МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и информационных технологий

МОДЕЛИРОВАНИЕ СМАРТ-КОНТРАКТОВ АВТОМАТНЫМИ ФУНКЦИЯМИ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 271 группы
направления 09.04.01 – Информатика и вычислительная техника
факультета компьютерных наук и информационных технологий
Семенисовой Софьи Петровны

Научный руководитель:
доцент, к.ф.-м.н. _____ Л.Б. Тяпаев

подпись, дата

Зав. кафедрой:
доцент, к.ф.-м.н. _____ Л.Б. Тяпаев

подпись, дата

Саратов 2025

ВВЕДЕНИЕ

Современные информационные технологии активно проникают во все сферы жизни, и блокчейн, изначально созданный для поддержки Bitcoin, не стал исключением. После долгого периода относительной неизвестности его популярность резко возросла вместе с развитием криптовалют. Сегодня блокчейн внедряется в экономику и финансы, обсуждается на государственном уровне, а его ключевая особенность — децентрализованная архитектура, позволяющая проводить транзакции без доверия между участниками.

Истоки криптовалют восходят к 1992 году, когда энтузиасты криптографии начали работу над их созданием. В 1998 году В. Дай описал концепцию цифровой валеты с анонимными контрактами, но лишь в 2008 году Сатоши Накамото представил Bitcoin, ставший отправной точкой для блокчейн-технологии. Пик популярности криптовалют пришёлся на 2017 год, и тогда же началось активное развитие смарт-контрактов, которые сегодня исследуются для применения в бизнесе и госуправлении. Эта технология меняет экономические отношения, позволяя автоматически исполнять договоры без участия человека.

Термин «смарт-контракт» ввёл в 1996 году Ник Сабо, определив его как цифровой набор обязательств с протоколами выполнения. Простейший аналог — вендинговые автоматы, совершающие сделки без человека. Хотя идея существовала задолго до блокчейна, именно он дал смарт-контрактам широкое практическое применение.

Анализ блокчейн-среды основан на теоретико-автоматных моделях, поскольку его работа детерминирована: добавление нового блока зависит от предыдущих записей и времени. Это позволяет описать процесс как временной автомат (timed automaton). Моделирование смарт-контрактов играет ключевую роль в исследовании цифровой экономики, использующей блокчейн и временные автоматы. Для этого применяется язык Uppaal, формально описывающий модели на основе автоматов с временными

метками. Любой юридически корректный контракт можно представить как конечный автомат, а методы автоматического преобразования смарт-контрактов в автоматные модели учитывают их поведение в динамичной блокчейн-среде.

Таким образом, взаимодействие смарт-контрактов в блокчейне можно рассматривать как скоординированную работу временных автоматов. Такое моделирование помогает оценивать устойчивость системы к атакам: контракты обрабатывают входные данные от пользователей, других контрактов и временных меток, формируя выходные сигналы, влияющие на всю сеть. Ошибка в одном контракте может вызвать каскадный сбой.

Смарт-контракты обладают высокой сложностью как в юридической, так и в программной части, что делает ручную проверку трудоёмкой. Однако моделирование позволяет автоматизировать тестирование, исследуя реакции на различные входные данные и прогнозируя поведение в разных условиях.

В данной работе цифровая экономика анализируется через теоретико-автоматное моделирование блокчейн-среды, где смарт-контракты описываются как автоматы с временными метками, а физическое время представлено 2-адическими числами. Полученная модель — классический автомат, но преобразование слов в нём реализуется не через таблицу переходов, а линейной программой из базовых процессорных команд (арифметических и побитовых операций).

Поскольку автомат стандартный, его поведение можно исследовать через функцию на пространстве целых 2-адических чисел. Любая детерминированная автоматная функция является p-адической, удовлетворяющей условию Липшица с константой 1, что позволяет применять методы p-адического анализа и алгебраической динамики. Хотя 2-адическое представление времени не общепринято, оно используется в p-адической физике как модель физического времени.

Функции, удовлетворяющие 2-адическому условию Липшица, известны как T-функции (в криптографии), автоматные функции (в теории

автоматов) или совместимые функции (в алгебре). Их ключевое свойство — возможность программной реализации без таблиц переходов, в виде линейных программ из стандартных команд: арифметических операций, побитовых логических операций, сдвигов и масок. Этот подход применим и к автоматам с более сложными алфавитами, соответствующим многомерным Т-функциям.

В практической части исследованы алгоритмы хэширования, играющие ключевую роль в блокчейне. С позиции автоматного подхода хэширование — это итеративное вычисление Т-функции, формирующее траектории в пространстве 2-адических чисел. К ним предъявляются криптографические требования: высокая скорость вычислений, равномерное распределение траекторий и повышенная линейная сложность последовательностей.

Цель магистерской работы заключается в исследовании моделей смарт-контрактов, посредствам реализации проекций Т-функций и их анализе.

Поставленная цель определила **следующие задачи**:

- изучение методов хеширования, а том числе особенностей хеширования в блокчейн, анализ генерации псевдослучайных последовательностей и линейной сложности;
- изучение аспектов теории автоматов, связанных с классическими автоматами, автоматами с метками времени, асинхронными автоматами;
- изучение блокчейн-технологий, автоматных моделей представления блокчейна и особенностей архитектуры распределенных систем;
- изучение смарт-контрактов, представления смарт-контрактов автоматными моделями, а также рассмотрение смарт-контрактов в контексте автоматов с непрерывным временем и возможности продолжения автоматных функций на пространстве действительных чисел;
- разработка программы, для построения и визуализации Т-функций,

моделирующих смарт-контракты.

Методологические основы исследования представлены в работах Анашина В.С. [1], А. Климова А. [2], Тяпаева Л.Б. [3] и других ученых и специалистов, посвященных теоретико-автоматным моделям, криптографии и блокчейн-технологиям.

Теоретическая значимость магистерской работы заключается в развитии методов моделирования смарт-контрактов с использованием автоматных функций и Т-функций.

Практическая значимость магистерской работы состоит в разработке программного инструмента для визуализации и анализа Т-функций, что может быть использовано для оценки криптографической стойкости смарт-контрактов.

Структура и объём работы. Магистерская работа состоит из введения, 5 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 57 страниц, включая 33 рисунка, использовано 42 источника литературы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел «Хэширование информации» раскрывает теоретические основы хэширования и включает четыре подраздела.

В подразделе «Хэширование в криптографии» рассматриваются процесс хэширования, хэш-функции и связанные с ними элементы в контексте криптографии. Сегодня криптографические хэш-функции играют ключевую роль, являясь важным инструментом шифрования с широким спектром применения. Однако создание надежной хэш-функции остается сложной задачей. Хэш-функция $h(x)$ принимает на вход строку M произвольной длины и возвращает строку фиксированной длины.

Во втором подразделе «Хэширование в технологии блокчейн» описывается роль хэш-функций в блокчейне, их практическое использование и значимость. Хэширование — неотъемлемая часть блокчейн-технологий, применяемая для адресации, создания цифровых подписей и майнинга криптовалют. Формально хэш-функция представляет собой отображение Ξ множества всех сообщений W (конечных непустых двоичных слов) в множество F_2^m слов фиксированной длины m.

Третий подраздел «Псевдослучайные генераторы» посвящен их описанию, принципам работы и критериям качества.

Одна из моделей псевдослучайных генераторов — конечный автомат

$$\mathfrak{A} =< S, O, S, O, s_0 > ,$$

где: S — множество состояний; O — выходной алфавит; S: $S \to S$ — функция перехода; O: $S \to O$ — функция выхода; $s_0 \in S$ — начальное состояние.

Четвертый подраздел «Линейная сложность» рассматривает линейную сложность и линейный ранг с l ошибками. Линейная сложность — важная характеристика криптографической стойкости бинарной последовательности, определяемая как минимальная длина линейного регистра сдвига, способного ее воспроизвести. Она позволяет оценить сложность восстановления начального состояния через решение системы линейных уравнений.

Второй раздел «Автоматные модели» посвящен рассмотрению автоматных моделей, играющих важную роль в данном исследовании. Раздел включает два основных аспекта изучения теории автоматов.

Первый подраздел «Классические автоматы» охватывает классические автоматные модели, включая дискретные системы с дискретным временем, детерминированные автоматы, автоматы-определители и преобразователи, а также автоматы Мили и их синхронные и асинхронные модификации. Теория автоматов, являющаяся разделом теории управляющих систем, занимается изучением математических моделей обработки дискретной информации и ведет свою историю с середины XX века, когда началось систематическое исследование свойств конечных автоматов.

Второй подраздел «Автоматы с метками времени» посвящен специализированному классу конечных автоматов, расширенных механизмом временного контроля. Эти модели используют конечное множество временных меток, синхронно изменяющихся с реальным временем, что позволяет осуществлять контроль абсолютного и относительного времени событий. Особенностью таких автоматов является возможность сравнения временных меток с целыми значениями, их сброса и использования для управления переходами. Формально, автоматы с временными метками могут быть представлены как системы с двумя типами входов и выходов: действительными числами (временные параметры) и символами конечных алфавитов, что относит их к подклассу гибридных автоматов. Данные модели обладают значительными преимуществами при моделировании систем с временными ограничениями и сложными временными зависимостями.

В третьем разделе «Блокчейн технология» рассматриваются ключевые аспекты технологии блокчейн, представленные в двух тематических подразделах.

Первый подраздел «История развития» содержит исторический обзор развития технологии, начиная с 1991 года, когда Стюартом Хабером и У.

Скоттом Шторнеттой было предложено первое практическое решение для защиты цифровых документов с использованием временных меток. В данном подразделе также анализируется эволюция блокчейна через смену поколений (в настоящее время выделяют три сформировавшихся поколения и разрабатываемое четвёртое) и рассматриваются базовые принципы функционирования криптовалютных систем.

Второй подраздел «Определение блокчейна» даёт формальное определение блокчейна в рамках автоматной теории, представляя его как последовательность двоичных слов (блоков) B_i, где каждый блок формируется путём конкатенации различных компонентов. Для начального блока (i=0) используется случайное слово w_0 и временная метка t_0, хэшируемые функцией Ξ. Последующие блоки (i>0) включают информационное слово w_i (список транзакций), временную метку t_i и хэш-значение предыдущего блока $\Xi(B_i-1)$, образуя таким образом криптографически связанную цепочку. Здесь L обозначает длину блока, k - длину временной метки, а m - размер выхода хэш-функции, что в совокупности определяет структуру и безопасные свойства системы.

В четвертом разделе «Смарт-контракты» разделе представлен комплексный анализ смарт-контрактов, структурированный в пять взаимосвязанных подразделов.

Первый подраздел «Определение смарт-контракта» вводит концепцию смарт-контрактов через историческую ретроспективу, начиная с работ Ника Сабо в 1996 году, который впервые предложил использовать цифровые протоколы для автоматизации выполнения договорных обязательств. Особое внимание уделяется преимуществам смарт-контрактов перед традиционными юридическими соглашениями, их практическому применению и перспективам развития в контексте распределенных реестров.

Во втором подразделе «Автоматное представление смарт-контрактов» разрабатывается формальная модель представления смарт-контрактов как автоматов с временными метками. Подчеркивается принципиальное отличие

смарт-контрактов от обычных юридических соглашений - их полная автономность исполнения и невозможность оспаривания условий после развертывания в блокчейн-среде. Все транзакционные данные при этом фиксируются в распределенном реестре.

Третий подраздел «Моделирование смарт-контрактов» посвящен методологии моделирования смарт-контрактов, где сравниваются два основных подхода:

- использование автоматов с временными метками, наиболее адекватно отражающих временные аспекты выполнения контрактов в блокчейн-среде;
- применение T-функций (2-адических автоматных функций), предлагающих альтернативную парадигму представления временных параметров.

В четвертом подразделе «Автоматы с непрерывным временем» проводится сравнительный анализ дискретного и непрерывного временных подходов, формализуется понятие непрерывного времени через метрические пространства.

В пятом подразделе «Автоматные функции, продолженные на пространство действительных чисел» исследуются вопросы продолжения автоматных функций на пространство действительных чисел, с акцентом на отображения рациональных p-адических чисел. Доказывается, что автоматные функции сохраняют рациональность при отображении, однако обратное утверждение не всегда справедливо.

Пятый раздел «Построение модели смарт-контрактов» посвящен практической части данной работы и содержит три раздела.

В первом подразделе «Проекции T-функций» основное внимание уделяется необходимой теоретической программной реализации построения проекций T-функций и анализу полученных результатов. Смарт-контракты, основанные на блокчейне, используют хеширование, реализуемое через T-функции, которые представляют собой автоматные или 1-Липшицевы

функции. Эти функции находят широкое применение не только в блокчейне, но и в других областях криптографии, таких как поточные шифры и генераторы псевдослучайных чисел. Проекции Т-функций строятся путем вычисления координат точек в единичном квадрате, что позволяет детально анализировать их свойства.

Второй подраздел «Программная реализация» посвящен разработке программного приложения для построения проекций Т-функций. Была разработана программа на языке Python [4] с использованием библиотек matplotlib [5] для визуализации графиков и tkinter для создания пользовательского интерфейса. Программа состоит из трех основных компонентов: модуля Cor.py для вычисления координат, Interface.py модуля интерфейса и основного файла main.py для запуска приложения. Интерфейс позволяет вводить функцию и параметр точности k, а также отображает полученную проекцию в единичном квадрате.

В подразделе «Построение проекций и их анализ» В ходе анализа проекций были рассмотрены различные типы функций. Линейные функции, такие как $f(x) = 3x$ или $f(x) = x + 1$, демонстрируют нигде не плотные графики с мерой Лебега 0. Дробно-линейные функции, например $f(x) = \frac{3}{5}x + \frac{1}{7}$, описываются через обмотки тора, где количество обмоток зависит от мультипликативного порядка. Квадратичные и полиномиальные функции, такие как $f(x) = 7x^2 + 37x + 7$ или $f(x) = x^3 - 2x^2 + 5x - 1$, показывают более сложные структуры, включая фрактальные patterns и равномерное распределение. Особый интерес представляют нелинейные функции с битовыми операциями, например $f(x) = (xXOR1)XOR\Big(2\big(xAND(1 + 2x)AND(3 + 4x)AND(7 + 8x)AND(15 + 16x)AND(31 + 32x)AND(63 + 64x)\big)\Big)XOR(4(x + 15))$, которые в зависимости от модификаций могут иметь меру Лебега 0 или 1. Также были исследованы функции Климова-

Шамира вида $f(x) = x + (x^2 ORC)$, где анализировались их эргодические свойства и линейная сложность.

На основе проведенного анализа сформулированы ключевые требования к Т-функциям для использования в криптографии. Во-первых, функция должна быть эргодической и транзитивной, чтобы обеспечивать равномерное распределение значений. Во-вторых, она должна быть вычислительно эффективной, предпочтительно представлять собой полином степени не выше 2, реализуемый через простые и быстрые операции. В-третьих, важно, чтобы функция обладала высокой линейной сложностью, в идеале стремящейся к бесконечности. Однако даже для квадратичных полиномов этот вопрос остается до конца не изученным, что указывает на необходимость дальнейших исследований. Полученные результаты демонстрируют, что проекции Т-функций являются мощным инструментом для анализа их криптографических свойств. В то время как линейные функции оказываются непригодными для практического использования в криптографии из-за низкой сложности, нелинейные функции представляют значительный интерес, хотя и требуют дополнительного изучения. Разработанная программная реализация значительно упрощает процесс визуализации и анализа Т-функций, что способствует их эффективному применению в смарт-контрактах и других блокчейн-решениях.

ЗАКЛЮЧЕНИЕ

В рамках данного исследования была успешно достигнута основная цель – был осуществлено моделирование смарт-контрактов посредствам построения проекций Т-функций и проведен их анализ проекций. Полученные проекционные модели были применены для детального изучения распределения последовательностей пар вида $(x,\ f(x))$, что позволило экспериментально исследовать линейную сложность последовательностей, генерируемых в процессе итеративного применения (например, при хэшировании) Т-функции f.

Для реализации поставленной цели был выполнен ряд важных исследовательских задач:

– были изучены методы хеширования, а том числе особенности хеширования в блокчейн, анализ генерации псевдослучайных последовательностей и линейной сложности;

– были изучены аспекты теории автоматов, связанных с классическими автоматами, автоматами с метками времени, асинхронными автоматами;

– были изучены блокчейн-технологии, автоматные модели представления блокчейна и особенности архитектуры распределенных систем;

– были изучены смарт-контракты, представления смарт-контрактов автоматными моделями, а также рассмотрены смарт-контракты в контексте автоматов с непрерывным временем и возможности продолжения автоматных функций на пространстве действительных чисел;

– была разработана программы, для построения и визуализации Т-функций, моделирующих смарт-контракты.

В процессе исследования методов моделирования смарт-контрактов был сделан принципиально важный вывод: для эффективного моделирования работы блокчейн-среды и смарт-контрактов нет необходимости использовать сложные и ресурсоемкие модели, основанные на концепции автоматов с

временными метками. Вместо этого достаточно ограничиться моделированием с использованием T-функций, которые могут быть реализованы в виде линейных программ, состоящих из последовательностей стандартных команд. Такие реализации отличаются относительной простотой и высоким быстродействием.

Ключевым выводом исследования стало определение требований к T-функциям для задач хэширования: необходимы эргодические T-функции с высокой (в идеале - бесконечной) линейной сложностью. Анализ полученных графиков выявил важные закономерности: все исследованные функции демонстрируют линейную структуру, при этом точки распределяются по конечному числу параллельных прямых, что указывает на неудовлетворительное распределение пар. Также было обнаружено, что различные функции могут иметь идентичные проекции. С точки зрения автоматного моделирования смарт-контрактов это означает, что различные автоматы в процессе функционирования сходятся к одному и тому же минимальному подавтомату.

Этот феномен имеет серьезные практические последствия: при длительной эксплуатации различных смарт-контрактов цифровая экономическая система может перейти в особый режим (соответствующий минимальному подавтомату в автоматной модели), при котором логика работы изначально различных контрактов становится неразличимой. Более того, после перехода в такой режим выход из него становится принципиально невозможным. Решение этой фундаментальной проблемы, вероятно, требует разработки новых подходов к представлению автоматов, например, через их продолжение до отображений из $\mathbb{R}$ в $\mathbb{R}$.

Для характеристики «качественных» T-функций были сформулированы три ключевых критерия:

- функция должна быть эргодической (и, следовательно, транзитивной);
- функция должна обладать высокой вычислительной эффективностью (что исключает использование полиномов степени выше 2 и требует

построения функций из простых быстровычислимых операций);

– функция должна демонстрировать высокую (в идеале - бесконечную) линейную сложность.

Однако следует констатировать, что задача поиска Т-функции, одновременно удовлетворяющей требованиям вычислительной эффективности и обеспечивающей оптимальное распределение пар, до сих пор не имеет окончательного решения и остается актуальным направлением для дальнейших исследований.

Основные источники информации:

1 *Анашин, В. С.* Неархимедов анализ, Т-функции и криптография / В. С. Анашин. — Москва, 2007. — 57 с.

2 *Klimov, A.* A new class of invertible mappings / A. Klimov, A. Shamir // *Cryp- tographic Hardware and Embedded Systems 2002*. — 2002. — Vol. 2523. — Pp. 470–483.

3 *Тяпаев, Л. Б.* Классы автоматных отображений, продолженных по непре- рывности на пространство действительных чисел / Л. Б. Тяпаев // *Компью- терные науки и информационные технологии*. — 2021. — С. 182–186.

4 Welcome to Python.org [Электронный ресурс]. — URL: https://www.python.org/ (Дата обращения 26.05.2025).

5 Matplotlib — Visualization with Python [Электронный ресурс]. — URL: https://matplotlib.org/ (Дата обращения 27.05.2025). Загл. с экр. Яз. англ.