МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

01.03.02 Прикладная математика и информатика
(код и наименование направления подготовки / специальности)

Компьютерные технологии и математическое моделирование
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(БАКАЛАВРСКАЯ РАБОТА)

на тему «Исследование алгоритмов майнинга криптовалют»

Обучающийся А.О. Скворцов
(Инициалы Фамилия) (личная подпись)

Руководитель д.т.н., доцент, С.В. Мкртычев
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант к.п.н., доцент, Т.С. Якушева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Тема выпускной квалификационной работы – «Исследование алгоритмов майнинга криптовалют».

Помимо конфигураций и вычислительной мощности используемых для майнинга компьютеров одним из критериев выбора конкретной программы майнинга является эффективность используемого в ней алгоритма майнинга.

Исследование и особенности практического применения алгоритмов майининга представляет актуальность и научно-практический интерес.

Объектом исследования бакалаврской работы является майнинг криптовалют.

Предметом исследования бакалаврской работы являются алгоритмы майнинга криптовалют.

Цель бакалаврской работы – исследование и реализация алгоритмов майнинга криптовалют.

Методы исследования – методы и алгоритмы майнинга криптовалют, технологии реализации алгоритмов на языках высокого уровня.

Практическая значимость бакалаврской работы заключается в разработке и тестировании программы, реализующей эффективные алгоритмы майнинга криптовалют.

Результаты бакалаврской работы представляют научно-практический интерес и могут быть рекомендованы для анализа и программной реализации методов и алгоритмов майнинга криптовалют.

Бакалаврская работа состоит из 41 страницы текста, 10 рисунков, 2 таблиц и 21 источника.

Abstract

The title of the graduation work is: «Research of cryptocurrency mining algorithms».

In addition to the configurations and computing power used for mining computers, one of the criteria for choosing a particular mining program is the efficiency of the mining algorithm used in it.

The study and features of the practical application of mining algorithms is of relevance and scientific and practical interest.

The object of study of the bachelor's work is the mining of cryptocurrencies.

The subject of research of the bachelor's work is the mining algorithms of crypto-currencies.

The purpose of the bachelor's work is the study and implementation of cryptocurrency mining algorithms.

The research methods include methods and algorithms of cryptocurrency mining, technologies for implementing algorithms in high-level languages.

The practical significance of the bachelor's work lies in the development and testing of a program that implements effective cryptocurrency mining algorithms.

The results of the bachelor's work are of scientific and practical interest and can be recommended for the analysis and software implementation of methods and algorithms for cryptocurrency mining.

The bachelor's thesis consists of 41 pages of text, 10 figures, 2 tables and 21 literature sources.

Оглавление

Введение 5

Глава 1 Постановка задачи исследования и анализ методов консенсуса в блокчейне 7

1.1 Постановка задачи исследования 7

1.2 Методы консенсуса в блокчейне 8

Глава 2 Обзор и анализ алгоритмов майнинга криптовалют 17

2.1 Алгоритм SHA-256 17

2.2 Алгоритм Ethash 21

2.3 Алгоритм Scrypt 24

2.4 Алгоритм CryptoNight 27

Глава 3 Программная реализация и тетсирование алгоритмов майнинга криптовалют 31

Заключение 37

Список используемой литературы и используемых источников 39

Введение

В последнее время в России на разных уровнях власти активно рассматривается вопрос о регулировании криптовалюты.

Так, в феврале 2022 г. правительство России утвердило концепцию оборота цифровых валют, акцент в которой сделан на защиту прав рядовых инвесторов.

В документе отмечается, «что целью регулирования концепции является интеграция механизма оборота цифровых валют в финансовую систему и обеспечение контроля за денежными потоками в контуре кредитных организаций» [9].

Ключевая роль в регулировании криптовалюты отводится майнингу криптовалют.

В настоящее время разработано много различных программ майнинга криптовалют.

Помимо конфигураций и вычислительной мощности используемых для майнинга компьютеров одним из критериев выбора конкретной программы является эффективность используемого в ней алгоритма майнинга.

Исследование и особенности практического применения алгоритмов майининга представляет актуальность и научно-практический интерес.

Объектом исследования бакалаврской работы является майнинг криптовалют.

Предметом исследования бакалаврской работы являются алгоритмы майнинга криптовалют.

Цель бакалаврской работы – исследование и реализация алгоритмов майнинга криптовалют.

Для достижения данной цели необходимо выполнить следующие задачи:

– выполнить постановку задачи исследования и проанализировать методы консенсуса блокчейна;

– проанализировать алгоритмы майнинга криптовалют;
– разработать и протестировать программу, реализующую алгоритмы майнинга криптовалют.

Методы исследования – методы и алгоритмы майнинга криптовалют, технологии реализации алгоритмов на языках высокого уровня.

Практическая значимость бакалаврской работы заключается в разработке и тестировании программы, реализующей эффективные алгоритмы майнинга криптовалют.

Данная работа состоит из введения, трех глав, заключения и списка используемой литературы.

Первая главе работы посвящена постановке задачи исследования и анализу методов консенсуса блокчейна.

Вторая глава работы посвящена обзору и анализу алгоритмов майнинга криптовалют.

В третьей главе рассматривается программная реализация и тестирование алгоритмов майнинга криптовалют.

В заключении описываются результаты выполнения выпускной квалификационной работы.

Бакалаврская работа состоит из 41 страницы текста, 10 рисунков, 2 таблиц и 21 источника.

Глава 1 Постановка задачи исследования и анализ методов консенсуса в блокчейне

1.1 Постановка задачи исследования

Криптовалюта — это цифровая или виртуальная валюта, защищенная криптографией, что делает практически невозможным ее подделку или двойную трату [6].

Многие криптовалюты (например, биткоин) представляют собой децентрализованные сети, основанные на технологии блокчейна – распределенной бухгалтерской книге, управляемой разрозненной сетью компьютеров.

Блокчейн – это децентрализованная, распределенная и общедоступная цифровая бухгалтерская книга, которая используется для записи транзакций на многих компьютерах, поэтому запись не может быть изменена задним числом без изменения последующих блоков и сговора сети [15].

Каждый блок содержит три элемента:

- криптографический хэш для предыдущего блока;
- отметка времени;
- данные транзакции.

Майнинг криптовалюты – это процесс, посредством которого новая криптовалюта вводятся в обращение.

Это также способ, которым сеть подтверждает новые транзакции, и является важным компонентом обслуживания и развития реестра блокчейна.

Майнинг выполняется с использованием сложного оборудования, которое решает чрезвычайно сложную вычислительную математическую задачу с помощью алгоритмов майнинга криптовалют [16].

Схема процесса облачного майнинга представлена на рисунке 1.

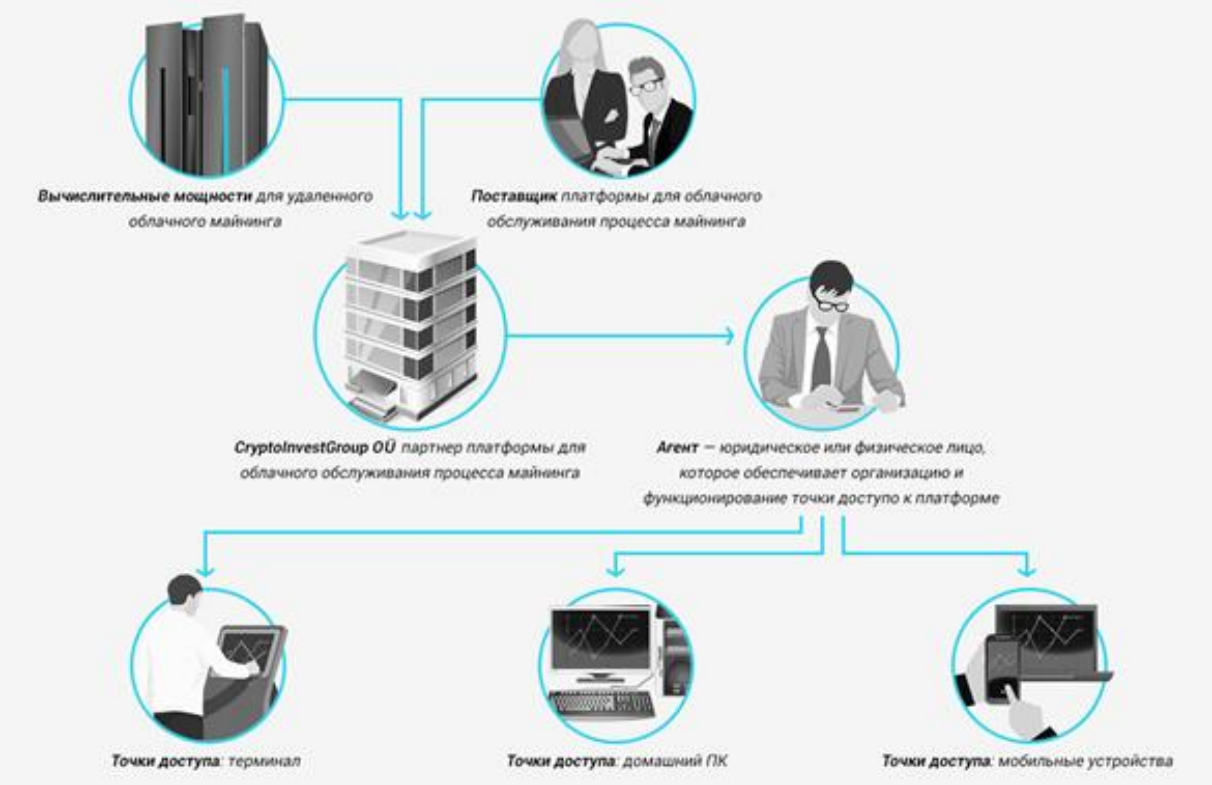

Рисунок 1 – Схема процесса облачного майнинга

Алгоритмы майнинга криптовалют или алгоритмы хэширования – это набор специфических криптографических механизмов и правил, которые шифруют цифровую валюту.

Майнеры при помощи специального оборудования расшифровывают алгоритм конкретной криптовалюты – этот процесс заключается в поиске хэша.

Задача настоящего исследования заключается в математическом описании и анализе алгоритмов майнинга криптовалют.

1.2 Методы консенсуса в блокчейне

В основе алгоритмов майнинга криптовалют лежат методы консенсуса блокчейна [7].

Блокчейн – это технология децентрализованного хранения и

распределенного внесения записей о транзакциях, основанная на криптографических методах защиты информации, позволяющая исключить посредника.

Метод консенсуса блокчейна – это способ, благодаря которому децентрализованные ноды сети достигают согласия (или консенсуса) о текущем состоянии данных во всех блоках.

Под нодой понимается любой компьютер, подключенный к блокчейну, который проверяет и подтверждают транзакции, а также хранит копию блокчейна.

Методы и созданные на их основе алгоритмы консенсуса гарантируют соблюдение правил протокола и достоверность всех транзакций. Иными словами, они отвечает за то, чтобы все ноды сети были согласны с добавлением в нее нового блока [5].

Рассмотрим основные методы консенсуса.

1.2.1 Метод Proof-of-Work

Proof-of-Work (доказательство выполнения работы, PoW) – алгоритм консенсуса, который впервые был представлен в сети первой криптовалюты Bitcoin.

Концепция PoW основана на том, что майнеры могут добавлять новые блоки транзакций в блокчейн. Чтобы подтвердить транзакцию, майнеры должны решить криптографическую головоломку, также известную как хэш-головоломка.

Рассмотрим математическую модель PoW.

Пусть PoW – это математическая задача, целью которой является создание связи между двумя блоками [17].

Эта ссылка будет реализована в заголовке второго блока. Тот, кто пытается разработать PoW, называется майнером.

Рассмотрим два блока, обозначенных B^{prev} и B, и число, называемое битами и обозначаемое b. b измеряет, насколько сложно доказательство

работы: из b можно напрямую вычислить целевое число.

Эта цель представляет собой 64-значное шестнадцатеричное число с несколькими цифрами 0 вместо символов, например:

0000000000000000021047526c065745de75af 6dcd473556dced2bc

Предположим, что известен хэш предыдущего блока, $H(\mathrm{B}^{\mathrm{prev}})$.

Определим хэш данного блока.

Решение PoW для блока B, также известное как майнинг блока B, сводится к нахождению одноразового кода nonce, такого, что (1):

$$H(H(B^{\mathrm{prev}}) \oplus R^{\mathrm{H}}(B) \oplus \mathrm{timestamp}(t) \oplus b \oplus \mathrm{nonce}) \leq \mathrm{target}, \qquad (1)$$

где $\oplus$ – операция конкатенации;

timestamp(t) – текущее время с точностью до секунд.

Так как H является хэш-функцией, единственная возможность найти подходящий значение nonce — это жестко попытаться увеличить значение nonce во время движения t.

Мы предполагаем, что в момент времени t^0 мы находим значение nonce^0, которое является решением PoW.

Хэш $H(B)$ блока B определяется следующим образом (2):

$$H(H(B^{\mathrm{prev}}) \oplus R^{\mathrm{H}}(B) \oplus \mathrm{timestamp}(t^0) \oplus b \oplus \mathrm{nonce}^0) \leq \mathrm{target} \qquad (2)$$

Поскольку хэш блока определяется рекурсивно в соответствии с описанной выше процедурой (предполагается, что $H(B^{\mathrm{prev}})$ уже известно), нам нужна инициализация: если B – первый блок, то предыдущего блока нет, поэтому $H(B^{\mathrm{prev}})$ – простая условность.

Блок-схема классического алгоритма PoW показана на рисунке 2 [20].

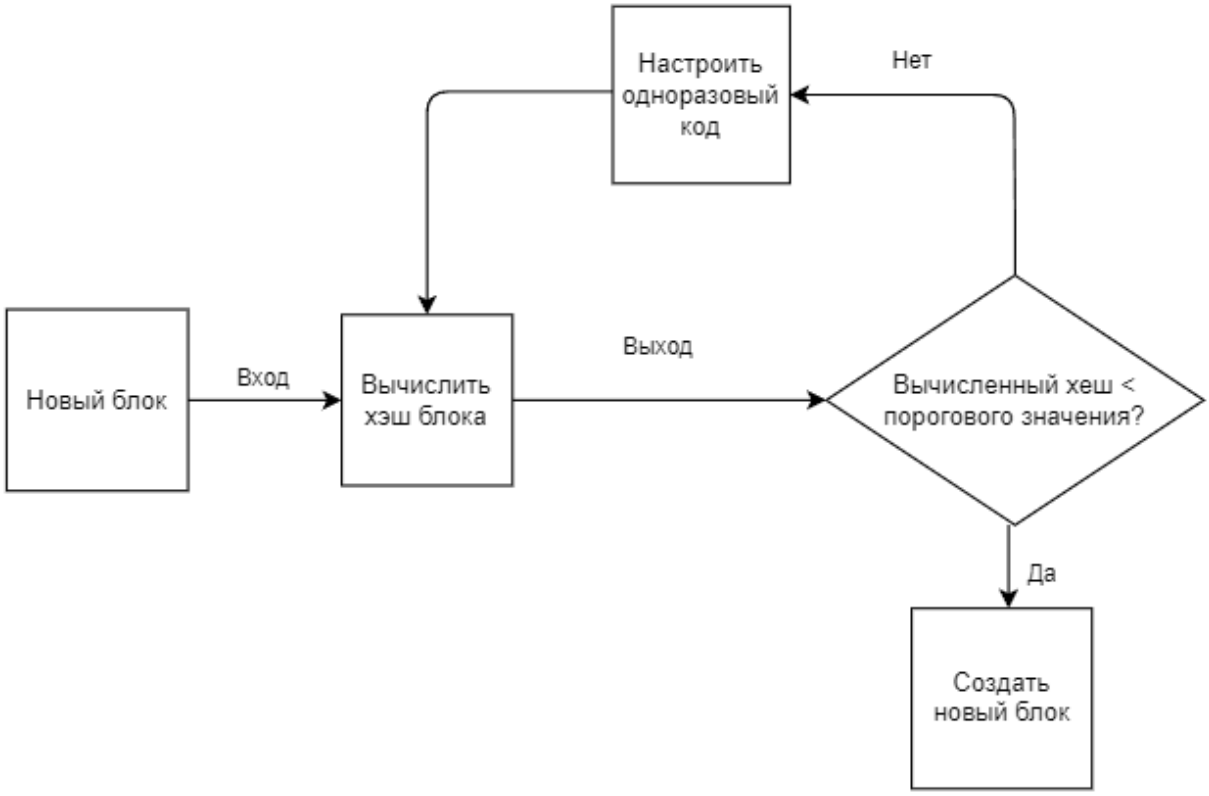

Рисунок 2 – Блок-схема классического алгоритма PoW

Преимущества метода PoW [12]:

– обеспечение надежного механизма для достижения консенсуса и предотвращения злоупотреблений и неправомерного использования. Следует напомнить, что консенсус лежит в основе технологии блокчейн и ее конкретных приложений, включая криптовалюты, а также ее преимуществ, таких как безопасность, доверие и легитимность, а также децентрализация;
– следует отметить, что блокчейн – это децентрализованная или распределенная база данных, которая представляет собой реестр транзакций. Одноранговая сеть участников поддерживает базу данных путем достижения консенсуса или согласования таких вещей, как порядок транзакций и остатки на счетах;
– по сути PoW – это система аутентификации транзакций без необходимости участия третьей стороны, а также предотвращения

несанкционированного доступа отдельных лиц или организаций к базе данных. Этот механизм затрудняет изменение любого аспекта реестра транзакций, тем самым обеспечивая подлинность и отслеживаемость каждой транзакции;

– зависимость от вычислительных возможностей. Хотя теоретически человеческий фактор может повлиять на блокчейн, для этого потребуется затратить вычислительные мощности, которые непрактичны и неэкономичны до такой степени, что затраты значительно перевешивают выгоды.

Недостатки метода PoW:

– самый большой недостаток доказательства работы заключается в вычислительных возможностях, необходимых для решения математических задач при аутентификации транзакций в блокчейне. Следует обратить внимание, что это также один из самых больших недостатков блокчейна, причина серьезной критики криптовалют и основная причина негативного воздействия блокчейнов на основе PoW на окружающую среду;
– для участия в сети блокчейнов, использующей PoW в качестве механизма консенсуса, майнер должен иметь мощный компьютер, оснащенный передовым оборудованием. Масштабирование операции означает покупку и настройку более дорогих компьютеров;
– стоимость не ограничивается вышеупомянутыми покупками. Мощные компьютеры по своей природе потребляют много энергии. Кроме того, этим машинам требуется эффективная система управления теплом или система охлаждения, чтобы оставаться в рабочем состоянии и предотвращать перегрев, а также связанные с этим повреждения аппаратных компонентов из-за внутреннего накопления тепла;
– та же энергоемкость является и причиной более конкретных недостатков PoW. Например, из-за затрат, связанных с запуском и

обслуживанием мощных компьютерных систем, блокчейны на основе PoW имеют ограничения по масштабируемости. Кроме того, связанные с этим затраты также не позволяют ряду лиц и организаций участвовать в конкретной сети блокчейнов. Следовательно, в то время как технология блокчейна основана на концепции децентрализации посредством участия общественности, стоимость служит ключевым барьером для участия широкой общественности, тем самым создавая некоторое подобие централизации.

Недостатки метода PoW в совокупности представляют собой основную причину, по которой некоторые блокчейн-платформы используют альтернативные механизмы консенсуса, например, Proof-of-Stake.

1.2.2 Метод Proof-of-Stake

Алгоритм Proof-of-Stake (доказательство владения долей, PoS) решает проблему высокого энергопотребления при добыче биткойнов. Для добавления новых транзакционных блоков в PoS каждый майнер тратит часть своих монет в качестве доли в монетах системы.

Идея PoS заключается в решении проблемы PoW, связанной с большими тратами электроэнергии. Вместо вычислительных мощностей участников, имеет значение количество криптовалюты, находящейся у них на счету.

Так, вместо использования большого количества электроэнергии для решения задачи PoW, у участника PoS ограничен процент возможных проверок транзакций. Ограничение соответствует количеству криптовалюты, находящейся на счету у участника.

Рассмотрим математическое описание алгоритма PoS на примере системы Peercoin.

Участники сети Peercoin имеют возможность создать блок исходя из следующего условия (3) [13]:

$$H(B^{prev}Data, time^{InSeconds}, txout_A) \leq d_0 * coins(txout_A) * time^{weight}(txout_A), (3)$$

где $time^{InSeconds}$ – текущее время, в данном неравенстве ограничивает попытки хеширования и блокирует создание следующего блока;

$txout_A$ – результат транзакции;

$coins(txout_A)$ – количество неизрасходованной криптовалюты транзакции;

$time^{weight}$ – время, прошедшее с момента включения в блок результата транзакции $txout_A$;

$B^{prev}Data$ – данные предыдущего блока. Участник, владеющий значительной частью всей криптовалюты системы, имеет возможность генерировать значительную часть блоков, так как вероятность генерации блока пропорциональна количеству монет, находящихся у него на счету. Поэтому, время от времени, заинтересованная сторона имеет возможность генерировать цепочки последовательных блоков;

d_0 – постоянная, которая корректируется так, что блоки генерируются в среднем каждые 10 минут.

Блок-схема классического алгоритма PoS показана на рисунке 3.

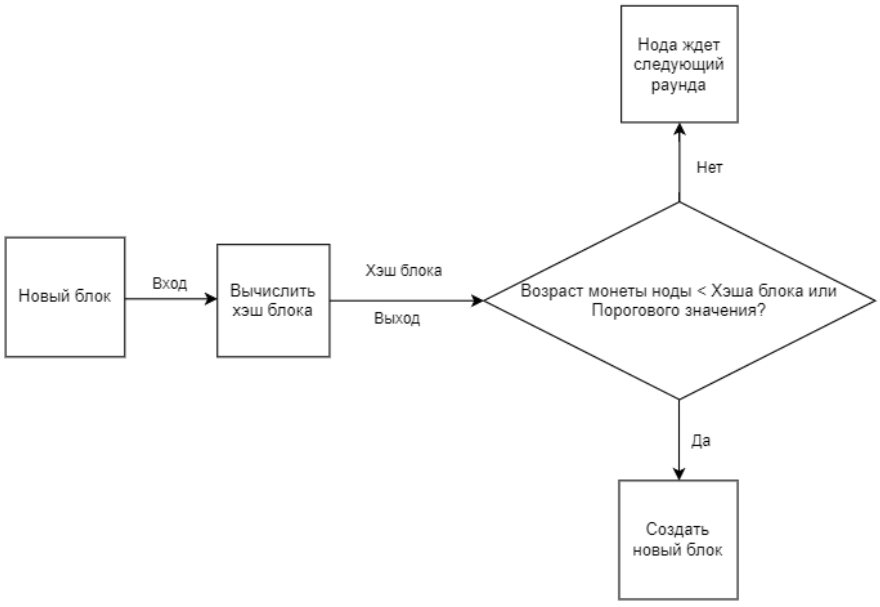

Рисунок 3 – Блок-схема классического алгоритма PoS

Принимая во внимание проблемы с PoW, можно выделить следующие конкретные преимущества метода PoS [11]:

– PoS более энергоэффективен, поскольку не требует затрат вычислительных ресурсов, а отдельные лица могут участвовать в вовлеченной одноранговой сети без необходимости покупки и настройка дорогих мощных компьютеров и систем охлаждения;
– PoS делает блокчейн безопасным, стимулируя надлежащую проверку и препятствуя ненадлежащей проверке. Как уже упоминалось, валидаторы получают часть комиссии за транзакцию и теряют долю, если одобряют мошеннические транзакции;
– по сравнению с PoW, который по своей природе медленнее, когда дело доходит до обработки транзакций из-за требований к вычислительным ресурсам, тем самым поднимая проблемы масштабируемости, блокчейн-платформа, основанная на PoS, более масштабируема, потому что она более децентрализована и позволяет участвовать большему количеству людей и групп.

Основными недостатками метода PoS являются ограничение доступности и подверженность хакерским атакам [19].

Для сравнения методов консенсуса блокчейна используем таблицу 1.

Таблица 1 – Сравнение методов консенсуса блокчейна

Критерий	PoS	PoW
Как получить вознаграждение	Купить монеты и хранить на балансе	Использовать вычислительные мощности ПК
Какое оборудование используется	Не нужно	Процессор, видеокарта, специализированные ASIC
Какие расходы несет майнер	На инвестиции в монету	На сборку фермы и поддержание ее

		работоспособности

Продолжение таблицы 1

Критерий	PoS	PoW
Уязвимость к атаке 51% и централизация	Есть проблема централизации. Все пользователи стремятся получить больший доход, собрав в одних руках максимум активов	Чтобы контролировать сеть, нужно не 51% токенов, а вычислительных мощностей

Таким образом, основными недостатками метода PoS являются ограничение доступности и подверженность хакерским атакам.

Поэтому более распространены алгоритмы метода PoW.

Выводы по главе 1

Первая глава посвящена постановке задачи на исследование, обзору и анализу методов консенсуса блокчейна.

Результаты проделанной работы позволили сделать следующие выводы:

- в основе алгоритмов майнинга криптовалют лежат методы консенсуса блокчейна;
- главным преимуществом метода PoW является обеспечение надежного механизма для достижения консенсуса и предотвращения злоупотреблений и неправомерного использования. Главным недостатком – высокая энергоемкость;
- главным преимуществом метода PoS является его энергетическая эффективность.

Основными недостатками метода PoS являются ограничение доступности и подверженность хакерским атакам.

Поэтому более распространены алгоритмы метода PoW.

Глава 2 Обзор и анализ алгоритмов майнинга криптовалют

Рассмотрим свойства популярных алгоритмов майнинга криптовалют.

2.1 Алгоритм SHA-256

Алгоритм SHA (Secure Hash Algorithm 2)-256 является разновидностью SHA-2, который был создан Агентством национальной безопасности в 2001 году как преемник SHA-1.

SHA-256 — это запатентованная криптографическая хэш-функция, которая выводит значение длиной 256 бит.

Основные характеристики алгоритма:

- длина сообщения: длина открытого текста не должна превышать 264 бита. Размер должен быть в области сравнения, чтобы дайджест был как можно более случайным;
- длина дайджеста. Длина хэш-дайджеста должна составлять 256 бит в алгоритме SHA-256, 512 бит в SHA-512 и т. д. Большие дайджесты обычно предполагают значительно больше вычислений за счет скорости и места;
- необратимость: по замыслу все хэш-функции, такие как SHA-256, необратимы.

Алгоритм SHA-256 состоит из следующих шагов [14]:

Шаг 1. Добавление заполняющих битов.

Добавляет к сообщению несколько дополнительных битов, так что его длина была ровно на 64 бита меньше числа, кратного 512 (4):

$$M + P + 64 = n \times 512, \quad (4)$$

где M – длина исходного сообщения;

P – добавленные биты.

Биты, которые мы добавляем к сообщению, должны начинаться с «1», а следующие биты должны быть «0».

Шаг 2. Добавление битов длины.

Теперь, когда мы добавили биты заполнения к исходному сообщению, мы можем добавить биты длины, которые эквивалентны 64 битам, ко всему сообщению, чтобы сделать его кратным 512.

Шаг 3. Инициализация буферов.

Необходимо инициализировать значения по умолчанию для восьми буферов, которые будут использоваться в итерациях следующим образом:

a = 0x6a09e667

b = 0xbb67ae85

c = 0x3c6ef372

d = 0xa54ff53a

e = 0x510e527f

f = 0x9b05688c

g = 0x1f83d9ab

h = 0x5be0cd19

Шаг 4. Функция сжатия.

Основная часть алгоритма хеширования заключается в этом шаге.

Весь блок сообщения, который у нас равен «n x 512» бит, делится на «n» фрагментов по 512 бит, и каждый из этих 512 бит затем проходит через 64 итерации, а полученный выход является входом для следующей итерации.

На рисунке 4 показаны 64 цикла операций, выполняемых над 512-битным сообщением.

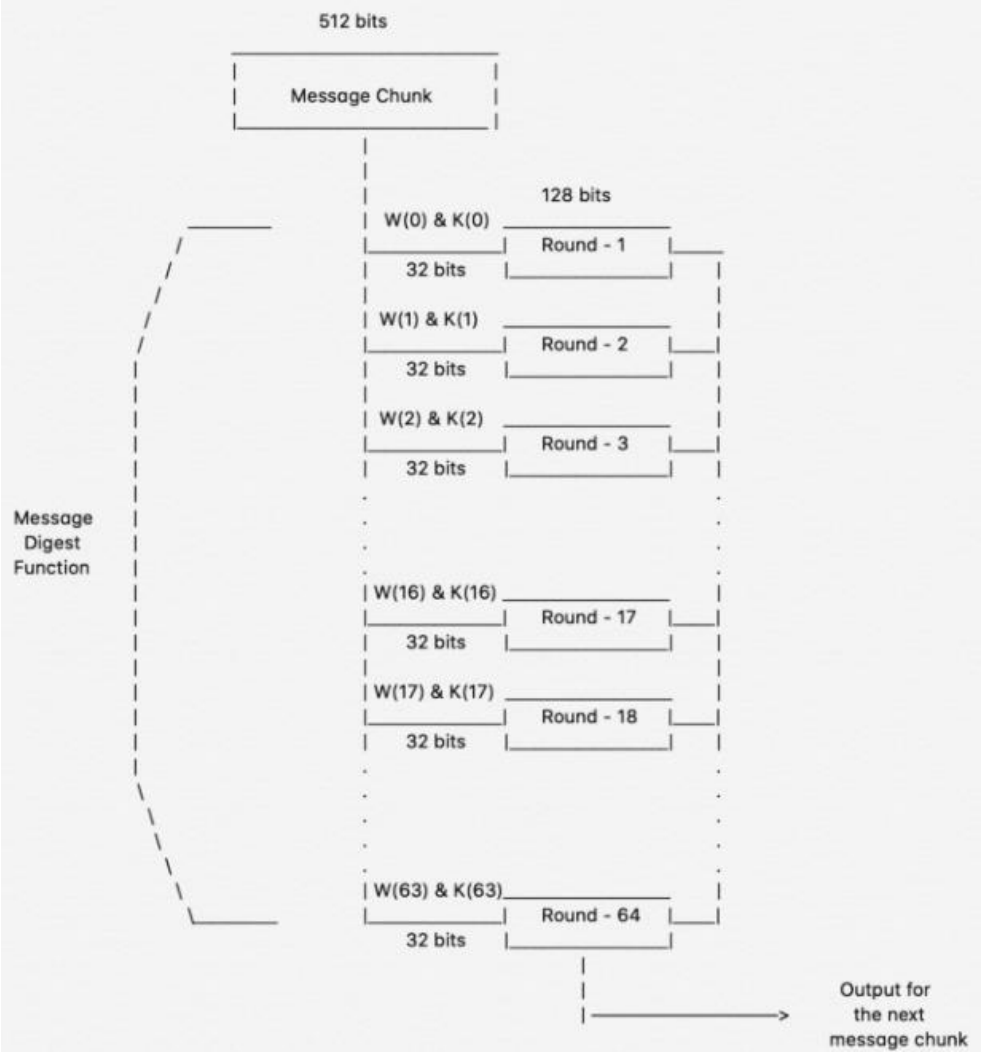

Рисунок 4 – Схема функции сжатия

Отметим, что два входа, которые мы отправляем, это W(i) и K(i).

Для первых 16 итераций мы далее разбиваем 512-битное сообщение на 16 частей, каждая из которых по 32 бита, но после этого нам нужно вычислить значение для W(i) на каждом шаге по формуле (5):

$$W(i) = W^{i-16} + \sigma^0 + W^{i-7} + \sigma^1 \quad (5)$$

где σ^0 – $(W^{i-15}\ ROTR^7(x))$ XOR $(W^{i-15}\ ROTR^{18}(x))$ XOR $(W^{i-15}\ SHR^3(x))$;

σ^1 – (W^{i-2} ROTR^{17} (x)) XOR (W^{i-2} ROTR^{19} (x)) XOR (W^{i-2} SHR^{10} (x));

ROTR^n(x) – циклическая правая ротация «x» на «n» бит;

SHR^n(x) – циклический сдвиг вправо 'x' на 'n' бит.

Структурная схема одной итерации показана на рисунке 5.

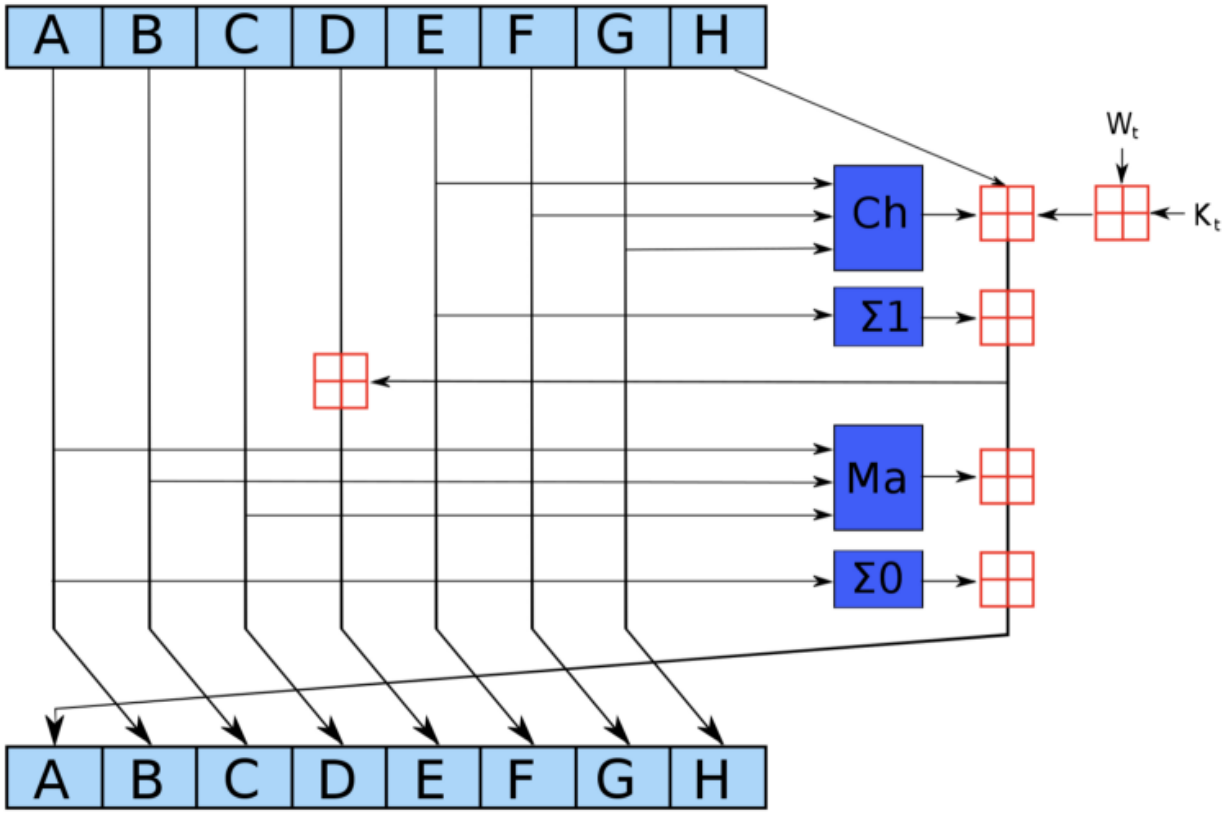

Рисунок 5 – Структурная схема одной итерации

Шаг 5. Вывод результата.

Выход каждой итерации действует как вход для следующей итерации.

Этот процесс продолжается до тех пор, пока не останутся последние биты сообщения и результат последней итерации для n-й части блока сообщения не даст нам результат, т.е. хэш для всего сообщения.

Длина вывода составляет 256 бит.

Алгоритм SCH-256 используется для майнинга таких криптовалют, как Bitcoin, Mastercoin, MazaCoin, Namecoin и др.

Следует отметить, что в майнинге биткоина SCH-256 используется как PoW-алгоритм.

SHA-256 – самый распространённый PoW-алгоритм майнинга. Он зарекомендовал себя как устойчивый к взломам и эффективный алгоритм как для задач майнинга, так и для других целей.

Главным недостатком SHA-256 считается его подконтрольность майнерам: обладатели самых больших вычислительных мощностей получают большую часть криптовалюты, что исключает один из основополагающих принципов криптовалют – децентрализованность [1].

Версия SHA-256+ ECDSA алгоритма основана на методе PoS.

2.2 Алгоритм Ethash

Алгоритм майнинга Ethash — это алгоритм, который выполняет операцию майнинга для кримптовалюты Ethereum.

Это алгоритм высокого качества, который использует очень сложные компьютерные технологии, чтобы гарантировать максимально возможную безопасность.

Алгоритм Ethash основан на алгоритме Dagger-Hashimoto и состоит из следующих шагов [21]:

Шаг 1. Сгенерировать начальное число. Расчетное начальное число создается с использованием заголовков блоков до момента начала майнинга.

Шаг 2. Создать кэш. Полученное начальное число используется для расчета и создания псевдослучайного кэша объемом 16 МБ.

Шаг 3. Создать набор данных. Кэш используется для создания набора данных размером более 4 ГБ (DAG-файл). Этот набор данных является полупостоянным и обновляется каждые 30 тысяч блоков. Таким образом, DAG-файл меняется для каждого «сезона добычи».

Шаг 4. После создания DAG-файла начинается майнинг. Этот процесс берет случайные значения из DAG-файла и объединяет их, используя данные, предоставленные сетью, и транзакции, которые необходимо проверить.

Шаг 5. Выполняется проверка с помощью процесса, который регенерирует определенные части набора данных с использованием кэш-памяти, что ускоряет этот процесс.

Блок-схема алгоритма Ethash показана на рисунке 6.

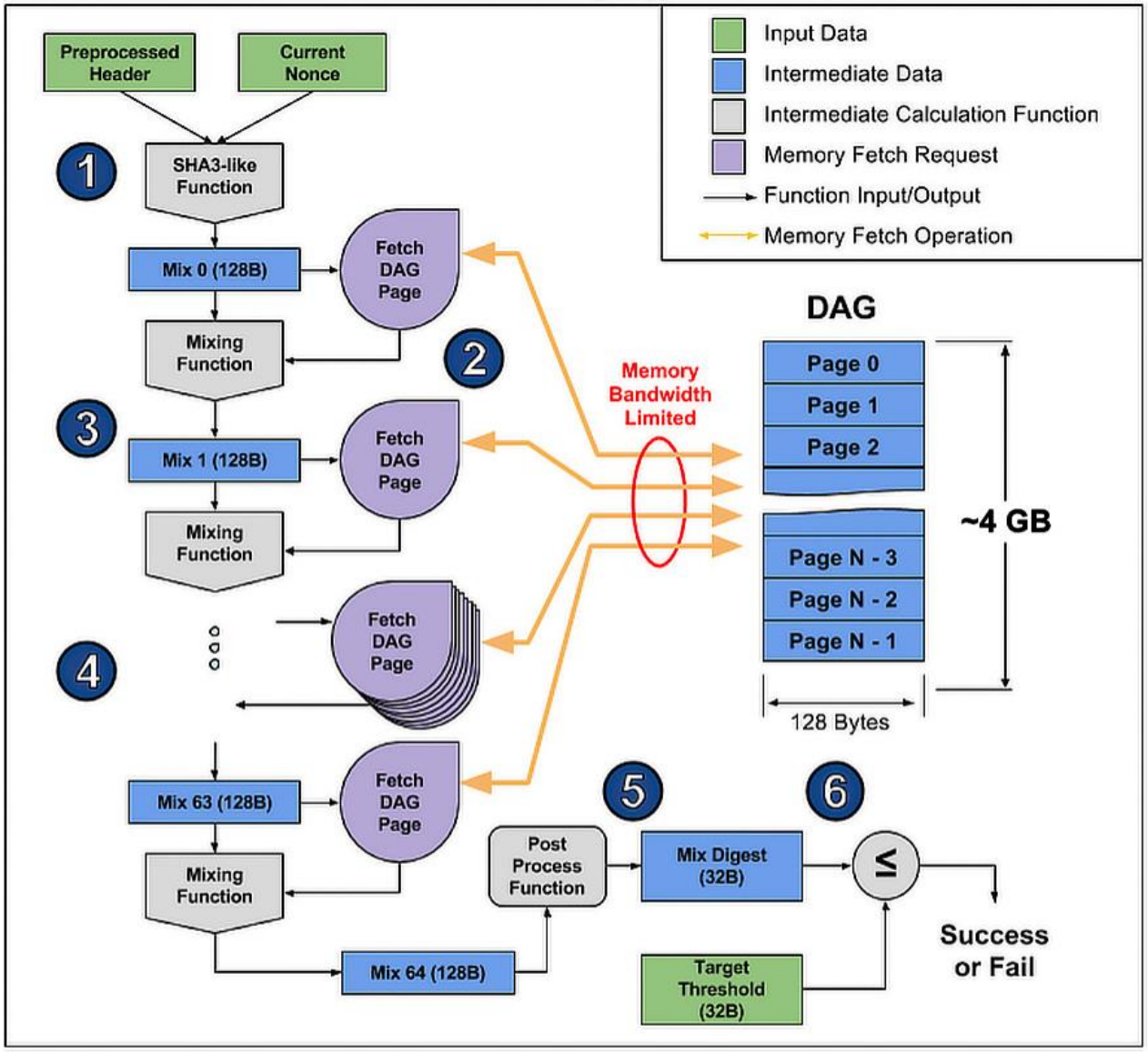

Рисунок 6 – Блок-схема алгоритма Ethash

На протяжении всего процесса используются функции Keccak-256 и Keccak-512, алгоритм, на основе которого был разработан стандарт SHA-3.

Эти обновления обеспечивают решение проблем устранения уязвимостей, оптимизации и модификации, чтобы сделать работу майнинга удобной для пользователя.

Основные характеристики алгоритма:

- сильно зависит от операций в оперативной памяти, потребляя большое количество пропускной способности. Операции, необходимые для создания DAG-файла и рабочего кэша Ethash, сильно зависят от этих функций;
- совместим с GPU. Следует напомнить, что современные видеокарты или графические процессоры обладают огромной мощностью. На самом деле движущаяся графика, как в современных играх, требует огромных объемов памяти и непревзойденной параллельной обработки. Это дополнительное преимущество, если запускается майнинг с использованием Ethash, потому что можно использовать память графического процессора, чтобы иметь в памяти весь DAG-файл вместе с кэшем и выполнять все вычисления в высокоскоростном рабочем пространстве. В результате есть возможность добывать криптовалюту гораздо быстрее;
- предлагает отличные возможности проверки для тонких клиентов. Имея около 16 МБ ОЗУ, можно создать тонкий клиент, способный очень легко и быстро проверять транзакции. В дополнение к этому тонкий клиент может быть запущен и выполнять процесс проверки всего за 30 секунд.

Преимущества Ethash:

- простота реализации и безопасность;
- высокое быстродействие. Использование DAG-файла в памяти, кэша и функции Keccak делают этот алгоритм эффективным при

производстве блоков. Благодаря этому Ethereum может рассчитывать на регулируемое время производства в соответствии с потребностями сети, всегда обеспечивая баланс между безопасностью и масштабируемостью.

Главным недостаток Ethash являются высокие требования к оперативной памяти, что очень затрудняет майнинг на недорогом оборудовании. Так, для эффективной работы требуется иметь видеокарты с большим объемом ОЗУ и желательно на основе микропроцессоров AMD.

Алгоритм Ethash используется для майнинга таких криптовалют, как Ethereum, Krypton, Shif и др.

2.3 Алгоритм Scrypt

Алгоритм Scrypt используется во многих криптовалютах в качестве алгоритма проверки работоспособности. Алгоритм начали использоваться в качестве инструмента PoW в сети Litecoin с сентября 2012 года.

Scrypt основан на известном методе повышенного извлечения ключей через жесткие последовательные функции памяти.

Scrypt хэширует с использованием ключа, ряда ключевых точек, отмеченных в алгоритме хэширования и добавляющих много шума.

Шум в Scrypt на самом деле представляет собой серию случайных чисел, которые генерируются алгоритмом и сохраняются в памяти. Цель этих чисел – замаскировать ключевые данные алгоритма, чтобы усложнить работу по взлому указанных хэшей.

С помощью этой операции Scrypt решает две задачи:

- хэширует пароли, чтобы злоумышленник, получивший доступ к файлу паролей, не сразу получил содержащиеся в нем пароли;
- создание криптографических ключей, которые будут использоваться для шифрования или аутентификации данных.

Блок-схема алгоритма Scrypt изображена на рисунке 7.

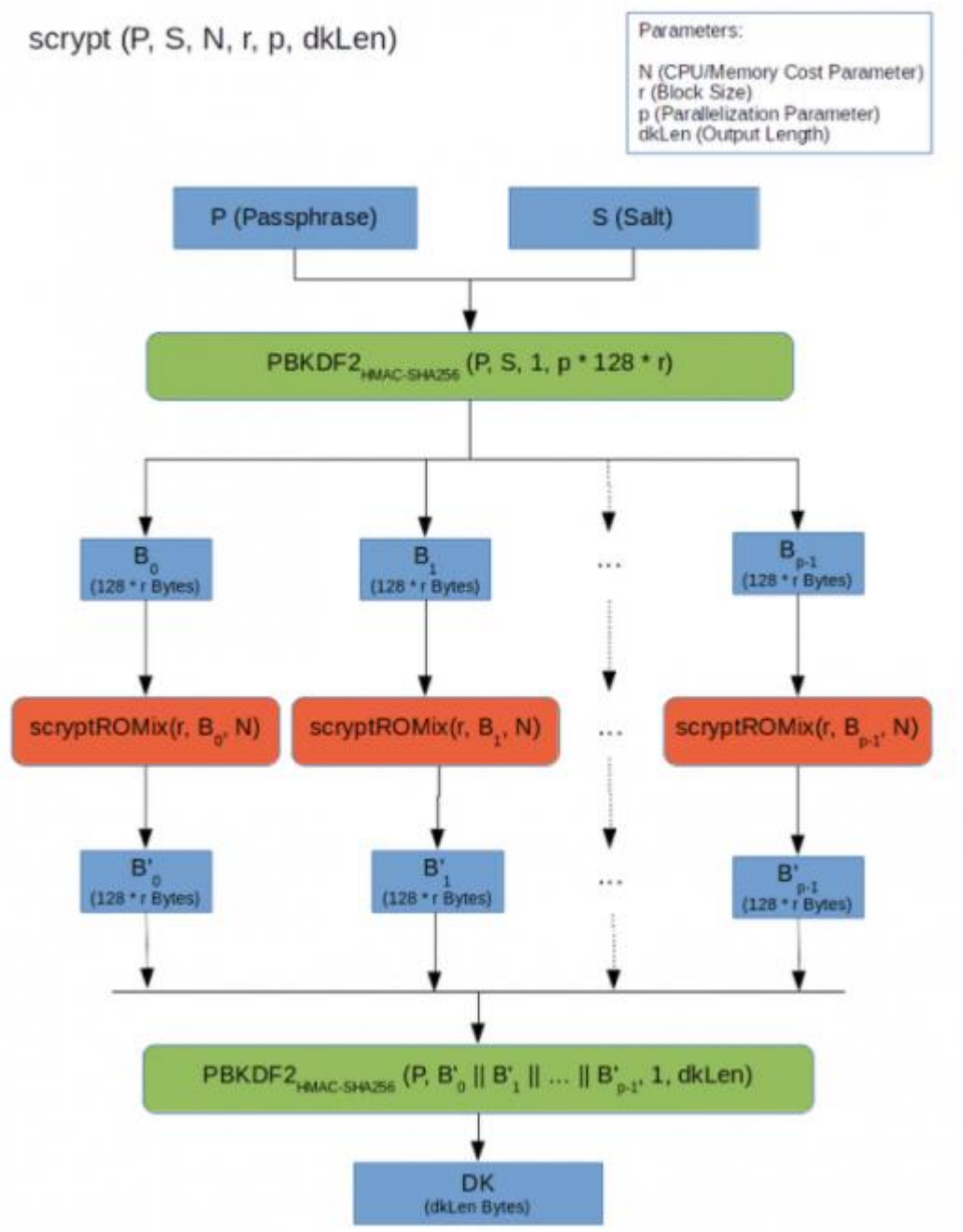

Рисунок 7 – Блок-схема алгоритма Scrypt

Алгоритм Scrypt имеет следующие параметры [18]:

– параметр N, который определяет стоимость с точки зрения ресурсов, задействованных в выполнении алгоритма;
– параметр p, определяющий распараллеливание;
– параметр r, определяющий размер блоков и, следовательно, используемую память.

Есть и другие параметры, связанные с хэш-функцией и длиной выходного хэша.

Scrypt имеет два начальных параметра, а именно сообщение Passphrase (P), которое нужно зашифровать, и Salt (S), случайную строку, используемую для добавления энтропии и защиты системы от атак на основе предварительно вычисленных таблиц Rainbow.

Они представляют собой не что иное, как ассоциативные таблицы, которые предлагают компромисс времени и памяти для восстановления чистых ключей шифрования из хешированных ключей.

Затем данные передаются в специальную функцию получения ключа на основе пароля 2 – PBKDF2. Эта функция, используя параметры, ранее продиктованные алгоритмом, еще больше снижает уязвимость зашифрованного ключа к атакам грубой силы.

PBKDF2 генерирует число p из 128*r байтовых блоков [B0…Bp-1].

В этот момент с помощью функции ROMix, в данном случае последовательного жесткого типа памяти, блоки смешиваются, даже параллельно.

Выходные смешанные блоки затем передаются как параметр Salt другой функции PBKDF2, которая генерирует ключ нужной длины.

Преимущества алгоритма Scrypt:

- высокое быстродействие. Алгоритм Scrypt проще и быстрее алгоритма SHA-256. Скорость хэширования Scrypt измеряется в килохэшах в секунду или тысячах хэш-вычислений в секунду;
- относительно высокий уровень безопасности. Алгоритм устроен так, что программист может увеличивать или уменьшать различные переменные, влияющие на уровень безопасности. Но в дополнение к этому алгоритм обладает высокой устойчивостью к атакам грубой силы, что делает его идеальным для распределенных систем, где важна безопасность.

К основным недостаткам алгоритма относят сложность и дороговизну реализации.

Алгоритм Ethash используется для майнинга таких криптовалют, как Dogecoin, Litecoin, Potcoin, Starcoin и др.

2.4 Алгоритм CryptoNight

CryptoNight используется для майнинга монет с протоколом CryptoNote, включая Monero. Это функция, строго привязанная к памяти (жесткий хэш памяти), в данном случае к кэш-памяти третьего уровня процессоров, поскольку она ориентирована на задержку.

CryptoNight ryptoNight работает на основе ряда свойств, которые делают его очень удобным для майнинга на GPU.

Перечислим эти свойства:

- использование собственного алгоритма шифрования AES. Процессоры с возможностью аппаратного ускорения для вычислений AES могут значительно выиграть от этого факта и обладают превосходным потенциалом майнинга;
- использование безопасных хеш-функций, таких как Keccak и Blake-256;
- использование набора 64-битных быстрых множителей (чистые 64-битные архитектуры ЦП очень эффективны);
- алгоритм можно использовать на процессорах типа VLIW от 128 до 512 бит, где алгоритм может использовать преимущества параллельных пулов майнинга за счет повышения производительности;
- интенсивное использование кэшей процессора. Алгоритм CryptoNight регулирует использование кеша, чтобы получить от него максимальную отдачу. На самом деле, чем больше кэш-памяти процессора, тем выше его производительность.

Схема работы алгоритма показана на рисунке 8.

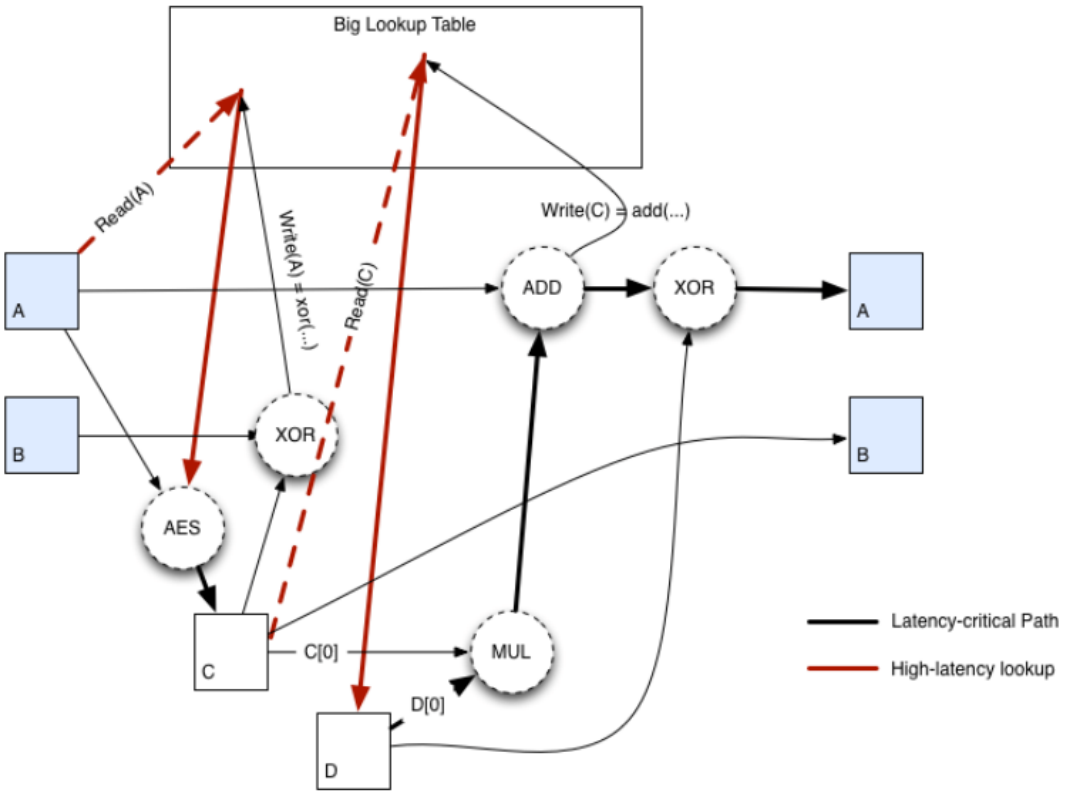

Рисунок 8 – Схема работы алгоритма CryptoNight

Ввод хэша инициализируется с использованием Keccak (функция SHA3) с параметрами B, равными 1600, и C, равными 512.

Окончательные параметры Keccak, т. е. байты от 0 до 31, интерпретируются как ключ AES 256 и расширяются в 10 круглые ключи.

Байты между 64-м и 191-м извлекаются в восемь блоков по 16 байт каждый, которые затем шифруются.

Затем все размещается в блокноте, который имеет размер, близкий к 2 МБ, как описано ранее.

Как только это будет сделано, между первыми 63 байтами Keccak накладывается операция XOR, чтобы инициализировать ограничения A и B, каждое из 32 байтов.

Эти переменные и их обработка используются для наложения цикла

непрерывных чтений и записей (524288 раз) в блокнот, так что алгоритм строго привязан к задержке памяти.

Наконец, вычисляется окончательная хеш-последовательность ранее полученных данных.

Преимущества алгоритма CryptoNight:

- широкие возможности для настройки. Такие данные, как цель майнинга и сложность, можно регулировать между блоками, не создавая угрозы для безопасности сети;
- ориентация на центральный процессор (ЦП). Это делает майнинг с использованием ASIC сложным и дорогостоящим;
- безопасность на криптоуровне. Использование AES-256 и привязка методов шифрования и хэш-функций определенным образом гарантируют, что всегда будет обеспечиваться высокий уровень безопасности;
- энергетическая эффективность;
- для обеспечиваемого уровня безопасности размер результатов криптографического теста CryptoNight невелик. Это позволяет максимизировать количество транзакций внутри блоков.

Основные недостатки:

- CryptoNight чрезвычайно сложен и труден для аудита. По этой причине разработчики имеют большую кривую сложности для проверки возможных ошибок в этом алгоритме;
- использование определенных инструкций ЦП, таких как AES, может привести к внешним атакам на алгоритм. Существует вероятность использования уязвимостей внутри процессора, которые могут нарушить безопасность алгоритма.

Алгоритм CryptoNight используется для майнинга таких криптовалют, как Bytecoin и Monero.

Для удобства сравнения и оценки характеристик алгоритмов майнинга

криптовалют используем таблицу 2 [2].

Таблица 2 – Характеристики алгоритмов майнинга криптовалют

Алгоритм	Метод консенсуса	Криптовалюты	Преимущества	Недостатки
SHA-256	PoW, PoS	Bitcoin, Steemit, DigiByte, Peercoin и др.	Широкая распространенность	Подконтрольность майнерам
Ethash	PoW	Ethereum, Expanse, Ubiq, SOILcoin, Bowhead и др.	Простота реализации и безопасность	Высокие требования к ОЗУ
Scrypt	PoW	Litecoin, Dogecoin, Syscoin, BelaCoin, и др	Высокое быстродействие	Сложность и дороговизна реализации
CryptoNight	PoW	Monero, ByteCoin, Dashcoin, CryptoNoteCoin и др.	Высокая безопасность и энергетическая эффективность	Сложен и труден для аудита

Как показывает анализ, правильный подбор алгоритма является одним из ключевых условий обеспечения эффективного майнинга криптовалют [4].

Выводы по главе 2

Вторая глава посвящена обзору и анализу алгоритмов майнинга криптовалют.

Результаты проделанной работы позволили сделать следующие выводы:

Эффективность майнинга зависит от таких параметров, как мощность и производительности оборудования, вида и типа майнинга, а также от корректности подбора алгоритмов.

Глава 3 Программная реализация и тестирование алгоритмов майнинга криптовалют

Рассмотрим примеры программной реализации самого популярного алгоритма хэширования SHA-256.

В языке PHP имеется встроенная функция hash, которая генерирует хэш-код [10].

Описание:

hash(

string $algo,

string $data,

bool $binary = **false**,

array $options = []

): string

Параметры:

– algo – имя выбранного алгоритма хеширования (например, "sha256");

– data – сообщение для хеширования;

– options – опции для различных алгоритмов хеширования.

Функция hash возвращает строку хеш-кода в шестнадцатеричной кодировке в нижнем регистре.

На рисунке 9 показан пример реализации данной функции.

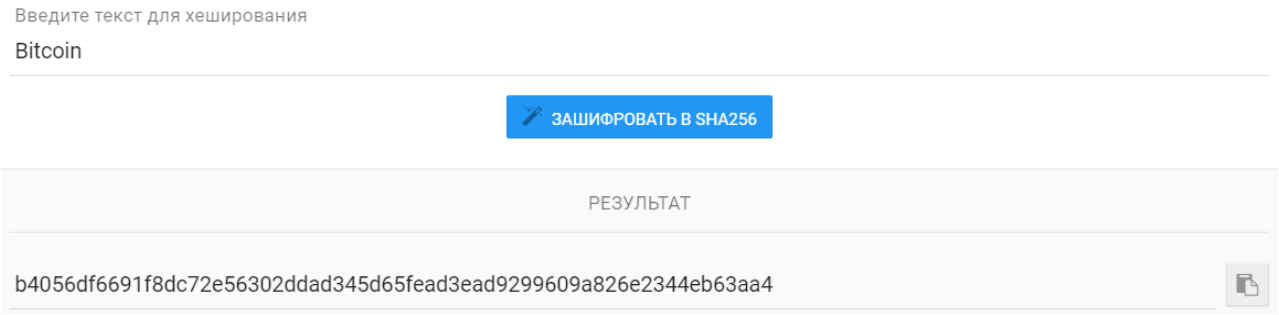

Рисунок 9 – Онлайн-генератор хеш-кода (SHA-256)

Как было отмечено выше, в алгоритме CryptoNight для шифрования используется алгоритм AES-256.

AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США.

Использование данного алгоритма существенно повышает безопасность шифрования.

Рассмотрим пример реализации подписи данных SHA + AES на платформе «1С: Предприятие 8» [3].

Общий алгоритм создания подписи данных состоит следующих шагов.

Шаг 1. На входе получаем подписываемые данные в виде строки или двоичных данных.

Шаг 2. Получаем из них хэш SHA-256.

Шаг 3. Далее получаем случайное число, 64 бит. Заполняем им выходной буфер (повторами).

Шаг 4. Далее получаем отметку времени и XOR-им с серединкой выходного буфера.

Шаг 5. Делаем операцию XOR хэша с концом выходного буфера.

Шаг 6. Шифруем всё секретным ключом.

В листинге 1 представлен код 1С8 функции подписи SHA + AES на языке 1С8 [8].

Листинг 1 – Код функции подписи SHA + AES

```
Функция Подписать(Данные, Ключ256) Экспорт
// Получаем хэш SHA-256
Хеш = Новый ХешированиеДанных(ХешФункция.SHA256);
Хеш.Добавить(Данные);
SHA256 = Хеш.ХешСумма;
```

```
ЧтениеХэш      = Новый ЧтениеДанных(SHA256);
БуферХэш       = ЧтениеХэш.ПрочитатьВБуферДвоичныхДанных();
ЧтениеХэш.Закрыть();
ВремяСозданияАлгоритма = 63739655820000; // Дата("20201030115700") - Дата("00010101") UTC
Сейчас = ТекущаяУниверсальнаяДатаВМиллисекундах() - ВремяСозданияАлгоритма;
ГенераторСлучайныхЧисел = Новый ГенераторСлучайныхЧисел(Сейчас % 4294967295);
Ч1 = ГенераторСлучайныхЧисел.СлучайноеЧисло();
Ч2 = ГенераторСлучайныхЧисел.СлучайноеЧисло();
Буфер = Новый БуферДвоичныхДанных(48);
Буфер.ЗаписатьЦелое32(0, Ч1);
Буфер.ЗаписатьЦелое32(4, Ч2);
Буфер_R = Буфер.Скопировать();
Буфер.ЗаписатьЦелое64(8, Сейчас);
Буфер.Записать(16, БуферХэш, 32);
Буфер.ЗаписатьПобитовоеИсключительноеИли(8, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(16, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(24, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(32, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(40, Буфер_R, 8);
Поток= Новый ПотокВПамяти(Буфер);
ДанныеПодписи= Поток.ЗакрытьИПолучитьДвоичныеДанные();
Возврат ЗашифроватьAES(ДанныеПодписи, Ключ256);
КонецФункции
// Подписать
```

Обработка тестировалась на платформе 1С:Предприятие 8.3.

Сеанс выполнялся на ядре с тактовой частотой 1,58 ГГц (максимальная

3,3 ГГц).

За каждую итерацию выполняется подпись и проверка подписи - то есть два действия. В качестве подписываемых данных генерится строка, кратная одному блоку AES (16 байт): от 16 до 512 байт.

Для каждой длины делается 10 итераций и берётся среднее время.

Код процедуры тестирования представлен в листинге 2.

Листинг 2 – Код процедуры тестирования

```
&НаСервере
Процедура ТестСкоростиНаСервере()
ОбработкаОбъект        = РеквизитФормыВЗначение("Объект");
СчётчикПаролей         = 1;
ИсходнаяСтрока         = "";
Для ЧислоБлоков = 1 по 32 Цикл
Данные= ПолучитьДанные(ЧислоБлоков);
СреднееВремя = 0;
Для НомерИтерации = 1 по 10 Цикл
Ключ256 = ПолучитьКлюч256(Формат(СчётчикПаролей, ""));
СчётчикПаролей = СчётчикПаролей + 1;
Время1 = ТекущаяУниверсальнаяДатаВМиллисекундах(); // СТАРТ!
Результат= ОбработкаОбъект.Подписать(Данные, Ключ256);
ИсходныеДанные= ОбработкаОбъект.ПроверитьПодпись(Данные, Результат,
Ключ256);
Время2 = ТекущаяУниверсальнаяДатаВМиллисекундах(); // СТОП!
СреднееВремя = СреднееВремя + Время2 - Время1;
КонецЦикла;
ТекстСообщения = СтрШаблон( "%1;%2",Формат(ЧислоБлоков, "ЧН=; ЧГ=")
,Формат(СреднееВремя / 10, "ЧРД=,; ЧН=; ЧГ="));
Сообщить(ТекстСообщения);
```

КонецЦикла;

КонецПроцедуры

Обработка тестировалась на платформе 1С: Предприятие 8.3.

Сеанс выполнялся на ядре с тактовой частотой 1,58 ГГц (максимальная 3,3 ГГц).

За каждую итерацию выполняется подпись и проверка подписи.

В качестве подписываемых данных используется строка, кратная одному блоку AES (16 байт): от 16 до 512 байт.

Для каждой длины делается 10 итераций и берётся среднее время.

Результат тестирования обработки показан на рисунке 10.

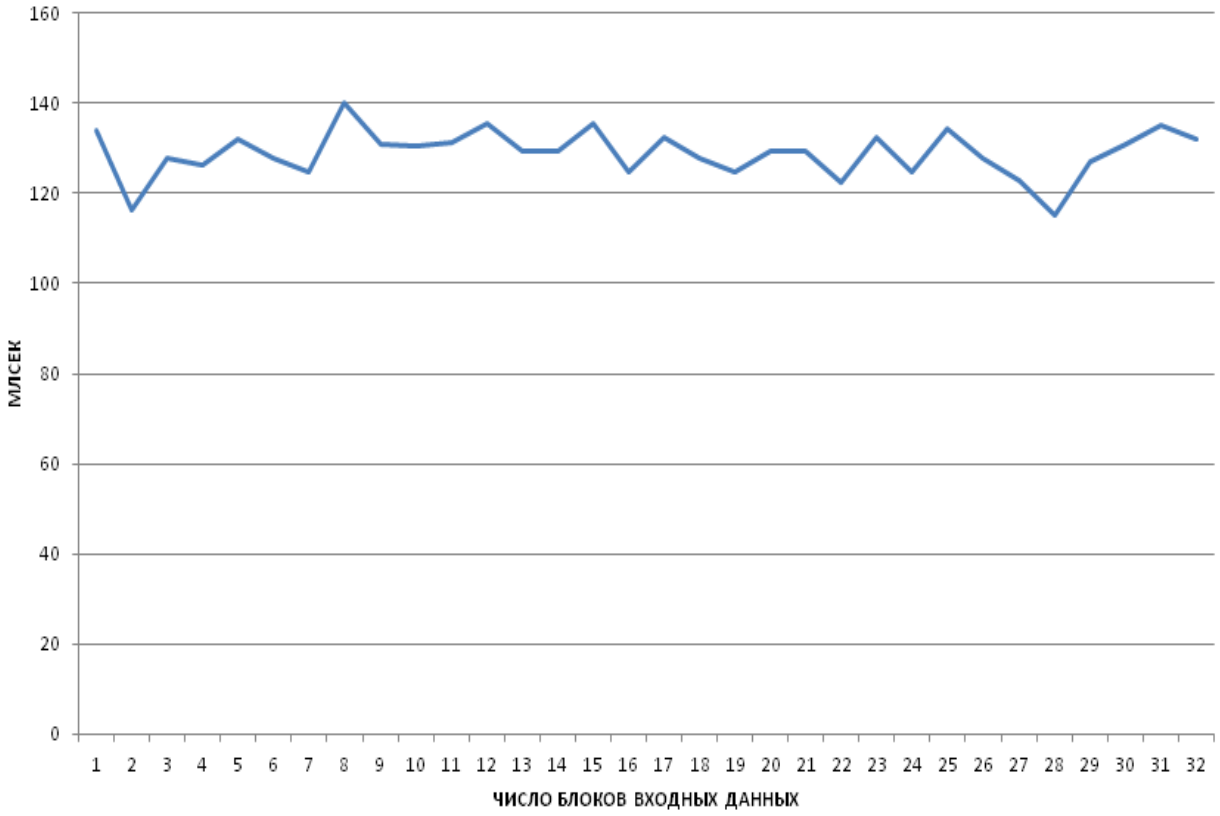

Рисунок 10 – График результатов тестирования обработки

На графике: ось X – число блоков в сообщении, ось Y– среднее количество миллисекунд, необходимое для зашифровки и расшифровки этого сообщения 256-битным ключом за 10 итераций.

Как следует из графика, среднее время выполнения обработки находится в пределах 120-140 мс, что вполне соответствует требованиям по быстродействию.

При этом благодаря совместному использованию алгоритмов SCH-256 и AES-256 обеспечивается высокая безопасность шифрования.

Выводы по главе 3

Третья глава посвящена программной реализации и тестированию алгоритмов майнинга криптовалют.

Результаты проделанной работы позволили сделать следующие выводы:

- в языке PHP имеется встроенная функция hash, которая генерирует хэш-код;
- использование алгоритма AES-256 существенно повышает безопасность шифрования.

Как показали результаты тестирования обработки на 1С8, среднее время выполнения обработки находится в пределах 120-140 мс, что вполне соответствует требованиям по быстродействию.

При этом благодаря совместному использованию алгоритмов SCH-256 и AES-256 обеспечивается высокая безопасность шифрования.

Заключение

Выпускная квалификационная работа посвящена актуальной проблеме исследования и практического применения алгоритмов майнинга криптовалют.

В настоящее время разработано много различных программ майнинга криптовалют.

Помимо конфигураций и вычислительной мощности используемых для майнинга компьютеров одним из критериев выбора конкретной программы является эффективность используемого в ней алгоритма майнинга.

Цель бакалаврской работы – исследование и реализация алгоритмов майнинга криптовалют.

Для достижения данной цели в процессе работы над бакалаврской работой решены следующие задачи:

- выполнена постановка задачи исследования и проанализированы методы консенсуса в блокчейне. Как показал анализ, в основе алгоритмов майнинга криптовалют лежат методы консенсуса блокчейна: Proof-of-Work (PoW) и Proof-of-Stake (PoS). Дано математическое описание методов. Главным преимуществом метода PoW является обеспечение надежного механизма для достижения консенсуса и предотвращения злоупотреблений и неправомерного использования. Главным недостатком – высокая энергоемкость. Главным преимуществом метода PoS является его энергетическая эффективность. Основными недостатками метода PoS являются ограничение доступности и подверженность хакерским атакам. Как показал анализ, более распространены алгоритмы метода PoW.
- проанализированый алгоритмы майнинга криптовалют: SCH-256, Ethash, Scrypt и CryptoNight. Каждый алгоритмы используется для

майнинга конкретного набора криптовалют. Как показал анализ, эффективность майнинга зависит от таких параметров, как мощность и производительности оборудования, вида и типа майнинга, а также от корректности подбора алгоритмов.

- выполнена программная реализация и тестирования алгоритмов майнинга. В качестве примера использован популярный алгоритм SHA-256. Выполнена реализация данного алгоритма на языке программирования PHP. Рассмотрен пример реализации подписи данных SHA + AES на платформе «1С: Предприятие 8». Как показали результаты тестирования обработки на 1С8, среднее время выполнения обработки находится в пределах 120-140 мс, что вполне соответствует требованиям по быстродействию. При этом благодаря совместному использованию алгоритмов SCH-256 и AES-256 обеспечивается высокая безопасность шифрования.

Результаты бакалаврской работы представляют научно-практический интерес и могут быть рекомендованы для анализа и программной реализации методов и алгоритмов майнинга криптовалют.

Список используемой литературы и используемых источников

1. Алгоритм шифрования SHA-256: особенности, преимущества и недостатки, майнинг [Электронный ресурс]. URL: https://ecrypto.ru/blokchejn/algoritm-shifrovaniya-sha-256-osobennosti-preimushhestva-i-nedostatki-majning.html#anchor1.3 (дата обращения: 10.03.2022).
2. Алгоритмы майнинга криптовалют [Электронный ресурс]. URL: https://prostocoin.io/blog/algorithm (дата обращения: 10.03.2022).
3. Архитектура платформы 1С: Предприятие 8 [Электронный ресурс]. URL: https://v8.1c.ru/platforma/ дата обращения: 10.03.2022).
4. Бушуев А.Х., Марченко А.В. Обзор алгоритмов хэширования на персональном компьютере // Политехнический молодежный журнал. 2020. № 3(44). С. 1-7.
5. Как устроены алгоритмы консенсуса в блокчейнах [Электронный ресурс]. URL: https://businessfm.kz/business/finance/kak-ustroeny-algoritmy-konsensusa-v-blokchejnah#:~:text=%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%BA%D0%BE%D0%BD%D1%81%D0%B5%D0%BD%D1%81%D1%83%D1%81%D0%B0%20%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD%D0%B0%20%E2%80%94%20%D1%8D%D1%82%D0%BE%20%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1,%D1%82%D1%80%D0%B0%D0%BD%D0%B7%D0%B0%D0%BA%D1%86%D0%B8%D0%B8%2C%20%D0%B8%20%D1%85%D1%80%D0%B0%D0%BD%D0%B8%D1%82%20%D0%BA%D0%BE%D0%BF%D0%B8%D1%8E%20%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD%D0%B0. (дата обращения: 10.03.2022).
6. Максуров А. А. Блокчейн, криптовалюта, майнинг: понятие и

правовое регулирование [Электронный ресурс] : монография. Москва : Дашков и К, 2021. 212 c. URL: https://www.iprbookshop.ru/107773.html (дата обращения: 09.03.2022).

7. Методы консенсуса в блокчейне [Электронный ресурс]. URL: https://www.invest-rating.ru/financial-encyclopedia/proof-of-stake-proof-of-work/ (дата обращения: 10.03.2022).

8. Подпись данных алгоритмами SHA + AES собственным модулем [Электронный ресурс]. URL: https://infostart.ru/public/1319502/ (дата обращения: 10.03.2022).

9. Правительство утвердило Концепцию законодательного регулирования оборота цифровых валют [Электронный ресурс]. URL: http://government.ru/news/44519/ (дата обращения: 10.03.2022).

10. Руководство по PHP [Электронный ресурс]. URL: https://www.php.net/manual/ru/function.hash.php (дата обращения: 10.03.2022).

11. Advantages and Disadvantages of Proof-of-Stake [Электронный ресурс]. URL: https://www.profolus.com/topics/pos-advantages-and-disadvantages-of-proof-of-stake/ (дата обращения: 10.03.2022).

12. Advantages and Disadvantages of Proof-of-Work [Электронный ресурс]. URL: https://www.profolus.com/topics/pow-advantages-and-disadvantages-of-proof-of-work/ (дата обращения: 10.03.2022).

13. Bentov I., Gabizon A., Mizrahi A. (2016) Cryptocurrencies Without Proof of Work. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg.

14. Breaking Down : SHA-256 Algorithm [Электронный ресурс]. URL: https://infosecwriteups.com/breaking-down-sha-256-algorithm-2ce61d86f7a3 (дата обращения: 10.03.2022).

15. Dhariwal K. Cryptocurrency Mining Algorithms and Popular Cryptocurrencies [Электронный ресурс]. URL: https://medium.com/@Mr.dhariwal/cryptocurrency-mining-algorithms-and-

popular-cryptocurrencies-48176d3559d6 (дата обращения: 10.03.2022).

16. How Does Bitcoin Mining Work? [Электронный ресурс]. URL: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ (дата обращения: 10.03.2022).

17. How to represent a Blockchain through a mathematical model? [Электронный ресурс]. URL: https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf (дата обращения: 10.03.2022).

18. Pegliari E. Mining algorithms (Proof of Work): SHA-256, Scrypt, CryptoNight, Ethash and X11 [Электронный ресурс]. URL: https://en.cryptonomist.ch/2019/06/15/mining-algorithms-proof-of-work/ (дата обращения: 10.03.2022).

19. PoS-mining: как зарабатывать деньги при минимальных усилиях? [Электронный ресурс]. URL: https://howtotrade.biz/pos-mayning/ (дата обращения: 10.03.2022).

20. Sharma V. and Niranjan L. A novel comparison of consensus algorithms in blockchain, Advances and Applications in Mathematical Sciences Volume 20, Issue 1, November 2020, Pages 1-13 © 2020 Mili Publications.

21. What is the Ethash mining algorithm? [Электронный ресурс]. URL: https://academy.bit2me.com/en/what-is-the-algorithm-of-ethash-mining/ (дата обращения: 10.03.2022).