Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Системотехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження використання блокчейн технології при розробці ігрових застосунків
(тема)

Виконав:
студент II курсу, групи ІТПм-21-2
Лимар Л.В.
(прізвище, ініціали)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*
Освітня програма Інформаційні технології проектування
(повна назва освітньої програми)

Керівник *проф. Калита Н. І*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри СТ _____ *проф. Гребеннік І.В.*
(підпис) (прізвище, ініціали)

2022 р

Я як студентка ХНУРЕ розумію і підтримую політику закладу із академічної доброчесності. Я не надавала і не одержувала недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

18.12.2022 Лимар Л.В.

Кваліфікаційна робота не містить відомостей заборонених до відкритого опублікування.

Кваліфікаційна робота виконана у відповідності до стандартів, що діють в Україні.

Попередній захист проведено 18 грудня 2022 р.

Керівник кваліфікаційної роботи проф. Калита Н.І.

Харківський національний університет радіоелектроніки

Факультет Ком'ютерних наук

Кафедра Системотехніки

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні технології проектування
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Лимар Ліліані Вадимівні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження використання блокчейн технології при розробці ігрових застосунків
затверджена наказом університету від 21 листопада 2022 р. № 1504Ст
2. Термін подання студентом роботи до екзаменаційної комісії 18.12.2022 р.
3. Вихідні дані до роботи методи та механізми застосування блокчейн технології в ігрових застосунках, методи дослідження та розрибки критерій ефективності. Перелік використовуваних програмних засобів: Visual Studio Code, Draw io, Dark Forest, Galcon 2, Gnosis Chain, Ethereum.

4. Перелік питань, що потрібно опрацювати в роботі 4.1Вступ. 4.2 Аналіз предметної області. 4.2.1 Опис предметної області. 4.2.2 Опис ігрових застосунків. 4.2.3 Опис блокчейн технології. 4.2.4 Огляд існуючих ігрових застосунків, створених з використанням блокчейну. 4.2.4.1 CryptoKitties. 4.2.4.2 Axie Infinity. 4.2.4.3 The Sandbox. 4.2.4.4 Thetan Arena. 4.2.4.5 Core. 4.2.4.6 Аналіз розглянутих ігор. 4.3 Огляд методів та технологій, які застосовуються в предметній області. 4.3.1 Огляд криптовалют. 4.3.2 Огляд блокчейн платформ. 4.3.2.1 Огляд смарт контрактів. 4.3.2.2 Огляд NFT. 4.3.3 Огляд Oracle сервісів. 4.3.4. Огляд технології IPFS. 4.4 Постановка задачі дослідження. 4.5 Розробка методу. 4.5.1 Опис досліджуваного ігрового застосунку. 4.5.2 Опис ігрового застосунку аналогу для порівняння. 4.5.3 Докази з нульовим знанням. 4.5.4 Використання доказів з нульовим знанням в Dark Forest. 4.5.5 Опис взаємодії з мовою Circom. 4.5.6 Опис мережевої архітектури застосунків. 4.5.7. Огляд блокчейну Gnosis Chain. 4.5.8. Ідея агностичного ігрового застосунку в Dark Forest. 4.5.9. Розробка показників ефективності використання блокчейн технології в ігрових застосунках. 4.6 Експериментальні дослідження. 4.6.1 Опис методів збору інформації. 4.6.2 Дослідження часу відповіді на запит у блокчейн. 4.6.3 Дослідження тривалості генерації хешу при ініціалізації гравця. 4.6.4 Дослідження кількості транзакцій в секунду в блокчейні. 4.6.5 Дослідження вартості

підтвердження транзакції. 4.6.6 Дослідження надійності NFT. 4.6.7 Висновки з результатів дослідження.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) 5.1 Схематичне зображення блокчейну (1 аркуш формату А4). 5.2 Схема процесу валідації транзакції в блокчейні (1 аркуш формату А4). 5.3 Схема роботи технологій HTTP та IPFS (1 аркуш формату А4). 5.4 Схема централізованої та децентралізованої системи (1 аркуш формату А4). 5.5 Схема взаємодії мови Circom з JS бібліотекою та блокчейном (1 аркуш формату А4). 5.6 Схема роботи однорангової архітектури (1 аркуш формату А4). 5.7 Схема клієнт-серверної архітектури (1 аркуш формату А4). 5.8 Схема архітектури Dark Forest (1 аркуш формату А4). 5.9 Результат роботи плагіну (1 аркуш формату А4). 5.10 Результат роботи програми (1 аркуш формату А4). 5.11 Графік порівняння результатів дослідження часу відповіді на запит (1 аркуш формату А4). 5.12 Результат роботи плагіну, що вимірює час генерації хешу (1 аркуш формату А4). 5.13 Розрахунок кількості запитів в секунду (1 аркуш формату А4). 5.14 Деталі транзакції в блокчейні Gnosis Chain (1 аркуш формату А4).

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

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Отримання завдання кваліфікаційної роботи*	10.10.2022	
2	Огляд літератури та аналіз предметної області	11-19.10.2022	
3	Аналіз ігор-аналогів	20-24.10.2022	
4	Огляд методів та технологій	25-29.10.2022	
5	Постановка задачі дослідження	30.10-07.11.2022	
6	Вибір ігор для збору даних дослідження	08-12.11.2022	
7	Розробка показників ефективності	13.11-19.11.2022	
8	Розробка програм для дослідження	20-29.11.2022	
9	Збір даних дослідження	30.11-12.11.2022	
10	Оформлення пояснювальної записки	13-16.12.2022	
11	Оформлення додатків	17.12.2022	
12	Представлення на рецензування	18.12.2022	

Дата видачі завдання 10 жовтня 2022 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Калита Н.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 64 с., 21 рис., 2 додатків, 46 джерел інформації.

БЛОКЧЕЙН, ІГРОВІ ЗАСТОСУНКИ, СЕРВЕРНА АРХІТЕКТУРА, NFT, ZKSNARKS

Об’єктом досліджень є процес використання блокчейну в ігрових застосунках як ігрового серверу та бази даних у вигляді NFT.

Предметом досліджень є особливості блокчейн технології, критерії ефективності використання блокчейну, ігрові застосунки створені на базі блокчейну.

Метою кваліфікаційної роботи є дослідження використання блокчейн технології при розробці ігрових застосунків.

Методи дослідження – системний аналіз, технології блокчейн, планування експерименту.

В роботі проведено аналіз предметної області, що відноситься до ігрових додатків та блокчейну, оглянуті методи та технології, що використовуються в предметній області, розроблено методи дослідження та експериментально зібрано результати дослідження.

Галузь застосування – сфера комп’ютерних ігор та блокчейн технологій.

ABSTRACT

Master`s Theses: 64 p., 21 fig., 2 appendices, 46 title.

BLOCKCHAIN, GAMING APPLICATIONS, SERVER ARCHITECTURE, NFT, ZKSNARKS

The object of research is the process of using blockchain in game applications as a game server and database in the form of NFT.

The subject of research is the features of blockchain technology, criteria for the effectiveness of using blockchain, game applications created based on blockchain.

The purpose of the work is to study the use of blockchain technology in the development of game applications.

Research methods - system analysis, blockchain technology, experiment planning.

The work analyzes the subject area related to gaming applications and blockchain, reviews the methods and technologies used in the subject area, develops research methods and experimentally collects research results.

The novelty of the work lies in the lack of comparison of the effectiveness of using blockchain in gaming applications.

Scope of usage – field of computer games and blockchain technologies.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС – інформаційна система;

DLT – Distributed Ledger Technology, технологія розподіленого реєстру

PoW – proof of work, підтвердження роботи

PoS – proof of stake, підтвердження частки

NFT – non-fungible token, не взаємозамінний токен

IPFS – InterPlanetary File System, міжпланетна файлова система

ZKP – Zero-Knowledge Proof доказ нульового знання

ZkSNARK – Zero-Knowledge Succinct Non-Interactive Argument of Knowledge стислий неінтерактивний аргумент нульового знання про знання

EVM – (Ethereum Virtual Machine) - віртуальне обчислювальне середовище Ethereum

ВСТУП

В сучасному світі важко уявити людину, яка ніколи не грала в ігрові застосунки, адже вони є популярним та цікавим методом проведення часу та оточують людей на будь-якому пристрої, починаючи з персональних комп’ютерів та мобільних телефонів, закінчуючи спеціальними ігровими консолями. Історія розвитку ігрової індустрії налічує більше, ніж 50 років з моменту створення першого ігрового застосунку [1]. Якщо на самому початку ігри були простими програмами, то зараз вони представляють собою складний комплекс різноманітних технологій.

Одним із ключових факторів розвитку ігрових застосунків є технологічний прогрес. Все частіше розробники можуть розраховувати на нові інструменти, щоб здивувати публіку, чи то за допомогою периферійних та інших пристроїв, чи то за допомогою додатків штучного інтелекту. Кожна технологічна інновація, яка виходить на ринок, може мати великий вплив як в економічному плані, так і на сам сектор: можливості практично безмежні, оскільки вони впливають на нього різними способами [2].

Однією із новітніх технологій, яку почали використовувати в ігрових застосунках є блокчейн. Спочатку з’являлися нескладні застосунки, з NFT предметами, а потім і повноцінні ігри з цікавим ігровим процесом. В 2021 році блокчейн ігри набули найбільшої популярності, і деякі проекти почали налічувати більше одного мільйона активних гравців [3]. Але всі ці ігри використовували блокчейн лише зі сторони монетизації власного проекту. Існує набагато більше можливостей використання блокчейн технології в ігрових застосунках, але кількість ігор що це реалізує незначна. Інформації про ефективність рішень, щодо використання блокчейну вкрай мало.

Таким чином, в роботі розглядається рішення актуального завдання оцінка можливостей використання блокчейн технології для розробки ігрових застосунків.

Об’єктом досліджень є процес використання блокчейну в ігрових застосунках як ігрового серверу та бази даних у вигляді NFT.

Предметом досліджень є особливості блокчейн технології, критерії ефективності використання блокчейну, ігрові застосунки створені на базі блокчейну.

Метою кваліфікаційної роботи є дослідження використання блокчейн технології при розробці ігрових застосунків.

Результати роботи доповідались на 1-й Міжнародній науково-практичній конференції «SCIENCE: DEVELOPMENT AND FACTORS ITS INFLUENCE» у секції «Інформаційні та веб технології» [4].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Опис предметної області

Інформаційна система (ІС) - це формальна, соціотехнічна, організаційна система, призначена для збору, обробки, зберігання та розповсюдження інформації [5]. З соціотехнічної точки зору, інформаційні системи складаються з чотирьох компонентів: завдання, люди, структура (або ролі) та технологія. Інформаційні системи можуть бути визначені як інтеграція компонентів для збору, зберігання та обробки даних, з яких дані використовуються для надання інформації, сприяння розвитку знань, а також цифрових продуктів, які полегшують прийняття рішень [6]. Інформаційна система є формою комунікаційної системи, в якій дані представляють і обробляються як форма соціальної пам'яті. Інформаційну систему також можна розглядати як напівофіційну мову, яка підтримує прийняття рішень та дії людини.

ІС можна розуміти з технологічної та бізнес точки зору, а також з соціальної та процесної точки зору. Як правило, більшість систем є компонентами більших систем, наприклад, організації. Вони можуть бути організовані в ієрархічну або навіть більш загальну структуру. Деякі системи, такі як Інтернет, з'єднують інші системи і в кінцевому підсумку створюють набагато більшу систему.

Розглянемо класифікацію ІС за аспектами:

– організаційний аспект: ІС є частиною організації. Інформаційна система буде мати стандартну операційну процедуру та культуру організації, вбудовану в них. Це включає в себе функціональні спеціальності, бізнес-процеси, культуру, політичні групи інтересів;

– управлінський вимір: менеджери сприймають бізнес-проблеми в навколишньому середовищі. Інформаційні системи надають інструменти та інформацію, необхідні менеджерам для розподілу, координації та моніторингу

своєї роботи, прийняття рішень, створення нових продуктів і послуг та прийняття довгострокових стратегічних рішень;

– технологічний вимір: менеджмент використовує технології для виконання своїх функцій. Вони складаються з комп'ютерного обладнання/програмного забезпечення, технології управління даними, мережевих/телекомунікаційних технологій. це один з багатьох інструментів, які менеджери використовують для того, щоб впоратися зі змінами [7].

Комп'ютерна ІС - система, призначена для зберігання, пошуку та оброблення інформації, та відповідні організаційні ресурси (людські, технічні, фінансові тощо), що забезпечують і поширюють інформацію. Призначена для своєчасного забезпечення належних людей належною інформацією, тобто для задоволення конкретних інформаційних потреб у межах певної предметної області, при цьому результатом функціонування комп'ютерних інформаційних систем є інформаційна продукція - документи, інформаційні масиви, бази даних та інформаційні послуги. Одним з прикладів комп’ютерної ІС є ігрові застосунки

1.2 Опис ігрових застосунків

Ігровий застосунок (комп'ютерна гра або відеогра) - це застосунок, що використовує електроніку для створення інтерактивної системи, яка передбачає взаємодію з користувацьким інтерфейсом або пристроєм введення - таким як джойстик, контроллер або клавіатуру, - для отримання візуального зворотного зв'язку. Цей зворотний зв'язок здебільшого відображається на пристрої відображення відео, такому як телевізор або монітор. Відеоігри часто доповнюються звуковим зворотним зв'язком, що передається через динаміки або навушники [8].

Основою ігрового застосунку є геймплей (ігровий процес) - це специфічний спосіб взаємодії гравців з грою. Як правило, геймплей вважається загальним досвідом гри у застосунок, не враховуючи такі фактори,

як графіка та звук. Тобто геймплей становить сукупність таких частин гри, як ігрова механіка, що являє собою набір правил у грі, які призначені для отримання приємного ігрового досвіду, виклики та їх подолання, сюжет та зв'язок гравця з ним.

Геймплей визначає певну ціль гри, що мотивує гравця рухатися далі по сюжету або рівнях. Зазвичай мотивацію в іграх поділяють на зовнішню і внутрішню. Внутрішня мотивація - особисті цілі гравця для реалізації себе в рамках ігрової системи. Це може бути поліпшення часу проходження рівня або відточування навички в змагальній грі. Зовнішня мотивація - мотивація, що диктується ігровою системою. Це може бути нагорода за виконання завдання або згадка гравця в щотижневому дайджесті найкращих гравців на сервері. Вважається, що внутрішня мотивація сильніша за зовнішню, оскільки вона продиктована особистістю гравця. Однак зовнішня мотивація може бути настільки цікавою, що вона переростає у внутрішню [9].

Сукупність геймплейних рішень та ігрових задач формують класифікацію ігрових застосунків за жанровою ознакою.

Основними жанрами ігрових застосунків є:

– екшн - акцентують увагу на фізичних випробуваннях, які вимагають зорово-моторної координації та рухових навичок для подолання. Вони зосереджені навколо гравця, який контролює більшу частину дій. Екшн-ігри класифікуються за багатьма піджанрами. Платформні ігри та файтинги є одними з найвідоміших піджанрів, в той час як шутер став і продовжує залишатися одним з домінуючих жанрів у відеоіграх;

– пригодницький екшн - як правило, мають довготривалі перешкоди, які необхідно подолати, використовуючи інструмент або предмет як важіль (знайдений раніше), а також багато менших перешкод, що майже постійно виникають на шляху, для подолання яких потрібні елементи екшн-ігор. Пригодницькі ігри, як правило, зосереджені на дослідженні і зазвичай включають збір предметів,

вирішення простих головоломок і бої. "Пригодницький екшн" став ярликом, який іноді прикріплюють до ігор, які не вписуються в інший добре відомий жанр;

– пригодницька - вимагають від гравця вирішення різних головоломок шляхом взаємодії з людьми або навколишнім середовищем, найчастіше в не конфронтаційний спосіб;

– пазл - зосередитися на логічних та концептуальних проблемах;

– рольові (RPG) - гравець виступає в ролі персонажа, який зростає в силі та досвіді протягом гри. Долаючи складні випробування та/або перемагаючи монстрів, гравець отримує очки досвіду, які відображають прогрес персонажа в обраній професії або класі (наприклад, рукопашному бою або магічних заклинаннях дальньої дії) і дозволяють гравцеві отримати нові здібності після отримання певної кількості очок;

– симулятор - призначені для точного моделювання аспектів реальної або вигаданої дійсності;

– стратегія - зосередженість на ігровому процесі, що вимагає ретельного та вмілого мислення і планування для досягнення перемоги, та масштаби дій від світового панування до тактики на рівні загону;

– спортивна - імітують спортивні або аркадні ігри. Командою (командами) суперників можуть керувати інші реальні люди або штучний інтелект.

– ритмічна - вимагає тримати певний ритм під аудіо супроводження.;

– ідл - включає в себе ігри, які орієнтують гравця на виконання тривіального завдання, наприклад, натискання на печиво; і в міру проходження гри гравець поступово винагороджується певними оновленнями за виконання цього завдання. Загалом, ці ігри вимагають дуже мало участі від гравця, і в більшості випадків він грає сам за себе; звідси і використання слова ідл, що означає бездіяльність [10].

В перші роки розвитку ігрової індустрії жанри відеоігор були досить чітко визначені, що не можна сказати про сьогодення. Кожен жанр поділяється на десятки піджанрів, що формує різноманітність ігрових застосунків разом з

комбінацією вибору сеттінгу - середовища, в якому відбувається дія в грі. Існують найрізноманітніші сеттінги, наприклад наукова фантастика, фентезі, постапокаліптичний світ, кіберпанк, тощо. Від вибору сеттінгу залежить вся візуальна частина гри: стиль персонажів, будівель, міст.

Протягом всієї історії відеоігор для відображення ігрового контенту використовувалися різноманітні методи комп'ютерної графіки. Переважання окремих методів змінювалося з плином часу, в першу чергу через розвиток апаратного забезпечення та обмежень, таких як обчислювальна потужність центральних або графічних процесорів.

Ігрові застосунки по графіці класифікують на:

– текстові - використовують текстові символи для відображення змісту гри;

– векторні - використання геометричних примітивів, таких як точки, лінії та криві (тобто фігур, заснованих на математичних рівняннях) замість растрової графіки, що залежить від роздільної здатності;

– повноцінне відео (FMV) - попередньо записані записи телевізійної або кінематографічної якості та анімації, а не спрайти, вектори або 3D-моделі для відображення дій у грі;

– 2D - використовують паралельну проекцію, зазвичай використовують двомірну растрову графіку на противагу тривимірній геометрії на основі трикутників, що дозволяє розробникам створювати великі, складні ігрові світи ефективно і з відносно невеликою кількістю художніх ресурсів, розділяючи їх на спрайти або плитки і повторно використовуючи їх багаторазово (хоча в деяких іграх використовується поєднання різних технік);

– 3D - тривимірне представлення ігрового світу, де об'єкти візуалізуються в реальному часі.

З стрімким розвитком ігрової індустрії з’явилось безліч ігрових платформ, на яких можна грати в гру. Кожна платформа має свою специфіку розміщення та розробки ігрового застосунка, але зазвичай розробники

випускають ігри на декілька типів приладів одночасно, щоб збільшити можливу аудиторію.

Основними платформами, для яких розробляються ігри є:

– персональні комп’ютери та ноутбуки;
– консолі;
– портативні консолі;
– браузери;
– мобільні пристрої;
– VR прилади.

По кількості гравців ігри поділяють на:

– однокористувальницькі (офлайн);
– багаторисувальницькі (онлайн).

За типом монетизації ігри поділяють на:

– роздрібна торгівля - є традиційним методом, за допомогою якого ігри продаються в звичайних магазинах або інтернет-магазинах;

– цифровий розподіл - Замість того, щоб купувати гру через фізичний магазин, клієнти купують свої ігри в Інтернеті та завантажують дані гри безпосередньо на свої пристрої;

– підписка - бізнес-модель, де гра вимагає постійних, постійних платежів від клієнтів для того, щоб грати в гру;

– мікротранзакція - це бізнес-модель, де аспекти вмісту гри можна придбати для покращення ігрового досвіду для гравця;

– завантажуваний контент (DLC) - це різновид мікротранзакції, яка розширює базову гру, надаючи додатковий контент;

– лутбокс - це різновид мікротранзакції, винагорода за яку є випадковою. Гравець не має контролю над винагородою, яку він отримує за оплату в ігровій або реальній валюті, хоча гра часто показує список можливих здобичі, яку гравець може отримати зі скриньки з лутом;

– торгівля між гравцями - це бізнес-модель, де внутрішньоігрові предмети та цифрові валюти можуть торгуватися між гравцями на ігровому

ринку, що дозволяє видавцеві отримувати частку від транзакцій, які здійснюють гравці [11].

Про розвиток ігрової індустрії свідчить не тільки різноманіття жанрів, технологій, що використовуються для їх розробки, бюджет ігрових студій, але й використання ігор у сферах відмінних від розважальних. Професійний гравець є почесною професією на рівні олімпійського чемпіона, що підтверджується гонораром команди-переможця на турнірі The International 2022 по грі Dota 2, що становить близько 8,5 мільйонів доларів, а кіберспорт офіційно визнаний в багатьох країнах, з 2020 року і в Україні. Розповсюджені також локальні турніри, наприклад університетський турнір в ХНУРЕ [12]. Каліфорнійський університет в Ірвіні має програму з комп'ютерних наук в галузі ігрових технологій. Студенти вивчають комп'ютерні науки через проектування та створення комп'ютерних ігор. В університеті розвивається кіберспорт та створена спеціальна створена спеціальна арена для проведення турнірів [13].

Також ігрові застосунки активно використовуються в навчанні: розвиваючі ігри для дітей, вивчення програмування та іноземних мов. Навіть ігрові застосунки, створені для розваг, можуть бути використані в навчальних цілях. Дослідники з Техаського університету в Далласі вважають, що модифікація популярної відеогри Minecraft може запропонувати потужний інструмент для навчання студентів університетів матеріалознавству [14]. Існують навіть ігрові застосунки для навчання майбутніх пілотів та воєнних. America's Army - серія відеоігор-шутерів від першої особи, розроблених і виданих армією США, призначених для інформування, навчання та вербування майбутніх солдатів.

Комп'ютерні ігри з 2011 року офіційно визнані урядом США і американським Національним фондом окремим видом мистецтва, поряд з театром і кіно. Якщо раніше була тенденція до розробки ігрових застосунків на основі популярних витворів мистецтва (наприклад ігрова серія відьмак розроблена на основі книг польського письменника Анжея Сапковського), то

зараз все більше фільмів та серіалів знімаються по сюжетам ігор (Uncharted, Resident Evil, Monster Hunter). Так в 2022 році зняли аніме серію Cyberpunk Edgerunners базовану на всесвіті гри Cyberpunk 2077, завдяки чому гра повернулися в топи по кількості користувачів через рік після релізу.

З усього цього випливає, що комп'ютерні ігри щільно влилися в наше нинішнє життя. Більш того, сфера їх використання за останні 10 років сильно зросла. Такий стрімкий розвиток індустрії передбачає використання все більш нових і сучасних технологій. Наприклад, ігри, що використовують блокчейн технології.

1.3 Опис блокчейн технології

Блокчейн - це тип технології розподіленого реєстру (DLT), який складається зі зростаючого списку записів, які називаються блоками, що надійно пов'язані між собою за допомогою криптографії. Кожен блок містить криптографічний хеш попереднього блоку, позначку часу та дані про транзакцію (як правило, представлені у вигляді дерева Меркла, де вузли даних представлені листям) [15], схематичне зображення представлене на рисунку 1.1.

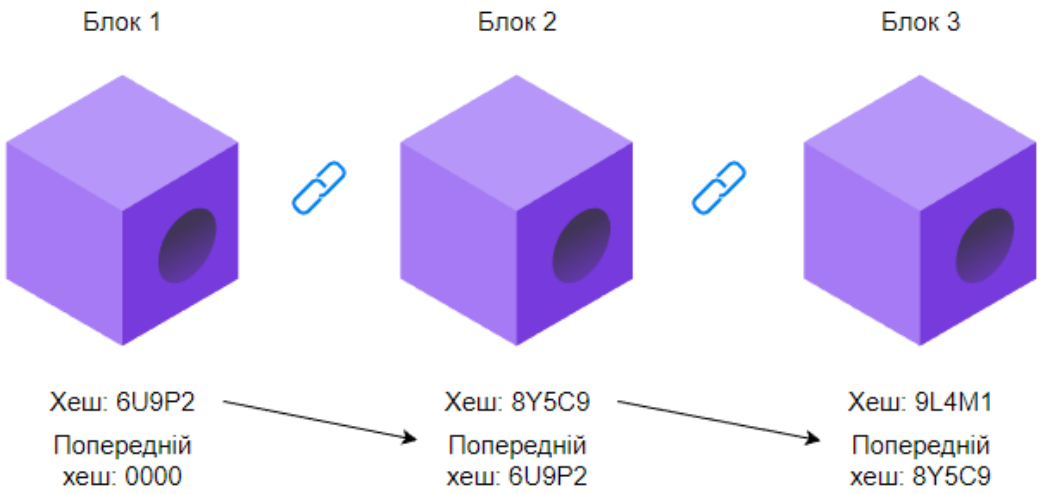

Рисунок 1.1 – Схематичне зображення блокчейну

Оскільки кожен блок містить інформацію про попередній блок, вони фактично утворюють ланцюжок, при цьому кожен наступний блок пов'язаний з попередніми. Мітка часу підтверджує, що дані про транзакцію існували на момент створення блоку. Транзакції в блокчейні є незворотними в тому сенсі, що після їх запису дані в будь-якому блоці не можуть бути змінені заднім числом без зміни всіх наступних блоків [16].

Криптограф Девід Чаум вперше запропонував протокол, подібний до блокчейну, у своїй дисертації 1982 року "Комп'ютерні системи, створені, підтримувані та довірені взаємно підозрілими групами" [17]. Подальша робота над криптографічно захищеним ланцюжком блоків була описана в 1991 році Стюартом Хабером та В. Скоттом Сторнеттою. Вони хотіли впровадити систему, в якій часові мітки документів не можуть бути підроблені. У 1992 році Хейбер, Сторнетта і Дейв Байєр включили в проект дерева Меркла, що підвищило його ефективність, дозволивши зібрати кілька сертифікатів документів в один блок. Під керівництвом їх компанії Surety хеші сертифікатів документів публікуються в The New York Times щотижня з 1995 року [18].

Перший децентралізований блокчейн був розроблений людиною (або групою людей), відомою як Сатоші Накамото в 2008 році. Накамото вдосконалив дизайн важливим чином, використовуючи метод, подібний до Hashcash, для позначення часу блоків, не вимагаючи їх підписання довіреною стороною, і ввівши параметр складності для стабілізації швидкості, з якою блоки додаються до ланцюга. Дизайн був реалізований наступного року Накамото як основний компонент криптовалюти біткойн, де він служить публічною книгою для всіх транзакцій в мережі [19]. Криптовалюта - це цифрова або віртуальна валюта, яка захищена криптографією, що практично унеможливлює її підробку або подвійне використання. Визначальною особливістю криптовалют вважається те, що вони, як правило, не випускаються жодним центральним органом влади, що робить їх теоретично не підвладними державному втручанню або маніпуляціям [20].

За даними [21] на 2016 рік блокчейн досяг 13,5% рівня прийняття у фінансових послугах, таким чином, досягнувши фази ранніх послідовників. Галузеві торгові групи об'єдналися для створення Глобального форуму блокчейнів у 2016 році, ініціатива Палати цифрової торгівлі.

Однією з особливостей технології блокчейн є децентралізованість. Зазвичай бази даних та сервери реалізовані як централізовані, що тягне за собою проблеми втрати даних, редагування чи знищення даних. Блокчейн вирішує цю проблему завдяки копіюванню бази данних (всього ланцюга) на комп'ютер кожного ноду (учасника мережі). Кожен вузол децентралізованої системи має копію блокчейну. Якість даних підтримується за рахунок масової реплікації бази даних та "обчислювальної довіри". Не існує централізованої "офіційної" копії, і жодному користувачеві не "довіряють" більше, ніж будь-якому іншому і навіть якщо один з них втратить чи намагатиметься змінити дані, вся інформація залишається цілою. На етапі валідації, якщо різні ноди видають різні результати, то прийнято вважати достовірною інформацію яка має більше голосів (не менше ніж 51%). Схема процесу валідації зображена на рисунку 1.2.

Однорангові блокчейн-мережі не мають централізованих точок вразливості, якими можуть скористатися комп'ютерні зловмисники; так само вони не мають центральної точки відмови. Методи безпеки блокчейну включають використання криптографії з відкритим ключем. Відкритий ключ (довгий, випадковий на вигляд рядок чисел) є адресою в блокчейні [15]. Токени цінності, що надсилаються через мережу, записуються як такі, що належать до цієї адреси. Закритий ключ схожий на пароль, який надає його власнику доступ до його цифрових активів або засобів для іншої взаємодії з різними можливостями, які зараз підтримуються блокчейнами. Дані, що зберігаються в блокчейні, як правило, вважаються непідкупними.

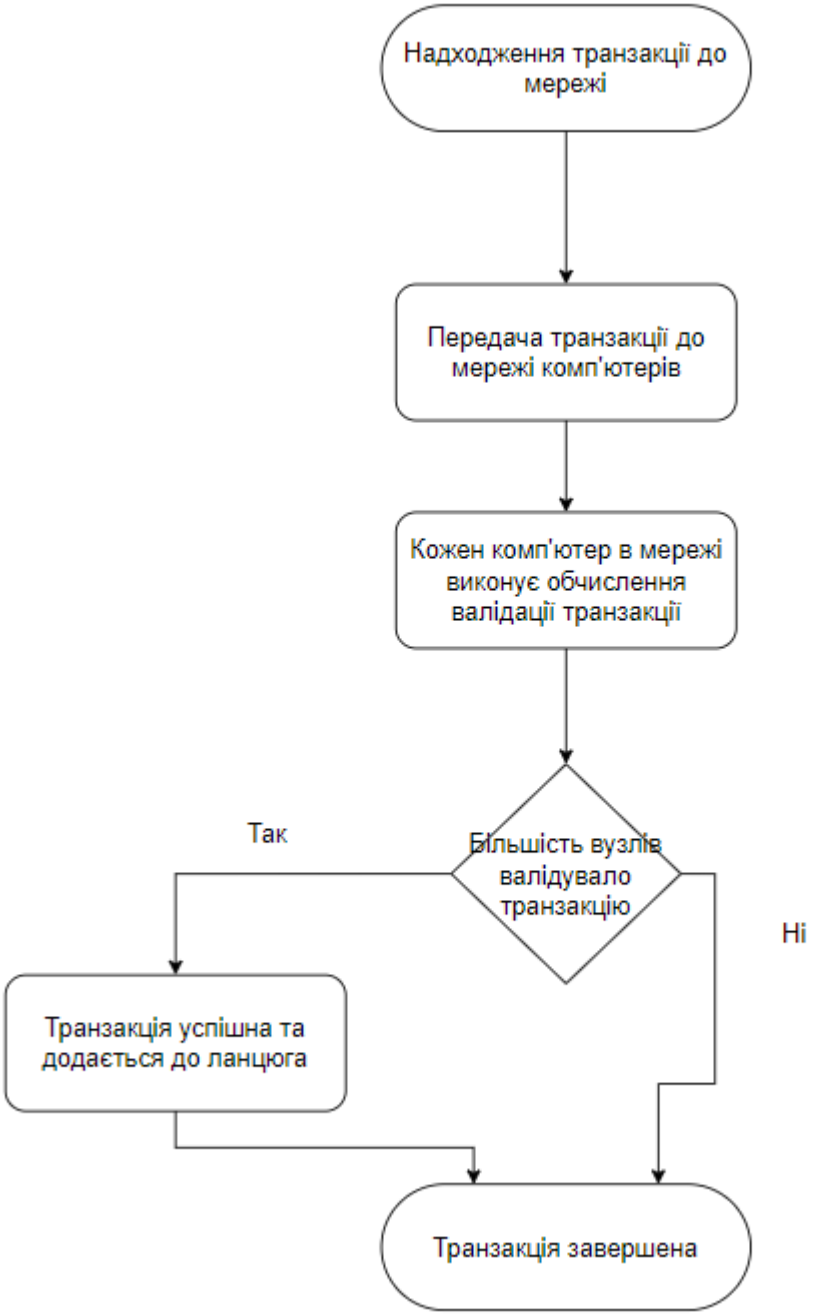

Рисунок 1.2 – Схема процесу валідації транзакції в блокчейні

В блокчейні існує декілька способів валідації транзакцій:

– підтвердження роботи (PoW);
– підтвердження частки (PoS).

В “підтвердженні роботи” валідація передбачає виконання конкретної роботи комп’ютером. Ноди які валідують транзакції у мережі також можно назвати майнерами. Кожен з них виконує потужні обчислення на своєму

комп’ютері необхідні для знаходження хешу транзакції. Після цього хеш порівнюється з результатом інших нодів та приймається рішення щодо подальшого включення транзакції в блок чи ні в випадку, колу хеш не співпадає з більшістю хешів в мережі. Нагородою за знаходження хешу є криптовалюта. Цей спосіб не є енергоефективним і саме тому на зміну йому деякі блокчейни використовують “підтвердження частки”. Цей спосіб валідації відрізняється тим, що використовує накопичену криптовалюту валідатора як основу довіри. Тобто маючи певну кількість криптовалюти можно заблокувати її в мережі і на основі цієї кількості буде прийматися рішення про транзакції. І чим більша ця кількість, тим більшу нагороду отримує володар. Позитивною стороною цього методу є низька енергозатратність на відміну від PoW. Але при цьому має важливу вразливість - якщо якийсь з нодів буде володіти більш ніж 50% від кількості криптовалюти, то він матиме змогу маніпулювати даними на свій розсуд [22].

Наразі існує чотири типи блокчейн-мереж:

– публічний - не має абсолютно ніяких обмежень доступу. Будь-хто, хто має підключення до Інтернету, може надсилати до нього транзакції, а також стати валідатором (тобто брати участь у виконанні протоколу консенсусу). Одними з найбільших, найвідоміших публічних блокчейнів є блокчейн біткойн та блокчейн Ефіріум;

– приватний - Доступ учасників та валідаторів обмежений. Щоб відрізнити відкриті блокчейни від інших однорангових децентралізованих застосунків баз даних, які не є відкритими спеціальними обчислювальними кластерами, для приватних блокчейнів зазвичай використовується термінологія розподілений реєстр (DLT);

– гібридний - поєднанує приватий і публічний підхід. Дозволяє організаціям створювати приватну систему, що базується на дозволах, поряд з публічною системою без дозволів, що дозволяє їм контролювати, хто може отримати доступ до певних даних, що зберігаються в блокчейні, і які дані будуть відкриті для громадськості;

– консорціумний - схожий на гібридний блокчейн, оскільки має риси приватного та публічного блокчейнів. Але він відрізняється тим, що кілька членів організації співпрацюють в децентралізованій мережі. По суті, консорціумний блокчейн - це приватний блокчейн з обмеженим доступом для певної групи, що усуває ризики, які виникають, коли лише одна організація контролює мережу в приватному блокчейні [23].

Технологія блокчейн може бути інтегрована в різні сфери. В першу чергу, метою блокчейну є надати здатність користувачам записувати та розповсюджувати цифрову інформацію без змоги редагування. Таким чином, блокчейн є базою для бухгалтерських операцій або записів про транзакції які не можуть бути відредаговані, видалені чи знищені. Тому основне використання блокчейнів - це розподілений реєстр для криптовалют. Більшість криптовалют використовують технологію блокчейн для запису транзакцій. Наприклад, мережа Біткоїн та мережа Етеріум базуються на блокчейні.

За останні кілька років з'явилося багато компаній, що пропонують децентралізовані криптовалютні біржі. Використання блокчейну для бірж дозволяє здійснювати транзакції швидше і дешевше. Крім того, децентралізована біржа не вимагає від інвесторів депонувати свої активи в централізованому органі, а це означає, що вони зберігають більший контроль і безпеку [24].

Технологія блокчейн може бути використана для створення постійної, публічної, прозорої системи обліку для збору даних про продажі, відстеження цифрового використання та виплат творцям контенту. Нові методи розподілу доступні для страхової галузі, такі як однорангове страхування, параметричне страхування та мікрострахування після прийняття блокчейну.

Блокчейн є потенційним шляхом монетизації ігрових застосунків. Багато ігор пропонують опції внутрішньоігрової кастомізації, такі як скіни персонажів або інші внутрішньоігрові предмети, які гравці можуть заробляти і торгувати з іншими гравцями, використовуючи внутрішньоігрову валюту.

Підгрупа цих ігор також відома як "грай, щоб заробляти", оскільки вони включають системи, які дозволяють гравцям заробляти криптовалюту через ігровий процес.

1.4 Огляд існуючих ігрових застосунків, створених з використанням блокчейну

1.4.1 CryptoKitties

Перша відома гра з використанням технологій блокчейн, випущена компанією Axiom Zen у листопаді 2017 року для персональних комп'ютерів [9]. Гравець купував NFT за криптовалюту Етеріум, кожен NFT складався з віртуального вихованця, якого гравець міг розводити з іншими для створення потомства з комбінованими ознаками як нових NFT (рис.1.3).

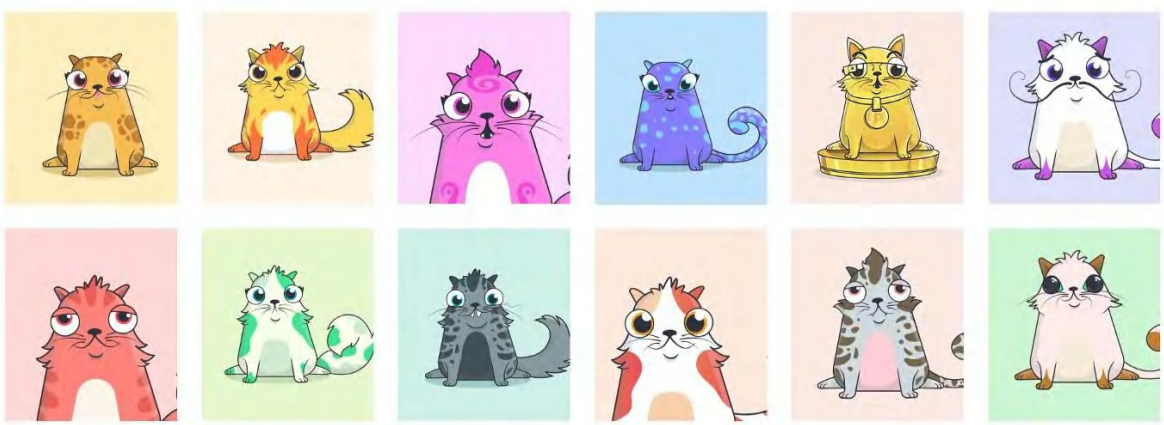

Рисунок 1.3 - Приклад NFT вихованців у грі CryptoKitties

NFT розшифровується як невзаємозамінні токени, тобто кожен токен є унікальною одиницею.

CryptoKitties потрапила в заголовки газет у грудні 2017 року, коли один віртуальний вихованець був проданий за понад 100 000 доларів США [25]. CryptoKitties також виявила проблеми з масштабуванням ігор на Етеріумі,

коли вона створила значні перевантаження в мережі Етеріум незабаром після свого запуску, приблизно 30% всіх транзакцій Етеріум на той час припадало на гру, а перевантаження затримувало транзакції гравців.

До недоліків гри можна віднести відносно слабкий геймплей, адже вся суть в створенні нових NFT, задля продажу, тобто застосунок більше схожий на веселу імітацію фондової біржі, де кожен намагається заробити більше грошей. З однієї сторони проект розпочав еру розробки ігрових застосунків з використанням блокчейну, а з іншої створив сумнівну репутацію для наступних проектів.

1.4.2 Axie Infinity

Випущена у 2018 році компанією Sky Mavis, є прикладом гри "грай, щоб заробляти", де гра стимулює гравців купувати, а потім покращувати NFT за допомогою внутрішньоігрових дій, а потім продавати токени іншим гравцям.

В основі геймплею полягає ідея створення гравцем унікальних монстрів Аксі (NFT) задля перемоги в боротьбі з іншими гравцями. Кожен Аксі має унікальні сильні і слабкі сторони, засновані на його генах. Ігровий процес реалізований в жанрі пошагової карткової стратегії (рис.1.4).

Рисунок 1.4 - Ігровий процес гри Axie Infinity

Гра працює на блокчейні Етеріум за допомогою Ронін, сайдчейна, який допомагає мінімізувати комісії та затримки транзакцій. Сайдчейн - це окрема мережа блокчейну, яка з'єднується з іншим блокчейном, який називається батьківським блокчейном або основною мережею, за допомогою двостороннього зв'язку [26]. Ці вторинні блокчейни мають власні протоколи консенсусу, що дозволяють мережі блокчейн підвищити рівень конфіденційності та безпеки, а також мінімізувати додаткову довіру, необхідну для підтримки мережі.

Після злому на початку 2022 року, в результаті якого у видавця Axie Infinity було викрадено понад 600 мільйонів доларів США, гра зазнала значного падіння кількості гравців, що вплинуло на економіку гри [27]. Компанія Sky Mavis видалила посилання на гру "грай і заробляй" на своїх веб-сайтах і в маркетингових матеріалах, оскільки її токени різко впали в ціні.

Axie Infinity є розвинутим нащадком CryptoKitties та повноцінною грою. Головним недоліком є неможливість грати без купівлі початкових Аксі, тобто NFT. На піці популярності для початку гри потрібно було інвестувати декілька тисяч долірів, що свідчить про таку саму проблему, як у CryptoKitties.

1.4.3 The Sandbox

Багатокористувацька онлайн гра, що використовує технологію блокчейна з елементами децентралізованих фінансів (DeFi) і незамінних токенів (NFT). Sandbox - це цілий ігровий метавсесвіт, у якому гравці можуть купувати й продавати "Землі", створювати й реалізовувати свої "Активи" - NFT-токени, а також брати участь в управлінні проектом, визначаючи вектор його подальшого розвитку. Метавсесвіт - це глобальна платформа, яка є і соціальною MMO, і ігровим конструктором.

The Sandbox позиціонує себе як платформа для створення і монетизації ігрового досвіду, в якій учасники створюють свої ігри та цілі віртуальні світи, при цьому творці мають право власності на свої творіння.

Sandbox користувач може пересуватися картою, виконувати різні завдання і проходити міні-ігри. Для нових гравців відкриваються не всі рівні, спочатку доступна тільки частина завдань. За успішне проходження видається нагорода [28].

Як приклад можна навести міні-гру parkour-game. У рамках цього квесту необхідно рухатися за вказаним маршрутом і збирати кубики, що світяться, долаючи поточні перешкоди (рис.1.5).

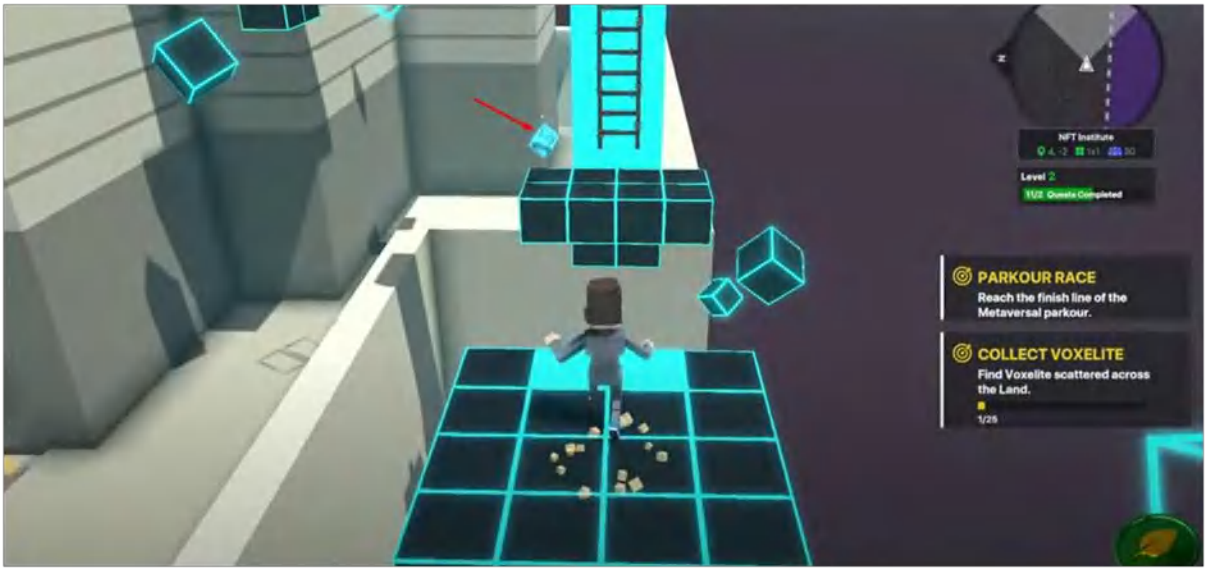

Рисунок 1.5 - Приклад користувальницької гри в метаверсі The Sandbox

Sandbox є аналогом популярної ігрової платформи Roblox, але замість спеціальної ігровою валюти використовується криптовалюта, а також в додаток користувачі самі створюють контент та обирають ціну.

Головним недоліком є обмеження самого ігрового рушія Sandbox: малий функціонал, відсутність можливості програмувати, наявність лише одного візуального стилю графіки з маленьких кубиків – вокселів. Тому створювати складні проекти поки не є можливим. Також для публікації гри потрібно придбати частинку на мінімапі проекті, так звану «Землю». Чим ближче ця

зона до іменитого проекту, тим дорожче вона коштує, але й більш приваблива для гравців.

1.4.4 Thetan Arena

Thetan Arena - це гібридна гра в жанрі MOBA, яка поєднує в собі моделі Free-to-Play і Play-to-Earn. В грі можна отримати безкоштовних героїв або придбати NFT, щоб почати заробляти. Геймплей доволі різноманітний: є багато героїв з різними здібностями та різні ігрові режими. Здібності та ефективність атаки персонажів залежать від їхнього класу. У персонажів є дві замінні здібності, які можна налаштувати перед початком гри, і одна унікальна незмінна – лють (рис. 1.6).

Рисунок 1.6 - Приклад геймплею гри Thetan Arena

Thetan Arena є прикладом хорошої гри з цікавими механіками, яка не робить основною ціллю гравця заробіток токенів, а в першу чергу виконує розважальну ціль, і додатково до цього надає можливість заробляти.

1.4.5 Core

Core - це безкоштовна онлайн-відеогра з інтегрованою системою створення ігор, розроблена компанією Manticore Games (рис.1.7). Вона вийшла у вигляді відкритої альфа-версії 16 березня 2020 року, а 15 квітня 2021 року стала доступною в режимі раннього доступу. Вбудований ігровий рушій має багато можливостей для створення власних проектів. Спочатку Core розроблявся як аналог Roblox, і тому розробники можуть монетизувати свій контент додаючи внутрішньоігрові покупки. Влітку 2022 року в Core почали інтегрувати блокчейн на базі криптовалюти Етеріум, з доступних функцій лише розміщення власних NFT на зображення свого аватару та у ігрових світах, але вже зараз з таким функціоналом розробники можуть швидко створювати свої блокчейн проекти.

Рисунок 1.7 - Приклад гри, розміщеної на платформі Core

Перевагою цієї гри є підхід до використання блокчейну, розробники Core лише дають користувачам можливість для створення власних світів і NFT тут не є єдиним шляхом, а просто додатковою можливістю.

1.4.6 Аналіз розглянутих ігор

З розглянутих ігрових застосунків можна зробити висновок, що найбільш популярний варіант використання блокчейну в таких проектах - це монетизація продукту та маркетинг, завдяки ідеї “грати для заробітку”. В більшості випадків для монетизації використовується метод торгівлі між гравцями. Гравець отримує ігровий предмет у вигляді NFT та має змогу продати його іншій людині. Такий спосіб зустрічається і в звичайних іграх з торгівельним майданчиком (DOTA 2 або CS:GO), тільки в них не гарантується володіння предметом, і якщо, наприклад, акаунт гравця заблокують, то він втратить всі свої ігрові предмети. Ця проблема вирішується використанням блокчейн технології, оскільки володіння предметом гарантоване.

Блокчейн ігри з’явилися доволі нещодавно, через що наразі досить небагато цікавих і унікальних проектів. З початку такі ігрові застосунки майже не мали геймплею, і були зосереджені лише на монетизації проекту. Нові блокчейн ігри характеризуються звичним для гри ігровим процесом та лише додатковою можливістю заробітку, що безумовно є позитивним розвитком індустрії. Саме агресивна монетизація та залучення гравців через ідею “грати для заробітку” породило велику кількість критики і недовіри в сторону ігрових застосунків з блокчейном. Основною проблемою жанру “грати для заробітку” також є економічна сторона, в якій токени гри видаються гравцю за різні дії, і коли інвестиції в гру становлять меншу частину, ніж кількість згенерованих токенів, то їх курс падає. Це спричиняє спад кількості гравців, а в випадках, коли це є основою геймплею - занепад проекту.

Аналіз предметної області показав, що блокчейн технології в розробці ігрових застосунків використовуються в більшості для створення ігрової економіки та опису володіння ігровим предметами, що зумовлено історією створення блокчейн технології. Одним із новітніх варіантів застосування блокчейн технології в ігрових застосунках є збереження ігрового процесу в

транзакціях та використання смарт-контрактів, розміщених в блокчейні як серверної частини гри. Такий підхід потребує дослідження його ефективності.

2 ОГЛЯД МЕТОДІВ ТА ТЕХНОЛОГІЙ, ЯКІ ЗАСТОСОВУЮТЬСЯ В ПРЕДМЕТНІЙ ОБЛАСТІ

2.1 Огляд криптовалют

Криптовалюта - це цифрова валюта, яка використовує криптографію для захисту, перевірки та полегшення транзакцій. Вона дозволяє користувачам здійснювати платежі в Інтернеті, не проходячи через традиційні платіжні системи, такі як банки та компанії, що видають кредитні картки [29].

Криптовалюта забезпечує безпечні та швидкі платежі за різні внутрішньоігрові покупки, такі як аватари, бонуси, теми, унікальні артефакти тощо. Це також дозволяє гравцям заробляти винагороди або крипто-жетони під час гри.

Криптовалюта виробляється всією системою колективно, за курсом, який визначається при створенні системи і який публічно оголошується. У централізованих банківських та економічних системах, таких як Федеральна резервна система США, корпоративні ради або уряди контролюють пропозицію валюти. У випадку з криптовалютою, компанії або уряди не можуть виробляти нові одиниці, і до цього часу не надавали підтримку іншим фірмам, банкам або юридичним особам, які володіють вартістю активів, виміряною в ній.

Більшість криптовалют призначені для поступового зменшення виробництва цієї валюти, встановлюючи обмеження на загальну суму цієї валюти, яка коли-небудь буде в обігу. У порівнянні зі звичайними валютами, що зберігаються фінансовими установами або зберігаються як готівка в касі, криптовалюти може бути важче вилучити правоохоронними органами [29].

Криптовалютний гаманець - це засіб зберігання публічного та приватного "ключів" (адреси) або "seed", які можуть бути використані для отримання або витрачання криптовалюти. За допомогою приватного ключа можна робити записи в публічній книзі, ефективно витрачаючи пов'язану з

ним криптовалюту. За допомогою відкритого ключа інші можуть надсилати валюту до гаманця.

Існує кілька методів зберігання ключів або seed в гаманці. Ці методи варіюються від використання паперових гаманців (які є публічними, приватними або насіннєвими ключами, записаними на папері), до використання апаратних гаманців (які є апаратним забезпеченням для зберігання інформації про ваш гаманець), до цифрового гаманця (який є комп'ютером з програмним забезпеченням, що містить інформацію про ваш гаманець), до розміщення вашого гаманця за допомогою біржі, де торгується криптовалюта, або шляхом зберігання інформації про ваш гаманець на цифровому носії, такому як відкритий текст.

2.2 Огляд блокчейн платформ

Блокчейн платформа - це структура з мовами сценаріїв, які є достатньо складними та надійними для створення та управління низкою функцій Web3, включаючи, але не обмежуючись ними, NFT, ініціювання та виконання транзакцій та створення смарт-контрактів [30].

Багато блокчейн-платформ є продуктами та підтримуються некомерційними фондами, як у випадку з різними криптовалютами, серед яких Ethereum, Tron, Ripple, Stellar, Solana та Polkadot.

Найвидатнішим кроком для розвитку блокчейн технологій послугувало створення блокчейн Етеріум, головною особливістю якого є змога створювати смарт-контракти.

2.2.1 Огляд смарт-контрактів

Смарт-контракти це програми розміщені в блокчейні і з якими користувачі мають змогу взаємодіяти. Зазвичай вони використовуються для автоматизації виконання угоди, щоб всі учасники могли бути відразу впевнені

в результаті, без участі посередників або втрати часу. Вони також можуть автоматизувати робочий процес, запускаючи наступну дію при виконанні певних умов[31].

Оскільки ці програми розміщені в блокчейні увесь їх код є публічним і кожен користувач має до нього доступ і може його перевірити. Така відкритість і прозорість є найголовнішою перевагою блокчейну над звичайними способами взаємодії. Наприклад, якщо порівняти такий підхід зі звичайною веб-сторінкою, то виявиться, що користувачу ніколи не відомо що насправді відбудеться після того як він натисне кнопку, особливо це стосується дій, що виконуються на сервері. Це є звичайною практикою, коли серверний код схований та не доступний користувачам.

Проте, важливо зазначити, що навіть при змозі подивитися смарт-контракт, це не значить, що він не зловживає людською довірою. Є безліч механізмів які важко помітити не спеціалісту в сфері аудиту або розробки смарт-контрактів. Наприклад, розробники можуть писати код в стилі, який буде важко прочитати чи зрозуміти. Також можливо неправильна назва змінних та методів. Або порушення принципів програмування задля заплутаності коду. Найчастіше розробники залишають для себе змогу маніпулювати даними. І частіше за все це можливість відправити на свій гаманець кошти які належать іншим людям. Через це для того щоб можна було довіряти якомусь проекту базованому на блокчейні розробники повинні надати свій проект до аудити і лише після публікації висновків можна взаємодіяти з їхніми смарт-контрактами.

Також важливо зазначити про детермінованість блокчейну, а саме усі операції в смарт контракті завжди призводять до одного й того самого результату. Простіше кажучи 5 + 8 завжди буде дорівнювати 13. Це здається надто звичайним, але це є класичною проблемою в програмуванні яка трапляється при роботі з числами з плаваючою комою. Кожен процесор по різному виконує обчислення і звичайна математична операція 0.25 + 0.25

по- перше ніколи дорівнюватиме 0.5, а по-друге результат буде різний на різних пристроях.

Самі по собі смарт-контракти не можуть отримувати інформацію про події "реального світу", оскільки вони не можуть відправляти HTTP-запити. Це передбачено конструкцією. Покладання на зовнішню інформацію може поставити під загрозу консенсус, який є важливим для безпеки та децентралізації [32].

Контракти з мультипідписом - це акаунти смарт-контрактів, які вимагають декількох дійсних підписів для виконання транзакції. Це дуже корисно для уникнення єдиної точки відмови для контрактів, що містять значну кількість Етеріума або інших токенів. Мультипідписи також розподіляють відповідальність за виконання контракту і управління ключами між декількома сторонами і запобігають втраті одного приватного ключа, що призводить до незворотної втрати коштів [30]. З цих причин контракти з мультипідписом можуть використовуватися для простого управління DAO. Для виконання мультипідпису потрібно N підписів з M можливих прийнятних підписів (де $N \leq M$, а $M > 1$). Зазвичай використовуються $N = 3$, $M = 5$ та $N = 4$, $M = 7$. Мультипідпис 4/7 вимагає наявності чотирьох з семи можливих дійсних підписів. Це означає, що кошти все ще можна отримати, навіть якщо три підписи будуть втрачені. У цьому випадку це також означає, що більшість власників ключів повинні погодитися і поставити свої підписи для того, щоб контракт був виконаний.

Після появи смарт-контрактів користувачі почали створювати свої застосунки з використанням блокчейну. Децентралізовані обмінники, де можна було без ризиків обміняти криптовалюти і нарешті NFT.

2.2.2 Огляд NFT

NFT - розшифровується як невзаємозамінні токени. Тобто кожен токен є унікальною одиницею. Прикладом взаємозамінного токену є гроші в

справжньому світі або поштові марки з однаковими зображеннями чи інше. Звичайним прикладом невзаємозамінних токенів є колекційні предмети такі як картини та витвори мистецтва.

В першу чергу NFT слугує для чіткого відображення права власності користувача над електронним чи реальним майном. Також це дозволяє визначити наперед способи майбутньої взаємодії' з предметом, чи якісь сторонні явища [15]. Наприклад, художник створив зображення та розмістив його у блокчейні цим самим він є єдиним власником цього предмету і лише своїми діями він може передати власність комусь іншому. Також він може налаштувати яку частину коштів він буде отримувати після кожного продажу його картини між користувачами. І користувачі не матимуть змогу обійти ці налаштування. Саме це привабило багатьох художників створювати NFT та обрати цей напрямок як свою основну працю.

Конкретні стандарти токенів підтримують різні варіанти використання блокчейну. Ethereum був першим блокчейном, який підтримав NFT за допомогою свого стандарту ERC-721, і в даний час він є найбільш широко використовуваним. Багато інших блокчейнів додали або планують додати підтримку NFT.

ERC-721 був першим стандартом для представлення невзаємозамінних цифрових активів в блокчейні Ethereum. ERC-721 є успадкованим стандартом смарт-контрактів Solidity; "успадкований" означає, що розробники можуть створювати нові контракти, сумісні з ERC-721, шляхом копіювання з еталонної реалізації. ERC-721 надає основні методи, які дозволяють відстежувати власника унікального ідентифікатора, а також дозволений спосіб для власника передавати актив іншим особам.

Стандарт ERC-1155 пропонує напівзамінність, а також забезпечує аналог функціональності ERC-721 (це означає, що актив ERC-721 може бути побудований з використанням ERC-1155). На відміну від ERC-721, де унікальний ідентифікатор представляє один актив, унікальний ідентифікатор токена ERC-1155 представляє клас активів, і є додаткове поле кількості для

представлення кількості класу, який має певний гаманець. Активи одного класу є взаємозамінними, і користувач може передавати будь-яку кількість активів іншим.

2.3 Огляд Oracle сервісів

Більшість розробників розглядають смарт-контракти як просто фрагменти коду, що виконуються за певними адресами в блокчейні. Однак більш загальний погляд на смарт-контракти полягає в тому, що вони є самодостатніми програмними продуктами, здатними забезпечувати виконання угод між сторонами після виконання певних умов.

Але використання смарт-контрактів для забезпечення виконання угод між людьми не є простим, враховуючи, що Ethereum є детермінованою системою. Детермінована система - це система, яка завжди видає однакові результати, враховуючи початковий стан і конкретні вхідні дані - немає ніякої випадковості або варіацій в процесі обчислення вихідних даних на основі вхідних.

Щоб досягти детермінованого виконання, блокчейн обмежує вузли в досягненні консенсусу щодо простих бінарних (істина/хибність) питань, використовуючи тільки дані, що зберігаються в самому блокчейні.

Для публічного блокчейну, такого як Ethereum, з тисячами вузлів по всьому світу, які обробляють транзакції, детермінізм має вирішальне значення. За відсутності центрального органу, який слугує джерелом істини, очікується, що вузли повинні прийти до однакового стану після застосування одних і тих же транзакцій. Випадок, коли вузол А виконує код смарт-контракту і отримує в результаті "3", в той час як вузол Б отримує "7" після виконання тієї ж транзакції, призведе до руйнування консенсусу і знищить цінність Ethereum як децентралізованої обчислювальної платформи. Також великою проблемою в смарт-контрактах є отримання випадкових чисел, адже якщо згенерувати число на основі відомої інформації (зазвичай

використовують час), то його буде легко передбачити, чим можуть користуватися шахраї. Це підкреслює проблему з проектуванням блокчейнів для отримання інформації із зовнішніх джерел. Oracles, однак, вирішує цю проблему, беручи інформацію з позамережевих джерел і зберігаючи її в блокчейні для споживання смарт-контрактами. Оскільки інформація, що зберігається в ланцюжку, є незмінною і загальнодоступною, вузли Ethereum можуть безпечно використовувати дані поза ланцюжком для обчислення змін стану, не порушуючи консенсус.

Oracle - це застосунки, які отримують, перевіряють і передають зовнішню інформацію (тобто інформацію, що зберігається поза ланцюжком) смарт-контрактам, що працюють на блокчейні. Oracle діють як "міст", що з'єднує смарт-контракти на блокчейні з позамережевими постачальниками даних [33]. Без Oracle застосунків смарт-контракти могли б отримати доступ тільки до даних в ланцюжку. Oracle забезпечує механізм запуску функцій смарт-контракту за допомогою позамережевих даних.

Для цього Oracle, як правило, складається зі смарт-контракту, що працює в мережі, і деяких позамережевих компонентів. Внутрішньосистемний контракт отримує запити на дані від інших смарт-контрактів, які він передає позасистемному компоненту (який називається вузлом оракула). Цей вузол-оракул може запитувати джерела даних - наприклад, використовуючи інтерфейси прикладного програмування (API) - і відправляти транзакції для зберігання запитаних даних у сховищі смарт-контракту.

По суті, Oracle блокчейну заповнює інформаційний розрив між блокчейном і зовнішнім середовищем, створюючи "гібридні смарт-контракти". Гібридний смарт-контракт - це контракт, який функціонує на основі комбінації коду онлайн контракту та позамережевої інфраструктури. Гібридні смарт-контракти дають змогу використовувати передові форми економічної та соціальної кооперації, які володіють властивостями блокчейн, що забезпечують захист від злому і незмінність

2.4 Огляд технології IPFS

Збереження великих даних безпосередньо в блокчейні є дорогим, тому для другорядної інформації використовують технологію IPFS. IPFS (InterPlanetary File System) - протокол зв'язку для створення розподіленої файлової системи, покликаний замінити існуючий інтернет-протокол HTTP. Контент, розміщений в IPFS, зберігається не на одному сервері, а на безлічі вузлів.

IPFS - важливе інфраструктурне рішення для Web3, яке дає змогу децентралізувати зберігання даних у різних децентралізованих застосунках, зокрема NFT, GameFi, DeFi [34].

Ключова відмінність IPFS від наявного інтернет-протоколу HTTP у тому, що доступ до даних здійснюється не за місцем розташування сайту, а безпосередньо за адресою його вмісту (файлу, документу, зображення, папки).

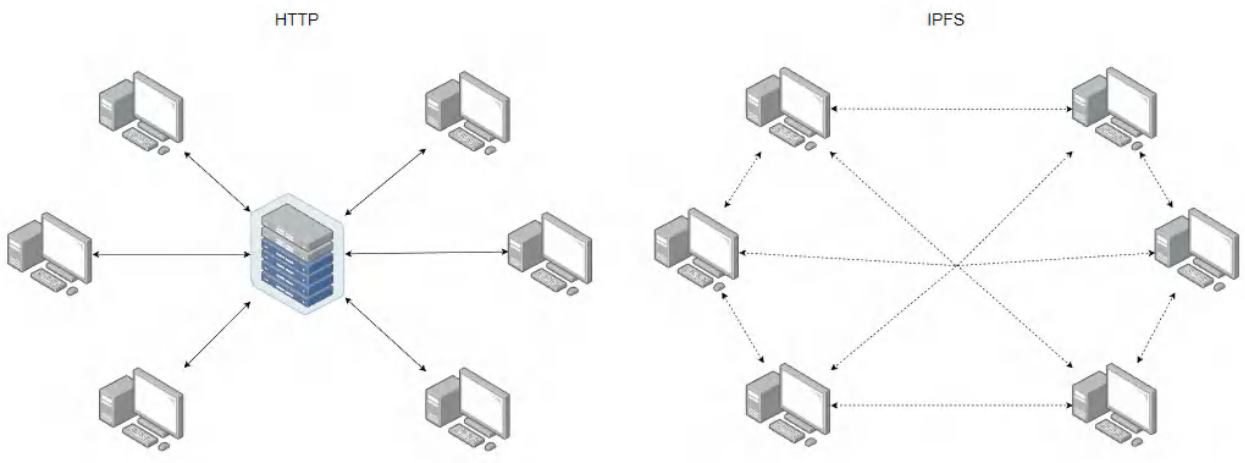

Рисунок 2.1 – Схема роботи технологій HTTP та IPFS

Під час завантаження контенту в IPFS адреса для доступу до об'єкта, файлу або користувацьких даних у системі формується з прив'язкою не до адреси сервера, якою є IP-адреса, а до його унікального криптографічного хеш-ідентифікатора Content Identifier (CID) [35].

Під час повторного завантаження файлу CID не змінюється, а оновленим версіям файлу присвоюються нові хеш-ідентифікатори. Щоб отримати доступ до ранньої версії файлу, застосовується сервіс імен InterPlanetary Naming System (IPNS) - аналог реєстру DNS.

Файли IPFS розміром понад 256 Кб розбиваються на частини, хешуються й організовуються в IPLD-об'єкти (InterPlanetary Linked Data). IPLD складається з двох компонентів: самих даних і посилань на частини файлу, пов'язаних між собою через спрямований ациклічний граф дерева Меркла (Merkle DAG).

3 ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

В межах дослідження, що проводиться можна поділити ігрові застосунки на 2 типи:

– ігри розроблені з використанням блокчейну;
– ігри розроблені без використання блокчейну.

Кожен тип ігрового застосунку характеризується певним набором параметрів, що можна класифікувати з точки зору користувача застосунку, тобто розробника і гравця.

Ігри розроблені з використанням блокчейну з боку гравця:

– повне право на володіння ігровими предметами;
– гарантії в цілісності даних;
– сплата комісій за транзакції;
– для оцінки надійності гри на блокчейні потрібно мати мінімальні знання про дану сферу технологій;
– гарантії в тому, що розробники не можуть змінити ключові параметри гри, збережені в блокчейні.

Ігри розроблені з використанням блокчейну з боку розробника:

– висока складність розробки;
– відсутність інформації щодо ефективності блокчейну в іграх;
– надійне зберігання даних гравця;
– прозорість інформації щодо стану ігрових предметів;
– низький рівень складності створення ігрових активів у вигляді NFT.

Ігри розроблені без використання блокчейну з боку гравця:

– простота розуміння надійності проекту;
– покупка віртуальних предметів відбувається за реальну валюту, тому гравцям не потрібно розбиратися в криптовалюті;
– шанс втрати ігрового акаунту;
– можливість придбати гру на всесвітньовідомих платформах;

Ігри розроблені без використання блокчейну з боку розробника:

– низька складність реалізації серверної частини гри;
– велика кількість досліджень ефективності;
– велика кількість готових рішень щодо реалізації серверної частини;
– простота розміщення гри на сервері.

Необхідно дослідити ефективність використання блокчейну в ігрових застосунках як технології для реалізації серверної частини гри та збереження ігрових активів у вигляді NFT.

Для оцінки ефективності використання блокчейну в ігрових застосунках потрібно розробити показники для її визначення, на основі яких провести експериментальне дослідження на прикладі гри розробленої з використанням блокчейну та гри розробленої без використання блокчейну. Результати дослідження необхідно порівняти та зробити висновки щодо ефективності блокчейну в ігрових застосунках.

4 РОЗРОБКА МЕТОДУ

4.1 Опис досліджуваного ігрового застосунку

За час розвитку блокчейн технологій з’явилась велика кількість ігрових застосунків, що використовують блокчейн для побудови ігрових механік. Одним із провідних прикладів використання блокчейну в ігрових застосунках є Dark Forest (рис. 4.1).

Рисунок 4.1 – Геймплей ігрового застосунку Dark Forest

Dark Forest – це браузерна 2.5D багатокористувацька онлайн-стратегія в жанрі космічних завоювань, де гравці відкривають і завойовують планети в нескінченному, процедурно-генерованому, криптографічно заданому всесвіті. В обчислювальній техніці процедурне генерування - це метод створення даних алгоритмічно, а не вручну, як правило, за допомогою поєднання створених людиною ресурсів та алгоритмів у поєднанні з комп'ютерною випадковістю та обчислювальною потужністю. У комп'ютерній графіці він зазвичай використовується для створення текстур і 3D-моделей. У відеоіграх він використовується для автоматичного створення великої кількості контенту в

грі [36]. Процедурна генерація дозволяє створювати багаті ігрові світи (ландшафти, підземелля, замки, хмари і тд.) програмно за допомогою виразних, але недорогих алгоритмів, які можна запускати на блокчейні. Алгоритми процедурної генерації, як правило, намагаються імітувати природні процеси формування світу, вкладаючи різноманітність і реалістичність в псевдовипадковість своїх результатів. Тобто карта ігрового застосунку в кожній ітерації буде різною та унікальною. Вигляд карти залежить від кількості гравців в ігровій сесії та масштабу їх дослідження ігрового світу (автоматично додаватимуться нові планети, кожен гравець отримуватиме випадкове місце для бази в галактиці).

Криптографія - це метод захисту інформації та комунікацій за допомогою використання кодів, щоб тільки ті, для кого інформація призначена, могли її прочитати і обробити. Поняття криптографічно заданого всесвіту означає, що місцезнаходження інших гравців захищене в блокчейні.

Основний ігровий цикл Dark Forest полягає в дослідженні всесвіту і поступовому завойовуванні все більше планет і розширенні космічної імперії. Всі гравці з’являються з рідною планетою і баченням над невеликою областю в своєму куточку всесвіту, з туманом війни (відображення областей ігрової карти, які знаходяться за межами поля зору гравця або які гравець ще не відкрив), що покриває карту. Планети мають енергію, яка з часом регенерується. Для завоювання планети потрібно посилати енергію зі своїх планет на інші. На деяких планетах є срібло та артефакти, які дають додаткові бали, що визначають ранг гравця.

Ігрові сесії проходять у вигляді раундів, які тривають декілька днів. В кожному раунді гравцеві надається додаткова ціль, наприклад, знайти певні види небесних об'єктів, які називаються астероїдними полями, видобути на них ресурси, переправити їх на торгові пости і таким чином вивести їх з гри. Гравці отримують бали в залежності від того, наскільки добре вони змогли це зробити. Отже, гравець досліджує всесвіт, розвиває свою імперію, виконує

певні завдання, конкурує з іншими гравцями, вступає з ними в дипломатичні відносини.

Dark Forest належить до ігрових застосуноків з неповною інформацією - це застосунки, в яких гравці можуть не знати повного стану світу. Наприклад, покер є грою з неповною інформацією, оскільки гравець не знає які карти у його опонента на руках. Стратегічні ігри, такі як StarCraft і EVE Online, також потрапляють в цю категорію. У StarCraft та інших стратегіях в реальному часі приховування інформації забезпечується за допомогою туману війни - ділянки ігрової карти затушовуються до тих пір, поки вони не будуть досліджені гравцем. Ігри з неповною інформацією дозволяють гравцям досліджувати більш багатий і драматичний простір стратегій. Інформаційна асиметрія уможливлює такі речі, як обман, умовна координація та складна соціальна динаміка. Через це майже кожна популярна ММО-гра (massively multiplayer online game, масова багатокористувацька онлайн-гра) є неповною інформаційною грою.

ММО це онлайн-відеогра з великою кількістю гравців, часто сотнями або тисячами, на одному сервері [8]. ММО зазвичай мають величезний, постійний відкритий світ, хоча є ігри, які відрізняються. Ці ігри можуть дозволити гравцям співпрацювати і змагатися один з одним у великих масштабах, а іноді і змістовно взаємодіяти з людьми по всьому світу. Вони включають в себе різноманітні типи геймплея, що представляють багато жанрів відеоігор.

До цього часу було майже неможливо побудувати неповні інформаційні налаштування в децентралізованих системах. Це пов'язано з тим, що шари даних більшості децентралізованих систем за своєю структурою є повністю відкритими і прозорими. Якщо повний стан гри зберігається в прозорому шарі даних, який може перевірити будь-хто, не може існувати поняття приватної інформації.

У традиційній системі існує один централізований суб'єкт, який є посередником для всіх інших – це сервер. Мережа виглядає як центральний вузол, що з'єднує всі підпорядковані йому вузли.

У системі блокчейн немає центрального серверу, всі рівні. Для комунікації хтось звертається до сусідніх вузлів, які, в свою чергу, спілкуються зі своїми сусідами, поки повідомлення не поширюється по всій системі (рис. 4.2).

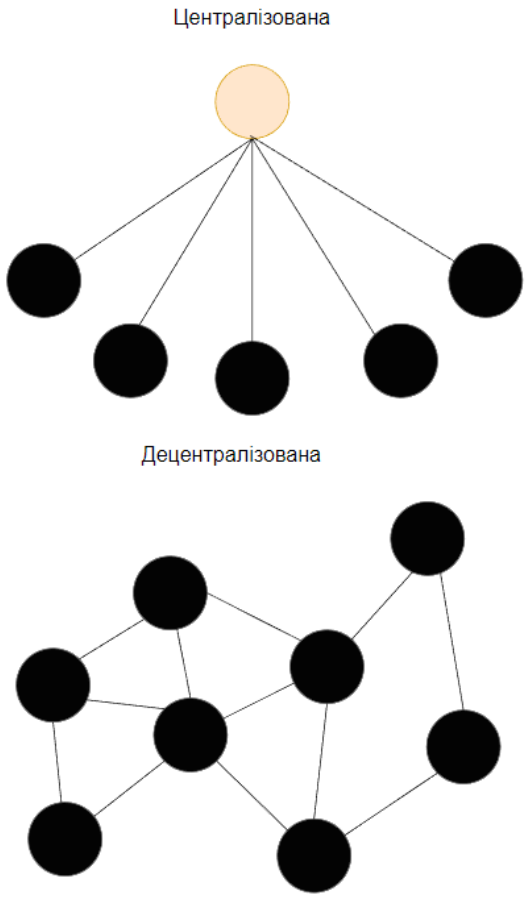

Рисунок 4.2 – Схема централізованої та децентралізованої системи

Ігровий стан Dark Forest зберігається в блокчейні. Кожен раз, коли гравець виконує якусь дію, наприклад, запускає космічний корабель, він відправляє транзакцію для оновлення стану ланцюжка. Dark Forest працює на блокчейні Ethereum та сайдчейні Gnosis Chain. Приховані координати планети

гравця в публічному блокчейні доступні завдяки доказам з нульовими знаннями.

4.2 Опис ігрового застосунку аналогу для порівняння

Ігровим застосунком, що є найбільш схожим на Dark Forest за ігровим процесом та механіками серед ігор, що не використовують блокчейн, є Galcon 2 (рис. 4.3). Galcon 2 – це 2D стратегія в режимі реального часу з багатокористувальницьким та однокористувальницьким режимами гри. Суть застосунку полягає в тому, що гравці використовують своїх поступово згенерованих юнітів, щоб перемогти інших гравців. Кожен гравець починає з однаковою кількістю баз і повинен використовувати своїх юнітів для захоплення нейтральних баз, щоб збільшити загальне виробництво юнітів.

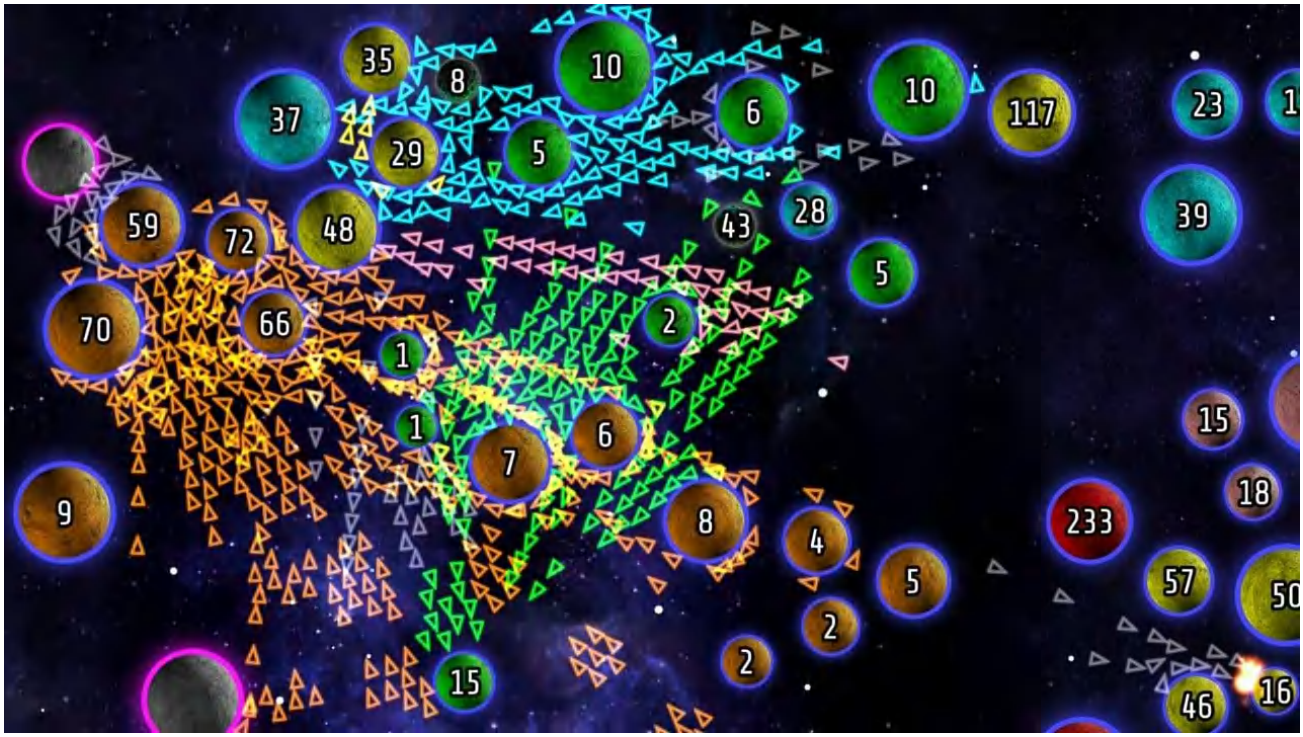

Рисунок 4.3 - Геймплей ігрового застосунку Galcon 2

4.3 Докази з нульовими знаннями

Доказ з нульовим знанням (Zero-Knowledge Proof, ZKP) - це протокол, який дозволяє довести, що вам відомий деякий конкретний математичний факт, не розкриваючи при цьому ніякої інформації про сам факт. Доказ, згенерований в протоколі з нульовим знанням, називається доказом з нульовим знанням. Щоб зробити це можливим, протоколи нульового знання покладаються на алгоритми, які приймають деякі дані на вході і повертають "істину" або "брехню" на виході [37].

Рання версія ZKP дозволяла доводити лише один вид математичних фактів на той час і для вирішення цієї проблеми було розроблено zkSNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, стислий неінтерактивний аргумент нульового знання про знання) - метод, що може згенерувати ZKP для будь-якої математичної функції [37]. zkSNARK також гарантує, що доказу є "стислим" та "неінтерактивним": можна створити цей доказ у лінійному часі, а інші можуть перевірити його у постійному часі, не ставлячи доказуючому додаткових запитань. Ці властивості роблять SNARKs корисними для блокчейн-додатків, де користувачі можуть створювати докази локально, а потім завантажувати короткі докази для перевірки в постійному часі всередині смарт-контракту, де обчислення є дорогим.

Наразі докази zkSNARK залежать від початкової довірливої установки між тим, хто перевіряє, і тим, хто верифікує, що означає, що для створення доказів з нульовим розголошенням для приватних транзакцій потрібен набір відкритих параметрів. Ці параметри майже відповідають правилам гри, вони закодовані в протокол і є одним із необхідних чинників, які підтверджують, що транзакція була дійсною.

ZkSNARK розширює можливості блокчейн технології. За замовчуванням, все в блокчейні є загальнодоступним. Будь-хто може переглянути всю історію транзакцій і переконатися, що все було виконано правильно до цього моменту. Однак у цього є і зворотна сторона, яка полягає

в тому, що всі дані про транзакції є загальнодоступними. Таким чином, zkSNARKS в основному дозволить здійснювати транзакції в більш приватній манері, де буде можливість частково приховати або зашифрувати певні ключові частини даних, зберігаючи при цьому гарантії безпеки і властивості перевірки, які так важливі для блокчейнів. Іншою перевагою є масштабованість. Ідея в основному полягає в тому, що за допомогою zkSNARKS можна згорнути обчислення в одну лише перевірку, таким чином, що якщо хтось хоче згенерувати доказ того, що він виконав обчислення правильно, то для того, щоб перевірити правильність результатів цих обчислень, все, що потрібно зробити, це перевірити доказ. Така перевірка доведення за допомогою zkSNARKS є досить ефективною та прискорює багато операцій, які зазвичай вимагають великий об’єм обчислювальної потужності.

Оскільки zkSNARKS дозволяють виконувати обчислення над приватними даними, але таким чином, щоб їх можна було перевірити, вони відкривають можливості використання блокчейну для ігор з неповною інформацією, які раніше були неможливі через прозорий і відкритий характер даних на блокчейні.

4.4 Використання доказів з нульовим знанням в Dark Forest

Центральною механікою в Dark Forest є туман війни. Туман війни гарантує, що гравець не знає, де знаходяться всі гравці, планети та інші точки інтересу у всесвіті, а повинен витрачати обчислювальні ресурси, щоб виявити їх. Цю механіку забезпечують zkSNARKs.

У всесвіті з туманом війни локації всіх гравців є приватними і приховані один від одного. Це означає, що гравці не завантажують координати своїх планет в блокчейн Ethereum, які можуть бути публічно перевірені. Замість цього кожен гравець завантажує в блокчейн хеш свого місцезнаходження. Це гарантує, що гравці залишаються "прив'язаними" до певного місця, але також

і те, що місце розташування не може бути визначене шляхом перевірки шару даних Ethereum.

Без zkSNARKs існує вектор атаки - якщо гравець завантажує випадковий рядок байтів, який не відповідає реальному і дійсному місцезнаходженню, і цілісність гри порушується. Щоб запобігти цьому, Dark Forest вимагає від гравців надсилати zkSNARK з кожним ходом, щоб переконатися, що гравці дійсно надсилають хеші, що відповідають дійсним координатам, які їм відомі.

Коли гравці роблять ходи, вони також зобов'язані подавати ZK-докази того, що їхні ходи є дійсними - гравець не можете рухатися занадто далеко або занадто швидко. Без zkSNARK зловмисний гравець міг би робити незаконні "телепортаційні" ходи, стверджуючи, що хеш, з якого він рухається, знаходиться поруч з хешем, до якого він рухається, навіть якщо ці дві локації насправді знаходяться на протилежних сторонах всесвіту. Знову ж таки, вимога доказів ZK робить гравців чесними [38]. Використовуючи шахову аналогію, необхідні ZK-докази, по суті, говорять контрагенту: "Я переміщаю свого коня; я не збираюся говорити вам, звідки я перемістив свого коня або куди я його перемістив, але цей доказ доводить, що він дійсно перемістився в легальній L-формі".

Функції zkSNARKs записані у вигляді схем на мові Circom - надійній та масштабованій мові для побудови складних схем з нульовими знаннями. Dark Forest захищений двома ланцюгами нульового знання: *init* і *move*. Гравці генерують ZKP з ланцюга *init*, коли вони приєднуються до гри, і ZKP з ланцюга *move*, коли вони роблять хід.

Для створення хешу місцезнаходження використовуються хеш-функції MiMC. MiMC - це хеш-функція з сімейства "SNARK-дружніх" хеш-функцій, для яких легко генерувати ZKP. SNARK-дружні функції - це функції, які максимально наближені до базової арифметики. Хеш-функція MiMC спеціально розроблена для мінімізації розміру схеми і, отже, вартості ZKP завдяки використанню тільки додавання і множення.

Хеш-функція в Dark Forest включає в себе послідовність 220 повторюваних операцій множення і додавання, що достатньо для того, щоб спроба зворотного інжинірингу попереднього зображення хешу була надзвичайно дорогою, але достатньо мало для того, щоб її все ще можна було обчислити сучасними інструментами SNARK.

Під час ініціалізації гравці можуть вибрати будь-яку допустиму рідну планету для початку гри. Гравці вибирають деяку локацію *(x,y)*, обчислюється хеш *h* місцезнаходження, і хеш відправляється в блокчейн разом з ZKP, щоб довести, що хеш з дійсного місцезнаходження. Допустимим розташуванням є будь-яка пара координат *(x,y)* що не перевищує r одиниць від початку координат, де *r* поточний радіус світу (гравці не можуть ініціалізуватись як завгодно далеко). Отже, SNARK повинен довести 2 речі:

$$MiMC(x,y)=h$$
$$x2+y2\leq r2$$

Смарт-контракт отримає публічні сигнали, *r* і *h*, разом з ZK-доказом того, що вони відповідають дійсній приватній парі координат *(x,y)*. Якщо цей zkSNARK працює коректно, то контракт зможе перевірити достовірність початкових координат, не маючи жодного уявлення про те, якими вони є насправді.

4.5 Опис взаємодії з мовою Circom

Circom - це предметно-орієнтована мова для визначення арифметичних схем, яка може бути використана для генерації доведень з нульовим знанням [39]. Компілятор Circom - це компілятор мови Circom, написаний на Rust, за допомогою якого можна згенерувати файл R1CS з набором пов'язаних з ним обмежень та програму (написану на C++ або WebAssembly) для ефективного обчислення допустимого присвоєння значень всім схемам мови Circom. R1CS

(rank-1 constraint system, система обмежень 1-го рангу) – формат для вираження розрахунку програми, що відстежує значення, які приймає кожна змінна під час обчислення, і пов'язує взаємозв'язки між усіма тими змінними, які маються на увазі в самому обчисленні.

Однією з головних особливостей мови Circom є її модульність, що дозволяє програмістам визначати параметризовані схеми, які називаються шаблонами, які можуть бути конкретизовані для формування більших схем. Ідея побудови схем з невеликих окремих компонентів полегшує тестування, огляд, аудит або формальну перевірку великих і складних схем Circom. У зв'язку з цим користувачі Circom можуть створювати власні шаблони або копіювати шаблони з CircomLib, загальнодоступної бібліотеки, яка налічує сотні схем, таких як компаратори, хеш-функції, цифрові підписи, двійкові та десяткові перетворювачі та багато іншого.

Circom має на меті надати розробникам цілісний фреймворк для побудови арифметичних схем за допомогою простого у використанні інтерфейсу та абстрагування від складності механізмів доведення.

Dark Forest є браузерною грою, клієнтська версія якої розроблена на мові програмування TypeScript, що є мовою, яка розширює можливості JavaScript. Тому застосунок використовує snarkjs – JavaScript реалізацію схем zkSNARK. Snarkjs містить код для генерації та перевірки доказів ZK з схем, створених мовою Circom.

Взаємодія мови Circom з snarkjs та блокчейном виконується за таким алгоритмом:

- арифметична схема функції записується на мові Circom;
- схема інтерпретується до рівня R1CS в компіляторі Circom;
- snarkjs приймає R1CS та на основі отриманих даних генерує доказовий ключ та ключ валідації;
- в snarkjs генерується доказ zkSNARK на основі доказового ключа;
- доказ на основі ключа валідації підтверджується в snarkjs або смарт-контрактах, після чого генерується код перевіряючого.

Схематичне зображення взаємодії мови Circom з snarkjs зображено на рис. 4.4

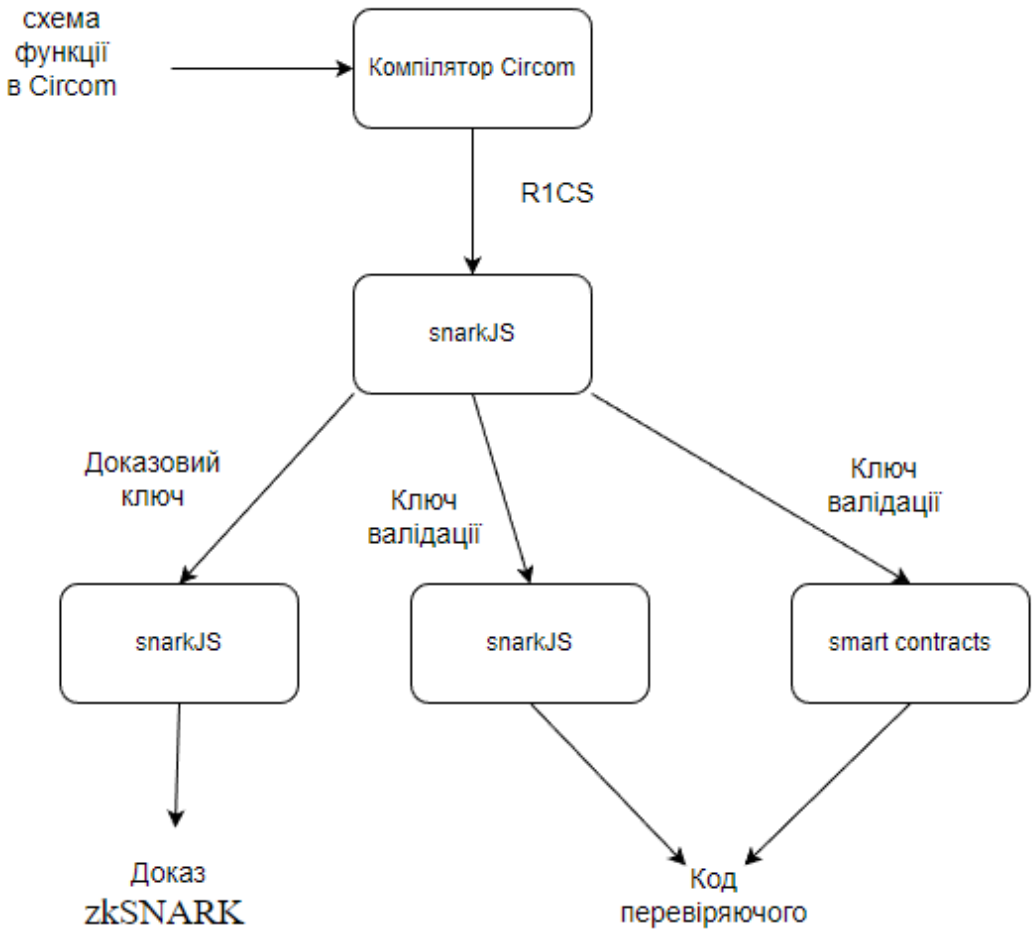

Рисунок 4.4 – Схема взаємодії мови Circom з JS бібліотекою та блокчейном

4.6 Опис мережевої архітектури ігрових застосунків

Основною частиною онлайн гри є мережева взаємодія між гравцями, для реалізації якої існує декілька архітектурних рішень: однорангова та клієнт-серверна. Однорангова (Peer-to-peer, P2P) — варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів [40]. Комп'ютерні мережі типу P2P засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи можуть зв'язуватися між собою (рис. 4.5).

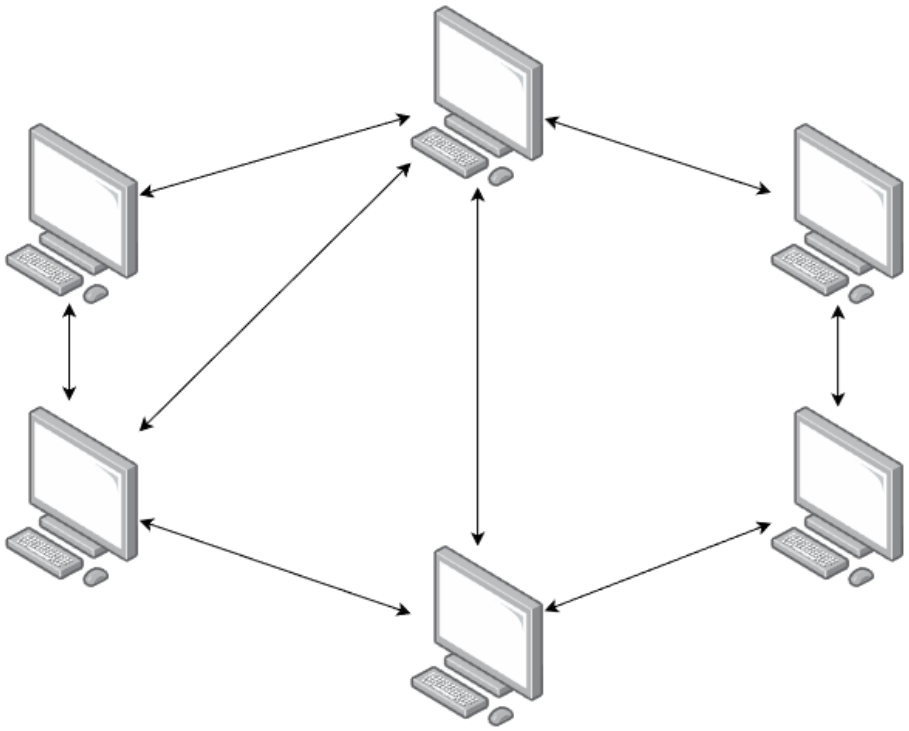

Рисунок 4.5 – Схема роботи однорангової архітектури

В одноранговій архітектурі не існує нейтральної інстанції, яка б керувала грою, тому довіру доводиться покладати на одного або декількох клієнтів (комп'ютер/пристрій, що фактично використовує послугу або приймає інформацію) в мережі. Це надзвичайно ускладнює запобігання шахрайству з боку мотивованого зловмисника, оскільки він може маніпулювати даними через мережеві комунікації. Тому більше популярним та надійним рішенням для розробки онлайн ігор є клієнт-серверна архітектура.

В архітектурі клієнт-сервер кожен гравець керує власним клієнтом, а всі гравці підключені до центрального сервера (рис 4.6). Сервер - це віддалений комп'ютер, який забезпечує доступ до даних і послуг [40]. Сервери, як правило, є фізичними пристроями, такими як стійкові сервери, хоча зростання хмарних обчислень призвело до появи віртуальних серверів. Сервер виконує ігрову логіку і транслює стан гри клієнтам. Клієнти відтворюють стан і збирають вхідні дані від гравців. Сервер використовує вхідні дані для модифікації симуляції.

Рисунок 4.6 – Схема клієнт-серверної архітектури

Архітектура Dark Forest відповідає традиційному ігровому бекенду та являє собою набір смарт-контрактів, розгорнутий на блокчейні Gnosis Chain, сумісному з віртуальною машиною Ethereum. В якості клієнтської версії гри є веб-клієнт, що дозволяє взаємодіяти з грою. Це просто статичний сайт, який по суті підключається до вузла блокчейну і дозволяє завантажувати дані з блокчейну, на основі отриманих даних відмальовується графічне зображення гри. Коли гравець робить хід, він відправляє транзакцію на блокчейн, і коли ця транзакція буде підтверджена і видобута, вона відобразиться у браузері гравця. Вся приватна інформація (координати планети гравця) зберігається в локальному сховищі браузера. Схема архітектури Dark Forest зображена на рисунку 4.7.

Всі публічні дані в Dark Forest зберігаються в сховищі EVM. EVM (Ethereum Virtual Machine) - віртуальне обчислювальне середовище, розподілений комп'ютер, що відповідає за виконання алгоритмів в мережі Ethereum. Основне призначення - обчислення стану мережі, а також запуск і

компіляція різних типів коду смарт-контрактів в читабельний формат байт-код.

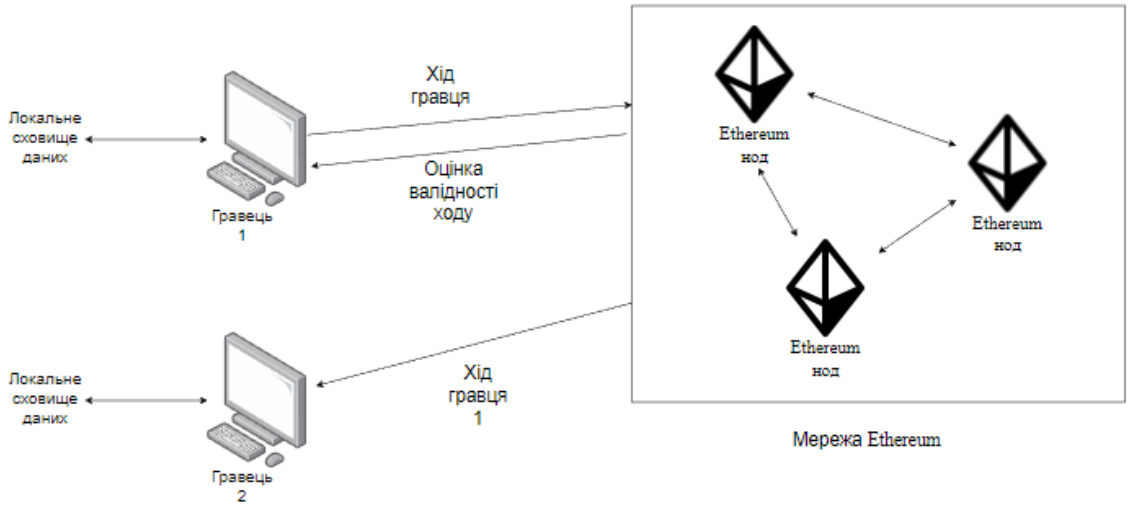

Рисунок 4.7 – Схема архітектури Dark Forest

4.7 Огляд блокчейну Gnosis Chain

Gnosis Chain - швидкий та енергоефективний блокчейн, сумісний з Ethereum та спрямований на вирішення багатьох проблем його масштабування. Gnosis Chain є асоційованим ланцюжком рівня виконання для стабільних транзакцій. Це дозволяє розробникам легко розгортати смарт-контракти і децентралізовані застосунки з Ethereum в новому ланцюжку [41].

Як децентралізована автономна організація (decentralized autonomous organization, DAO), Gnosis використовує створювані нею продукти для прийняття рішень щодо розвитку, підтримки та управління своєю екосистемою.

Сама мережа Gnosis Chain захищена рівнем консенсусу, який називається Gnosis Beacon Chain (GBC). GBC використовує систему Proof-of-Stake, за допомогою якої користувачі блокують певну кількість GNO для участі в процесі перевірки транзакцій. GNO є нативним токеном екосистеми

Gnosis. Він використовується для стейкінга в ланцюжку Gnosis і виступає в якості токена управління для GnosisDAO.

4.8 Ідея агностичного ігрового застосунку в Dark Forest

В обчислювальній техніці вважається, що пристрій або програма є агностичними або агностичними до даних, якщо метод або формат передачі даних не має відношення до функції пристрою або програми. Це означає, що пристрій або програма може отримувати дані в різних форматах або з різних джерел, і при цьому ефективно обробляти ці дані.

Ігровий застосунок Dark Forest вважається агностичним, адже неважливо яким способом були отримані дані, блокчейн сторона буде приймати лише ті дані, що пройшли перевірку zkSNARK. Тобто гравці можуть створювати власні версії гри або додавати плагіни, адже верифікація даних забезпечує відсутність неможливих ходів та зловживання зі сторони гравців. Плагіни - це програмний компонент, який додає певну функцію до існуючої комп'ютерної програми.

Також в Dark Forest повністю відкритий та безкоштовний вихідний код, що забезпечує прозорість відносин між розробниками та гравцями.

В іграх, що не використовують блокчейн технології, агностичні застосунки зазвичай є лише однокористувальницькими, коли від доброчесності гравця нічого не залежить. У багатокористувальницьких іграх зміна коду гри або використання плагінів є правопорушенням, за яке акаунт гравця можуть заблокувати. Також навіть з уніфікованими клієнтами існує проблематика застосування чітів (несанкціонована розробником гри діяльність, яка змінює поведінку гравця, шляхом застосування спеціально створених або модифікованих програм або обладнання в онлайн-іграх, щоб дати одному гравцю перевагу над іншим) гравцями, специфіка роботи яких різниться від жанру гри.

Реалізація zkSNARK з’явилася доволі нещодавно і використовується в основному в блокчейн програмах. Розробка ігрових застосунків з використанням цієї технології є досить новою сферою діяльності. Dark Forest є яскравим прикладом початку нового жанру серед багатокористувальницьких ігор, в яких гравці самі можуть створювати версію гри, яка їм до вподоби. Одне із угрупувань гравців Dark Forest розробляють власну версію гри Dark Forest Arena, що зменшує масивний всесвіт Dark Forest до невеликого поля бою. Замість одного матчу, що триває днями, раунд Арени складається з сотень поєдинків, які закінчуються за лічені хвилини. Dark Forest Arena демонструє потенціал нового жанру мережевої гри створеного на блокчейні: Battle Arena. Стрімкий ігровий процес протягом коротких сесій створює конкуренцію на будь-якому рівні майстерності та формує захоплюючу взаємодію гравців.

4.9 Розробка показників ефективності використання блокчейн технології в ігрових застосунках

Основою онлайн ігор є швидкість оновлення даних між клієнтом і сервером. В Dark Forest крім цього використовується хешування даних та zkSNARK, які можуть уповільнювати передачу даних як на клієнтській стороні, так і на стороні блокчейну. Також важливо окремо оцінити час генерації хешу при ініціалізації гравця в системі.

Важливими показниками ефективності є продуктивність самого блокчейну. Одним із показників є транзакції в секунду (Transactions Per Second , TPS), що означає, скільки транзакцій може бути здійснено за секунду. TPS використовується для визначення здатності блокчейну обробляти дані і його потреб в масштабуванні. Специфікою блокчейну є наявність комісії за транзакцію, що сплачується валідаторам мережі за їхні послуги блокчейну. Кожна дія в Dark Forest є транзакцією, яку має сплатити гравець, тому потрібно окремо оцінити вартість за транзакцію. Також всі транзакції в блокчейні проходять етап валідації, швидкість якого має бути оцінена.

В застосунку Dark Forest також є ігрові предмети, що видаються гравцю у вигляді NFT, таким способом має бути закріплена абсолютна власність гравця над цим предметом. Для оцінки ефективності використання NFT потрібно оцінити надійність.

Отже для оцінки ефективності використання блокчейну в Dark Forest потрібно виміряти та порівняти такі показники ефективності:

– час відповіді на запит у блокчейн – від часу відправки запиту до часу отримання відповіді;

- тривалість генерації хешу при ініціалізації гравця;
- кількість транзакцій в секунду в блокчейні;
- вартість підтвердження транзакції;
- тривалість часу валідації транзакції;
- надійність NFT предметів.

5 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

5.1 Опис методів збору інформації

Оскільки Dark Forst має агностичну клієнтську версію та відкритий вихідний код, збір показників ефективності можна провести, використовуючи плагіни для ігрового застосунку, а також власноруч модифіковану версію гри. Це дозволить зібрати інформацію прямо в ігровому процесі. Для виміру деяких показників будемо використовувати дослідження та інформацію з відкритих джерел про ефективність блокчейну Gnosis Chain, на якому розроблено серверну частину Dark Forest.

В Galcon 2 зашифрваний вихідний код гри і зміна клієнтської частини є складною задачею, тому для оцінки показників ефективності використовуєтся сервер подібної конфігурації та загальноприйняті вимоги до серверної частини ігрового застосунку.

5.2 Дослідження часу відповіді на запит у блокчейн

Час відповіді на запит є одним з найважливіших показників для багатокористувальницьких ігор. Для жанрів ігрових застосунків зі швидким ігровим процесом, як онлайн шутер, цей показник має бути максимально низьким, адже гра буде виглядати не плавною, гравці будуть стикатись з різними проблемами синхронізації даних та відображення стану гри на стороні клієнту. Для кожного ігрового жанру існують свої потреби у показнику часу відповіді, але загалом оптимальним є 200-400 мс. Час відповіді на запит залежить від декількох чинників:

- обладнання серверу;
- складність серверної логіки;
- навантаження серверної логіки на сервер;
- кількість даних, що передаються.

Для проведення дослідження було розроблено плагін до Dark Forst, що дозволяє відобразити в інтерфейсі ігрового застосунку час відповіді на запит під час ігрового процесу (Додаток А). Робота плагіну закладається в створенні контекстного меню і грі, в якому відображається інформація. Клас EventHandler реалізує підписку на події об’єкту гравця, що містить інформацію про його дії. Код класу, що відображає інформацію зображено в лістингу 5.1.

Лістинг 5.1 – Програмний код класу, що відображає інформацію щодо часу відповіді на запит

```
class EventHandler {
      constructor() {
          Player.playerTurnEvent.Connect((data)                    =>
levelMenu.appendChild(REQUEST     COMPLETED     +     “     “     +
data.requestDuration)
         }
       async render(div) {
         div.style.width = "400px";
         const firstTextDiv = document.createElement("div");
         firstTextDiv.innerText = "Add the url that points to your
snarker below.";
         const input = document.createElement("input");
         input.style.width = "100%";
         input.placeholder = "https://snarker.orden.gg";
         const button = document.createElement("button");
         button.innerHTML = "Start Remote Snarker";
         button.onclick = () => {
           patchSnarkProverQueue(input.value);
         };
         div.appendChild(firstTextDiv);
         div.appendChild(document.createElement("br"));
         div.appendChild(input);
         div.appendChild(document.createElement("br"));
```

```
            div.appendChild(document.createElement("br"));
            div.appendChild(button);
          }
        }
export default EventHandler;
```

Приклад відображення результатів збору даних дослідження зображено на рисунку 5.1.

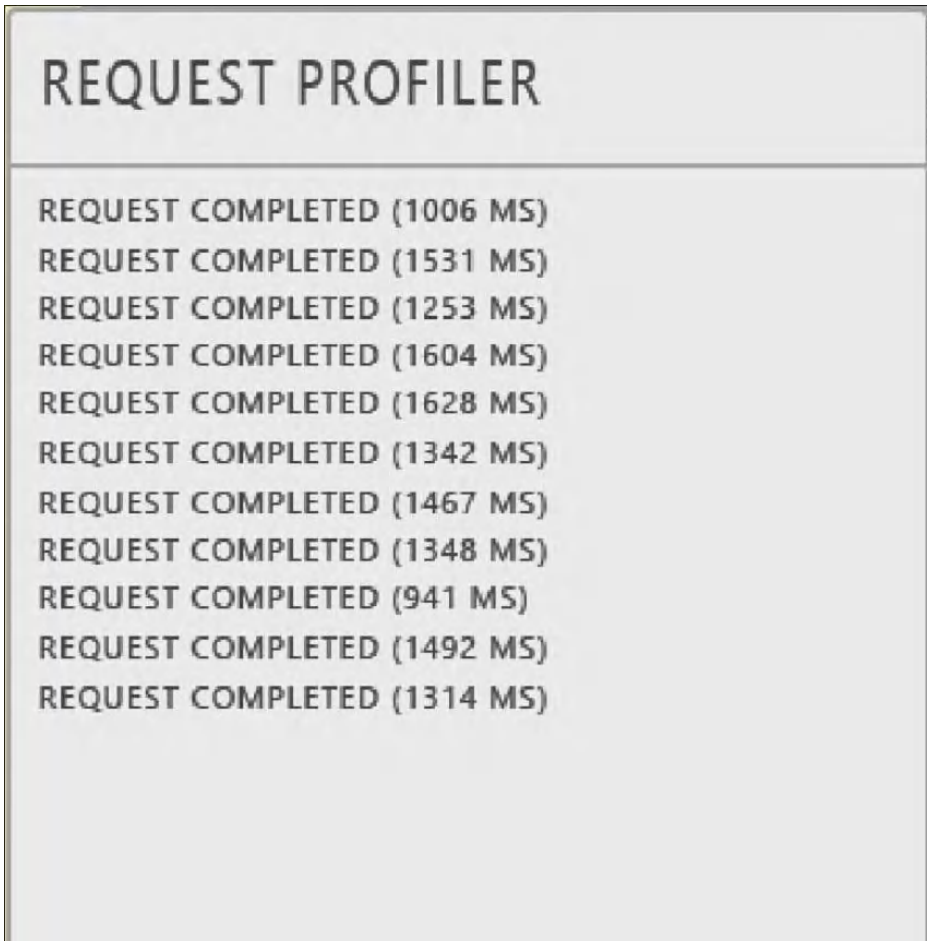

Рисунок 5.1 – Результат роботи плагіну

Для збору результатів з гри Galcon 2 було обрано конфігурацію серверу, що потрібна для реалізації механік гри та підтримки близько 100 гравців на сервері. Обрана конфігурація:

– центральний процесор (CPU) : Intel Xeon-E 2386G - 6c/12t - 3.5 GHz/4.7 GHz;

– оперативна пам’ять (RAM) : 32 GB ;
– сховище збереження даних : 500 Гб SSD NVMe

Для збору показників такого серверу розроблено JavaScript програму (Додаток Б), що підключається до серверу з обраною конфігурацією та вимірює час від відправки запиту з випадковим набором даних довжиною в 220 символів (розмір хешу в Dark Forst) до отримання відповіді від серверу, та відображає результати в консолі браузеру (рис 5.2).

Рисунок 5.2 – Результат роботи програми

Результати дослідження наведено в таблиці 5.1.

Таблиця 5.1 – Результати дослідження часу відповіді на запит

№ дослідження	Результат Dark Forst, мс	Результат серверу,мс
1	1006	242
2	1531	163
3	1253	181
4	1604	174
5	1628	256
6	1342	175
7	1467	201
8	1348	203
9	941	360
10	1492	198
11	1314	124

12	1471	327
13	1508	263
14	1622	281
15	1728	294
16	1903	262
17	1960	244
18	1802	238
19	1844	252
20	1103	263

Отримані результати дослідження часу відповіді на запит зображені у вигляді графіку (рис 5.3). Середнім результату для блокчейну є 1493.35 мс, для серверу - 235.05.

Рисунок 5.3 - Графік порівняння результатів дослідження часу відповіді на запит

Отже, між сервером та блокчейном є досить велика різниця у показнику часу відповіді на запит, що в середньому становить 1258 мс. На даному етапі розвитку блокчейну, він ще є досить повільним, порівняно з традиційним підходом. Одною з причиною таких результатів є використання методу підтвердження даних SNARK в застосунку Dark Forest, адже спочатку клієнт має згенерувати ZKP, відправити його до блокчейну, де виконається перевірка дій гравця. Тому блокчейн з використанням SNARK не може бути використаним для реалізації на ньому ігрового застосунку будь-якого жанру.

5.3 Дослідження тривалості генерації хешу при ініціалізації гравця

Тривалість генерації хешу при ініціалізації гравця характерна лише для ігор з використанням технологій SNARK і не має аналогів у застосунках без використання блокчейну. Оскільки цей процес відбувається на початку гри, важливо оцінити його тривалість, адже він впливає на перше враження гравця. Тому час генерації хешу має відповідати загальноприйнятим нормам щодо максимального часу запуску ігрового застосунку. В іграх без використання блокчейну та простою 2D графікою нормальним часом запуску застосунку є до 15 секунд, в іграх з 3D графікою – до 60с [42].

Для виконання результату дослідження розроблено програмний застосунок до Dark Forest, що дозволяє відобразити в інтерфейсі гри проміжок часу, за який було згенеровано початковий хеш місцезнаходження гравця (рис 5.4). Також важливо зазначити, що важливим показником в генерації хешу є конфігурація приладу, на якому це відбувається. Дослідження проводилось на персональному комп’ютері з такими характеристиками:

- центральний процесор (CPU) : AMD Ryzen 7 3700X, 4300 MHz
- оперативна пам’ять (RAM) : 32 GB ;
- сховище збереження даних : 500 Гб SSD NVMe;
- відеокарта: NVIDIA GeForce RTX 2070S (8 Gb).

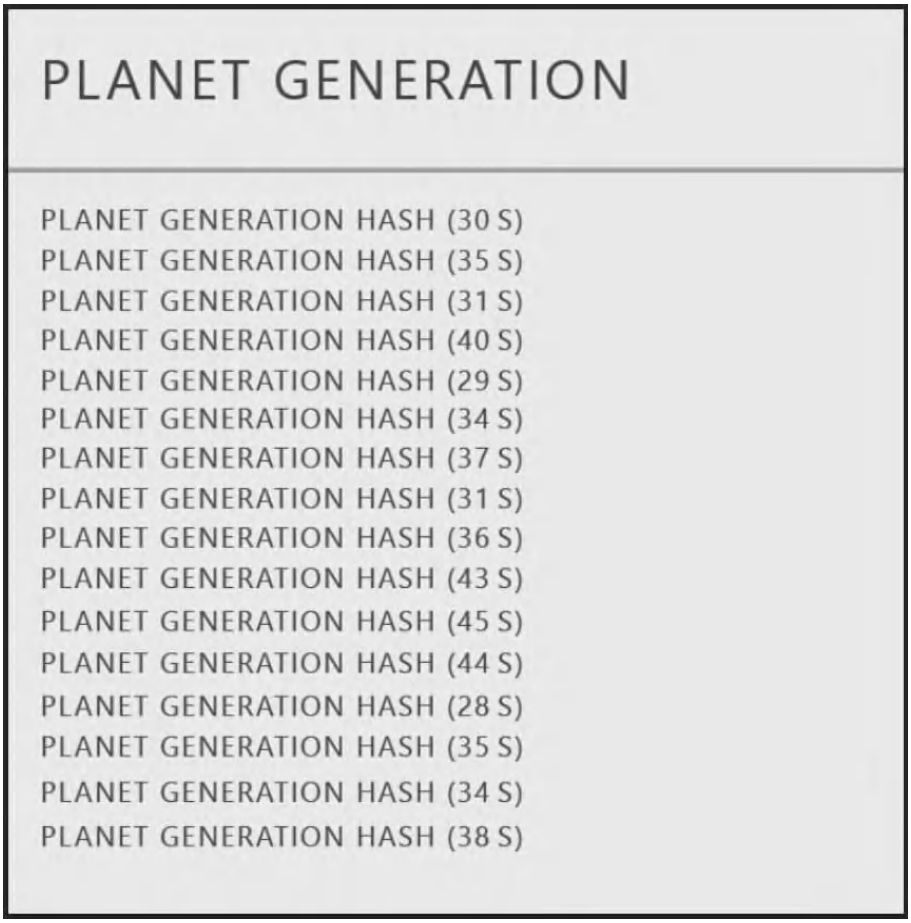

Рисунок 5.4 – Результат роботи плагіну, що вимірює час генерації хешу

Результати дослідження зображені в таблиці 5.2

Таблиця 5.2 – Результати дослідження часу генерації хешу

№ Дослідження	Час генерації, с
1	30
2	35
3	31
4	40
5	29
6	34
7	37
8	31
9	36

10	43
11	45
12	44
13	28
14	35
15	34
16	38
17	37
18	27
19	42
20	36

Отже, генерація хешу відбувається в середньому за 35.6 с, що є швидким результатом для функції такої складності, але все ще може бути проблемою першого враження гравця. Запуск клієнтської частини Dark Forest відбувається досить швидко (в проміжку від 2 до 5 с), що є чудовим результатом.

5.4 Дослідження кількості транзакцій в секунду в блокчейні

Показник кількості транзакцій в секунду використовується для оцінки швидкості транзакцій в мережі. TPS мережі є важливим, оскільки він вимірює здатність мережі обробляти транзакції в режимі реального часу, а також її потенціал до масштабування для забезпечення нових випадків використання та нових користувачів у майбутньому.

Показником аналогом для серверу є кількість запитів в секунду (Requests per second, RPS). Основна функція веб-сервера полягає в отриманні та обробці запитів, але якщо сервер перевантажений запитами, продуктивність може постраждати. RPS - це показник, який обчислює кількість запитів, отриманих

протягом певного періоду моніторингу, часто в діапазоні від однієї до п'яти хвилин.

Згідно до публічної інформації [43] Gnosis Chain може обробляти 90 транзакцій в секунду. Розрахування кількості запитів на серверу порахуємо з формули, RPS дорівнює (RAM/ використання пам'яті задачею) * (1 / час виконання задачі) і отримаємо проміжок від 4000 до 8000 при часу виконанні задачі 100 і 50 мс відповідно (рис. 5.6).

Total RAM	Worker Memory	Task Time	RPS
32Gb	40Mb	100ms	4000
32Gb	40Mb	50ms	8000

Рисунок 5.6 - Розрахунок кількості запитів в секунду

Отже, серверний підхід в порівнянні з блокчейном Gnosis Chain підтримує набагато більше запитів в секунду.

5.5 Дослідження вартості підтвердження транзакції

Комісія за транзакції - це плата, яку користувачі сплачують за відправлення транзакції або взаємодію зі смарт-контрактом в мережі блокчейну. Існує дві основні причини, чому користувачам необхідно платити комісію при відправці транзакції. Перша причина - це плата майнерам або валідаторам (також відомим як вузли) за забезпечення безпеки мережі. В обмін на захист мережі та забезпечення відсутності шахрайських транзакцій ці вузли отримують винагороду у вигляді комісії за транзакції в блокчейні. Мережеві валідатори дозволяють блокчейну працювати децентралізовано, без необхідності покладатися на централізовані структури, щоб гарантувати, що в мережі не відбувається ніякої зловмисної діяльності.

Друга причина, по якій користувачі платять комісію за транзакції - це забезпечення роботи смарт-контрактів. Як і користувачі, смарт-контракти також повинні платити комісію, оскільки вони також відправляють транзакції.

Оскільки за виконання транзакцій повинен сплачувати гравець, то це є важливим показником, адже ніхто не буде грати в гру, якщо хід коштує занадто дорого. Аналогічним показником в сервері є вартість хостингу, але на відміну від підходу з блокчейном, його буде сплачувати сам розробник.

Конфігурація серверу, розроблена в пункті 5.2 коштуватиме близько 100 USD в місяць згідно інформації з ресурсу [44].

Згідно до офіційного сайту Gnosis Chain [43] середня вартість транзакції становить 0.00014232656 xDai ($0.000142 USD). Приклад даних, описаних в деталях транзакції зображено на рисунку 5.7.

Ціна за 1000 транзакцій буде становити 0,142 USD, тобто вартість 700 тисяч транзакцій коштує близько 100 USD.

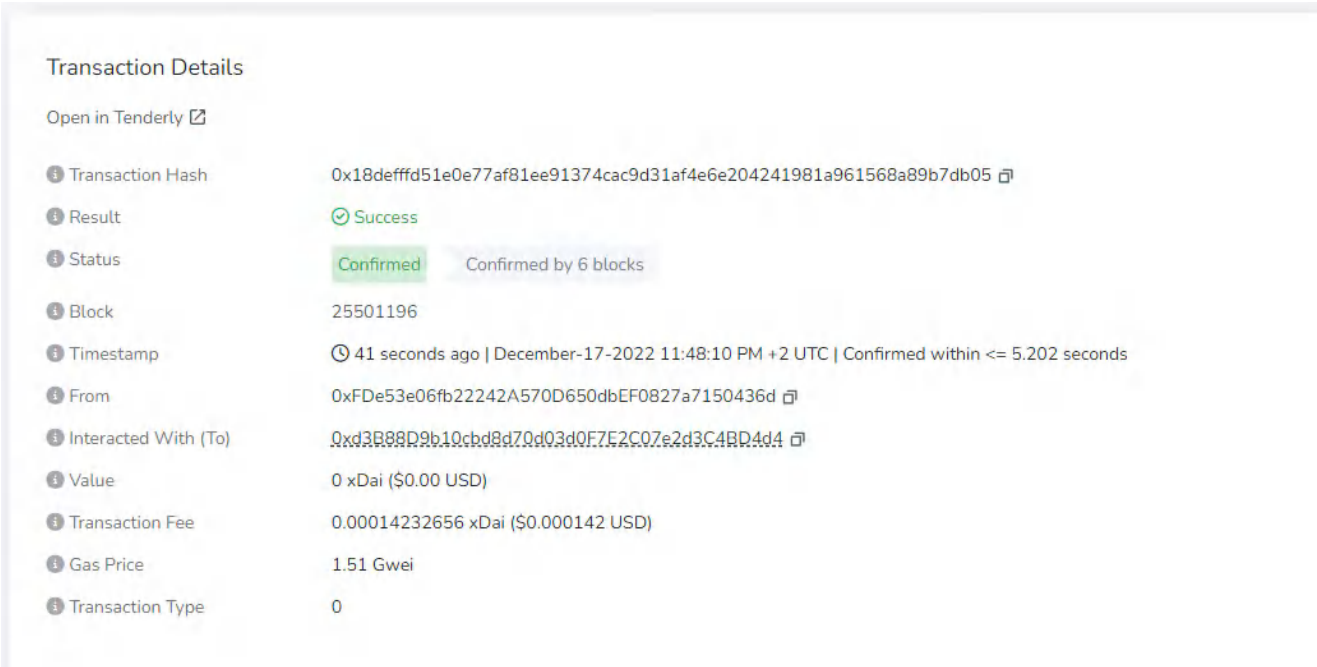

Рисунок 5.7 - Деталі транзакції в блокчейні Gnosis Chain

Загальна сума для кожного гравця буде різною в залежності від стиля гри та часу проведеного в грі, 7000 транзакцій дорівнює близько 1 USD, що є

досить недорого і коштує менше, ніж більшість підписок на популярні сервіси або ігри. Також Dark Forest усі гравці отримують по 0.15 USD на початку раунду від розробників, що дозволяє пограти досить довго та сформувати свій погляд про гру, незалежно від існування платні за дії в застосунку.

5.6 Дослідження надійності NFT

NFT в ігрових застосунках є методом збереження власності гравця, такої як внутрішньоігрові предмети. Аналогом даного підходу в іграх без блокчейну є збереження даних в базі даних.

База даних використовує структуру даних для зберігання інформації. Всі дані, які зберігаються в базі даних, можуть бути переглянуті за допомогою спеціальної мови запитів, відомої як мова структурованих запитів (structured query language, SQL). База даних може працювати майже з усіма типами даних і допомагає підтримувати всі сучасні підприємства [45]. Реляційна модель є зручною і дає можливість власнику працювати з різними базами даних одночасно. Для ефективної організації баз даних використовуються системи управління базами даних. За своєю суттю елементи даних зберігаються в таблицях. Таблиця складається з полів, які можуть записувати різні типи даних, відомі як атрибути.

Дослідження надійності збереження даних в NFT та базі даних потребує додаткової розробки показників ефективності.

Засновник Ethereum Віталій Бутерін усвідомив важливість децентралізації, коли компанія Blizzard в односторонньому порядку оновила правила щодо одного з його активів World of Warcraft [46]. Гравець відчув себе обманутим розробниками, оскільки зрозумів, що не є справжнім власником своїх активів. Тому потрібно порівняти NFT та базу даних за критерієм можливості зміни даних.

В таких ігрових застосунках як Dota 2 або CS:GO гравець може втратити всю свою власність, у випадку якщо йому заблокують акаунт, тому оцінки потребує такий критерій, як можливість втрати даних.

Важливими показниками також є ймовірність невдачі, тип мережевої архітектури, швидкість, можливі операції над даними, тип доступу перегляду даних.

Результати дослідження по обраним критеріям надійності наведено в таблиці 5.3.

Таблиця 5.3 – Результати порівняння надійності зберігання даних в NFT та базі даних

Критерій оцінки	NFT	База даних
Тип мережевої архітектури	Однорангова	Клієнт-серверна
Тип доступу перегляду даних	Публічний	За дозволом (правами адміністратора)
Можливі операції над даними	Запис та зчитування	Запис, читання, оновлення та видалення
Швидкість	Залежить від мережі, але повільніша за БД	Дуже швидка
Ймовірність невдачі	Ні	Так
Можливість втрати даних	Ні	Так
Можливість зміни даних	Ні	Так

Отже, підхід з традиційною базою даних є більш швидким, та зручним в маніпулюванні даними зі сторони розробника. Зберігання даних гравця у NFT

є набагато надійнішим і є підтвердження власності гравця, що не може бути змінено або видалено.

5.7 Висновки з результатів дослідження

Отримані результати відображають, що використання блокчейну як серверної частини ігрового застосунку значно поступається традиційному підходу. Реалізація Dark Forest гарантує вищу прозорість та захист даних, для більшості існуючих ігор використання таких технологій (на даному етапі їх розвитку) буде не потрібним. Незважаючи на це, розробка таких ігрових застосунків вкрай важлива для розвитку технології блокчейну. Декілька років тому важко було навіть уявити, що блокчейн можна буде використовувати як ігровий сервер, а нині існує кілька десятків ігор такого типу.

Згідно до результатів проведеного дослідження можна зробити висновок, що доцільним використанням розміщення механік ігрового застосунку на блокчейні є жанри, в яких є висока потреба захищення даних гравця (наприклад карткові ігри, в яких гравці не розкривають свої карти публічно, але має бути метод підтвердження правильності їх ходу) або жанри, в яких швидкість сервера не є важливим показником, що впливає на ігровий процес (наприклад стратегії в реальному часі).

ВИСНОВКИ

В ході виконання кваліфікаційної роботи проведено аналіз предметної області, в якому описано програмні застосунки та блокчейн технологію. Проведено порівняння існуючих ігрових застосунків, з якого виявлено, що основним варіантом використання блокчейну в іграх є монетизація проектів. На даному етапі визначено проблему відсутності досліджень показників використання блокчейну як повноцінного ігрового серверу, на якому б розміщувались основні механіки гри та використання NFT для збереження ігрових предметів гравця.

Проведено огляд технологій, які застосовуються в блокчейн розробці та розроблено постановку задачі дослідження. Для проведення дослідження обрано багатокористувальницьку гру Dark Forest, що повністю працює на блокчейні, має відкритий вихідний код та використовує zkSNARK для збереження приватної ігрової інформації гравця і в цей же час забезпечує валідацію всіх ігрових дій гравця. Для порівняння обрано гру Galcon 2 зі схожим жанром та ігровим процесом, що має серверну архітектуру. Для оцінки ефективності використання блокчейну в Dark Forest розроблено такі показники ефективності: час відповіді на запит у блокчейн – від часу відправки запиту до часу отримання відповіді; тривалість генерації хешу при ініціалізації гравця; кількість транзакцій в секунду в блокчейні; вартість підтвердження транзакції; тривалість часу валідації транзакції; надійність NFT предметів.

За розробленими критеріями проведено дослідження, в якому порівняли блокчейн з сервером та NFT з базою даних. Згідно до результатів дослідження зроблено висновок, що використання блокчейну як серверної частини ігрового застосунку значно поступається традиційному підходу, але гарантує вищу прозорість та захист даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Kent, Steven L. The Ultimate History of Video Games. San Val Inc, 2001. 155 p.

2 How the Video Game Industry Is Changing. URL: https://www.investopedia.com/articles/investing/053115/how-video-game-industry-changing.asp (дата звернення: 13.11.22).

3 NFT games with the highest player count. URL: https://www.statista.com/statistics/1266486/blockchain-games-user-number/ (дата звернення: 13.11.22).

4 Лимар Л.В. Ефективність використання блокчейн технології в ігрових застосунках. Матеріали 1-ї Міжнародної науково-практичної конференції «SCIENCE: DEVELOPMENT AND FACTORS ITS INFLUENCE». December 26-28, 2022, Amsterdam, Netherlands.

5 Information system. URL: https://www.britannica.com/topic/information-system (дата звернення: 13.11.22).

6 Information Technology Vs Information Systems. URL: https://www.cityu.edu/information-technology-vs-information-systems/ (дата звернення: 15.11.22).

7 Types Of Information System. URL: https://www.geeksforgeeks.org/types-of-information-system/ (дата звернення: 15.11.22).

8 Video Game. URL: https://en.wikipedia.org/wiki/Video_game (дата звернення: 16.11.22).

9 Designing for Motivation. URL: https://www.gamedeveloper.com/design/designing-for-motivation (дата звернення: 16.11.22).

10 Arsenault, Dominic (2009). "Video Game Genre, Evolution and Innovation". Eludamos. Journal for Computer Game Culture. **3** (2): 149–176

11 University Of California Irvine. URL: https://majoringingaming.com/gaming-programs/university-of-california-irvine/ (дата звернення: 16.11.22).

12 У хнуре стартувала регіональна кваліфікація до першого чемпіонату україни з кіберспорту. URL: https://nure.ua/u-hnure-startuvala-regionalna-kvalifikacija-do-pershogo-chempionatu-ukraini-z-kibersportu (дата звернення: 17.11.22).

13 DCU research looks at how students and teachers can benefit from using Minecraft in class. URL: https://www.dcu.ie/commsteam/news/2021/nov/dcu-research-looks-how-students-and-teachers-can-benefit-using-minecraft (дата звернення: 17.11.22).

14 Learn how these digital public ledgers enable crypto and NFTs. URL: https://www.investopedia.com/terms/b/blockchain.asp (дата звернення: 17.11.22).

15 Blochain. URL: https://en.wikipedia.org/wiki/Blockchain (дата звернення: 19.11.22).

16 Sherman, Alan T.; Javani, Farid; Zhang, Haibin; Golaszewski, Enis (January 2019). "On the Origins and Variations of Blockchain Technologies". IEEE Security Privacy. **17** (1): 72–77.

17 Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. **3** (2): 99–111.

18 The great chain of being sure about things. URL: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (дата звернення: 19.11.22).

19 Cryptocurrency Explained With Pros and Cons for Investment. URL: https://www.investopedia.com/terms/c/cryptocurrency.asp#:~:text=A%20cryptocurrency%20is%20a%20digital,a%20disparate%20network%20of%20computers (дата звернення: 21.11.22).

20 The future of blockchain in 8 charts. URL: https://www.raconteur.net/the-future-of-blockchain-in-8-charts/ (дата звернення: 21.11.22).

21 Blockchain. URL: https://builtin.com/blockchain (дата звернення: 21.11.22).

22 What is "proof of work" or "proof of stake". URL: https://www.coinbase.com/th/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake (дата звернення: 23.11.22).

23 What are the 4 different types of blockchain technology. URL: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology#:~:text=There%20are%20four%20main%20types,benefits%2C%20drawbacks%20and%20ideal%20uses (дата звернення: 23.11.22).

24 Applications for Blockchain Technology. URL: https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-applications/ (дата звернення: 24.11.22).

25 Meet CryptoKitties, the $100,000 digital beanie babies epitomizing the cryptocurrency mania. URL: https://www.cnbc.com/2017/12/06/meet-cryptokitties-the-new-digital-beanie-babies-selling-for-100k.html (дата звернення: 23.11.22).

26 An Introduction to Sidechains. URL: https://www.coindesk.com/learn/an-introduction-to-sidechains/ (дата звернення: 23.11.22).

27 'Play-to-earn' workers abandon hacked NFT game, stranding digital 'landlords'. URL: https://www.gamesradar.com/play-to-earn-workers-abandon-hacked-nft-game-stranding-digital-landlords/ (дата звернення: 24.11.22).

28 Что такое Sandbox. URL: https://www.binance.com/ru/blog/nft/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-sandbox-6211244094972798802 (дата звернення: 24.11.22).

29 Cryptocurrency. URL: https://en.wikipedia.org/wiki/Cryptocurrency (дата звернення: 25.11.22).

30 Blockchain Platforms Driving the Industry. URL: https://builtin.com/blockchain/blockchain-platforms (дата звернення: 25.11.22).

31 Introduction To Smart Contracts. URL: https://ethereum.org/en/developers/docs/smart-contracts/ (дата звернення: 25.11.22).

32 Smart Contract Development. URL: https://limechain.tech/blockchain-development/smart-contract-development/ (дата звернення: 25.11.22).

33 Oracles. URL: https://ethereum.org/en/developers/docs/oracles/ (дата звернення: 26.11.22).

34 IPFS вместо HTTP. URL: https://forklog.com/cryptorium/chto-takoe-ipfs (дата звернення: 26.11.22).

35 A Technical Guide to IPFS – the Decentralized Storage of Web3 URL: https://www.freecodecamp.org/news/technical-guide-to-ipfs-decentralized-storage-of-web3/ (дата звернення: 26.11.22).

36 Brown, Joseph Alexander; Scirea, Marco (2018). "Procedural Generation for Tabletop Games: User Driven Approaches with Restrictions on Computational Resources". SEDA 2018: Proceedings of 6th International Conference in Software Engineering for Defence Applications. International Conference in Software Engineering for Defence Applications. Rome, Italy. pp. 44–54.

37 Zero-Knowledge Proofs for Engineers: Introduction. URL: https://blog.zkga.me/intro-to-zksnarks (дата звернення: 29.11.22).

38 ZKPs for Engineers: A look at the Dark Forest ZKPs. URL: https://blog.zkga.me/df-init-circuit (дата звернення: 29.11.22).

39 Circom Documentation. URL: https://docs.circom.io/ (дата звернення: 01.12.22).

40 Briceño, L.D., Siegel, H.J., Maciejewski, A.A., Hong, Y., Lock, B., Panaccione, C., Wedyan, F., Teli, M.N., Zhang, C.: Resource allocation in a client/server system for massive multi-player online games. IEEE Trans. Comput. 63(12), 3127–3142 (2014).

41 What is Gnosis? (GNO). URL: https://www.kraken.com/learn/what-is-gnosis-gno (дата звернення: 05.12.22).

42 Why your game needs to load within 30 seconds. URL: https://www.pocketgamer.biz/monetizer/59041/opinion-why-your-game-needs-to-load-within-30-seconds/ (дата звернення: 08.12.22).

43 Gnosis Chain Explorer. URL: https://gnosisscan.io/ (дата звернення: 08.12.22).

44 How to Calculate Server Max Requests per Second. URL: https://medium.com/geekculture/how-to-calculate-server-max-requests-per-second-38a39bb96a85 (дата звернення: 12.12.22).

45 Білова Т.Г., Дьоміна В.М., Побіженко І.О. Композиційне проектування та реструктуризація глобальної схеми мультибази даних. АСУ и приборы автоматики. 2021. № 177. С. 64–68 (фахове)

46 Vitalik Buterin suggests making NFTs ‘soulbound’ like World of Warcraft items. URL: https://cointelegraph.com/news/vitalik-buterin-suggests-making-nfts-soulbound-like-world-of-warcraft-items