsina-na-zemlyu-skladatime-153-tis-za-ga-i-vona-ne-padatime.

20. Для створення українського блокчейну залучать іноземних партнерів, – Держгеокадастр [Електронний ресурс] // AgroPolit.com. – 2020. – Режим доступу до ресурсу: https://agropolit.com/news/14893-dlya-stvorennya-ukrayinskogo-blokcheynu-zaluchat-inozemnih-partneriv--derjgeokadastr.

21. Реєстри Національних інформаційних систем. [Електронний ресурс] // nais.gov.ua. – 2023. – Режим доступу до ресурсу: https://nais.gov.ua/registers.

22. What is Ethereum Gas? [The Most Comprehensive Step-By-Step Guide Ever!] [Електронний ресурс] // blockgeeks.com. – 2022. – Режим доступу до ресурсу: https://blockgeeks.com/guides/ethereum-gas/.

23. Bitcoin consumes more electricity than Argentina [Електронний ресурс] // bbc.com. – 2021. – Режим доступу до ресурсу: https://www.bbc.com/news/technology-56012952.

24. Кравченко П. Блокчейн і децентралізовані системи: навч.посібник для студ.закладів вищ. освіти в 3 частинах. Ч.1, 2 / П.Кравченко, Б.Скрябін, О.Курбатов, О.Дубініна. – Харків, 2019 – С.412.

25. Hardware requirements [Електронний ресурс] // Ethereum.org. – 2023. – Режим доступу до ресурсу: https://geth.ethereum.org/docs/getting-started/hardware-requirements

26. Задача візантійських генералів [Електронний ресурс] // Wikipedia.org. – 2023. – Режим доступу до ресурсу:

https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B4%D0%B0%D1%87%D0%B0_%D0%B2%D1%96%D0%B7%D0%B0%D0%BD%D1%82%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D1%85_%D0%B3%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D0%BB%D1%96%D0%B2

27. Bitcoin Classic: what it means, how it works [Електронний ресурс] // Investopedia.com. – 2023. – Режим доступу до ресурсу: https://www.investopedia.com/terms/b/bitcoin-classic.asp

28. Visa fact sheet [Електронний ресурс] // visa.co.uk. – 2023. – Режим доступу до ресурсу: https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

29. A blockchain platform for the Enterprise Hyperledger Fabric [Електронний ресурс] // Hyperledger-fabric.readthedocs.io. – 2023. – Режим доступу до ресурсу: https://hyperledger-fabric.readthedocs.io/en/release-2.2/

30. The C4 model for visualising software architecture [Електронний ресурс] // c4model.com . – 2023 . – Режим доступу до ресурсу: https://c4model.com.

31. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К.: Видавнича група BHV, 2009. — С. 608.

32. D. Ferraiolo Role-Based Access Controls [Електронний ресурс] // csrc.nist.gov. – 1992. – Режим доступу до ресурсу: https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased-access-controls/final/docs/ferraiolo-kuhn-92.pdf

33. Керування доступом на основі ролей [Електронний ресурс] // Wikipedia.org . – 2022. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9A%D0%B5%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96_%D1%80%D0%BE%D0%BB%D0%B5%D0%B9.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Магістерська робота

«ВДОСКОНАЛЕННЯ ПРОЦЕСУ ОБЛІКУ НЕРУХОМОСТІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН»

Виконав: студент групи ПДМ-62 Єрмоленко Євген Михайлович

Керівник: к.т.н., доц., доцент кафедри ІПЗ Негоденко Олена Василівна

Київ - 2024

МЕТА, ОБ'ЄКТА ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи: підвищення рівня безпеки системи обліку нерухомості шляхом автоматизації процесів за допомогою технології блокчейн.

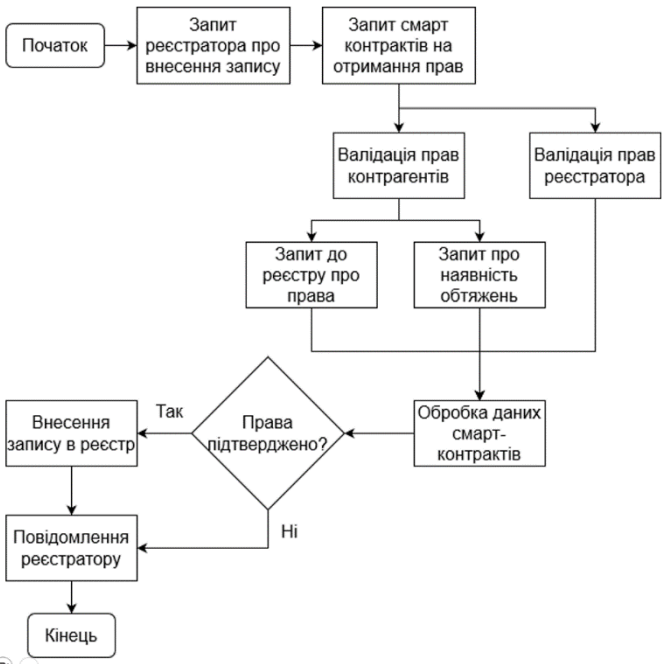
Об'єкт дослідження: автоматизація процесів обліку нерухомості.

Предмет дослідження: технології блокчейн.

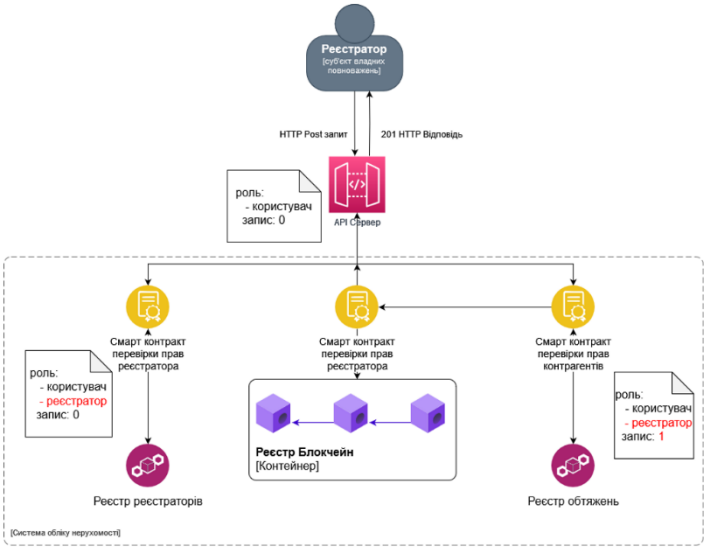
АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ЇХ МОДЕЛЕЙ

Країна	Система	Модель	Недобросовісний актор	Суб'єктивне прийняття рішення
Україна	Державний Земельний Кадастр;	Держземкадастр в процесі переведення на технологію блокчейн, призупинено	Так	Так
Швеція	Єдиний банк про нерухомість	Банк поділений на реєстри (реєстр нерухомості, будинків, земельний, прав), які формують державні та місцеві органи	Так	Так
Грузія	Реєстр Національного агентства публічного реєстру	Гібридна система - приватний блокчейн обробляє дані для запису в публічний реєстр.	Ні	Частково
Запропонована система	Програмна система реєстрів	Гібридна система - програмна система із записом у блокчейн	Ні	Ні

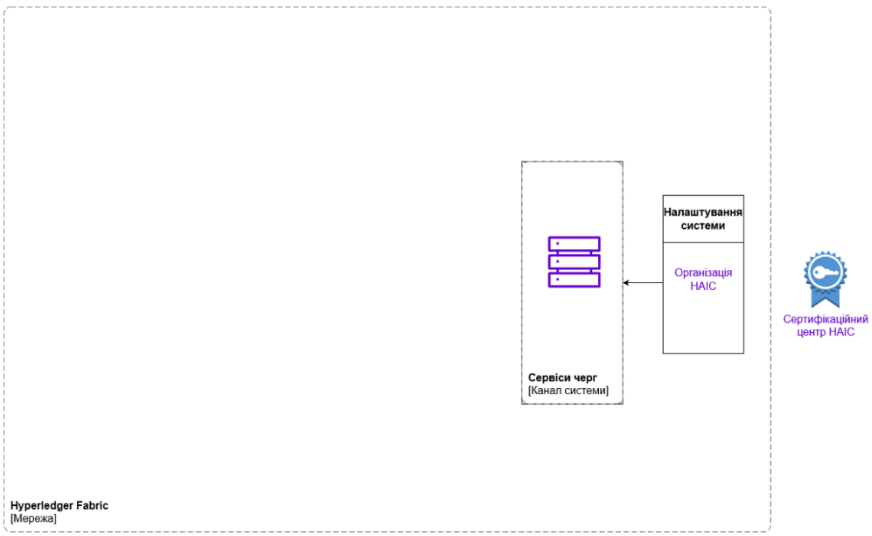
АЛГОРИТМ ВНЕСЕННЯ ЗАПИСУ В РЕЄСТР



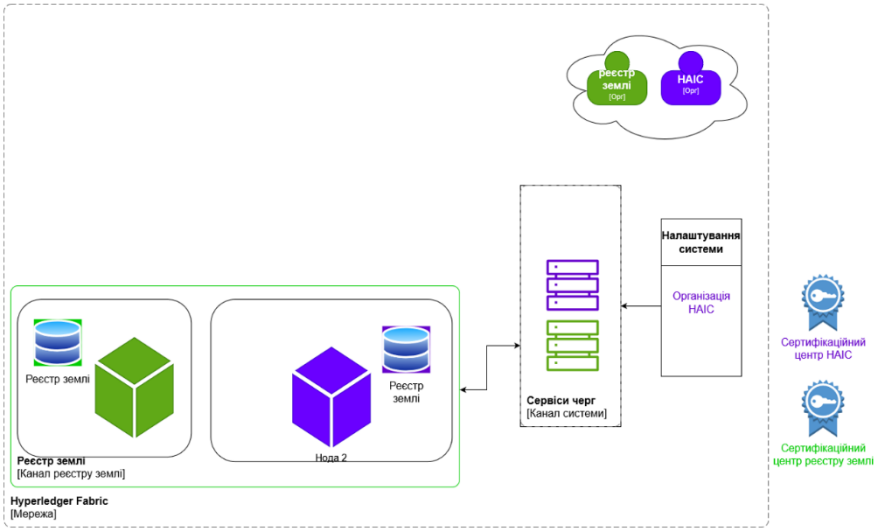
ПРИКЛАД ОТРИМАННЯ ПРАВ ДОСТУПУ НА ЗАПИС



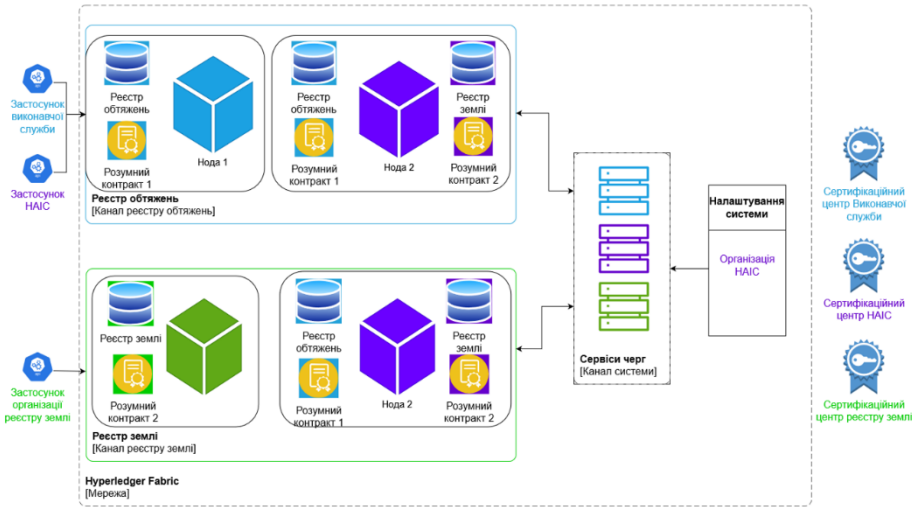
ДІАГРАМА РОЗГОРТАННЯ МЕРЕЖІ HYPERLEDGER FABRIC



ДІАГРАМА РОЗГОРТАННЯ МЕРЕЖІ HYPERLEDGER FABRIC. ПРИЄДНАННЯ ОРГАНІЗАЦІЇ ТА СТВОРЕННЯ КАНАЛУ.



ДІАГРАМА КОМПОНЕНТІВ СИСТЕМИ ОБЛІКУ НЕРУХОМОСТІ



МАТЕМАТИЧНА МОДЕЛЬ КЕРУВАННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ

$$PA \subseteq P \times R$$

$$SA \subseteq S \times R$$

$$RH \subseteq R \times R,$$

де

P - дозволи (множина прав доступу на об'єкти системи);

R - роль (множина ролей);

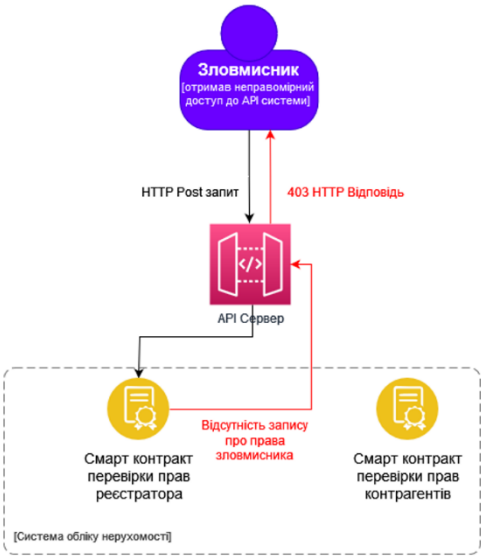
S - суб'єкт (множина користувачів);

PA - множина прав доступу для кожної ролі;

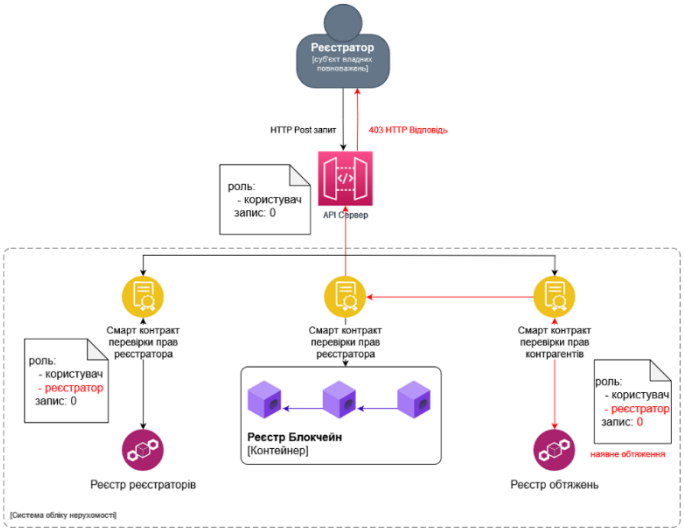
SA - призначення суб'єкта;

RH - частково впорядкована ієрархія ролей.

ПРИКЛАД ВІДМОВИ В РЕЄСТРАЦІЇ КОЛИ НЕДОБРОСОВІСНИЙ КОРИСТУВАЧ ОТРИМУЄ ДОСТУП ДО API СИСТЕМИ



ПРИКЛАД ВІДМОВИ В РЕЄСТРАЦІЇ ЧЕРЕЗ НАЯВНІСТЬ ОБТЯЖЕННЯ В РЕЄСТРІ БОРЖНИКІВ



ВИСНОВКИ

1. Проаналізовано проблематику процесів обліку нерухомості в Україні та світі.

2. Досліджено переваги та недоліки технології блокчейн при роботі з інформаційними системами.

3. Розроблено інформаційну систему, що усуває можливість недобросовісного запису в реєстр у розглянутих сценаріях.

ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ РОБОТИ

Тези доповідей:

1. Єрмоленко Є.М. Негоденко О.В. Покращення безпеки реєстру нерухомості за допомогою технології блокчейн // Реформування економіки України як фактор забезпечення сталого розвитку : Матеріали XIII Всеукраїнської наукової студентської інтернет-конференції. – Чернівці: ЧТЕІ ДТЕУ. – 2023р. – С.130.

1. Єрмоленко Є.М. Негоденко О.В. Перспективи реєстрів на технології блокчейн // Реформування економіки України як фактор забезпечення сталого розвитку : Матеріали XIII Всеукраїнської наукової студентської інтернет-конференції. –Чернівці: ЧТЕІ ДТЕУ. – 2023р. – С.133.

ДЯКУЮ ЗА УВАГУ!