

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»



Факультет комп'ютерних наук та технологій
Кафедра «Комп'ютерні системи та мережі»

ПИЛИПЕНКО ПАВЛО АНАТОЛІЙОВИЧ
Група КНТ-612м

FPGA СИСТЕМА ДЛЯ ХЕШУВАННЯ БЛОКЧЕЙНУ

АВТОРЕФЕРАТ

магістерської роботи на здобуття освітньо-кваліфікаційного
рівня «магістр» 123 «Комп'ютерна інженерія»
освітньої програми «Спеціалізовані комп'ютерні системи»

2023 р.

Магістерська робота є рукопис.

Робота виконана в Національному університеті «Запорізька політехніка», на кафедрі комп'ютерних систем та мереж

Керівник

кандидат технічних наук, доцент
ГРУШКО Світлана Сергіївна,
Національний університет «Запорізька
політехніка», доцент кафедри
комп'ютерних систем та мереж

**Офіційний
рецензент:**

**СТЕПАНЕНКО Олександр
Олексійович,**
к.т.н., доцент кафедри «Програмні
засоби» НУ «Запорізька політехніка»

Захист відбудеться "20" грудня 2023 р.

Секретар екзаменаційної комісії, старший викладач
кафедри комп'ютерних систем та мереж Куликовська Н.А.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми.

Магістерська робота присвячена розробці FPGA системи для ефективного хешування в контексті блокчейн технологій. У цій роботі підкреслюється значимість блокчейну у сучасному світі, особливо з акцентом на важливість хешування для забезпечення безпеки, конфіденційності та надійності системи.

Основна мета роботи полягає у створенні високоефективної та надійної системи на базі FPGA для хешування блокчейну, яка б забезпечувала безпеку, конфіденційність та цілісність даних у блокчейн мережах. У роботі також проведено аналіз апаратного та програмного забезпечення для реалізації запропонованої системи.

Актуальність цієї роботи полягає у зростаючій потребі високопродуктивних, надійних та безпечних систем хешування у сфері блокчейну. Блокчейн революціонізує багато галузей, надаючи можливість створювати надійні та безпечні системи обліку, що мінімізують необхідність довіряти посередникам. Це особливо важливо у фінансовому секторі, де блокчейн став основою для створення криптовалют та нових способів фінансового взаємодії.

Технологія блокчейну також знайшла застосування у багатьох інших галузях, включаючи логістику, юридичну сферу та інтернет речей, завдяки своїй здатності вирішувати проблеми прозорості та трасованості. Вона дозволяє детально відстежувати всі транзакції та події в реальному часі, що підвищує рівень довіри споживачів.

Хешування в блокчейну є фундаментальним елементом, який забезпечує надійну безпеку, конфіденційність та цілісність системи. Воно використовується для створення унікальних ідентифікаторів для блоків даних та для захисту конфіденційності даних. Хешування також грає ключову роль у процесі майнінгу, забезпечуючи безпеку блокчейн мережі.

Розвиток FPGA-технологій для хешування в блокчейну відкриває нові можливості для покращення ефективності та безпеки цих систем. Застосування FPGA дозволяє адаптувати системи під конкретні потреби блокчейн мережі, забезпечуючи при цьому високу продуктивність та енергоефективність.

Таким чином, магістерська робота актуальна та значуща у контексті сучасних тенденцій в блокчейн технологіях. Вона спрямована на вирішення реальних проблем у галузі криптографії та безпеки даних, що є важливими аспектами в сучасному цифровому світі.

Мета і завдання дослідження. Мета магістерської роботи полягає у створенні FPGA системи для покращення процесів хешування у контексті блокчейн технологій.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

- провести аналіз існуючих методів та технологій хешування, які використовуються в блокчейн мережах;
- розробити і впровадити нову архітектури FPGA системи, спеціально призначеної для хешування в блокчейн;
- провести тестування та оцінку ефективності розробленої системи з точки зору її продуктивності.

Об’єкт дослідження – блокчейн технології та процеси хешування в них.

Предмет дослідження – FPGA системи як засіб для оптимізації процесів хешування в блокчейн мережах.

Методи дослідження базуються на теоретичному аналізі літератури та існуючих технологій; експериментальний розробці та тестуванні FPGA системи, аналізі ефективності та порівняльній оцінці з іншими методами.

Наукова новизна отриманих результатів:

- розробка інноваційної FPGA системи, яка покращує ефективність процесу хешування в блокчейн технологіях;

– вдосконалення архітектури та методології хешування для забезпечення вищої продуктивності та безпеки.

Практичне значення отриманих результатів:

Реалізація алгоритму хешування на FPGA дозволяє заощадити апаратні ресурси і підвищити швидкість виконання операцій завдяки використанню паралельної обробки даних.

Структура та обсяг роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатку. Основна частина містить 96 сторінок, 18 рисунків і 2 таблиці, список використаних джерел з 44 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У першому розділі розглядаються ключові аспекти та виклики, пов'язані з технологією блокчейну та хешуванням. Блокчейн, характеризуючись інноваційністю та надійністю, впроваджує нові методи зберігання, обміну та обробки даних у безпечних і децентралізованих системах. Децентралізована природа блокчейну сприяє рівним правам учасників мережі та підвищує стійкість системи до збоїв і кібератак. Криптографія в блокчейні забезпечує безпеку і прозорість, а смарт-контракти автоматизують угоди, зменшуючи потребу в посередниках. Технологія гарантує трасованість та прозорість операцій, підвищуючи довіру у фінансових та інших сферах. Механізми консенсусу, такі як Proof of Work та Proof of Stake, гарантують надійність і єдність мережі.

У контексті хешування, різні апаратні платформи, як-от GPU, ASIC і FPGA, мають унікальні переваги та обмеження. GPU ефективні для паралельних обчислень, але вимогливі до ресурсів. ASIC, спеціалізовані на хешуванні та криптографічних обчисленнях, забезпечують високу продуктивність, але мають обмежену функціональність. FPGA, будучи програмованими та гнучкими, поєднують

переваги GPU та ASIC, адаптуючись до конкретних вимог блокчейна.

Детально розглядаються різні криптографічні хеш-алгоритми, кожен з яких має свої унікальні характеристики та застосування у контексті блокчейну та криптовалют. SHA-256, Кеццак (SHA-3), RIPEMD-160, Blake2, Scrypt, Ethash, X11 та Poseidon, кожен з яких вносить важливий вклад у безпеку, ефективність та гнучкість в світі цифрових технологій та криптовалют.

У другому розділі У другому розділі розглядаються технічні характеристики та можливості AMD Varium™ C1100, а також ключові програмні ресурси, які використовуються у роботі з цією розробницькою картою. AMD Varium™ C1100, заснована на архітектурі AMD UltraScale+, є спеціалізованою картою для блокчейну, призначеною для прискорення обчислювально інтенсивних задач, таких як валідація транзакцій і хеш-розрахунки. Ця карта вирізняється високою щільністю інтеграції, енергоефективністю та можливістю паралельного виконання обчислювальних задач. Програмувати Varium C1100 можна за допомогою середовища розробки Vitis™ від AMD, що робить її ідеальною для застосувань у сфері блокчейну, зокрема для криптомайнінгу.

Далі обговорюються три ключових програми: Ubuntu 20.04 (Focal Fossa), AMD Vitis Unified Software Platform та AMD-Xilinx Run Time (XRT) для Ubuntu 20.04. Ubuntu 20.04 - це стабільна та безпечна операційна система на базі Linux з тривалою підтримкою (LTS), оновленим користувацьким інтерфейсом та покращеною підтримкою апаратного забезпечення. AMD Vitis, інтегроване середовище розробки, полегшує розробку програмного та апаратного забезпечення, зокрема для FPGA. Це середовище дозволяє створювати ядра на C/C++ або RTL і інтегрується з хост-програмами через API XRT. AMD-Xilinx Run Time спеціально розроблене для

підтримки FPGA та інших апаратних пристроїв AMD Xilinx, включаючи драйвери та API для оптимізації продуктивності FPGA.

У цілому, другий розділ надає інформацію про технічні можливості AMD Varium™ C1100 та взаємодію між ключовими програмами, що забезпечують ефективне використання цієї картки в блокчейн застосуваннях, зокрема у сферах, де важливими є енергоефективність та екологічність.

У третьому розділі зазначається, що для ефективної FPGA системи для хешування блокчейну, необхідно врахувати наступні вимоги:

- інтерфейсування коду;
- потокова обробка даних;
- паралелізм;
- оптимізація займаної площі;
- балансування.

Також зазначається, що для забезпечення найкращої роботи системи необхідно врахувати:

–траєкторії переміщення даних, тобто необхідно зрозуміти, яким шляхом дані рухаються через мікросхему FPGA та як швидко це відбувається;

–взаємодію даних - важливо впевнитися, що зміни в даних не будуть негативно впливати на їх власний стан або стан інших даних у системі;

–використання ресурсів, тобто потрібно оцінити, скільки апаратних ресурсів необхідно для реалізації запланованого дизайну.

Акцентується увага на тому, що розробка на FPGA відбувається не тільки на рівні програмного забезпечення, але й включає фізичне створення схем на чіпі.

В цьому розділі описується процес створення проекту з кількома рівнями. Хост-додаток, який запускається на процесорі, буде надсилати та отримувати дані від ядра, тоді

як ядро-додаток, яке виконується на FPGA, забезпечуватиме прискорену обробку даних, а також здійснюватиме зв'язок між проектами.

Зазначається, що архітектура системи для хешування блокчейну на базі FPGA повинна бути спеціально розроблена для відповідності вимогам Filecoin - інноваційної платформи для розподіленого зберігання даних. Filecoin використовує кооперативний підхід до зберігання даних, нагороджуючи провайдерів криптовалютою FIL за використання невикористаного сховища. Система базується на IPFS, що дозволяє ефективно зберігати та доступ до файлів.

Основна увага приділяється алгоритму хешування Poseidon, використовуваному у Filecoin для формування Меркле дерев. Швидка обробка нових файлів цим алгоритмом є критичною для ефективності інтеграції даних у блокчейн, впливаючи на економічну вигоду та зниження витрат на апаратне забезпечення та енергію.

В даному проєкті Filecoin активно використовує GPU для прискорення обробки даних. Задача полягає в перенесенні та адаптації коду Poseidon OpenCL для оптимізації виконання на FPGA, вимагаючи розуміння математичної основи алгоритму та його адаптації під обмежені ресурси FPGA.

Обробка даних у системі включає розділення блоків на сегменти та послідовне проходження через раунди обчислень, включаючи квінтичні S-бокси та множення на константи. Це сприяє формуванню вузлів для Меркле дерева, ключового елемента для верифікації та безпеки в блокчейні.

В цьому розділі обговорюється синтез кернела, процес, що дозволяє перетворити високорівневий код програми, написаний на мовах C або C++, у апаратний опис на рівні RTL для FPGA. Це забезпечує прискорення центральної частини алгоритму або програми. Запуск C-синтезу (Емуляція-HW) перетворює високорівневий код на RTL,

дозволяючи його емуляцію на апаратному рівні. Після синтезу, Vitis HLS надає різні типи звітів, які дозволяють перевірити швидкість таймінгу годинника, затримку, інтервал ітерацій та використання ресурсів.

Процес оптимізації ядра включає повернення до коду для поліпшення таймінгу, зменшення затримки та оптимізації використання ресурсів, заснований на інформації з отриманих звітів. Використовуються рекомендації вкладки "Guidance" для подальшої оптимізації. Оптимізація ядра є ітеративним процесом, який може вимагати декількох циклів редагування, синтезу та аналізу.

Перша оптимізація включає застосування dataflow для покращення потокової обробки даних, забезпечуючи передачу даних між функціями як потік і уникнення затримок. Важливим елементом є використання `ap_uint<256>` для оптимізації обробки даних і врахування обмежень хоста.

Синтез кернела включає аналіз і оптимізацію шляхів логіки, зменшення використання ресурсів, як DSP, і використання `pragma HLS pipeline` для підвищення ефективності обробки даних. Оптимізація заснована на зменшенні числа шляхів логіки, об'єднанні функцій та ефективному використанні конвеєрної обробки. Наприкінці, Vitis HLS допомагає ідентифікувати можливі точки для покращення продуктивності і зменшення використання ресурсів.

Застосована конвеєрна обробка дозволяє значне покращення продуктивності. Якби FPGA працював з частотою 300 МГц, необхідно було б обчислювати 300 мільйонів раундів за секунду; з 65 раундами на кожну порцію даних, можна було б обробляти приблизно 4,6 мільйона повних хешів за секунду. Але в цьому випадку порушено баланс між паралелізмом та займаною площею, використовується 182% доступних DSP в FPGA.

Щоб зменшити використання ресурсів, необхідно було збільшити інтервали ітерації і потенційно обмежити використання певних ресурсів у логіці.

Побічним ефектом є подовження інтервалу ітерації до 12. З цією оптимізацією можливо обробляти новий раунд кожні 12 тактів годинника. З 65 раундами на кожну порцію даних, ми завершуємо хеш кожні 780 тактів. Якщо FPGA працює з частотою 300 МГц, то можна обробляти 384 615 хешів за секунду. До оптимізації можна було обробляти 5405 хешів за секунду.

ВИСНОВКИ

Результати, отримані в магістерській роботі, є рішенням практичної задачі підвищення ефективності алгоритмів хешування блокчейну.

Отримано такі теоретичні та практичні результати:

1. Розроблена FPGA система для хешування використовується для створення унікальних ідентифікаторів блоків даних у ланцюзі блоків блокчейну. Це забезпечує цілісність та непорушність блокчейну, оскільки кожен блок має свій унікальний хеш-код, що визначає його місце в ланцюгу;

2. Виконано оптимізацію хешування за допомогою FPGA системи, яка може підвищити ефективність майнінгу, знижуючи час та енергетичні витрати на виконання цього процесу. Хешування грає важливу роль у процесі майнінгу блокчейну, де комп'ютери в мережі конкурують за право додавання нових блоків до ланцюга. Для цього їм необхідно розв'язати складну математичну задачу, що базується на хеш-коді попереднього блоку. Цей процес, відомий як "доказ роботи", вимагає значної обчислювальної потужності і робить маніпуляцію з блоками практично неможливою.

3. Забезпечено безпеку та цілісність даних - розроблена система сприяє підвищенню безпеки та цілісності даних у блокчейн мережах. Ефективне хешування допомагає запобігати несанкціонованому доступу та маніпуляціям з даними, забезпечуючи надійне зберігання та передачу інформації.

Отже, результати магістерської роботи мають важливе практичне значення у сфері блокчейн технологій, сприяючи підвищенню ефективності, безпеки та цілісності даних в цих мережах.