

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

Кафедра дискретной математики и информационных технологий

**РЕАЛИЗАЦИЯ ДЕЦЕНТРАЛИЗОВАННОГО ПРИЛОЖЕНИЯ
«КНИЖНЫЙ МАГАЗИН»**

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Чернец Марии Владиславовны

Научный руководитель
доцент, к. ф.-м. н.

Л. Б. Тяпаев

Заведующий кафедрой
доцент, к. ф.-м. н.

Л. Б. Тяпаев

Саратов 2022

ВВЕДЕНИЕ

Развитие цифровой экономики является приоритетным направлением для России. При детальном рассмотрении можно увидеть, что она представляет собой взаимодействующие друг с другом смарт-контракты. В настоящее время главными нерешенными задачами в данной сфере являются проблемы устойчивости и проверки соответствий. Из данного факта вытекает необходимость более подробных исследований, которые основываются на моделировании. Моделирование поведения смарт-контрактов необходимо для глубокого анализа функционирования цифровой экономики, которая в свою очередь строится на основе блокчейна с помощью автоматов с метками времени [1].

В данной работе элементы цифровой экономики рассматриваются с использованием подхода к построению теоретико-автоматных моделей функционирования блокчейн-среды, в частности, функционирования смарт-контрактов в этой среде, как автомата с метками времени, в котором физическое время представляется не действительными, а 2-адическими числами [2]. Итоговая модель представляет собой автомат в стандартном понимании этого термина, при этом задаваемое автоматом преобразование слов реализуется не в виде таблицы переходов состояний, а в виде программы без ветвления, представляющей собой последовательность стандартных команд процессора, а именно арифметических и поразрядных логических операций. Поскольку полученный автомат является обычным автоматом, описание его функционирования может быть сведено к изучению функции, заданной и принимающей значения в пространстве целых 2-адических чисел ввиду того, что каждая детерминированная (по С. В. Яблонскому) функция есть p -адическая функция, удовлетворяющая условию Липшица с константой 1 относительно подходящей p -адической метрики, и обратно: все такие функции являются детерминированными [3]. К изучению таких автоматов (а значит, и к изучению функционирования смарт-контрактов в блокчейн-среде) применим развитый аппарат p -адического анализа и алгебраической динамики [3]. 2-Адическое время является хоть и не общепринятой, но тем не менее довольно широко используемой и во многих случаях релевантной математической моделью физического времени, активно изучаемой уже почти три десятилетия в рамках p -адической математической физики [4].

Практическая часть работы сфокусирована на применении блокчейн

технологий для решения проблемы публикации и распространения авторских электронных работ.

Целью работы является разработка смарт-контракта и децентрализованного приложения «Книжный магазин». Для достижения цели необходимо решить следующие задачи:

1. изучить принципы функционирования смарт-контрактов в блокчейн среде;
2. рассмотреть подход автоматного моделирования смарт-контрактов;
3. изучить возможность сведения Т-автоматов к Т-функциям;
4. разработать смарт-контракт «Книжный магазин»;
5. создать на его основе децентрализованное приложение.

Дипломная работа состоит из введения, пяти разделов с девятью под-разделами, заключения, списка использованных источников и четырех приложений. Общий объем работы — 75 страниц, из них 52 страницы — основное содержание, включая 33 рисунка и пять таблиц, список использованных источников из 33 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе дипломной работы рассмотрены основные элементы теории автоматов.

Абстрактным автоматом AA называется дискретный преобразователь информации, представляющий собой множество, состоящее из шести элементов: $AA = \{S, X, Y, \delta, \lambda, s_0\}$, где S — непустое множество состояний автомата; X — конечное множество входных символов, то есть входной алфавит автомата: $X = \{x_0, \dots, x_m\}$; Y — конечное множество выходных символов, то есть выходной алфавит автомата: $Y = \{y_0, \dots, y_p\}$; s_0 — начальное состояние автомата; δ — функция переходов автомата, отображающая множество $S \times X$ в S ; λ — функция выходов автомата, отображающая множество $S \times X$ в Y .

Автоматом-распознавателем A называется множество, состоящее из элементов: $A = \{S, X, F, \delta, s_0\}$, где S, X, δ, s_0 те же, что и в определении абстрактного автомата; $F \subseteq S$ — множество принимающих состояний.

Автомат-преобразователь $A = \{S, X, Y, \delta, \lambda, s_0\}$ есть абстрактный автомат из определения абстрактного автомата.

Асинхронным автоматом A называется множество, состоящее из элементов: $A = \{S, X, Y, \delta, \lambda\}$, где S — множество состояний (не обязательно конечное); X, Y те же, что и в определении абстрактного автомата; δ — функция переходов автомата, отображающая множество $X \times S$ в S ; λ — функция выходов автомата, отображающая множество $X \times S$ в Y^* .

Синхронным автоматом A называется множество, состоящее из элементов: $A = \{S, X, Y, \delta, \lambda\}$, где все компоненты обозначают тоже что и в определении асинхронного автомата, если для любых $x \in X, s \in S$ слово $\lambda(x, s)$ является однобуквенным.

Во втором разделе данной работы рассмотрена технология смарт-контрактов. Дано определение «смарт-контракта». Изучен принцип его работы в блокчейн среде. Также рассмотрены свойства, преимущества и недостатки, основные платформы для исполнения смарт-контрактов, и значение их в цифровизации экономики.

В третьем разделе рассмотрен подход моделирования смарт-контрактов с помощью Т-автоматов, который подразумевает, что функционирование смарт-контрактов в блокчейн-среде можно рассматривать как взаимо-

действие автоматов во времени, то есть Т-автоматов.

Автоматом с метками времени или Т-автоматом A является набор элементов: $A = \{S, X, C, I, E, s_0\}$, где S — конечное множество состояний автомата; X — конечное множество входных символов; s_0 — начальное состояние автомата; C — множество таймеров; I — это отображение, которое маркирует каждое состояние s некоторым ограничением таймеров в $\Phi(C)$; $E \subseteq S \times X \times 2C \times \Phi(C) \times S$ — это набор переключателей. Переключатель (s, x, ϕ, ξ, s) представляет путь от состояния s до состояния s на символе x . ϕ — это ограничение таймеров по C , и $\xi \subseteq C$ дает таймер, который будет сброшен с помощью этого переключателя.

Также рассмотрены задачи цифровой экономики: устойчивости и проверки соответствий.

В четвертом разделе данной работы изучена возможность сведения Т-автоматов к обычным автоматам, которые в случае с бинарным алфавитом есть ничто иное как Т-функции.

Функцией треугольного вида или Т-функцией от m переменных называют любое отображение вида:

$$F: (\dots, \alpha_2^\downarrow, \alpha_1^\downarrow, \alpha_0^\downarrow) \mapsto (\dots, \Phi_2(\alpha_0^\downarrow, \alpha_1^\downarrow, \alpha_2^\downarrow), \Phi_1(\alpha_0^\downarrow, \alpha_1^\downarrow), \Phi_0(\alpha_0^\downarrow)),$$

где $\alpha_i^\downarrow \in \mathbb{F}_2^m$ — m -мерный булев вектор-столбец; $\mathbb{F}_2 = \{0, 1\}$; отображение $\Phi_i: (\mathbb{F}_2^m)^{(i+1)} \rightarrow \mathbb{F}_2^n$ сопоставляет $(i+1)$ m -мерным булевым вектор-столбцам $\alpha_i^\downarrow, \dots, \alpha_0^\downarrow$ соответствующий n -мерный булев вектор-столбец $\Phi_i(\alpha_0^\downarrow, \dots, \alpha_i^\downarrow)$.

В пятом разделе описано созданное в рамках этой дипломной работы децентрализованное приложение «Книжный магазин».

Децентрализованное приложение — это приложение, в котором определяющую роль играет блокчейн и его реакция, прописанная в виде смарт-контрактов, на определенные события [5–8].

В первом подразделе пятого раздела указано назначение и описана область применения реализованного приложения.

Программа, разрабатываемая в рамках работы, предназначена для того, чтобы писатели могли напрямую, без издательств публиковать и продавать свои произведения. Смарт-контракт предоставляет право пользования произведениями, тем самым обеспечивает защиту авторских прав. Таким образом, весь процесс от публикации до продажи становится более простым,

для писателей, более эффективным и менее дорогостоящим для покупателей.

Входными данными являются: информация о книге, текстовый файл произведения, а также адреса счетов авторов и покупателей. При этом адреса имеют 34-значный формат. Выходными данными являются сообщение об успехе проведенной операции, либо сообщение о неправильных входных данных. Интерфейс приложения предоставляет базовую проверку данных, остальная проверка делается непосредственно смарт-контрактом.

Во втором подразделе пятого раздела описаны компоненты выбранной архитектуры приложения. Компонентами являются: веб-сайт, веб-API, база данных off-Chain и смарт-контракт.

В третьем подразделе пятого раздела приведено описание функциональности. Пользователями выступают авторы электронных работ и их покупатели. Функции приложения: добавлять книгу, обновлять и удалять информацию о ней и делать заказ.

В четвертом подразделе пятого раздела рассмотрены технологии, выбранные для разработки. В качестве блокчейн платформы был выбран NEO. Язык программирования системы — C#. Локальная база данных — LevelDB.

В пятом подразделе пятого раздела описан созданный в рамках этой дипломной работы смарт-контракт. Рассмотрены его компоненты, а также их поведение, с помощью UML диаграмм состояний.

В шестом подразделе пятого раздела показана функция «Добавление книги». Данная функция реализована в разработанном смарт-контракте. В рамках данной функциональности пользователь «Автор» может добавить книгу на продажу.

В седьмом подразделе пятого раздела описана функция «Обновление книги», которая реализована в разработанном смарт-контракте. В рамках данной функциональности пользователь «Автор» может изменить информацию о книге.

В восьмом подразделе пятого раздела показана функция «Удаление книги». Данная функция реализована в разработанном смарт-контракте. В рамках данной функциональности пользователь «Автор» может удалить информацию о книге.

В девятом подразделе пятого раздела описана функция «Заказ книги», которая реализована в разработанном смарт-контракте. В рамках данной функциональности пользователь «Покупатель» может приобрести любую книгу.

ЗАКЛЮЧЕНИЕ

В данной работе были изучены принципы функционирования смарт-контрактов в блокчейн среде. Рассмотрен подход моделирования смарт-контрактов Т-автоматами. Более того, была изучена возможность сведения Т-автоматов к Т-функциям. Проблема публикации и распространения авторских электронных работ была решена с помощью разработанного смарт-контракта и созданного на его основе децентрализованного приложения «Книжный магазин». Таким образом, все поставленные задачи были выполнены, цели работы можно считать достигнутыми.

Основные источники информации:

- 1 Andrychowicz, M. Modeling bitcoin contracts by timed automata / M. Andrychowicz, S. Dziembowski, D. Malinowski, L. Mazurek // ArXiv. - 2014. - V. 1405.1861, № 2. - 23 p.
- 2 Анашин, В. С. О теоретико-автоматных моделях блокчейн-среды / В. С. Анашин // Информатика и ее применения. - 2019. - Т. 13, № 2. - С. 29-36.
- 3 Anashin, V. Applied algebraic dynamics / V. Anashin, A. Khrennikov // De Gruyter expositions in mathematics. - 2009. - V. 49. - 533 p.
- 4 Dragovich, B. On p-adic mathematical physics / B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich // P-Adic Numbers Ultrametrics Analysis and Appl. - 2006. - V. 1. - P. 1-17.
- 5 Raval, S. Decentralized Applications / S. Raval. — Sebastopol, California: O'Reilly, 2016. - 103 p.
- 6 Децентрализованные приложения (DApps), преимущества и перспективы [Электронный ресурс]. — URL: <https://bitstat.top/blog.php> (дата обращения: 03.05.2022). - Загл. с экрана. - Яз. рус.
- 7 Технология блокчейн с точки зрения информационной безопасности. Часть 1 [Электронный ресурс]. — URL: <https://safe-surf.ru/specialists/article/5278/658923/> (дата обращения 04.05.2022). - Загл. с экрана. - Яз. рус.
- 8 Разработка децентрализованных приложений | JazzTeam Software Development Company [Электронный ресурс]. — URL: <https://jazzteam.org/ru/technical-articles/development-of-decentralized-applications/> (дата обращения: 10.05.2022). - Загл. с экрана. - Яз. рус.