МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Черняк Вадим Андрійович

Програмно-апаратна підсистема добування криптовалют на основі графічних процесорів / The hardware-software subsystem for cryptocurrency extraction based on graphics processors

напрям підготовки: 6.050102 - Комп’ютерна інженерія
фахове спрямування - Комп’ютерні системи та мережі
Бакалаврська робота

Виконав: студент групи КСМ-42/1
Черняк В.А.

Керівник к.т.н., доц., Касянчук М.М.

ТЕРНОПІЛЬ – 2018

РЕЗЮМЕ

Дипломна робота містить 60 сторінок пояснюючої записки, 13 рисунків, 13 таблиць, 1 додаток. Обсяг графічного матеріалу – 2 аркуші формату А3.

Метою дипломної роботи є розробка програмно-апаратної підсистеми для добування криптовалют на основі сучасних графічних процесорів.

Методи досліджень – методи добування криптовалют, методи обчислення хеш-функцій, схемотехнічні методи.

У даній дипломній роботі розроблено програмно-апаратну підсистему для добування криптовалют на основі сучасних графічних процесорів. На основі аналітичного огляду типів криптовалют, способів їх добування та характеристик сучасних графічних процесорів встановлено їх переваги та недоліки, що дозволило обґрунтувати вибір оптимальних механізмів для майнінгу. На основі аналізу технології блокчейну та хеш-функції SHA-256 сформульовано вимоги до програмного та апаратного забезпечення для оптимального добування криптовалют. На основі сформульованих вимог до графічних процесорів здійснено обґрунтування вибору програмного та апаратного забезпечення для побудови програмно-апаратної системи добування криптовалют. На основі вибраного програмного та апаратного забезпечення розглянуто особливості добування криптовалют за допомогою сучасних відеокарт та графічних процесорів. На основі відповідного програмного забезпечення здійснено налаштування програмно-апаратної підсистеми добування криптовалют на основі сучасних графічних процесорів.

Аналіз спроектованої системи дозволяє зробити висновок, що розроблена програмно-апаратна підсистема для добування криптовалют на основі графічних процесорів задовольняє вимогам сучасного ринку, які ставляться користувачами, проте сучасна елементна база та програмне забезпечення розвиваються стрімкими темпами і внесення змін і доповнень до даного продукту є обов’язковою вимогою.

Ключові слова: ПРОГРАМНО-АПАРАТНА ПІДСИСТЕМА, МАЙНІНГ, КРИПТОВАЛЮТА, ГРАФІЧНИЙ ПРОЦЕСОР, ВІДЕОКАРТА.

RESUME

Thesis contains 60 pages of explanatory note, 13 figures, 13 tables, 1 appendix. Volume of graphic material - 2 sheets of A3 format.

The purpose of the thesis is to develop a software and hardware subsystem for extracting cryptocurrencies based on modern graphics processors.

Research methods - methods of cryptocurrency extraction, methods of calculating hash functions, circuit design methods.

In this thesis, a software and hardware subsystem for extracting cryptocurrencies based on modern graphics processors. Based on the analytical review of cryptocurrency types, methods of their extraction and characteristics of modern graphics processors, their advantages and disadvantages are established, which allowed to justify the choice of optimal mechanisms for mining. Based on the analysis of blockchain technology and hash function SHA-256, the requirements for software and hardware for optimal cryptocurrency extraction are formulated. Based on the formulated requirements for graphics processors, the choice of software and hardware for the construction of software and hardware system for cryptocurrency extraction is substantiated. Based on the selected software and hardware, the peculiarities of cryptocurrency extraction with the help of modern video cards and graphics processors are considered. On the basis of the corresponding software the software-hardware subsystem of extraction of cryptocurrencies on the basis of modern graphic processors is adjusted.

Analysis of the designed system allows us to conclude that the developed software and hardware subsystem for cryptocurrency extraction based on graphics processors meets the requirements of the modern market set by users, but the modern element base and software are evolving rapidly and changes and additions to this product are required. language requirement.

Key words: SOFTWARE AND HARDWARE SUBSYSTEM, MINING, CRYPTOCURRENCY, GRAPHIC PROCESSOR, VIDEO CARD.

ЗМІСТ

ВСТУП

Криптовалюта – це є різновид цифрової валюти, створення і контроль за якою базується на криптографічних методах. Функціонування даної системи засновано на таких технологіях, як блокчейн, спрямований ациклічний граф, консенсусний реєстр (ledger) тощо. Інформація про транзакції зазвичай не повинна шифруватися і вона може бути доступною у відкритому вигляді. Для забезпечення незмінності бази ланцюжка блоків транзакцій використовуються елементи криптографії (цифровий підпис на основі асиметричної криптосистеми з відкритим ключем, послідовне хешування тощо).

Термін «криптовалюта» закріпився після публікації статті про систему біткойна «Crypto currency» (криптографічна валюта), опублікованій в 2011 році в журналі Forbes. Сам же автор біткойнів, як і багато інших, використовував термін «електронна готівка» (англ. Electronic cash). Криптовалюта може бути розроблена з нуля або використовувати загальнодоступний вихідний код іншої криптовалюти. Якщо, крім коду, нова криптовалюта також використовує вже наявний ланцюжок блоків вихідної криптовалют, то таку криптовалюту називають форком вихідної криптовалюти. Для своєї емісії різні криптовалюти застосовують майнінг, форжінг або ICO.

Про економічною суть і юридичну силу криптовалюти ведуться складні дискусії. Залежно від країни, криптовалюту розглядають або як платіжний засіб, або як специфічний товар, який може мати навіть повні обмеження в обороті (наприклад, заборона операцій з ними для банківських установ).

Ключовою особливістю криптовалюти є відсутність будь-якого внутрішнього або зовнішнього адміністратора. Тому банки, податкові, судові

та інші державні або приватні органи не можуть ніяк впливати на транзакції будь-яких учасників цієї платіжної системи. Передача криптовалюта незворотна - ніхто не може скасувати, заблокувати, оскаржити або примусово (без приватного ключа) здійснити деяку транзакцію. Однак учасники угоди можуть добровільно тимчасово взаємно блокувати свої криптовалюти в якості застави або встановити, що для завершення/скасування угоди потрібна згода всіх (або довільних додаткових) сторін.

З вищесказаного випливає, що криптовалюта дуже стрімко завойовує популярність як засіб платежу або зберігання коштів. На даний час в Україні, та і по всьому світу, фіксували значний дефіцит відеокарт, які використовують для майнінга криптовалют – отримання винагороди від сторін угоди за надання своїх потужностей. Тому метою нашої роботи є робробка програмно-апаратної підсистеми для добування криптовалюти.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

1.1 Типи криптовалют та способи їх добування

Криптовалюта – це є різновид цифрової валюти, створення і контроль за якою базується на криптографічних методах [1-3]. Функціонування даної системи засновано на таких технологіях, як блокчейн, спрямований ациклічний граф, консенсусний реєстр (ledger) тощо [4-6]. Інформація про транзакції зазвичай не повинна шифруватися і вона може бути доступною у відкритому вигляді. Для забезпечення незмінності бази ланцюжка блоків транзакцій використовуються елементи криптографії (цифровий підпис на основі асиметричної криптосистеми з відкритим ключем, послідовне хешування тощо) [7-9].

Термін «криптовалюта» закріпився після публікації статті про систему біткойна «Crypto currency» (криптографічна валюта), опублікованій в 2011 році в журналі Forbes. Сам же автор біткойнів, як і багато інших, використовував термін «електронна готівка» (англ. Electronic cash). Криптовалюта може бути розроблена з нуля або використовувати загальнодоступний вихідний код іншої криптовалюти. Якщо, крім коду, нова криптовалюта також використовує вже наявний ланцюжок блоків вихідної криптовалют, то таку криптовалюту називають форком вихідної криптовалюти. Для своєї емісії різні криптовалюти застосовують майнінг, форжінг або ICO [10].

Про економічною суть і юридичну силу криптовалюти ведуться складні дискусії. Залежно від країни, криптовалюту розглядають або як платіжний засіб, або як специфічний товар, який може мати навіть повні обмеження в обороті (наприклад, заборона операцій з ними для банківських установ) [11].

Ключовою особливістю криптовалюти є відсутність будь-якого внутрішнього або зовнішнього адміністратора. Тому банки, податкові, судові та інші державні або приватні органи не можуть ніяк впливати на транзакції будь-яких учасників цієї платіжної системи. Передача криптовалюта незворотна - ніхто не може скасувати, заблокувати, оскаржити або примусово (без приватного ключа) здійснити деяку транзакцію. Однак учасники угоди можуть добровільно тимчасово взаємно блокувати свої криптовалюти в якості застави або встановити, що для завершення/скасування угоди потрібна згода всіх (або довільних додаткових) сторін [12-14].

З вищесказаного випливає, що криптовалюта дуже стрімко завойовує популярність як засіб платежу або зберігання коштів. На даний час в Україні, та і по всьому світу, фіксували значний дефіцит відеокарт, які використовують для майнінга криптовалют – отримання винагороди від сторін угоди за надання своїх потужностей. Тому метою нашої роботи є роббробка програмно-апаратної підсистеми для добування криптовалюти.

Криптовалюта - це різновид цифрових грошей, в основі якої лежить технологія криптографії, тобто, шифрування даних. Вона не має фізичного вигляду, а існує тільки в електронному вигляді. Її основні особливості - це анонімність, децентралізація і захищеність (рисунок 1.1).

Обіг криптовалют всередині системи відбувається безпосередньо (P2P) - без участі третьої сторони. Кожен з учасників - абсолютно рівний іншому. Ні у кого немає привілеїв, незалежно від його соціального і фінансового статусу. В основі цих віртуальних грошей лежить децентралізована відкрита база даних – блокчейн [15-17].

Більшість криптовалют мають стелю емісії (випуску в обіг нових монет). Так в Bitcoin він становить 21 мільйон «монет». А в таких валютах PPC і NVC обмежень по емісії немає.

Рисунок 1.1 – Властивості криптовалюти

Навіщо комусь потрібно було створювати криптовалюту? Відповідь на це питання залишається відкритим. Частково це пояснюється характеристиками криптовалюти. Раніше не було зручного і швидкого способу проводити анонімні платежі з високим рівнем захищеності. З появою Bitcoin і іншої криптовалюти ця задача стала вирішуваною.

Офіційним роком народження криптовалюти вважається 2009-й, коли почала функціонувати мережа Bitcoin. "Батьком" біткоіна і інших криптографічних валют вважається Сатоши Накамото - міфологізований персонаж або навіть група людей. Від цього імені вперше був опублікований протокол Bitcoin. Ним / ними ж і була проведена перша транзакція [18-20].

Очевидно, що Сатоши Накамото і КО реалізували багаторічні напрацювання фахівців в області криптографії та IT-технологій. Скільки років велися розробки і дослідження точно невідомо [21].

Зате відомо, що сам термін криптовалюта (cryptocurrency) вперше був використаний в матеріалі Forbes про Bitcoin в 2011-му році. Він настільки

сподобався і читачам, і шанувальникам нової віртуальної валюти, що незабаром почав характеризувати всю цю нішу.

При згадці слова «валюта», в розумі спливають образи банкнот, банків. Ми звикли до фіатного порядку у фінансових системах. Фіат - це стандартна, регульована валюта. Начебто долара або євро. Основні відмінності криптовалюта від фіатних валют полягають в наступному:

- криптовалюта не має фізичного вигляду. Так, фіат також існує в електронному вигляді, проте банкнот або кріптовалютних монет не буває. Не потрібно плутати фізичні монети, гаманці-накопичувачі і QR-коди, які використовують для роботи з криптовалютами;

- криптовалюта не випускається центральним банком і не прив'язана до економіки будь-якої країни. Випуск і емісія криптовалюта не контролюється кимось одним. Обмежити ці процеси не може ніхто. Тільки особливості самої системи. Курс сформований ринковим шляхом і безпосередньо ніяк не пов'язаний з економікою будь-якої країни;

- вона анонімна. Для роботи з банком, платіжними системами QIWI, Вебмані, Paypal необхідно вказувати хоча б частину особистих даних. У криптовалюта в цьому немає необхідності. Кожен учасник анонімний. Вся інформація про нього - це набір знаків в адресі гаманця;

- прямі транзакції. Ніяких процесингових центрів, посередників, емітентів і третіх сторін в цій віртуальній валютній системі немає. Є проста передача коштів між учасниками мережі безпосередньо.

Щоб користуватися криптовалютою, наприклад, Bitcoin, необхідно відкрити гаманець. Робиться це шляхом скачування клієнта на жорсткий диск, або в мережі. Популярний варіант онлайн-гаманця для біткоіни доступний на сайті blockchain.info (рисунок 1.2) [22-24].

Після швидкої реєстрації, вам буде привласнений гаманець з адресою. На цю адресу (27-34 знака) і будуть надходити платежі в подальшому (рисунок 1.3).

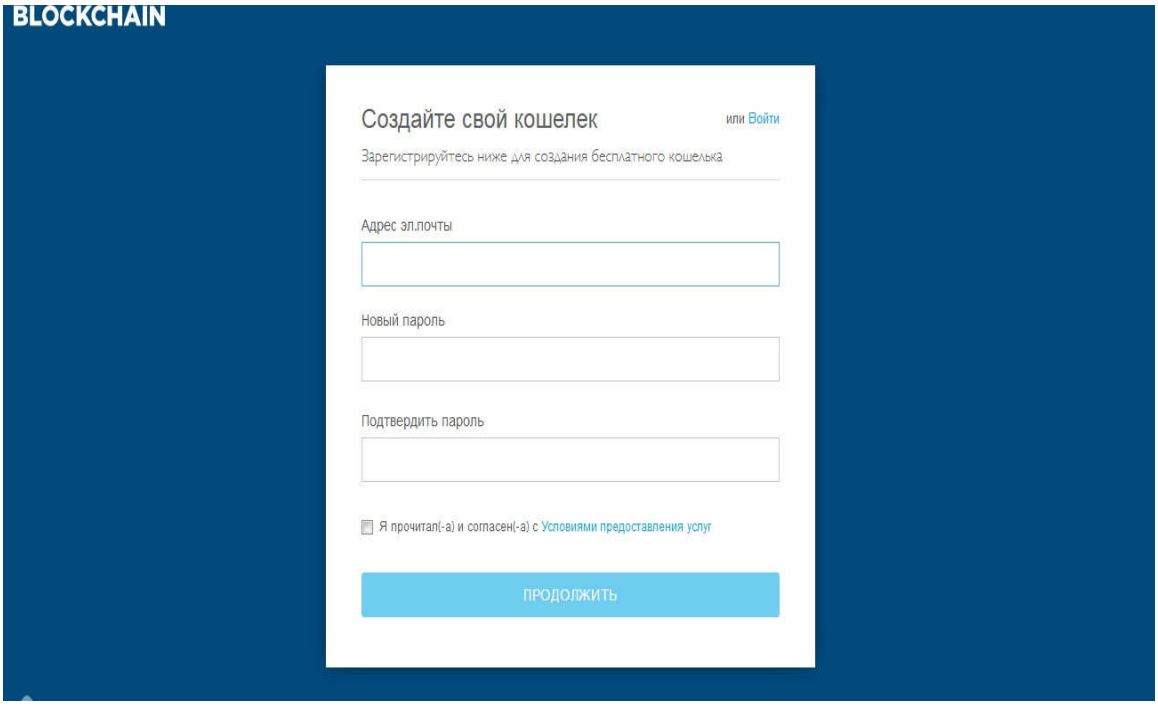

Рисунок 1.2 – Створення онлайн-гаманця

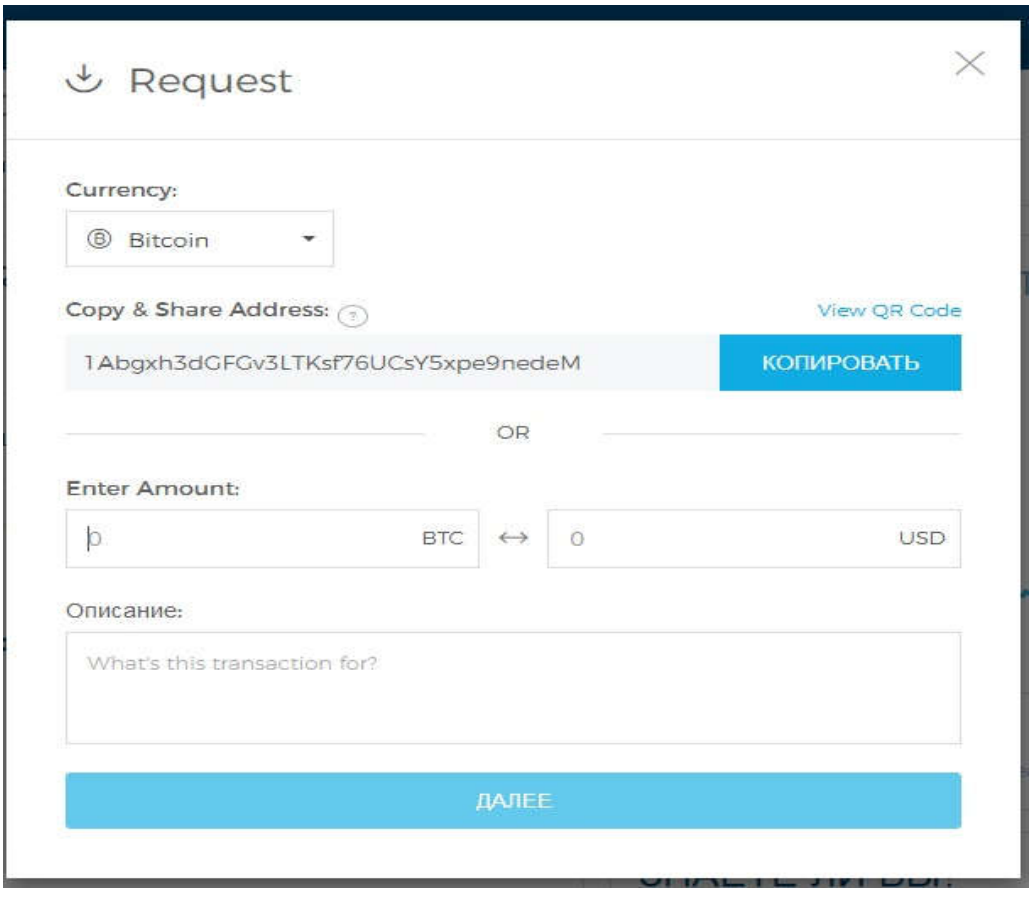

Рисунок 1.3 - Онлайн-гаманець з адресою

Криптовалюта корисна для різних цілей, починаючи від покупок і закінчуючи заощадженням грошей. Основні варіанти її використання:

- платежі. Причому не просто транзакції, а анонімні, швидкі і прямі транзакції. Здійснюються як між приватними особами, так і для покупки товарів або послуг в інтернеті;

- зберігання грошей. «Викрасти» криптовалюта з гаманця практично неможливо. Так як всі операції незворотні і використовують приватні ключі, перехопити їх або зламати неможливо. За умови, що ви нікому не дали свій приватний ключ, ваша криптовалюта буде завжди в цілості;

- інвестиції. Bitcoin і іншу крипту розглядають в якості інвестиційного активу за рахунок коливань курсу і загального зростання популярності. Причому криптовалюта підходить як для короткострокового заробітку шляхом торгівлі на біржі, так і для довгострокового, так як курс демонструє тенденцію до зростання;

- бізнес. Все більше компаній і сервісів підключають платежі у криптовалюті. Буденністю стали суто криптовалютні стартапи, що збирають кошти через ICO (краундфандінг). Якщо у вас особисто є бізнес-ідея, пов'язана з блокчейн або віртуальною валютою, то ви можете ініціювати збір коштів через ICO.

Найпоширенішим способом видобутку криптовалюти вважається Майнінг (від mining - добувати) [25-26]. Майнінг - це рішення криптографічних завдань різної складності з використанням потужностей обладнання. Є ще форджінг - спеціальна форма Майнінг з голосуванням і первинна емісія (ICO). Навіщо це взагалі потрібно і чому майнер отримують винагороду? Цей процес чимось нагадує роботу торрент-трекера. Учасники трекера займаються роздачею файлів і за це отримують рейтинг, який в подальшому використовується для скачування нових даних. Майнер ж, використовуючи обчислювальні потужності, підтримують працездатність мережі.

Кінцева мета майнінгу - підбір цифрового підпису, що закриває блок [27-28]. Як тільки це відбувається, блок закривається, майнер отримує винагороду і починає формуватися новий блок. Для видобутку різних криптовалют задіюється потужність процесора (CPU), відеокарт (GPU) або спеціалізоване обладнання (ASIC, FPGA). Майнінг - це один із способів заробітку на криптовалюті.

Для визначення способу Майнінг використовуються протоколи:

- Proof-of-Work (PoW) - «доказ роботи». Це алгоритм захисту, в якій справжність транзакцій підтверджується через виконання певних завдань. У PoW - чим вища продуктивність обладнання, тим більше видобувається монет;

- Proof-of-Stake (PoS) - «доказ частки». В якості ресурсу захисту вже використовується частка, тобто сама криптовалюта. PoS - це «кредитний» Майнінг. Чим більше на гаманці монет, тим більше винагорода;

- Proof-of-Activity (PoA) - «доказ активності». Гібридний варіант між PoS і PoW.

Інші, менш поширені протоколи: Proof-of-Capacity, Proof-of-Burn, Proof-of-Storage [29-30].

Вибір обладнання та його потужності залежить від алгоритму хешування. У Bitcoin це SHA-256. Цей алгоритм «зав'язаний» на продуктивності обладнання. У Litecoin - Scrypt, модифікований SHA-256, з великим упором на оперативну пам'ять.

1.2 Характеристики сучасних графічних процесорів

Сучасні центральні процесори (ЦП), якими оснащуються високопродуктивні обчислювальні системи, відрізняються дуже високою

частотою роботи і наявністю кількох ядер. Частота ЦП показує кількість вироблених кожним ядром процесора операцій в секунду. Основною характеристикою потужності і продуктивності майнингового обладнання є хеш в секунду – кількість операцій з 16-розрядними числами, які виробляються за 1 секунду. Чим вищою є ця величина, то тоді тим більшою буде найбільша максимальна продуктивність ферм із видобутку Bitcoin та інших криптовалют.

Найбільш відповідними елементами комп'ютера, здатними видавати велику потужність майнінгу є відеокарти і ЦП. Майнінг монет із застосуванням графічного процесора або відеокарти) отримав назву GPU видобутку, а при використанні процесорів – CPU майнінгу. Сучасні ЦП забезпечують максимальну потужність 1,4 Мегахеш/секунду. Використання GPU здатне забезпечити велику здобич, так як відеокарти мають обчислювальною потужністю в кілька разів вище процесорів, але вони все одно вимагають наявність материнської плати і процесора, і споживають багато електроенергії.

Для того, щоби розпочати майнінг, крім придбання потужного центрального процесора, необхідно завантажити сам майнер – це є відповідна програма для його роботи. Найбільш популярні майнери здатні при запуску майнінгу самі вибирати вигідні на даний момент кріптовалюти. Але їх вибір можливий за вашим бажанням. Налаштування майнера надають можливість вказати максимальне завантаження ЦП, кількість використовуваних ядер. Існує можливість додатково підключити до видобутку хорошу відеокарту.

Найефективнішими процесорами, що дозволяють майнити криптовалюту, є пристрої виробництва компаній Intel та AMD. Їх назви, частота роботи і майнінгова потужність представлені в таблицях відповідно 1.1 та 1.2.

Таблиця 1.1 – Характеристики процесорів компанії Intel

Найменування	Частота, Ггц	Потужність Кхеш/сек.
Intel Core i5-2320	3	700
Intel 2600K	4.5	1422
Intel Core i5-3570K	3.4	1100
Intel Core i5-3570K	4.223	1300
Intel Core i7-3770	3.4	1340

Таблиця 1.2 - Характеристики процесорів компанії AMD

Найменування	Частота, Ггц	Потужність Кхэш/сек.
AMD Phenom II X6 1075 6 ядер	2	1100
AMD Ryzen 1700X 8 ядер	3,6	1250

Для вирішення задачі видобутку на ЦП необхідно зробити кілька основних кроків. Для початку варто вибрати потужний ЦП, підібрати оптимальним чином материнську плату, необхідну швидкодіючу оперативну пам’ять, підключити жорсткий диск, блок живлення, монітор. На наступному кроці слід завантажити гаманець для обраної криптовалюти. Маючи адресу гаманця, потрібно вибрати програму – майнер і запустити видобуток криптовалюти.

Передові компанії з виробництва комп’ютерних ЦП змагаються, створюючи все більш досконалі пристрої. Лідерами цієї галузі є Intel і AMD. Популярними і поширеними серед людей, що займаються видобутком криптовалют, вважаються ЦП компанії Intel. Але останні розробки 8-ядерних

процесорів, що працюють на високих показниках частоти, від компанії AMD змушують багатьох фахівців звернути на них увагу. Вони більш економічні в плані споживання електроенергії.

Вибравши криптовалюту для майнінгу, необхідно завантажити з сайту її творця спеціальну програму – гаманець для зберігання намайненої криптовалюти за типом Bitcoin гаманця. Гаманець завантажується і встановлюється на жорсткий диск майнінгового обладнання. Після цього необхідно синхронізувати його з мережею. Завершальним етапом підготовки гаманця є отримання його праймкоін-адреси, яка буде використана у налаштуваннях запуску процесу видобутку bat-файлу.

Основним інструментом, що організовують і виконують всю роботу по видобутку монет, є спеціалізована програма – майнер (рисунок 1.4). В даний час існує понад 700 криптовалют. Кілька сотень з них володіють можливістю видобутку на аматорському рівні. Для процесорного видобутку підходять кілька десятків криптовалют, включаючи і Bitcoin. Але тільки кілька криптографічних валют раціонально добувати за допомогою процесора і для кожної з них підходить декілька алгоритмів і майнер.

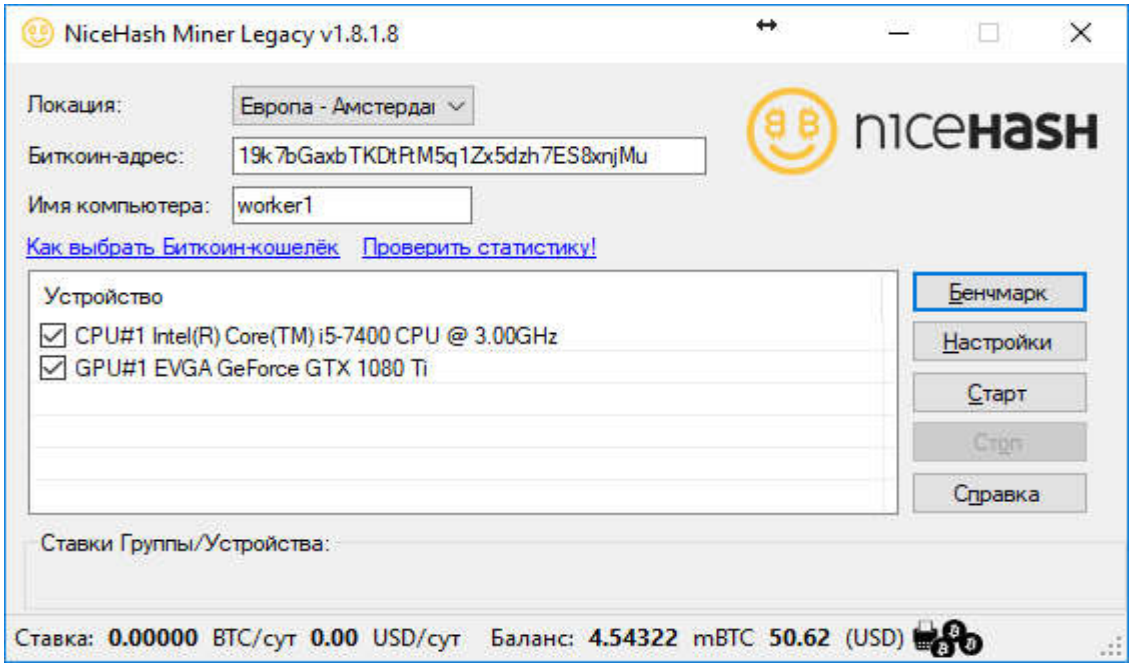

Рисунок 1.4 – Головне вікно майнера (NiceHash Legacy)

Вибравши оптимальний алгоритм і майнер для вашої крипти і типу ЦП, переходимо до створення об’єднуємно весь процес і запускаємо bat-файл. Це текстовий файл, який встановлює основні характеристики процесу видобутку і включає:

- назва файлу майнера;
- адреса порту та ідентифікатора на пулі, майнер;
- параметри, що вказують завантаження ЦП і виділяється під видобуток кількість ядер;
- виходячи з завантаження, вираховує і вказуєте максимально допустиму потужність;
- добровільний внесок власнику пулу.

Основою роботи з видобутку криптомонет є майнери. Підходять такі майнери, як wolf’s CPU miner, Ufasoft miner, Claymore CPU, Yam CPU, Ccminer, Ethminer, Nheqminer. Для видобутку більш відомих валют застосовуються такі майнери:

- CPU miner (pooler) – використовується для виробництва Litecoin;
- 50MINER – для Bitcoin, Litecoin;
- Ufasoft Miner – кілька криптовалют Roll-Ntime, TeneBrix, SolidCoin, BitForce;
- Jgarzik CPU miner – для видобутку тільки Bitcoin;
- GUI miner (Phoenix+Poclbm) – для Bitcoin;
- Eobot – для виробництва Bitcoin, Dogecoin.

Поняття ефективності видобутку криптовалют невіддільне від оцінки вартості і складності обладнання, витрат на конструкцію ферм, забезпечення безперебійним електропостачанням. При розгляді всього процесу в комплексі майнінг на процесорі виходить більш простим і менш залежить від енергоспоживання. А з урахуванням створення нових і порівняно недорогих ЦП, строки окупності процесорної ферми набагато коротше ферм на відеокартах або платах ASIC.

Майнінг Bitcoin на процесорі не ефективний, зважаючи всезростаючої складності видобутку. Купівля потужного комп'ютера або створення великої ферми з потужними відеокартами не дасть можливість заробити bitcoin, оскільки вкладення на створення нових блоків і всі обчислення набагато перевищують прибуток. В алгоритмі створення Bitcoin закладено зменшення в 2 рази винагороди за кожен блок після створення чергових 210 тис. штук. Зараз ця сума дорівнює 12,5 Bitcoin, що покриває витрати тільки завдяки високому курсу битка на ринку криптовалют.

Майнінг з використанням ЦП може виявитися ефективнішим в плані енергоспоживання і сумарної вартості обладнання, але менш доцільна по швидкості процесу. ЦП більш надійні і їх завжди можна використовувати в своїх комп'ютерах. CPU майнінг відрізняється здатністю виконувати різнопланові завдання одночасно, а GPU справляється з великими обсягами, але однотипної інформацією.

До мінусів видобутку на ЦП належить обмеження по потужності кожного процесора і складність побудови на їх основі ферм. Важливим є великі суми статей витрат при використанні найсучасніших ЦП на дорогі додаткові комплектуючі материнські плати останніх моделей, швидкодіючу оперативну пам'ять та інші.

1.3 Аналіз технічного завдання та постановка задачі

Метою даної дипломної роботи є розробка програмно-апаратної підсистеми добування крипто валют на основі сучасних графічних процесорів. На рисунку 1.5 представлено дерево рішень для розробки дипломної роботи.

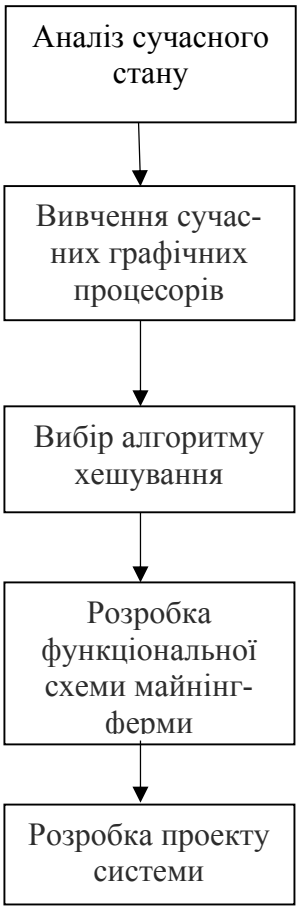

Рисунок 1.5 – Дерево рішень дипломної роботи

Для досягнення поставленої мети та виконання поставлених вимог необхідно вирішити такі завдання:

– провести огляд та аналіз типів криптовалют та способів їх добування;

– проаналізувати характеристики сучасних графічних процесорів;

– провести класифікацію методів добування криптовалют на основі технології блокчейну та різних хеш-функцій;

– сформувати вимоги до програмного та апаратного забезпечення;

– на основі сформованих вимог обґрунтувати вибір програмного та апаратного забезпечення з метою створення програмно-апаратної підсистеми для добування криптовалют;

– розробити структурну схему майнінг-ферми;

– дослідити схему запису транзакції в блокчейн;

– дослідити особливості алгоритмів майнінгу за допомогою відеокарт;

– здійснити налаштування програмно-апаратної підсистеми добування криптовалют.

2 ТЕХНОЛОГІЯ БЛОКЧЕЙНУ ТА ФОРМУВАННЯ ВИМОГ ДО ПРОГРАМНОГО І АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Характеристики різних типів криптовалют

Bitcoin - перша, найбільш популярна і дорога криптовалюта. Має неофіційний статус «криптозолота». Перші кілька років всі нові валюти базувалися на блокчейні Bitcoin. Тобто, були форком (або відгалуженням) першої в світі криптовалюти. Усю криптовалюту, крім Bitcoin, також називають альткоіни. У 2011-му році з'явилася монета Ripple зі своєю системою рукостискань і відсутністю майнінгу. Це був перший «не форк Bitcoin» в криптовалютному світі. У 2013 р з'явилися перші ICO-проекти: Mastercoin і NXT. NXT вирізняється тим, що вся емісія криптовалюти спочатку була розділена між 73 інвесторами.

У 2015 році запущена платформа Ethereum або ефіріум. Вона являє собою середовище для створення децентралізованих проектів на базі блокчейна з впровадженням «смарт-контрактів». Надалі ця криптовалюта стала другою найпотужнішою після Bitcoin. Ця платформа планує використовувати протокол Proof-of-Stake. В таблиці 2.1 наведені характеристики різних видів криптовалют.

Для видобутку криптовалюти потрібно потужне обладнання, яке споживає чимало електрики і поступово втрачає свою продуктивність. Виходить, що частково і амортизація переноситься на вартість монет.

Криптовалюта підкріплена системою блокчейна. Це те, чого немає в жодної іншої платіжної системи. Блокчейн універсальний, надійний, децентралізований. При цьому гарантує анонімність і високу швидкість транзакцій. Він застосовується в різних сферах. Починаючи від фінансового сектора, завершуючи альтернативною енергетикою. Його очевидні переваги визначають цінність криптовалюти.

Таблиця 2.1 - Характеристики різних видів криптовалют

Монета	Рік випуску	Максимальна емісія	Алгоритм хешування	Протокол
Bitcoin	2009	21 000 000	SHA-256	PoW
Ethereum	2015	90 000 000	Ethash	PoW, планується перехід до PoS
Litecoin	2011	84 000 000	Scrypt	PoW
Peercoin	2012	Необмежена	SHA-256	PoW-PoS гібрид
NXT	2013	1 000 000 000	-	PoS

Вартість віртуальних монет встановлюється ринковим шляхом. Чим більше попит на певну криптовалюта, тим вищий її курс. Попит же, в свою чергу, залежить від тих переваг, які пропонує монета. Якщо завтра Bitcoin зроблять офіційною валютою в Китаї, то її вартість «злетить до небес». Попит формується на тлі новин, нових розробок, анонсів компаній.

2.2 Технологія блокчейн

Блокчейн, напевно, найпопулярніше слово в сучасній бізнес-лексиці. В якому контексті його тільки не вживають! Добре відомо, що технологія блокчейн з'явилася порівняно недавно, в листопаді 2008 року, коли автор цієї технології Satoshi Nakamoto опублікував роботу «Bitcoin: A Peer-to-Peer Electronic Cash System».

Про сам Satoshi не відомо жодної інформації. Не відомо навіть, він це чи вона, можуть бути і вони, але точно відомо, що їм / їй / ними було зроблено - винайдена пірінгова система електронних платежів.

Bitcoin був першим додатком блокчейн технології, де він відмовився від централізованої бази даних для зберігання інформації про рахунки користувачів і запропонував використовувати розподілену базу даних, в якій записи зберігаються в формі ланцюжка блоків транзакцій: транзакції записуються в блоках, блоки зв'язуються в ланцюжок за допомогою криптографічного підпису .

На рисунку 2.1 показана схема ланцюжка блоків транзакцій, з'єднаних з використанням хеш-функції (криптографічного підпису).

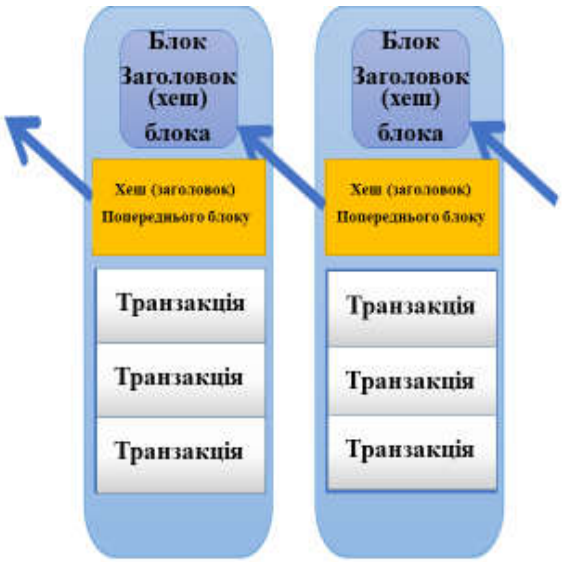

Рисунок 2.1 – Схема блоків транзакцій

Ось цей криптографічний підпис і забезпечує достовірність і незмінність даних, які можуть бути не тільки відомостями про операції з Bitcoin, але і з будь-якими іншими даними - від текстових повідомлень і записів про страхові випадки до угод з нерухомістю та фондовими активами.

Є одна важлива деталь: у блокчейні не можна зберегти сам документ, наприклад скан сторінки, але можна зберегти хеш цього документа і відомості про його передачу. Сам же документ буде зберігатися в звичайній

базі даних або просто на файл сервері. На рисунку 2.2 показана схема запису транзакції в блокчейн.

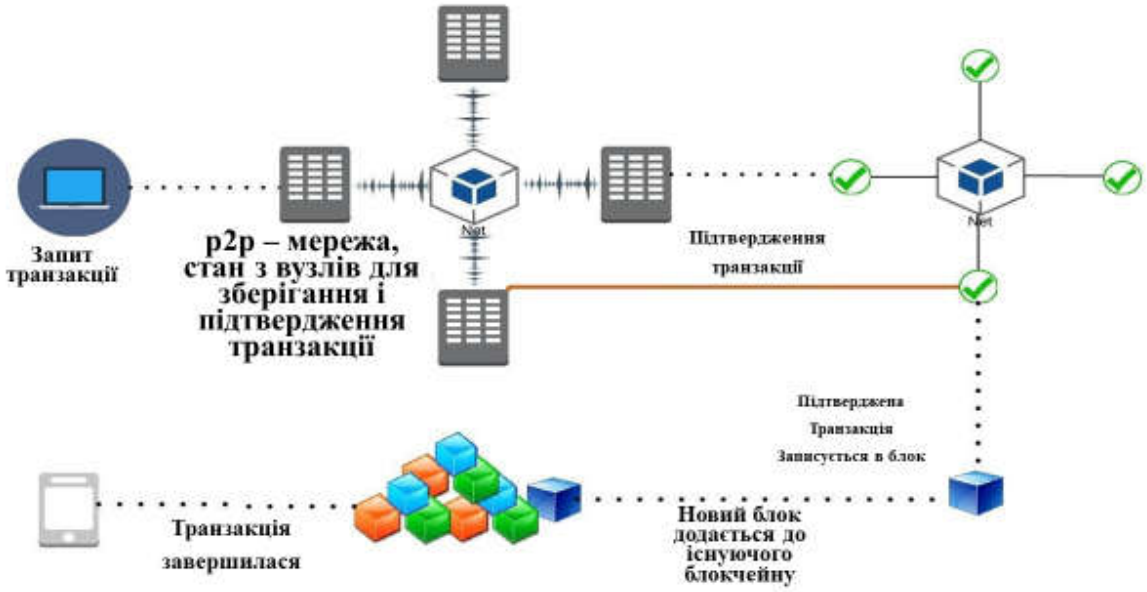

Рисунок 2.2 – Схема запису транзакції в блокчейн

З'являється механізм колективного зберігання на множині вузлів в мережі, забезпечується достовірність запису в базі даних, записи виявляються захищені від видалення-злому-зміни.

Користувач виграє за кількома напрямками:

- зникає армія посередників, вони просто не потрібні при колективному зберіганні даних;

- завдяки відсутності посередників вартість використання блокчейна виявляється набагато нижче, ніж у традиційних централізованих баз даних;

- за рахунок децентралізованності блокчейна, досягається значне зниження операційного ризику - неможливо «вимкнути» блокчейн поки працює хоч один вузол;

- кожен користувач має цифровий ідентифікатор і підпис, що дає високу ступінь захищеності.

Блокчейн може безпечно синхронізувати і зберігати не тільки дані про торговельні та фінансові потоки, але і відомості про будь-яких бізнес процесах і документах.

Ведення записів про поточні транзакції - базова функція будь-якого бізнесу. Ці записи відображають минулі дії та допомагають планувати майбутні.

Вони показують не тільки те, як організація працює всередині, але і її зовнішні відносини. Діючі стандарти і правила, пов'язані з веденням записів про транзакції абсолютно не вписуються в процеси цифрової трансформації.

Блокчейн може закрити цей розрив, ставши корисним інструментом цифрової трансформації зовнішніх і внутрішніх транзакцій при виконанні наступних умов:

- взаємодія безлічі незалежних учасників;

- незмінюваність бази даних, до якої мають доступ і можливість додавання даних всі учасники;

- передача цінних активів або критичних даних між учасниками;

- використання smart contracts для виконання договірних зобов'язань.

Блокчейн цікавий своїми застосуваннями в різних галузях, в даний час виділяються наступні (рисунок 2.3):

- фінансові послуги;

- голосування;

- охорона здоров'я;

- автомобілі.

На закінчення - трохи цифр. Згідно з даними "Markets and Markets", до 2021 року обсяг ринку блокчейн технологій виросте до 2,3 трл, з сукупним річним темпом приросту в 61,5%.

Однак якщо валюта являє собою електронний запис, тобто програмний код, то і ланцюжок відомостей про транзакціях (рисунок 2.4) також можна «причепити» до запису самого Bitcoin.

Рисунок 2.3 – Застосування блокчейн

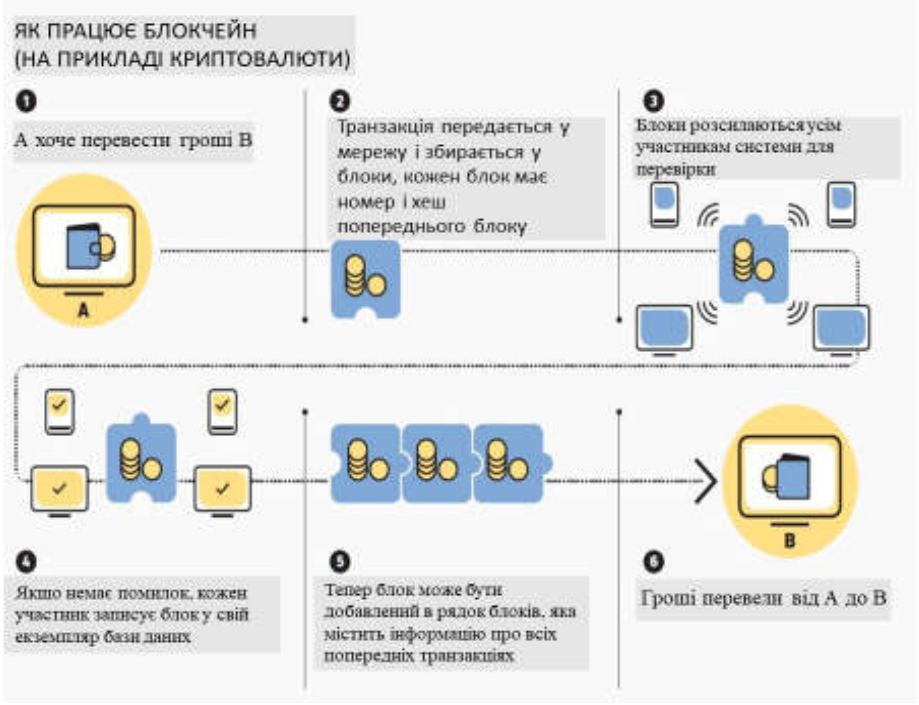

Рисунок 2.4 - Ланцюг відомостей про транзакціях

Якщо далі все це зашифрувати, потім декілька разів заархівувати, а наостанок закриптувати за допомогою потужних кодуючих програм, то фінальний результат вкладеться, наприклад, в 35 символів. Саме таку довжину має максимальний крипто-код Bitcoin.

Загальний принцип викладений цілком послідовно. Унікальність і непідробленість Bitcoin забезпечується перманентним внесенням в його програмний код всіх без винятку транзакцій. Більш того, інформація про це автоматично поширюється на всі інші існуючі блокчейни (які мають відношення до даної транзакції). Блок-чейн - ланцюжок блоків, кожен з яких несе дані про вчинений дії. Втрутитися в роботу даної системи ніхто не зможе. Структурна схема запису транзакції в блокчейн представлена на ДП.КСМ.07145/14.00.00.000 С1.

2.3 Хеш-функція SHA-256

SHA-256 являє собою криптографічний функцію хешування, яку розробили в Америці співробітники Агентства Національної Безпеки (АНБ).

Хеш-функція SHA-256 є односпрямованої функцією алгоритму SHA-2 (Secure Hash Algorithm Version 2). Основне застосування - захист інформації.

На рисунку 2.5 приведена схема однієї ітерації алгоритму SHA-256.

В основі хеш-функції лежить структура Меркле-Дамгарда, згідно з якою вихідне значення після доповнення розбивається на блоки, а кожен блок в свою чергу на 16 слів.

Кожен блок повідомлення пропускається алгоритмом через цикл з 80 або 64 Інтерацій, або раундами. На кожному раунді задається функція перетворення входять до складу блоку слів. Два слова з повідомлення перетворюються цією функцією. Отримані результати сумуються, а в результаті виходить значення хеш-функції. Для обробки наступного блоку використовуються результати обробки попереднього блоку. Незалежно один від одного блоки обробляти не можна.

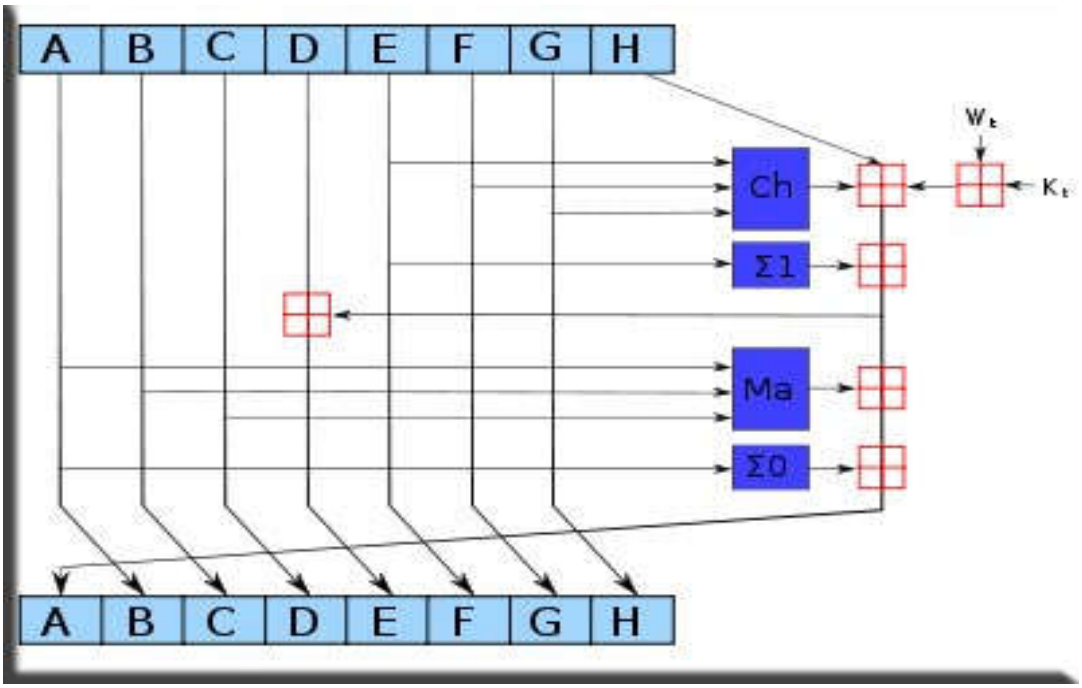

Рисунок 2.5 - Схема однієї ітерації алгоритму SHA-256

В роботі алгоритму SHA-2 використовуються бітові операції:

- || - конкатенація - операція склеювання об'єктів лінійної структури, рядків

- + - операція додавання

- and (&, &&) - побітова операція «І»;

- xor - операція, що виключає «АБО»;

- shr (shift right) - логічний зсув вправо;

- rots (rotate right) - циклічний зсув вправо.

Технічні характеристики хеш-функції SHA-256:

- довжина дайджесту повідомлення (біт) – 256;

- довжина внутрішнього стану (біт) - 256 (8x32);

- довжина блоку (біт) – 512;

- максимальна довжина повідомлення (біт) - 264-1;

- довжина слова (біт) – 32;

- кількість інтерацій в циклі – 64;

- швидкість (MiB / s) – 139.

Ось приклад використання функції хешування SHA-256. Результатом хешування фрази «Bitcoin is the most popular cryptocurrency» буде вираз: 6810abc7 27b7e113 c8aa73f6 15bdb2ba adb1aa9c f30e177c 16c4df1a 82caf226

При щонайменшій зміні тексту повідомлення результат хешування змінюється кардинально. Це є багаторазовим наслідком «лавинного ефекту» - важливих криптографічних властивостей для шифрування.

Варто змінити в вищевказаному прикладі першу букву «B» на маленьку «b», отримаємо наступний результат:

aa5415b4 cf0808fe 04457075 f5749564 9b45ca3a be9e9d11 bbb9fdae eab233ee.

2.4 Вимоги до програмного та апаратного забезпечення

Програмне забезпечення відграє таку ж важливу роль у підборі та складанні комп'ютера як і апаратне забезпечення.

Для коректної роботи усієї системи потрібно:

- операційну систему(windows10\7, Linux) обов’язково останьої версії щоб була сумістність із усіма драйверами;

- nvidia geforce experience для встановлення найновіших драйверів;

- MSI Afteburner для корегування та збільшення продуктивності відеокарт (виключно для nvidia);

- TeamViewer для перевірки та налаштування комп’ютера віддалено;

- Miner NiceHash Legacy для добування криптовалюти(одна із найпростіших програм) ;

- shell:startup для самостійної загрузки майнера після включення комп’ютера;

- мій комп’ютер – властивості – додаткові параметри системи – параметри – додатково – віртуальна пам’ять (змінити) – вказати розмір вручну (залежно від кількості відеокарт на кожну з яких слід виділяти по 2гб оперативної пам’яті) ;

- виключення усіх антивірусів та обновлення windows для безперебійної роботи комп’ютера;

- виключення функції перехід у режим сну;

- Aida64 для перевірки усього комп’ютера вручну;

- видалення лишнього софту;

- налаштування Bios для відеокарт AMD Crimson ReLive (виключно для Radeon) ;

- налаштування Bios материнської плати, змінюється у настройках перед запуском windows, у кожної материнської плати зовнішній вигляд Bios відрізгяєть проте характеристики які нам потрібно задати є у більшості плат;

Характеристики Bios материнської плати:

- автозапуск після появи електроенергії;

- прошивка до останьої версії Bios;

- включення режиму для майнингу або ж 4G ;

- виведення для пріоритету cpu відео для зняття лишньої нагрузки з основнрї відеокарти.

Для коректної роботи усієї системи потрібно таке апаратне забезпечення:

- материнську плату на чіпсеті 1150 або 1151(різні виробники, рекомендовано intel), asrock pro btc h81, gigabyte ga-h110-d3a(найбільш популярні) ;

- відеокарт від 960 до 1080ti nvidia або radeon 470\480-570\580 (відеокарти старішого екземпляру нерентабельні) ;

- блок живлення із запасом потужності від сумарної усієї системи понад 100-150 ват, для двох і більше блоків живлення використовують синхронізатор;

- жорсткий диск ssd для швидкої та безперебійної роботи системи;

- оперативна пам’ять ddr3(для z170\h81) або ddr4(для z270\z370\h110);

- процесор Pentium\i3\i5\i7 1150\1151(залежно від материнської плати);

- райзера та перехідники для відеокарт;

- watch Dog для автоматичної перезагрузки при зависанні операційної системи;

- додаткове охолодження при потребі.

3 ПРОЕКТУВАННЯ ПРОГРАМНО-АПАРАТНОЇ СИСТЕМИ ДЛЯ ДОБУВАННЯ КРИПТОВАЛЮТ

3.1 Обгрунтування вибору програмного і апаратного забезпечення

Виходячи з проведеного аналізу можливих структур побудови систем збору і обробки інформації майнінг-систем, система, що розробляється, повинна мати такі характеристики:

- повинна бути стаціонарною і незалежною;
- за способами з'єднання станційної апаратури з периферійними блоками його топологія повинна бути шлейфової без концентраторів;
- безпосередньо електропостачання повинно бути постійним, для стабільної роботи;
- безперебійний інтернет проведений оптоволокном для кращої стабільності;
- зібрана та налаштована спеціалістом у цій галузі для уникнення проблем.

Основними комплектуючими для майнінг-комп’ютера є:

- материнська плата;
- процесор;
- оперативна пам’ять;
- жорсткий диск;
- відеокарти;
- кулер процесорний з термопастою;
- райзера;
- блок живлення;
- перехідники;
- синхронізатор блоків живлення;
- WatchDog для перезавантаження;

– корпус;

– кнопка для включення;

– відпвідні умови для стабільної роботи;

– стабільна система з останніми драйверами;

– прошитий біос та відеокарти.

Материнська плата, структурна схема якої представлена на рисунку 3.1, повинна володіти такими характеристиками:

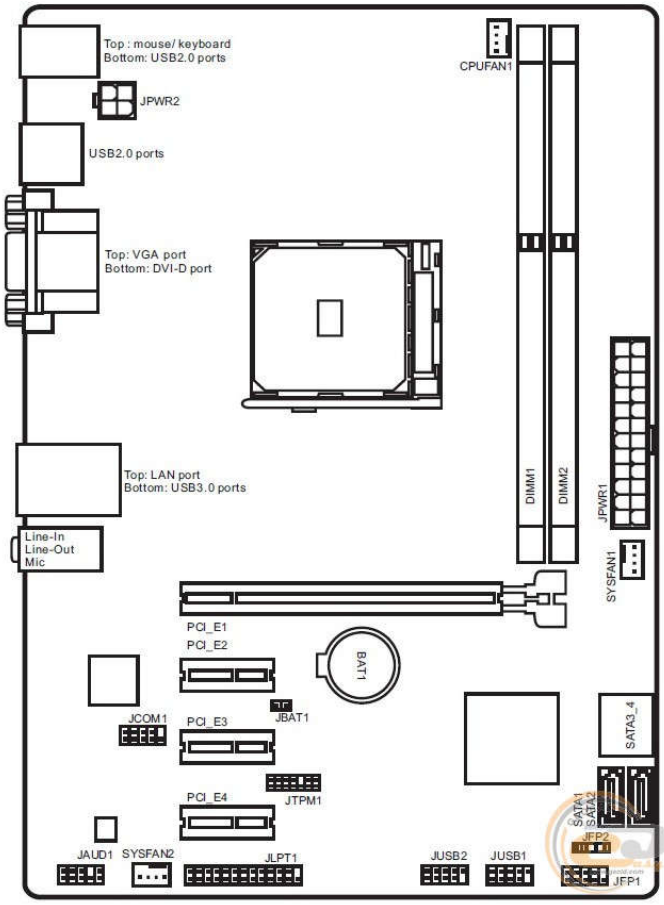

Рисунок 3.1 - Структурна схема материнської плати для майнингу

- ASRock Super Alloy;

- підтримка нових процесорів Intel® Xeon®/Core™ i7/i5/i3/Pentium®/Celeron® 4-го и 5-го покоління (Разъем 1150);

- твердотілі конденсатори;

- Digi Power, Система живлення 4;
- підтримка двухканальної DDR3 1600;
- 1 PCIe 2.0 x16, 5 PCIe 2.0 x1;
- пристрій графічного виводу даних: D-Sub, HDMI;
- встроєний аудіо 5.1 HD (Аудіокодек Realtek ALC662);
- 2 SATA3, 2 SATA2;
- 2 USB 3.1 Gen1, 6 USB 2.0 (4 передніх, 2 задніх);
- Realtek Gigabit LAN;
- підтримує Full Spike Protection, ASRock Live Update & APP Shop.

Загальна структурна схема майнінг-ферми показана на ДП.КСМ.07145/14.00.00.001 С1.

Вибір програми для майнінгу залежить від того, яку потрібно добувати криптовалюту. У майнінгу різних монет закладені різні алгоритми. Наприклад, біткоін працює на базі Blockchain, айота - на основі розподіленого реєстру Tangle, а в монери використовується алгоритм CryptoNight. Тому для видобутку тієї чи іншої криптовалюта підходять різні програми, які відповідають різним алгоритмам.

Далі потрібно оцінити потужність обладнання для Майнінг і підібрати відповідну програму.

Якщо процесор не може видати потужність, більше 20 MH/s, то немає сенсу ставити програму, розраховану на роботу з потужностями від 50 MH/s. Але і брати найпростіший софт, розрахований під слабке обладнання, теж не потрібно - це недоцільне використання наявних потужностей.

Третій важливий момент - тип майнінгу. Майнінг на відкритих процесорах і ASIC здійснюється різними додатками. Бувають і універсальні програми, але більша їх частина випускається окремо для GPU-, CPU- або ASIC-Майнінг.

Крім основних критеріїв, потрібно звертати увагу і на інші важливі параметри програм для Майнінг:

- можливість видобутку різних криптовалют (одні програми використовуються для конкретної криптовалюти, інші дозволяють майнінг різних монет);

- зручність інтерфейсу (інтуїтивно зрозумілий графічний, який підійде навіть новачкам, або консольний, де потрібні навички роботи зі скриптами);

- наявність додаткових функцій (регулювання нагріву, можливість роботи у фоновому режимі, автоматичний підбір обчислювальних алгоритмів тощо)

Новачкам працювати з графічним інтерфейсом простіше всього: інформація вводиться в спеціально виділені поля, а сам майнінг запускається простим натисканням кнопки.

Консольні програми дають більше можливостей для тонкої настройки майнінгу, але всі команди доводиться прописувати вручну в системному файлі з розширенням .bat. А для цього потрібно знати всі основні скрипти і додаткові команди.

Найпопулярніші програми для майнінгу криптовалют вже довели свою працездатність і обзавелися власними онлайн-спільнотами. Останній пункт важливий тим, що докладні інструкції по правильному встановленню та налагодженню таких програм можна знайти на тематичних форумах або сайтах, присвячених тій чи іншій програмі.

CG Miner - одна з найпопулярніших програм для видобутку біткоінів, підходить для майнінгу на процесорі або ASIC. Головна її перевага - висока стабільність і ефективна робота в фоновому режимі. Іншими словами, не потрібно постійно стежити за роботою програми. Крім того, це одна з небагатьох програм, до яких додається текстовий файл з інструкцією для користувача. Проте новачкам вона може здатися дуже складною. Це варіант для досвідчених користувачів, які звикли до роботи зі скриптами.

GUI Miner - проста, але функціональна програма для CPU-майнінгу біткоіна. По суті, це практично точна копія CG Miner, але загорнута в

графічну оболонку і, що дуже зручно, перекладена на російську мову. Працювати в ній набагато зручніше, але досвідчені майнери воліють звичну і більш надійну CG Miner. А от новачкам краще спочатку набити руку на GUI Miner, а потім, якщо потрібно, переходити і на CG Miner.

Nheqminer – це є складна консольна програма, яка дає можливість майнити Zec за допомогою відеокарти або процесора. Однак при CPU-Майнінг рівень навантаження на процесор може досягати 100%, через що обладнання часто ламається і виходить з ладу. Розробникам до сих пір не вдалося вирішити цю проблему, тому краще за все використовувати програму для майнінгу на відеокартах. Але потрібно також врахувати, що офіційної інструкції до програми немає, а всі команди потрібно вводити через консоль. Так що цей варіант підходить тільки для досвідчених користувачів, які вміють працювати з скриптами і шукають хорошу програму для майнінгу Zec.

Miner Gate - універсальна і дуже проста у використанні програма для майнінгу 14 криптовалют, в тому числі біткоіна, лайткоіна, ефіріума, Зет-кеша, монери, деша і байткоіна. Відрізняється зручною графічною панеллю і вбудованим конвертором віртуальних валют. А ще смарт-режимом, в якому система сама обирає, яку криптовалюту вигідніше добувати саме зараз. Свій вибір програма робить, виходячи з використовуваних потужностей і поточного курсу криптовалюти.

Claymore's Dual Miner - унікальна програма для одночасного майнінгу ефіріума і однією з чотирьох криптовалют на вибір (Pascal, Decred, Lbry або Siacoin). Оновлені версії програми підходять також для майнінгу монери, комодо, Зет-кеша і байткоіна. Підходить для роботи з потужними відеокартами NVidia і AMD. Дає можливість ефективно розганяти відеокарти.

3.2 Особливості алгоритмів майнінгу за допомогою відеокарт

Найбільш відомий алгоритм - SHA256. Такий алгоритм у Bitcoin (BTC, XBT), Bitcoin Cash (BCH, BCC), Namecoin (NMC), SwiftCoin (STC). Цей алгоритм найменш рентабельний в зв'язку з тим, що допускає наявність на ринку надпотужних обчислювальних пристроїв типу ASIC, що зводить боротьбу за винагороду в гру кількох великих інвесторів.

Наступний найбільш поширений алгоритм - Scrypt. Головна особливість - складність розрахунку хеш-суми, що вимагає наявність більшого об'єму оперативної пам'яті. На Scrypt «сидять» такі криптовалюти, як Litecoin (LTC), Dogecoin (DOGE, XDG), BlackCoin (BC), PotCoin (POT), BitConnect (BCC) та інші.

Ethereum (ETH), як і його форк Ethereum classic (ETC), добуваються за алгоритмом Ethash, який створювався як ASIC-стійкий аналог SHA256. Ethash є головним майнінг-конкурентом Equihash.

Останній заснований на концепції комп'ютерної науки і криптографії під назвою «Generalized Birthday Problem». Equihash задає алгоритм наступним крипті: Zcash (ZEC), Zcash Classic (ZCL), Zencash (ZEN) і Hush (HUSH). Як і в Scrypt, кількість намайнених монет в Equihash залежить від того, яка RAM-пам'ять.

Список PoW криптовалют, які можна рентабельно майнити на GPU пристроях, показано на рисунку 3.3. Найбільш прибуткові алгоритми для GPU Майнінг * (за вересень 2017).

Equihash - найприбутковіший за часом на сьогоднішній день майнінг-алгоритм для видобутку криптовалют на відкритих пулах. Це твердження справедливо і для наступних ТОП-5 GPU пристроїв:

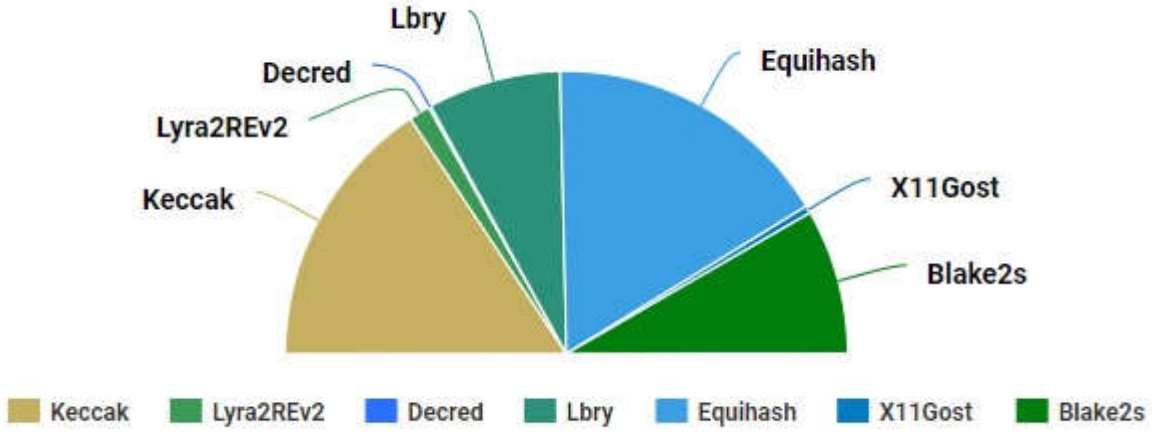

Рисунок 3.3 - Список PoW криптовалют, які можна рентабельно майнити на GPU пристроях

- NVIDIA GTX 1080 Ti;
- NVIDIA GTX 1080;
- NVIDIA GTX 980 Ti;
- AMD R9 Fury Nano;
- NVIDIA GTX 1070.

На окупність майнінгу впливають такі технічні характеристики відеокарт:

- обсяг пам'яті відеокарти, Mb;
- частота GPU, Mhz;
- частота пам'яті, Mhz;
- енергоспоживання, W.

Перші 3 показники будуть впливати на хешрейт (швидкість майнінгу). Четвертий - витрати на електроенергію. В таблиці 3.1 представлено порівняльні характеристики відеокарт для майнінгу.

Технологічно відрізняються тільки карти з GPU від різних виробників. Головні конкуренти стандартних комплектацій всім відомі - це AMD і NVIDIA. В іншому ж хешрейт, за великим рахунком, буде визначатися озвученими вище параметрами. Чим вище ці показники, тим вище хешрейт.

Таблиця 3.1 - Порівняльні характеристики відеокарт для майнінгу

Назва відеокарти	NVIDIA GeForce GTX 1080 Ti	NVIDIA GeForce GTX 1080	NVIDIA GeForce GTX 980 Ti	AMD Radeon R9 Fury X	NVIDIA GeForce GTX 1070
1	2	3	4	5	6
Техпроцес	16 нм	16 нм	28 нм	28 нм	16 нм
Об’єм пам’яті	11 264 Мб	8 192 Мб	6 144 Мб	4 096 Мб	8 192 Мб
Частота GPU	1632 МГц	1607 МГц	1025 МГц	1050 МГц	1607 МГц
Тип пам’яті	GDDR5X	GDDR5X	GDDR5	HBM	GDDR5
Частота пам’яті	11 448 МГц	10 000 МГц	7 010 МГц	1 000 МГц	8 108 МГц
Шина обміну з пам’яттю	352 бит	256 бит	384 бит	4096 бит	256 бит
Число універсальних процесорів	3584	2560	2816	4096	1920
Число текстурних блоків	224	160	176	256	120
Число блоків ростеризації	88	64	96	64	64
Підтримка CUDA	Так	Так	Так	—	Так
Підтримка AMD APP (ATI Stream)	—	—	—	ДА	—
Роз’єм додаткового живлення	8 pin + 8 pin	8 pin + 6 pin	8 pin + 6 pin	8 pin + 8 pin	8 pin + 6 pin

Продовження таблиці 3.1

1	2	3	4	5	6
Рекомендована потужність блоку живлення	600 Вт	500 Вт	немає даних	немає даних	500 Вт
TDP	250 Вт	180 Вт	250 Вт	275 Вт	150 Вт
Дизайн системи охолодження	custom	custom	custom	reference	custom

В таблиці 3.2 представлені ті ж самі топ-5 відеокарт з розрахунком окупності по кожній та з розрахунку найбільш прибуткового за часом майнінг-алгоритму для конкретної відеокарти за місяць.

Таблиця 3.2 - Термін окупності відеокарт

Назва відеокарти	GeForce GTX 1080 Ti	GeForce GTX 1080	GeForce GTX 980 Ti	AMD Radeon R9 Fury X	GeForce GTX 1070
Ціна (мінімальна), грн	32 661	15 723	25 997	14 404	16 988
Алгоритм	Equihash	Lyra2Rev2	Equihash	Equihash	NeoSkrypt
Хешрейт	630 Sol/s	49.11 MH/s	461 Sol/s	450 Sol/s	1.01 MH/s
Дохід у місяць, грн	2 513	2 153	1 909	1 592	1 585
Окупність (без урахування витрат на е/е і зміни курсу)	12 міс.	10 міс.	16 міс.	9 міс.	11 міс.

Найкраща карта в рейтингу опинилася AMD Radeon R9 Fury X - 9 місяців. Звичайно, потрібно обов'язково врахувати витрати на електроенергію, зміну швидкості мережі і волатильність курсу валют, яку майнити. Але тим не менш загальну картину окупності топ-відеокарт показано у схемі.

Купівля пристроїв на вторинному ринку - завжди ризик. Важливо знати наскільки дбайливо використовувалася, розганялася або ремонтувалася стара карта. Слід на місці перевірити б/у пристрій перед покупкою, розігнавши пристрій до максимальних меж. Цією можливістю користуються багато майнерів з метою швидше окупити дорогу покупку. Це може привести до втрати продуктивності через підвищену температуру і неправильну експлуатацію.

Тому бажано використовувати нові відеокарти або нові моделі, в які вже вбудована надійна система охолодження. Така система при розгоні не допустить перегріву. Як правило, чим пізніша дата випуску карти, тим стабільніша і ефективніша її робота при максимальних навантаженнях.

Якщо мета майнінгу - прибуток, коли отриманий дохід буде покривати всі витрати на оплату електрики, характеристики відеокарти повинні бути вищі мінімальної планки. Видобуток криптовалюти на дешевих картах буде економічно недоцільним, якщо продуктивність відеоадаптерів не буде забезпечувати цю умову.

Такий спосіб підійде, якщо системний адміністратор має необмежений доступ до досить великої комп'ютерної мережі, в якій можна організувати надійно прихований майнінг. Але це вже незаконна діяльність. На форумах майнери розповідають, що в місяць при середньому завантаженні кількох десятків ПК протягом робочого дня виходить добувати на досить велику суму коштів.

Переважна більшість виробників відеокарт, прогнозуючи подальший високий попит на свою продукцію, тому планують випуск спеціальних

майнінг-девайсів у найближчому майбутньому. Такі пристрої будуть призначені тільки для криптовалюти, а ціна на них буде значно нижча, ніж на GPU, які використовуються у повсякденних звичайних комп'ютерах та обчислювальних системах.

Компанія ASUS вже представила на своєму сайті модель Mining RX470-4G. Її характеристики:

- AMD Radeon RX 470;
- 7000 MHz (1750 MHz GDDR5);
- 256-bit;
- GDDR5 4GB.

Спеціалізовані карти не мають відеовиходів. У продажу їх поки немає, але вони будуть користуватися попитом і, що головне, звільнять ринок геймерських карт.

3.3 Налаштування програмно-апаратної підсистеми добування криптовалют

В материнську плату встановлюється процесор, кулер і плашка пам'яті. Підключається SSD диск з SATA кабелю. Заживлюється це все від від одного блоку живлення, він буде провідним блоком. Поки що можна поставити всього одну відеокарту.

Після запуску ферми треба зайти в BIOS і оновити його до останньої версії. Скачати її можна з сайту Asus. Для установки Bios буде потрібно записати файл з новою версією на флешку, натиснути F7 для розширених налаштувань BIOS, далі знайти ASUS EZ Flash Utility, вибрати USB і встановити потрібний файл з флешки. Після успішного оновлення BIOS потрібно налаштувати материнську плату для майнінгу та встановити

Windows 10 64bit за допомогою стандартної установки (рисунок 3.4), все зайве видаляється. Далі треба налаштувати інтернет і скачати з офіційного сайту драйвери для материнської плати. Встановити всі запропоновані сайтом Asus драйвера.

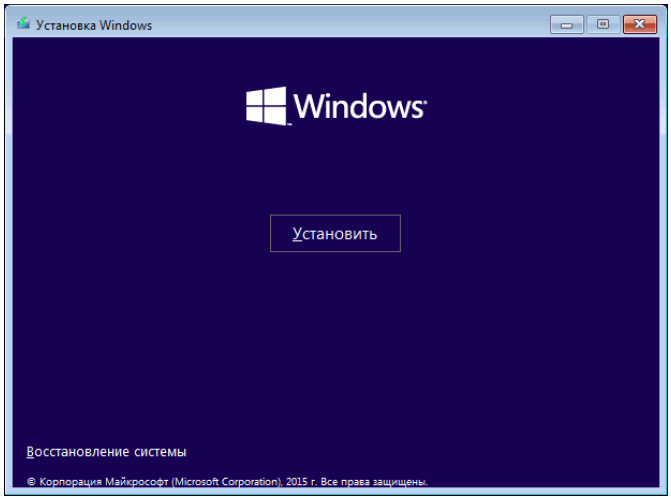

Рисунок 3.4 – Встановлення Windows 10 64bit

Крім того, треба змінити розмір файлу підкачки. Якщо SSD 80 ГБ, то ставити файл підкачки 30000 МБ. Поставити на ферму TeamViewer або інше програмне забезпечення для віддаленого управління.

Для установки відеокарт треба скачати драйвер для Nvidia або AMD, в залежності від того, які карти. Встановити драйвер, перезавантажити ферму і перевірити, що все працює. Далі перезавантажити ферму ще раз, зайти в BIOS (рисунок 3.5) і змінити ще одну настройку: перевести Above 4G Decoding в стан Enabled і оновити BIOS (рисунок 3.6).

Після вимкнення ферми треба підключити всі інші карти. Монітор бажано підключати в карту №1 (слот №1).

Підключати кабелі потрібно так, щоб карта і райзер, в який вона вставлена, брали електроенергію від одного блоку живлення!

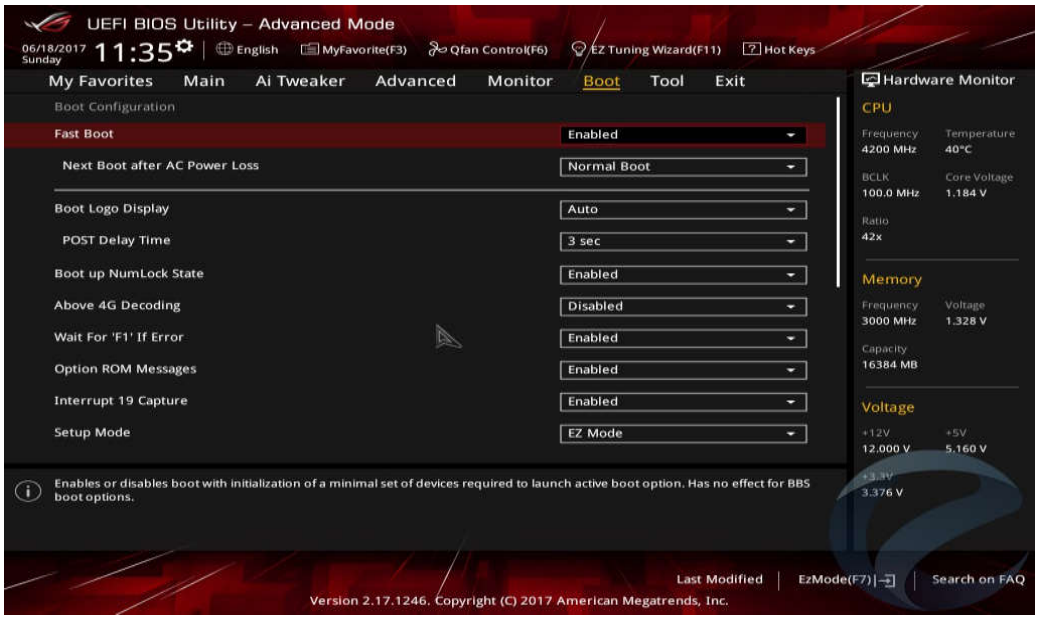

Рисунок 3.5 – Налаштування BIOS

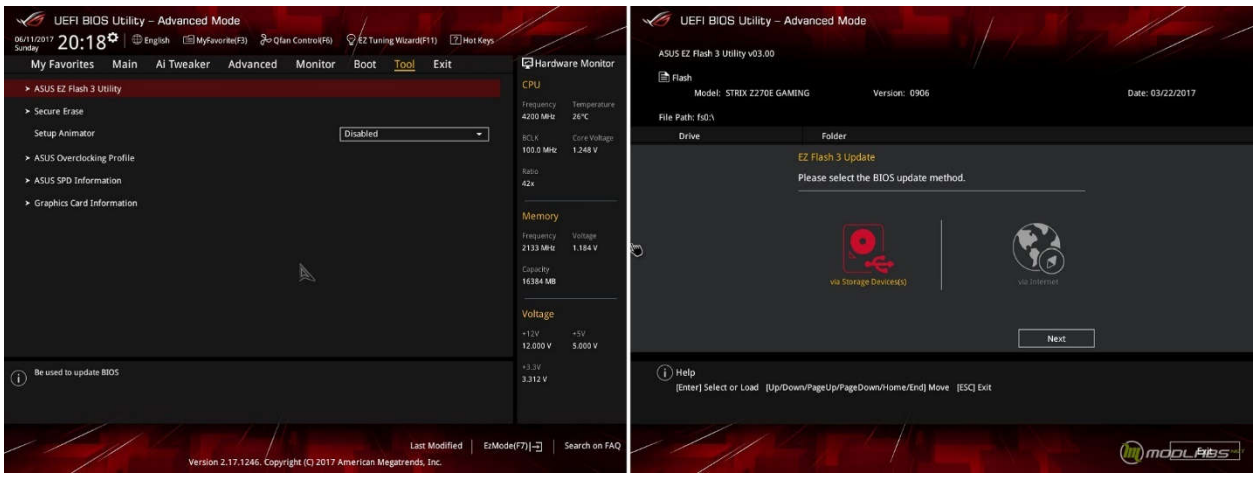

Рисунок 3.6 – Оновлення BIOS

Після включення ферми проходить деякий час. Windows буде поступово знаходити відеокарти. Якщо встановлений TeamViewer, то можна через нього стежити за тим, що відбувається з фермою. Буває деякі карти не встановлюються нормально і висять в невизначених відеоадаптерах. В цьому випадку треба поставити драйвер вручну, вказавши до нього шлях.

З картами AMD ситуація буває більш складна: карти встановлюються, але у кожної горить знак оклику. На допомогу прийде програма AMD atikmdag Patcher (рисунок 3.7). Потрібно натиснути «Yes» і після перезавантаження система повинна працювати.

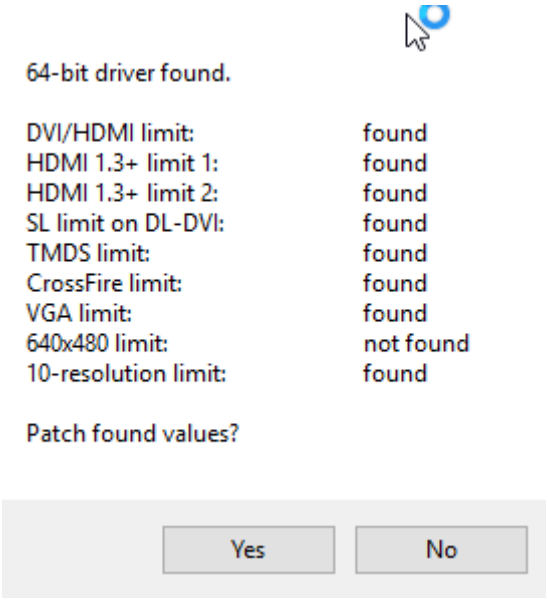

Рисунок 3.7 - Програма AMD atikmdag Patcher

Далі потрібно правильно підключити контакти WatchDog до контактів Reset і Power на материнській платі, щоб таймер міг перезавантажувати або вимикати/вмикати ферму. Встановлюється драйвер і програма сторожового таймера з офіційного сайту: драйвер, програма. Програму треба поставити у автозагрузку, і налаштувати в ній моніторинг, налаштовати моніторинг інтернету на сайт google.com, а моніторинг процесу на cmd.exe.

Крім того, треба відключити «засинання» системи в настройках електроживлення. Цю настройку найкраще зробити після всього, тому що при установці драйверів відеокарт вона може скидатися. Потрапити в це меню можна так: Windows -> Setting -> Перший пункт меню (рисунок 3.8).

Для збільшення продуктивності відеокарт використовується програма Afterburner, або точніше MSI Afterburner (рисунок 3.9). Для AMD карт потрібна остання Beta-версія.

Дослідження можливостей відеокарти і вихід за їх межі може здатися небезпечним заняттям, проте на ділі все не так страшно. Утиліта MSI Afterburner надає зручний доступ до всіх налаштувань графічної підсистеми комп'ютера.

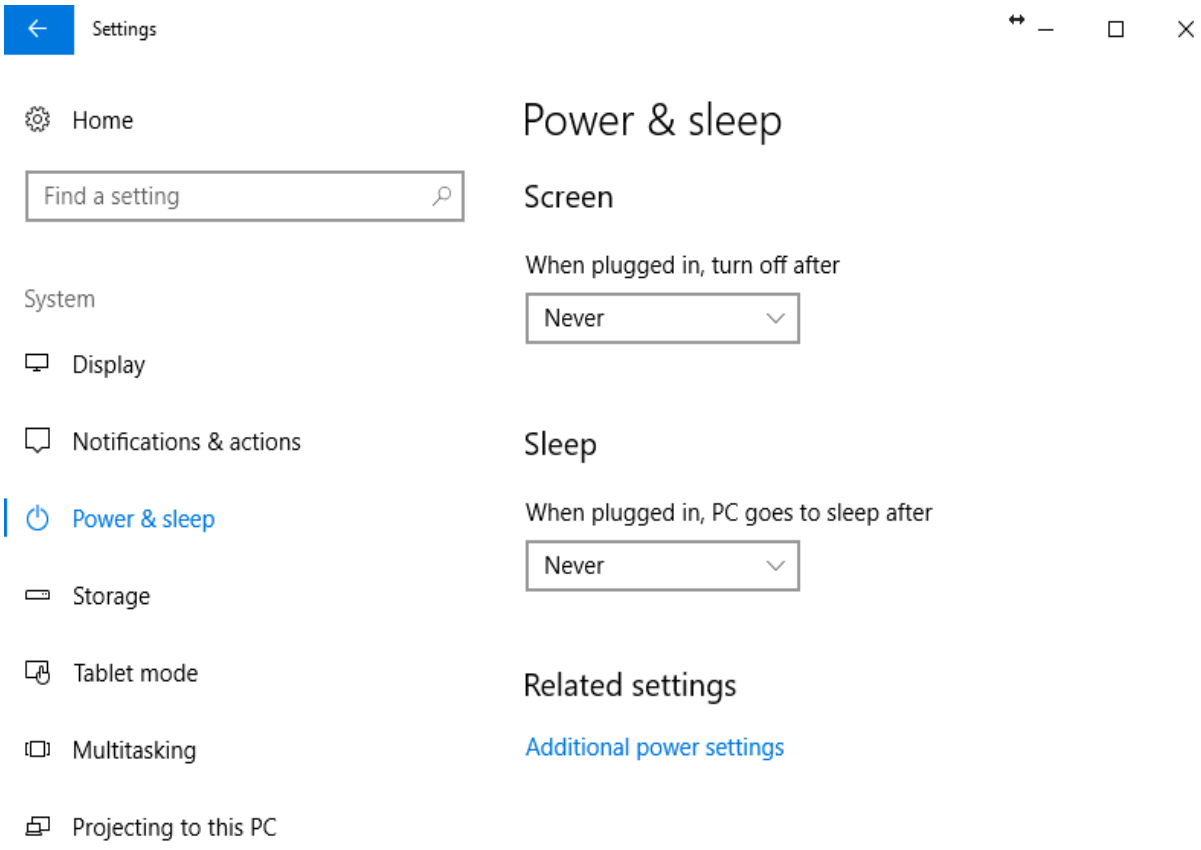

Рисунок 3.8 - Відключення «засинання» системи

Рисунок 3.9 - Програма MSI Afterburner

Керуючи швидкістю обертання вентиляторів р збільшенні частоти і напруги графічного процесора, можна знайти ідеальний баланс між продуктивністю і температурою. Візьміть управління комп'ютером в свої руки і розкрийте весь потенціал своєї відеокарти!

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

Метою техніко – економічного розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки програмно-апаратної підсистеми для добування криптовалют на основі графічних процесорів та прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки. Для проведення даного дослідження необхідно провести ряд розразунків.

4.1 Розрахунок витрат на розробку підсистеми

Витрати на розробку і впровадження апаратного модуля потокового шифрування на основі систем класів лишків (K) включають:

$$K = K_1 + K_2,$$

де K_1 - витрати на розробку апаратного забезпечення грн.;

K_2 - витрати на відлагодження і дослідну експлуатацію підсистеми, грн.

Витрати на розробку апаратних засобів включають:

- витрати на оплату праці розробників ($B_{ОП}$);
- витрати на відрахування у спеціальні державні фонди ($B_ф$);
- витрати на матеріали та комплектуючі ($П_в$);
- накладні витрати (H);
- інші витрати ($I_в$)
- витрати на використання комп’ютерної техніки($B_{КТ}$).

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт у людино-днях та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломант; консультант техніко-економічного розділу (таблиця 4.1).

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

№п/п	Посада виконавців	Місячний оклад, грн.
1	Керівник ДП, викладач	6026
2	Консультант техніко-економічного розділу, доцент	6026
3	Студент	1100

Витрати на оплату праці розробників проекту визначаються за наступною формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} \ , \qquad (4.1)$$

де n_{ij} – чисельність розробників i-ої спеціальності j-го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником i-ої спеціальності j-го тарифного розряду, год;

C_{ij} – годинна ставка працівника i-ої спеціальності j-го тарифного розряду, грн.,

Середньогодинна ставка працівника може бути розрахована за такою формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_i}, \qquad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника i-ої спеціальності j-го тарифного розряду, грн.;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ - місячний фонд робочого часу працівника i-ої спеціальності j-го тарифного розряду, год. (приймаємо 168 год.).

Коефіцієнт h, який визначає розмір додаткової заробітної плати, для керівника та консультанта техніко-економічного розділу дорівнює 0,47.

Результати розрахунку записують до таблиці 4.2.

Таблиця 4.2 - Розрахунок витрат на оплату праці

№ п/п	Посада виконавців	Час розробки, год	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн
1	Керівник ДП, доцент	16	88,6	1417,6
2	Консультант техніко-економічного розділу, доцент	2	88,6	177,2
3	Студент	144	6,55	943,2
Разом				2538

Відрахування на соціальні заходи. Величину відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного

законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати: $B_Ф = \frac{20,5}{100} \cdot 2538 = 520,29$ грн.

Загальна сума витрат на матеріальні ресурси (B_M) визначається за формулою:

$$B_M = \sum_{i=1}^{n} K_i \cdot Ц_i, \quad (4.3)$$

де K_i - витрата *i*-го типу матеріалу, натуральні одиниці вимірювання;

$Ц_i$ - ціна за одиницю *i*-го типу матеріалу, грн.;

i - тип матеріального ресурсу;

n - кількість типів матеріальних ресурсів.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Од. виміру	Факт. витра-чено матері-алів	Ціна за одиницю, грн.	Сума, грн	Транс-портні витрати (10% від суми)	Загальна сума, грн
Arduino UNO	шт	1	412	412	41,2	452.2
Папір (формат А4)	уп	2	80	160	16	176
Ручка кулькова	шт	2	10	20	2	22
Датчик температ. та вологості	шт	1	100	100	10	110
Герконовий датчик	шт	2	35.1	70.2	7	77.2
Датчик руху	шт	1	127	127	12.7	139.7
Датчик відстані	шт	1	88.5	88.5	8,85	96,85
Р а з о м						1073,95

Витрати на використання комп'ютерної техніки ($В_{КТ}$) включають витрати на амортизацію комп'ютерної техніки, витрати на користування програмним забезпеченням, витрати на електроенергію, що споживається

комп'ютером. За даними обчислювального центру ТНЕУ для комп'ютера типу IBM PC/ATX вартість години роботи становить 6 грн. Середній щоденний час роботи на комп'ютері – 2 години. Розрахунок витрат на використання комп'ютерної техніки приведений в таблиці 4.4.

Таблиця 4.4- Розрахунок витрат на використання комп'ютерної техніки

№ п/п	Назва етапів робіт, при виконанні яких використовується комп'ютер	Час використання комп'ютера, год.	Витрати на використання комп'ютера грн.
1	Проведення досліджень та оформлення їх результатів	60	360
2	Оформлення техніко-економічного розділу	8	48
3	Оформлення ДП	12	72
Разом		80	480

Накладні витрати проектних організацій включають три групи видатків: витрати на управління, загальногосподарські витрати, невиробничі витрати. Вони розраховуються за встановленими відсотками до витрат на оплату праці. Середньостатистичний відсоток накладних витрат приймемо 150% від заробітної плати: $H = 1{,}5 \cdot 1860{,}4 = 2790{,}6$ (грн).

Інші витрати є витратами, які не враховані в попередніх статтях. Вони становлять 10% від заробітної плати: $I_B = 1860{,}4 \cdot 0{,}1 = 186{,}04$ (грн).

Витрати на розробку програмного забезпечення складають:

$$K_1 = B_{ОП} + B_Ф + B_M + H + I_B + B_{КТ},$$

$$K_1 = 1860{,}4+381{,}38+1111{,}00+2790{,}6+186{,}04+480{,}00=6809{,}42 \text{ (грн)} .$$

Витрати на відлагодження і дослідну експлуатацію програмного продукту визначаємо за формулою:

$$K_2 = S_{м.г.} \cdot t_{від} \qquad (4.4)$$

де $S_{м.г.}$ - вартість однієї машино-години роботи ПК, грн./год;

$t_{від}$ - комп'ютерний час, витрачений на відлагодження і дослідну експлуатацію створеного програмного продукту, год.

Загальна кількість днів роботи на комп'ютері дорівнює 30 днів. Середній щоденний час роботи на комп'ютері – 2 години. Вартість години роботи комп'ютера дорівнює 6 грн., тому $K_2 = 6 \cdot 60 = 360$ грн.

4.2 Визначення експлуатаційних витрат

Для оцінки економічної ефективності розроблювальної системи моніторингу слід порівняти її з аналогом, тобто існуючим програмним забезпеченням ідентичного функціонального призначення.

Експлуатаційні одноразові витрати по програмному забезпеченню і аналогу включають вартість підготовки даних і вартість роботи комп'ютера (за час дії програми):

$$E_П = E_{1П} + E_{2П},$$

де $E_П$ - одноразові експлуатаційні витрати на ПЗ (аналог), грн.;

$E_{1П}$ - вартість підготовки даних для експлуатації ПЗ (аналогу), грн.;

$E_{2П}$ - вартість роботи комп'ютера для виконання проектного рішення (аналогу), грн.

Річні експлуатаційні витрати $B_{ЕП}$ визначаються за формулою:

$$B_{ЕП} = E_{П} * N_{П},$$

де $N_{П}$ - періодичність експлуатації ПЗ (аналогу), раз/рік.

Вартість підготовки даних для роботи на комп'ютері визначається за формулою:

$$E_{1П} = \sum_{l=1}^{n} n_i t_i c_i ,$$

де i - категорії працівників, які приймають участь у підготовці даних (i=1,2,...n);

n_i - кількість працівників i-ої категорії, осіб.;

t_i - трудомісткість роботи співробітників i-ої категорії по підготовці даних, год.;

c_i - середнього годинна ставка працівника i-ої категорії з врахуванням додаткової заробітної плати, що знаходиться із співвідношення:

$$c_i = \frac{c_i^0 (1+b)}{m},$$

де c_i^0 - основна місячна заробітна плата працівника i-ої категорії, грн.;

b - коефіцієнт, який враховує додаткову заробітну плату (приймемо 0,57);

m - кількість робочих годин у місяці, год.

Для роботи з даними як для проектного рішення так і аналогу потрібен один працівник, основна місячна заробітна плата якого складає: c = 3723 грн. Тоді:

$$c_1 = \frac{3723(1+0,57)}{22*8} = 33,21 \text{грн/год.}$$

Трудомісткість підготовки даних для проектного рішення складає 1 год., для аналога 1,5 год.

Таблиця 4.5 - Розрахунок витрат на підготовку даних та реалізацію проектного рішення на комп'ютері

№	Час роботи співробітників, год.	Середньогодинна заробітна плата, грн./год.	Витрати , грн.
Проектне рішення			
1	1	33,21	33,21
Аналог			
2	1,5	33,21	66,42

Витрати на експлуатацію комп'ютера визначається за формулою:

$$E_{2П} = t * S_{МГ}$$

де t - витрати машинного часу для реалізації рішення (аналогу), год.;

$S_{МГ}$ - вартість однієї години роботи комп'ютера, грн./год.

Далі:

$E_{2П}$ = 1* 6 = 6 грн.; $E_{2А}$=1,5*6 = 9 грн.

$E_{П}$=33,21+6=39,21 грн. ; $E_{А}$=66,42+9 = 75,42 грн.

$B_{ЕП}$= 39,21*252=9880,92 грн. ; $B_{ЕА}$=75,42 *252=19005,84 грн.

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 60–100 % від суми основної та додаткової заробітної плати працівників.

$$H_B = 0{,}7 * B_{ОП}\,, \tag{4.5}$$

де H_B – накладні витрати.

$$H_B=0{,}7*5845{,}11=4091{,}58 \text{ грн.}$$

Результати проведених розрахунків зведемо у таблицю 4.6.

Таблиця 4.6 - Кошторис витрат

№ п/п	Найменування витрат	Сума витрат, грн.
1	Витрати на оплату праці	1860,4
2	Відрахування у спеціальні державні фонди	381,38
3	Витрати на матеріали та комплектуючі	1074,00
4	Накладні витрати на розробку	2790,6
5	Інші витрати	186,04
6	Витрати на відлагодження і дослідну експлуатацію програмного продукту	360
7	Накладні витрати експлуатацію	4091,58
8	Річні експлуатаційні витрати	19005,84
Разом		29770,09

Договірна ціна ($Ц_Д$) для проектних рішень розраховується за формулою:

$$Ц_Д = B_{КС} \cdot \left(1+\frac{p}{100}\right), \tag{4.6}$$

де $B_{КС}$ – кошторисна вартість, грн.;

р - середній рівень рентабельності, % (приймаємо 26% за погодженням з керівником): $Ц_Д$ =29770,09·(1+0,26)=37524,47 грн.

4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень

Економічна ефективність ($E_ф$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_ф = \frac{П}{B_{КС}}\ , \qquad (4.7)$$

де $П$ – прибуток, грн.;

$B_{КС}$ – кошторисна вартість, грн..

$E_ф$=7812,27 грн. / 29786,09 грн. = 0,25.

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($Тр$):

$$T_Р = \frac{1}{E_Р}\ . \qquad (4.8)$$

Тобто: $T_Р$ =1/0,25 = 4р.

Прийнятним вважається термін окупності, близький до 7 років.

Розраховані економічні показники проекту занесемо до таблиці 4.7.

Таблиця 4.7 - Економічні показники розробки

№ п/п	Показник	Значення
1.	Собівартість, грн.	29786,09
2.	Плановий прибуток, грн.	7744,38в
3.	Ціна, грн.	37524,47
4.	Економічна ефективність	0,25
5.	Термін окупності, рік	4

Враховуючи основі економічні показники з таблиці 4.7, можна зробити висновок, що при економічній ефективності 0,25 та терміні окупності 4 роки проводити роботи по впровадженню даного програмного модуля є доцільним та економічно вигідним.

ВИСНОВКИ

1. На основі аналітичного огляду типів криптовалют, способів їх добування та характеристик сучасних графічних процесорів встановлено їх переваги та недоліки, що дозволило обґрунтувати вибір оптимальних механізмів для майнінгу.

2. На основі аналізу технології блокчейну та хеш-функції SHA-256 сформульовано вимоги до програмного та апаратного забезпечення для оптимального добування криптовалют.

3. На основі сформульованих вимог до графічних процесорів здійснено обґрунтування вибору програмного та апаратного забезпечення для побудови програмно-апаратної системи добування криптовалют.

4. На основі вибраного програмного та апаратного забезпечення розглянуто особливості добування криптовалют за допомогою сучасних відеокарт та графічних процесорів.

5. На основі відповідного програмного забезпечення здійснено налаштування програмно-апаратної підсистеми добування крипто валют на основі сучасних графічних процесорів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мащенко П.Л. Технология Блокчейн и ее практическое применение / П.Л. Мащенко, М.О. Пилипенко // Наука, техника, образование. – 2017. – № 32. – С. 61 – 64.

2. Теппер А.С. Биткойн – деньги для всех / А.С. Теппер. – М.: Independent Reserve, 2015. – 34с.

3. Хажиахметова Е.Ш. Криптовалюта - деньги XXI века / Е.Ш. Хажиахметова // Новая наука: от идеи к результату. – 2016. – №11. – С. 177 – 179.

4. Пещеров А.И. Понятие и место криптовалюты в системе денежных средств / А.И. Пещеров // Юридическая мысль. – 2016. – Т.95, №3. – С. 130 – 138.

5. Щербик Е.Е. Феномен криптовалют: опыт системного описания / Е. Е. Щербик. – М.: Концепт. – 2017. – 237 с.

6. Рисс В.И. К вопросу о коллективных валютах или частных деньгах / В.И. Рисс. – М.: Экономика, управление, и право: инновационное решение проблем. – 2017. – С. 21–23.

7. Алексеев Л.К. Криптовалюты. Правила применения / Л.К. Алексеев // Наука и жизнь. – 2018. – № 2. – С. 22–26.

8. Вернер М. Основы кодирования / М. Вернер. – М.: Техносфера, 2004. – 288 с.

9. Баженов Р.И. Информационная безопасность и защита криптовалют / Р.И. Баженов. – Биробиджан: Изд-во ГОУВПО «ДВГСГА», 2011. – 140 с.

10. Josang A. Authentication for humans. / A. Josang, M. Patton, A. Ho // Proceedings of the 9th International Conference on Telecommunication Systems (ICTS2001), 2010. – P. 61–67.

11. Швиденко М.З. Сучасні комп'ютерні технології блокчейну / М.З.Швиденко. – Л.: ННЦ Інститут комп'ютерної економіки, 2017. – 305 с.

12. Романец Ю.В. Все об криптовалюте и функции sha-256 / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин // Наука, техника, образование. – 2017. – № 12. – С. 122–136.

13. Хорев П.Б. Методы и средства защиты информации в компьютерных системах / П.Б. Хорев. – М.: Академия, 2015. – 256 с.

14. Yang J. Biometrics cryptopia./ J. Yang. – NY.: InTech, 2011. – 277 p.

15. Obaidat M. Keystroke Dynamics / M. Obaidat, B. Sadoun. – NY.: KDBA, 2008. – 153 p.

16. Bours P. Continuous authentication using biometric keystroke dynamics/ P. Bours and H. Barghouthi. – In The Norwegian Information Security Conference (NISK), 2009. – 91 p.

17. Горбоконенко В.Д. Кодирование информации функции sha-256 / В.Д. Горбоконенко, В.Е. Шикина. – Ульяновск: УлГТУ, 2006. – 56 с.

18. Цимбал В. П. Теория информации и кодирования / В.П. Цимбал. – К.: Вища школа, 1982. – 304 с.

19. Блейхут Р. А. Теория и практика кодов добычи криптовалют/ Р.А. Блейхут. – М.: Мир, 2013. – 376 с.

20. Лидовский В. В. Теория информации / В.В. Лидовский. – М.: Компания Спутник+, 2014. – 111 с.

21. Кузьмин И.В. Основы теории информации и кодирования блокчейн функций / И.В. Кузьмин, В.А. Кедрус. – К.: Вища школа, 2012. – 238 с.

22. Антонопулос А. М. Освоение Bitcoin: учимся понимать цифровые криптовалюты / А. М Антонопулос. – М.: Техносфера, 2014. – 298 с.

23. Свон М.А. Блокчейн / М.А. Свон. – М.: Олимп - Бизнес, 2017. – 56 с.

24. Frank D. Introduction to 3D game programming with DirectX 9.0 / D. Frank. – Wordware Publishing, Inc, 2003. – 421 p.

25. Gray K. Microsoft DirectX 9 Programmable Graphics Pipeline / K. Gray. – MS.: Press, 2003 – 458 p.

26. Tarditi D. Accelerator: Using Data Parallelism to Program GPUs for General-Purpose Uses / D. Tarditi, S. Puri, J. Oglesby. – NY.: Microsoft Research, 2006. – 115 p.

27. Luebke D. GPGPU: General Purpose Computation On Graphics Hardware / D. Luebke, M. Harris, J. Kruger. – NY.: SIGGRAPH, 2005. – 277 p.

28. Dixon A. Building Bitcoin use in South Florida and beyond / A. Dixon. – Miami: Herald, 2015. – 92 p.

29. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та мережі» / О.М. Березький, Л.О. Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2016. – 65 с.

30. Методичні вказівки до написання техніко-економічного розділу для дипломних проектів на здобуття освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» / І.Р. Паздрій. - Тернопіль: ТНЕУ, 2015.– 36 с.