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

Кафедра дискретной математики и информационных технологий

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ В БЛОКЧЕЙН-СРЕДЕ И ИХ АНАЛИЗ НА ОСНОВЕ АВТОМАТНЫХ МОДЕЛЕЙ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 271 группы
направления 09.04.01 — Информатика и вычислительная техника
факультета КНиИТ
Рожкова Максима Александровича

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

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

Саратов 2026

ВВЕДЕНИЕ

Одной из областей, на сегодняшний день активно внедряющих цифровые технологии, является экономика, в частности — приложения в сфере финансов. Особого внимания заслуживают смарт-контракты — алгоритмы, содержащие в себе условия соглашений и предназначенные для автономного контроля их исполнения [1]. Работа смарт-контрактов сопряжена с их размещением в сети блокчейна, конкретнее — с невозможностью внесения в них изменений. Соответственно, возникает потребность в доказательстве их корректной работы на этапе тестирования. Поскольку на сегодняшний день смарт-контракты достаточно широко распространены, цифровые рынки оперируют значительными финансовыми средствами и при этом являются системами с высоким уровнем риска, возникает необходимость в определенных инструментах анализа смарт-контрактов. Смарт-контракт может быть достаточно сложно устроен уже на уровне юридического соглашения, а для глубокого погружения в детали его программной реализации может потребоваться неопределенное время. В таком случае анализу нужно подвергнуть некоторую его модель. В данной работе основное внимание было сосредоточено на моделировании контрактов средствами хорошо изученной теории автоматов [2].

Целью магистерской работы является реализация алгоритма моделирования смарт-контрактов, основанного на формализме теории автоматов, и анализ поведения и структуры полученных объектов.

Для достижения поставленной цели решались следующие задачи:

- изучение теории автоматов, в частности автоматов Мили, автоматов-распознавателей, автоматов-преобразователей, асинхронных автоматов и автоматов с метками времени;
- изучение p-адического анализа, в частности представление автоматных функций на множестве действительных чисел;
- изучение теории графов, в частности ориентированных графов и их характеристик;
- изучение технологии блокчейн;
- изучение смарт-контрактов, в частности — возможности их представления автоматными моделями;
- разработка приложения для моделирования и исследования смарт-контрактов.

Исследования проводились на основе реальных финансовых соглашений: контракта займа [3], производственного соглашения [4], смарт-контракта удаленной безопасной покупки [5], и на модельном контракте, регулирующем игру в казино [6]. Полученные результаты впервые показали, что проведение аудита смарт-контрактов методами p-адического анализа возможно и позволяет выявить фундаментальные проблемы, касающиеся логики условий соглашения.

Выпускная квалификационная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 3 приложений. Результаты исследований представлены в тексте работы следующими разделами: объекты цифровой экономики и нерешенные проблемы предметной области (здесь дается экскурс в историю и современную проблематику цифровой экономики), автоматные модели (здесь представлены основные сведения из теории автоматов, необходимые для моделирования смарт-контрактов), методы исследования абстрактных автоматов (в нем приведены методы p-адического анализа и теории графов, используемые для численного анализа моделей) и моделирование смарт-контрактов средствами теории автоматов и анализ моделей (описываются используемые контракты и практические способы их моделирования и анализа).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе «Объекты цифровой экономики и нерешенные проблемы предметной области» дается представление о сущности смарт-контрактов, их применении на сегодняшний день и о связанных с этим проблемах.

Термин «смарт-контракт» был определен Ником Сабо в 1996 году, как компьютеризированный протокол транзакций, который выполняет условия контракта [1]. Широкого распространения в то время подобные алгоритмы не получили, ввиду невозможности заключать сделки без участия посредников (например, банков). В 2008 году с появлением блокчейна — технологии хранения информации в виде цепочки связных блоков — открылась перспектива полноценной автоматизации исполнения смарт-контрактов. Последнее значительное развитие смарт-контракты получили в 2015 году с появлением блокчейна Ethereum и полного по Тьюрингу языка программирования Solidity, на котором они описываются [7]. Однако, в силу неизменности смарт-контракта после его включения в блокчейн, возникают две основные проблемы объектов цифровой экономики: соответствия и устойчивости. Первая заключается в проверке равнозначности условий в коде смарт-контракта и условий юридического соглашения сторон. Вторая заключается в возможности или невозможности смарт-контракта прийти к некоторому состоянию, в котором его корректное завершение окажется невозможным.

Во втором разделе «Автоматные модели» представлены необходимые для проведения исследования сведения из теории автоматов. Данный раздел содержит 3 подраздела.

Первый подраздел «Классические автоматы» посвящен определению теории автоматов и изучаемых в ней объектов. Теория автоматов — раздел дискретной математики, изучающий математические модели преобразователей информации. Даются определения таких классов моделей, как абстрактные автоматы, автоматы-распознаватели (далее — d-автоматы), детерминированные конечные автоматы, автоматы-преобразователи (далее — f-автоматы) и автоматы Мили [2]. Также дается уточнение об использовании в выпускной квалификационной работе лишь синхронных автоматов.

Второй подраздел «Автоматы с метками времени» посвящен использованию автоматов с метками времени (далее — T-автоматов) для моделирования смарт-контрактов. Предлагается неформальное представление T-

автоматов, как автоматов с двумя входами и выходами — временным и алфавитным, поскольку T-автоматы описывают временные ограничения на переходы между состояниями. Благодаря этому они часто используются для моделирования смарт-контрактов. Однако, оно может быть сведено к моделированию d- или f-автоматами, исходя из вывода о кратности любого временного интервала некоторому минимальному интервалу [2].

Третий подраздел «Сплетения автоматов» посвящен определению сплетения автоматов. Здесь дается представление об автоматах, как об одном из способов задания динамических систем. Внешняя среда, из которой на вход автомата поступают последовательности символов входного алфавита, также является динамической системой. Тогда еще одним методом исследования смарт-контракта является построение сплетения автоматов, один из которых представляет собой неавтономную динамическую систему, а второй является генератором входных последовательностей для этой системы [8]. В этом подразделе приводится определение конгруэнтого генератора.

В третьем разделе «Методы исследования абстрактных автоматов» представлены необходимые для проведения анализа автоматных моделей контрактов сведения из областей p-адического анализа и теории графов. Данный раздел содержит 2 подраздела.

Первый подраздел «Методы p-адического анализа» дает определения способам визуализации реакции автоматов на входные последовательности и ее интерпретации. Дается определение графика 1-Липшицевой функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$, как замыкания в топологической плоскости объединения всех проекций $\mathcal{E}_{k\in\mathbb{N}}(f)$:

$$\mathcal{E}_k(f) = \left\{ \left(\frac{z \bmod p^k}{p^k}, \frac{f(z) \bmod p^k}{p^k} \right) \in \mathbb{I}^2 : z \in \mathbb{Z}_p \right\}.$$

Замыкание $P(f)$ множества объединения всех таких проекций $\mathcal{E}(f)$ в топологии плоскости $\mathbb{R}^2$ есть график функции f, который совпадает с предельным графиком автомата $\mathfrak{A}$, задающего автоматную функцию f. Ценность предельного графика состоит в возможности исследования поведения автомата при подаче на его вход бесконечных строк, то есть, в терминах динамических систем, визуализации его аттракторов. Помимо этого, вид графика позволяет делать выводы о сложности задаваемого автоматом отображения и оценивать его численно.

Также дается определение геометрического образа на словах длины k, как множества всех точек, полученных следующим образом [9]:

$$x = \sum_{i=0}^{k-1} x_i \cdot (N+1)^{-i} = x_0 + \frac{x_1}{(N+1)} + \cdots + \frac{x_{k-2}}{(N+1)^{k-2}} + \frac{x_{k-1}}{(N+1)^{k-1}};$$

$$y = \sum_{i=0}^{k-1} y_i \cdot (M+1)^{-i} = y_0 + \frac{y_1}{(M+1)} + \cdots + \frac{y_{k-2}}{(M+1)^{k-2}} + \frac{y_{k-1}}{(M+1)^{k-1}}.$$

Здесь x_i, y_i — соответственно, символы входной и выходной последовательностей автомата, представленные биекциями символов входного и выходного алфавитов на подмножества множества натуральных чисел, равномощные им. Геометрический смысл построенного образа заключается в отражении процесса эволюции автомата под действием входных последовательностей, в противовес визуализации предела этой эволюции в случае построения предельного графика. Поскольку геометрические образы часто представляют собой линейные или фрактальные структуры, с ними тесно связано понятие фрактальной размерности. Приводится алгоритм расчета значений фрактальной размерности методом ячеек.

Во втором подразделе «Методы теории графов» определяется возможность представления автоматов ориентированными графами и анализ таких моделей. Среди всех возможных характеристик ориентированных графов выделяются: наличие компонент сильной связности, степень посредничества каждой вершин, значение цикломатической сложности, вид матрицы достижимости, ее собственные числа и собственный вектор. Даются определения и способы расчета каждого из представленных параметров.

В четвертом разделе «Моделирование смарт-контрактов средствами теории автоматов и анализ моделей» представлены описания моделируемых контрактов, алгоритм построения моделей, описание и результаты работы приложения для анализа автоматных моделей на языке программирования Python. Данный раздел содержит 7 подразделов.

В первом подразделе «Материалы» представляются исследуемые контракты: контракт займа [3], производственное соглашение [4], смарт-контракт удаленной безопасной покупки [5] и контракт, регулирующий игру в казино с подбрасыванием монеты [6]. Для каждого контракта приводится краткое описание условий.

Второй подраздел «Автоматные модели исследуемых смарт-контрактов» посвящен описанию алгоритма аналитического синтеза автомата по услови-

ям контракта. Полученная в соответствии с алгоритмом модель является конечным детерминированным автоматом без выхода. Проведение численного анализа требует приведения модели к виду автомата Мили $\langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$, для чего в качестве символов выходного алфавита были приняты метки состояний автомата, в которых он оказывается после перехода. Для такого автомата $\mathcal{I}$ — входной алфавит событий, $\mathcal{S}$ — непустое множество финансовых состояний контракта, $\mathcal{O}$ — выходной алфавит, $|\mathcal{O}| = |\mathcal{S}|$, $S : \mathcal{I} \times \mathcal{S} \to \mathcal{S}$ — функция перехода, $O : \mathcal{I} \times \mathcal{S} \to \mathcal{O}$ — функция выхода, $s_0 \in \mathcal{S}$ — начальное состояние. Каждый символ входного алфавита биективно отображается в число из множества целых чисел $\{0, 1, \ldots, N-1\}$, где N — количество возможных событий. Такое же отображение, но на множество $\{0, 1, \ldots, M-1\}$, где M — количество состояний, выполняется для символов выходного алфавита. Таким образом задается автоматная модель состояний. Помимо нее в ходе работы используется бинарная автоматная модель, которая отличается двоичным представлением входного и выходного алфавитов, явным заданием принимающих состояний автомата $\mathcal{F} \subseteq \mathcal{S}$ и модифицированной функцией выхода:

$$\begin{cases} O(i,s) = g(S(i,s)), i \in \mathcal{I}, s \in \mathcal{S} \\ g(s) = 1, s \in \mathcal{F}, \\ g(s) = 0, s \notin \mathcal{F}. \end{cases}$$

Третий подраздел «Анализ автоматных моделей на языке Python» посвящен описанию разработанного приложения. Здесь описаны используемые библиотеки и модули, приводится структура приложения и алгоритм его работы с демонстрацией фрагментов кода.

В четвертом подразделе «Построение предельных графиков и геометрических образов автоматных моделей состояний» демонстрируются результаты работы кода по построению проекций предельных графиков и геометрических образов автоматных моделей состояний. По виду проекций предельных графиков делается вид о равенстве 0 их меры Лебега в $\mathbb{R}^2$. Более того, автоматные функции синтезированных моделей представляют собой наборы константных функций. Делается важное заключение: если контракт подразумевает наличие принимающих состояний в своей модели и решена задача соответствия, то накопление точек предельного графика в виде некоторых

константных функций позволяет делать вывод об успешном решении задачи устойчивости объекта цифровой экономики. Полученные проекции геометрических образов содержат фрактальные структуры, описывающие автономные компоненты автоматов. Значения фрактальной размерности D проекций геометрических образов: для контракта займа $D = 0.866564$, для производственного соглашения $D = 0.902356$, для смарт-контракта удаленной безопасной покупки $D = 0.855726$, для контракта, регулирующего игру в казино, $D = 0.989243$.

В пятом подразделе «Построение предельных графиков и геометрических образов автоматных моделей состояний» демонстрируются результаты работы кода по построению проекций предельных графиков, самих предельных графиков и геометрических образов бинарных автоматных моделей. Мера Лебега полученных проекций предельных графиков так же равна 0 в $\mathbb{R}^2$. Помимо этого, не изменилось представление реализуемых автоматами функций константами, что отчасти объяснимо принципом работы бинарной автоматной модели. Вывод, сделанный в прошлом подразделе и касающийся накопления точек предельного графика в виде некоторых констант, остается справедливым. Используемая модель упрощает решение задачи устойчивости объекта цифровой экономики. Полученные проекции геометрических образов бинарных автоматных моделей содержат фрактальные структуры, внешне напоминающие канторово множество. Это подтверждается расчетами значений фрактальной размерности D: для контракта займа $D = 0.593714$, для производственного соглашения $D = 0.651607$, для смарт-контракта удаленной безопасной покупки $D = 0.690279$, для контракта, регулирующего игру в казино, $D = 0.692773$.

В шестом подразделе «Сплетения автоматов с генераторами, моделирующими внешнюю среду» приводятся простейшие конгруэнтные генераторы [8,10], оперирующие заранее заготовленными входными последовательностями и управляющие работой автоматных моделей состояний контрактов. По виду управляющих последовательностей делается вывод о том, что исследуемые контракты предоставляют возможность выхода из промежуточных кризисов и успешного завершения.

Седьмой подраздел «Расчет характеристик ориентированных графов» посвящен исследованию внутренней структуры состояний и переходов между

ними методами теории графов. В качестве основы для построения ориентированных графов была взята автоматная модель состояний, из которой были удалены петлевые маршруты. Для контракта займа были выявлены две компоненты сильной связности, узлы которых оказались наиболее критичными в соответствии с рассчитанными значениями степени центральности. Такие состояния стоит считать критическими и избегать попадания в них, поскольку потенциально они ограничивают возможности «позитивного» завершения контракта. Для остальных орграфов автоматных моделей компоненты сильной связности, кроме отдельных узлов, выявлены не были. Были получены следующие значения цикломатической сложности графов автоматных моделей: для контракта займа — 47, для производственного соглашения — 7, для смарт-контракта удаленной безопасной покупки — 2, для контракта, регулирующего игру в казино — 5. Матрицы достижимости всех полученных орграфов похожи на верхнюю треугольную, что указывает на отсутствие глобальных циклов и может служить основанием вывода об ориентированности модели во времени. Анализ матрицы достижимости позволяет выделить критичные узлы, не входящие в компоненты сильной связности, а также задавать классификацию состояний автоматной модели.

ЗАКЛЮЧЕНИЕ

В ходе работы были достигнуты основные цели по моделированию смарт-контрактов и анализу получаемых моделей средствами p-адического анализа и теории графов. Для этого были предложены две автоматные модели: автоматная модель состояний и бинарная автоматная модель. Анализ проекций предельных графиков обеих моделей показал, что, по крайней мере при работе с имеющимися контрактами, синтезируемые ими автоматы обладают мерой Лебега 0 в $\mathbb{R}^2$. Неожиданным оказался вывод о том, что функции, реализуемые моделями, представляют собой наборы константных функций. Возможной причиной таких результатов является превалирование петель над действительными переходами между состояниями в автоматных моделях. Одним из важнейших сделанных в ходе практической деятельности является вывод, заключающийся в том, что накопление точек предельного графика в виде определенных константных функций служит доказательством решения задачи устойчивости смарт-контракта. Ведя речь о полученных проекциях предельных графиков для бинарной автоматной модели, можно утверждать о ее большей наглядности, поскольку любые точки, представляющие невозможность достижения принимающих состояний, представляются одной константной функцией. Вместе с тем, возникает опасение, что в результате упрощения модели были упущены неявные характеристики. На это косвенно указывает сравнение значений фрактальных размерностей двух моделей: значения фрактальной размерности для каждой бинарной модели ниже, чем у модели состояний.

Переходя к анализу построенных проекций геометрических образов, нужно, прежде всего, отметить наличие в них фрактальных структур, что показали обе используемые автоматные модели. Отдельно хочется выделить проекции модели состояний, поскольку в них четко прослеживается эволюция контрактов к принимающим состояниям. Проекции геометрических образов бинарной автоматной модели, кажутся более «фрактальными», что косвенно подтверждается значениями их фрактальных размерностей и их сравнением с оценкой данной характеристики множества Кантора. Промежуточный вывод можно сделать касательно возможности исследования и, в частности, аудита объектов цифровой экономики методами теории автоматов. Основываясь на предложенном в тексте выпускной квалификационной работы подходе мож-

но получить определенные результаты, позволяющие заявлять о степени корректности работы смарт-контрактов.

Несмотря на то, что построенные конгруэнтные генераторы не являются полноценными генераторами цепочек входных событий, они все-таки способны передавать такие входные воздействия на вход автомата, моделирующего смарт-контракт.

Анализ построенных на основе автоматной модели состояний орграфов исследуемых контрактов дает основания считать используемые методы теории автоматов полезными как с точки зрения настройки параметров автоматных моделей, так и для проведения независимого от теории автоматов исследования. Их применение позволяет, на примере контракта, регулирующего игру в казино, обнаруживать аномальные и критичные для работы цифрового соглашения состояния. Помимо этого, расчет матрицы достижимости и исследование ее структуры может служить основой для кластеризации состояний.

Основные источники информации:

1. Szabo N. Smart contracts: Building Blocks for Digital Markets // EXTROPY: The Journal of Transhumanist Thought. 1996. Vol. 18, №. 2. Pp. 28-39.
2. Анашин В. С. О теоретико-автоматных моделях блокчейн-среды // Информатика и её применения. 2019. Т. 13, №. 2, 2019. С. 48-55.
3. Flood M. D., Goodenough O. R. Contract as automaton: The computational representation of financial agreements // OFR Working Paper. 2015. Vol. 15, №. 4. 25 pp.
4. Holmes J. N., Beigi H. A Transaction Represented with Weighted Finite-State Transducers // arXiv preprint arXiv:2302.00200v1, 2023.
5. Solidity by Example [Электронный ресурс] // Solidity: [сайт]. URL: https://docs.soliditylang.org/en/v0.8.31/solidity-by-example.html (дата обращения: 13.05.2026) Загл. с экрана. Яз. англ.
6. Colombo C., Ellul J., Pace G. J. Contracts over smart contracts: Recovering from violations dynamically // International Symposium on Leveraging Applications of Formal Methods, 2018. Pp. 300-315.
7. Wood G. Ethereum: A Secure Decentralized Generalised Transaction Ledger // Ethereum Project Yellow Paper, 2014. 32 pp.
8. Anashin V. Applied algebraic dynamics / V. Anashin, A. Khrennikov //

Berlin: Walter de Gruyter, 2009. 557 pp.

9. Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика. 2006. Т. 6, №. 1. С. 121-133.
10. Ларин М. В., Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика, Т. 14, № 2, 2002. С. 20–32.