УДК 004.942 **DOI: 10.18413/2518-1092-2022-8-1-0-4**

Жихарев А.Г.[1]
Киданов В.В.[2]
Фефелов О.С.[2]

К ВОПРОСУ О БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СМАРТ-КОНТРАКТОВ

[1)] Белгородский государственный технологический университет им. В.Г. Шухова, ул. Костюкова, 46, Белгород, 308012, Россия
[2)] Белгородский государственный национальный исследовательский университет, ул. Победы, 85, Белгород, 308015, Россия

e-mail: zhikharev@bsu.edu.ru

Аннотация
В работе рассматриваются перспективы использования смарт-контрактов, а также вопрос их информационной безопасности. Проведен анализ мирового рынка смарт-контрактов, показано, что данная технология развивается и занимает свое место в сфере регулировки гражданско-правовых отношений. Рассмотрены наиболее популярные инструментальные площадки по созданию и реализации смарт-контрактов. Проведен анализ уязвимостей смарт-контрактов, связанных как со средой их разработки и исполнения, а также с программированием смарт-контрактов. Показано, что большинство уязвимостей имеют место в связи с отсутствием методологии и средств проектирования и верификации смарт-контрактов.
Ключевые слова: блокчейн; смарт-контракты; рынок смарт-контрактов; оракулы блокчейна; преимущества и недостатки технологии смарт-контрактов; типы уязвимостей смарт-контрактов
Для цитирования: Жихарев А.Г., Киданов В.В., Фефелов О.С. К вопросу о безопасности обработки информации с использованием смарт-контрактов // Научный результат. Информационные технологии. – Т.8, №1, 2023. С. 46-55. DOI: 10.18413/2518-1092-2022-8-1-0-4

Zhikharev A.G.[1]
Kidanov V.V.[2]
Fefelov O.S.[2]

ON THE SECURITY OF INFORMATION PROCESSING USING SMART CONTRACTS

[1)] Belgorod state technological university named after V.G. Shukhov , 46 Kostyukova street, Belgorod, 308012, Russian Federation
[2)] Belgorod state university, 85 Pobedy street, Belgorod, 308015, Russian Federation

e-mail: zhikharev@bsu.edu.ru

Abstract
The paper discusses the prospects for the use of smart contracts, as well as the issue of their information security. The analysis of the world market of smart contracts has been carried out, it has been shown that this technology is developing and taking its place in the field of regulation of civil law relations. The most popular instrumental platforms for the creation and implementation of smart contracts are considered. An analysis of the vulnerabilities of smart contracts related both to the environment for their development and execution, as well as to the programming of smart contracts, was carried out. It is shown that most of the vulnerabilities occur due to the lack of methodology and tools for designing and verifying smart contracts.
Keywords: blockchain; smart contracts; smart contract market; blockchain oracles; advantages and disadvantages of smart contract technology; types of smart contract vulnerabilities
For citation: Zhikharev A.G., Kidanov V.V., Fefelov O.S. On the security of information processing using smart contracts // Research result. Information technologies. – T.8, №1, 2023. – P. 46-55. DOI: 10.18413/2518-1092-2022-8-1-0-4

ВВЕДЕНИЕ

Блокчейн – это система распределенной базы данных, построенная на основе списка записей транзакций с отметками времени. Его главное новшество заключается в том, что он позволяет сторонам совершать сделки с недоверенными сторонами с использованием компьютерной сети [1]. Структура данных блокчейна представляет собой иерархию блоков, объединяющих транзакции. Каждый блок уникально идентифицируем и связан со своим предшественником в цепочке, а целостность обеспечивается с помощью методов, основанных на криптографии.

Узлы в сети блокчейнов могут выполнять произвольное или злонамеренное поведение или обладать дезинформацией. Таким образом, механизмы консенсуса являются ядром сетей блокчейнов, чтобы гарантировать, что все участники согласны с состоянием сети в таких ненадежных средах [4]. Наиболее важными алгоритмами консенсуса для блокчейнов являются Proof of Work (PoW) и Proof of Stake (PoS). В блокчейнах, использующих PoW (например, биткойн), алгоритм вознаграждает участников за решение головоломок на основе криптографии для проверки транзакций и создания новых блоков. В блокчейнах на основе PoS (например, предстоящая реализация Casper в Ethereum) валидаторы по очереди предлагают и голосуют за следующий блок. Вес голосов валидаторов зависит от их ставки или депозита в сети. PoS обеспечивает улучшенную масштабируемость, быстрые транзакции, низкий уровень вычислений и энергопотребления, а также высокий уровень безопасности.

Блокчейн изначально был разработан для работы в качестве не требующей доверия одноранговой сети для финансовых транзакций. С тех пор технология расширилась и теперь включает множество других приложений, включая смарт-контракты. Смарт-контракт живет в блокчейне и имеет свой уникальный адрес. Более того, технология смарт-контрактов позволяет пользователям создавать автономные приложения, работающие независимо без какого-либо вмешательства со стороны системного объекта. Хотя BLOR теоретически может поддерживать любой смарт-контракт с низкой вычислительной нагрузкой, в данной статье основное внимание уделяется его использованию в Ethereum для реализации благодаря его общедоступным платформам. Первоначально Ethereum разработал свою платформу на основе PoW, но недавно проводит значительное обновление для представления Ethereum 2.0 с использованием протокола Casper [4]. Протокол Casper упрощает переход от текущего PoW к чистому протоколу PoS. Криптовалюта Ethereum называется Ether. В текущей версии Ethereum работает через «газ», который представляет собой покупку потребляемых ресурсов на основе эфира. Это способствует Ethereum предотвратить DoS-атаки, бесконечные циклы внутри контрактов и в целом контролировать расход сетевых ресурсов. Каждая функция, такая как отправка и получение данных, выполнение вычислений и хранение данных, имеет стоимость «газа».

Смарт-контракты бывают двух типов: детерминированные и недетерминированные (Morabito, 2017). Код детерминированного смарт-контракта реализован на блокчейне с полной изоляцией от внешних сред, а решения и состояния контракта поддерживаются участниками внутри блокчейна. Напротив, недетерминированный код смарт-контракта нуждается во внешней информации для принятия решений, что делает его зависимым от участников вне сети блокчейна. Например, внешним субъектом может быть поставщик информации о погоде или поставщик данных датчиков, которые в блокчейне известны как оракулы.

Блокчейны произвели революцию в корпоративном управлении, поскольку они обеспечивают более высокую прозрачность для всех участников и простоту администрирования, а также предоставляют инновационные инфраструктуры для обмена бизнес-транзакциями в режиме реального времени. Хотя блокчейн обладает большим потенциалом для того, чтобы помочь предприятиям безопасно обмениваться данными и сотрудничать, было проведено очень мало исследований реальных приложений. По оценкам исследовательской фирмы Tractica, к 2025 году доход корпоративных приложений блокчейна достигнет 19,9 млрд долларов [4]. Большинство исследований применения блокчейна сосредоточено на экономике, энергетике [4] и приложений [5].

Смарт-контракты – это новая технология, которая может повысить эффективность в различных отраслях. Рентабельность, экономия времени, безопасность, прозрачность и точность — вот лишь некоторые из преимуществ. В результате этих преимуществ рынок смарт-контрактов, вероятно, будет расширяться. По мере совершенствования технологий все больше предприятий смогут использовать его для сокращения расходов и обеспечения быстрых и безопасных транзакций.

Следует отметить, что смарт-контракты, несмотря на их условную безопасность, имеют различные уязвимости, большинство из которых связаны исключительно с процессом разработки смарт-контракта. Таким образом остается актуальной задача создания технологий проектирования смарт-контрактов при условии минимизации уязвимостей первого.

АНАЛИЗ РЫНКА СМАРТ-КОНТРАКТОВ 2023–2028

По аналитическим данным исследований компании Valuates Reports прогнозируется, что размер мирового рынка смарт-контрактов достигнет 1460,3 млн долларов США к 2028 году по сравнению с 315,1 млн долларов США в 2021 году при совокупном годовом темпе роста (CAGR) в 24,2% в течение 2022-2028 годов.

Анализ рынка смарт-контрактов 2023-2028 гг. представлен на рис. 1.

Рис. 1. Рынок смарт-контрактов 2022-2028
Fig. 1. Smart contracts market 2022-2028

Ключевыми драйверами рынка смарт-контрактов являются растущие приложения в различных отраслях конечных пользователей. Появление технологии блокчейн будет способствовать дальнейшему росту рынка смарт-контрактов в течение прогнозируемого периода. Растущее осознание преимуществ смарт-контрактов будет способствовать расширению рынка в ближайшие годы. Смарт-контракты внедряются правительствами по всему миру, чтобы минимизировать затраты на управление контрактами за счет меньшего вмешательства человека.

Смарт-контракты создаются с использованием технологии блокчейна, а отсутствие стандартизации и взаимозаменяемости платформ блокчейна делает создание смарт-контрактов сложным и потенциально подверженным ошибкам.

Тенденции, влияющие на рынок смарт-контрактов:

А) Растущее использование в нескольких отраслевых вертикалях.

Смарт-контракты — это программы, хранящиеся в блокчейне, которые оптимизируют различные процессы и системы. Сбор налогов ускорится, поскольку данные можно будет сопоставить с совершенной транзакцией, и вся система станет эффективной. Правительства могут хранить важнейшие цифровые данные граждан в одном зашифрованном элементе, что обеспечивает удобство и легкий доступ для отдельных лиц. Точно так же смарт-контракты могут хранить личные медицинские карты пациентов, обеспечивать проверку ошибок и переводить платежи в финансовом секторе и страховании. Цепочки поставок выиграют от сокращения трудоемкой бумажной работы, которая увеличивает вероятность мошенничества или потерь. Эти факторы будут способствовать росту рынка смарт-контрактов в течение прогнозируемого периода [1].

Б) Технология блокчейн.

Смарт-контракты хранятся в блокчейне в виде программ в одном из блоков. Это обеспечивает неизменность, так как условия контракта не могут быть изменены, и они отслеживаются в режиме реального времени. Стоимость управления контрактами снижается с минимальным вмешательством человека или без него. Проверка проводится регулярно, и никто не может ею манипулировать. Распределенная функция и отсутствие третьей стороны обеспечивают более быстрое завершение и выполнение контракта.

В) Благоприятные факторы.

Смарт-контракты могут принести огромную пользу различным заинтересованным сторонам отрасли. Это обеспечивает скорость, безопасность и экономию средств за счет отсутствия брокеров или других посредников. Ручное заполнение исключено, а все необходимые данные надежно зашифрованы.

Г) Побочные эффекты.

Смарт-контракты сложно изменить. Любые ошибки в программе могут вскоре стать трудоемкими и раздражающими. Отсутствие стандартизации и взаимозаменяемости еще больше усугубляет проблему. Ожидается, что в систему будут закрадываться расплывчатые термины и лазейки. Это будет препятствовать расширению рынка смарт-контрактов в последующие годы.

Таблица 1

Анализ доли рынка смарт-контрактов

Table 1

Analysis of the market share of smart contracts

Метрика отчета	**Подробности**
Объем рынка в 2021 году	315,1 млн долларов США
Прогноз выручки в 2028 году	1460,3 млн долларов США
Скорость роста	CAGR 24,2% с 2022 по 2028 год
Прогнозный период	с 2022 по 2028 год
Рынок по типу	Публичный блокчейн, частный блокчейн, и другие
Рынок по приложениям/конечным пользователям	Финансы, правительство, страхование, здравоохранение, цепочка поставок, и другие
Сообщить о покрытии	Прогноз доходов и объемов, доля компании, конкурентная среда, факторы роста и тенденции

Ожидается, что на основе приложений государственный сектор сохранит лидерство на рынке смарт-контрактов благодаря их широкому использованию на предприятиях государственного сектора и в государственных организациях для ускорения и оптимизации систем.

Публичные блокчейны полностью бесплатны и в значительной степени следуют децентрализации. В то время как частные блокчейны имеют ограниченный вход проверенных участников.

ЗАЩИЩЕННОСТЬ СМАРТ-КОНТРАКТОВ

Технология блокчейн позволяет сократить роль посредников, обеспечивая самодостаточные цифровые контракты (так называемые смарт-контракты), выполнение которых не требует участия человека безопасным, надежным и неизменным способом. Появление блокчейна как революционной технологии сравнивают с Интернетом, и предсказывается, что он подорвет власть централизованных властей. Блокчейн, как услуга имеет многообещающий подход к поддержке деловое сотрудничество путем обеспечения прозрачности для всех заинтересованных сторон в случае возникновения конфликтов [2]. Однако интеграция блокчейна с внешними данными является одним из основных препятствий, препятствующих широкому внедрению.

В блокчейне термин оракул относится к объекту, который может получить доступ к внешним данным без ущерба для целостности блокчейна. Предполагается, что оракулы являются сторонними агентами, которым можно доверять и которые могут общаться с внешним миром и извлекать данные в блокчейн. Оракулы также могут подключать блокчейн к внешним базам данных. Таким образом, дорогостоящие вычисления могут выполняться вне блокчейна. Оракулы обеспечивают целостность извлеченных данных, предоставляя некоторые доказательства [2]. Таким образом, доказательства на основе криптографии, такие как те, которые используются Oraclize, 1 или надежные аппаратные доказательства, такие как те, которые используются системой Town Crier, которая использует Intel SGX [3], используются как часть ряда систем на основе оракула. Эти доказательства не только недостаточны для обеспечения защиты данных от несанкционированного доступа, но и непрактичны во многих реальных приложениях, где цифровые данные недоступны или требуется участие человека.

Оракулы могут демонстрировать злонамеренное поведение или быть неспособными выполнять свои задачи из-за нехватки возможностей и быть эгоистичными, не сообщая о своих реальных доступных ресурсах. Таким образом, размещение надежного механизма для выбора правильных оракулов играет важную роль в успехе сети блокчейн.

Смарт-контракты борются с основным ограничением работы с данными, которые находятся исключительно в сети блокчейн. Необходимость привлечения третьих лиц, известных как оракулы, для поддержки смарт-контрактов была признана с появлением технологии блокчейн. Оракулы могут быть девиантными и совершать злонамеренные действия или быть эгоистичными и скрывать свои фактически доступные ресурсы для получения оптимальной прибыли. Текущие исследовательские предложения используют оракулов в качестве доверенных объектов без надежного механизма оценки, что влечет за собой риск превращения их в централизованные точки отказа. Почему-то игнорируется необходимость в эффективном методе выбора наиболее экономичных и полезных оракулов, которые корыстны и действуют независимо.

В блокчейне термин оракул относится к объекту, который может получить доступ к внешним данным без ущерба для целостности блокчейна. Предполагается, что оракулы являются сторонними агентами, которым можно доверять и которые могут общаться с внешним миром и извлекать данные в блокчейн [1]. Оракулы также могут подключать блокчейн к внешним базам данных. Таким образом, дорогостоящие вычисления могут выполняться вне блокчейна.

ОРАКУЛЫ БЛОКЧЕЙНА

То, как оракул извлекает свои данные, зависит от того, полагается ли он на участие человека или полностью автоматизирован. Автоматизированные оракулы работают исключительно с помощью программного и аппаратного обеспечения, обращаясь к источнику данных и извлекая необходимые данные. Это означает, что оракул сам извлекает данные, а не является первоначальным источником данных. Автоматизированные оракулы предоставляют только детерминированные результаты запросов, поскольку они извлекают существующую информацию из источника данных. Однако это не относится к автономным оракулам или оракулам с участием человека. Эти оракулы способны не только передавать детерминированные данные, но и отвечать на произвольные запросы, которые трудно обработать на машине.

Системы Oracle могут быть централизованными или децентрализованными. Oraclize (теперь называется Provable) 2 – это централизованная служба оракула, основанная на веб-службе Amazon, которая обеспечивает обратную связь данных для смарт-контрактов и приложений блокчейна. Основное внимание Oraclize уделяет доказательству того, что полученные данные из первоисточника являются подлинными и неподделанными. Городской глашатай [4] также является централизованным потоком данных с проверкой подлинности, который работает как доверенный мост между существующими веб-сайтами с поддержкой HTTPS и Ethereum. Фактически, он использует надежное аппаратное и программное обеспечение, чтобы иметь возможность доказать, что задачи выполняются без вмешательства и результаты надежны. Однако, как и в случае с любым другим централизованным решением, его действительность зависит от центрального органа, и нет никакой гарантии, что задача будет выполнена правильно. Он также уделяет внимание надежному вводу данных в смарт-контракты, но ресурс данных вызывает сомнения. Chainlink [5] – это децентрализованная сеть оракулов на платформе Ethereum. Первоначально он направлен на предоставление защищенных от несанкционированного доступа данных для смарт-контрактов за счет доступа к ключевым ресурсам данных с использованием назначенных API. Chainlink работает с помощью моделей стимулирования и агрегации, однако у него есть проблемы с затратами и масштабируемостью. В другой попытке авторы Ma, Kaneko, Sharma [6] предложили децентрализованную систему оракулов, оснащенную механизмами проверки и оспаривания. АСТРЭЯ [6], представляет собой интересный децентрализованный оракул, работающий на основе игры с голосованием, чтобы определить правдивость предложений. Все избиратели делают некоторую ставку, чтобы иметь возможность проголосовать за случайно выбранное предложение. Авторы проанализировали теоретико-игровую структуру стимулов, чтобы доказать существование равновесия Нэша в предположении честности.

В двух словах, литература по блокчейн-оракулам ограничивается только автоматизированными решениями оракулов и проблемами доверия, связанными с передачей информации в смарт-контракты, и игнорирует вопросы доверия и качества, касающиеся самого источника данных. Автономные оракулы и оракулы, основанные на вмешательстве человека, не могут быть четко отделены от источника данных, и, насколько нам известно, нет предложений по решению проблемы надежности для этих типов оракулов, которые исследуются в данной статье.

АНАЛИЗ ЗАЩИЩЕННОСТИ СМАРТ-КОНТРКТОВ

Оракулы собирают информацию из реального мира и передают ее в блокчейн для дальнейшего использования. Следовательно, использование оракулов необходимо для содействия широкому внедрению смарт-контрактов. Тем не менее, исследования оракулов и их практического применения очень незрелые, основная проблема заключается в использовании интеллектуального механизма для выявления ненадежных и экономичных оракулов. Данная проблема может быть решена с помощью байесовской модели репутации, названной BLOR.

Ограничения разработки смарт-контрактов – технология BLOR на платформе Ethereum (консенсус PoW):

– Случайное число: в блокчейне нет чистого механизма генератора случайных чисел, потому что, когда код запускается другими узлами, все они должны достичь одного и того же результата для достижения консенсуса. Есть несколько возможных сценариев для генерации случайного числа, например, использование централизованной системы с использованием оракула, публично проверяемого обмена секретами или даже хэш-блока. BLOR использует номер блока для генерации хэш-числа, которое будет использоваться в качестве случайного числа. Это решение является практичным и эффективным, поскольку номер блока неизвестен до его создания.

– Ограниченное количество переменных: нет жесткого ограничения на количество переменных, но есть переменный предел, который в настоящее время составляет около 10 миллионов. Машинное обучение, искусственный интеллект и сложные алгоритмы бизнес-логики могут легко привести к высокому уровню больших переменных, если код не контролируется должным образом.

– Размер смарт-контракта: для смарт-контрактов Ethereum существует ограничение в 24 КБ, иначе они закончатся. Коды смарт-контрактов очень минималистичны, чтобы они могли работать быстрее, дешевле и, возможно, с меньшим количеством логических ошибок. Это ограничение может легко заблокировать разработку сложной логики, такой как алгоритмы машинного обучения и обучения с подкреплением. (Чтобы справиться с этой проблемой, BLOR использует как можно меньше операций чтения/записи; разделяет логику на функции только для чтения и записи, чтобы функции только для чтения можно было вызывать через Web 3 бесплатно или за небольшую плату; с возможностью распространения логики на несколько контрактов при необходимости).

– Плавающее число: блокчейн не поддерживает никаких плавающих/десятичных чисел с плавающей запятой. Причина в том, что все процессоры работают на основе бинарного механизма, а точного представления дробей в бинарном режиме нет, поэтому они округляются до ближайшего совпадения. По этой очень важной причине блокчейны не поддерживают числа с плавающей запятой. Даже для финансовых транзакций они ввели более мелкие единицы, такие как вэй, гвэй и т. д., вместо использования чисел с плавающей запятой. По сути, единственным поддерживаемым числовым типом данных в Ethereum является целое число (знаковое или беззнаковое). BLOR корректирует формулы путем масштабирования значений. (Например, если есть два числа с плавающей запятой, при масштабировании числа умножаются на 100).

– Расширенные математические функции: языки блокчейна по умолчанию не поддерживают сложные математические функции из-за различных проблем. В алгоритме BLOR используются сложные математические функции. (Для запуска BLOR на блокчейне, был создан новый контракт под названием «Math Contract». Математический контракт реализует необходимые функции, используя только четыре примитивные операции. Данный контракт поддерживает Sin, Cos, Log, экспоненту, гамма-функцию, квадратный корень (SQRT), бета-распределение и т. д. Данные функции разработаны в компании Solidity исключительно на основе целых чисел (без плавающей запятой) и примитивных операций.

Таблица 2

Преимущества и недостатки технологий Смарт-контрактов

Table 2

Advantages and Disadvantages of Smart Contract Technologies

Преимущества:	Безопасность и Распределенность Экономия средств и Точность Автоматизация и Скорость Гибкость и Настраиваемость Детерминированность и Компонуемость Неизменность и Повторное использование Нет доступа к данным за пределами сети блокчейна Резервное копирование Прозрачность и Более низкая стоимость
Недостатки:	Неизменность и Нехватка квалифицированных кадров Юридическая неопределенность и Возможность лазеек Неясные термины и Ошибки программного обеспечения

Типы уязвимостей:

1) Повторный вход.

Как самая известная уязвимость Ethereum, повторный вход рекурсивно запускает резервную функцию для кражи денег с баланса жертвы или истощения «газа» жертвы. Повторный вход происходит, когда внешним вызывающим объектам удается вызвать контракт вызываемого абонента до завершения выполнения исходного вызова. (подобное вызвано неправильным использованием функции remove() и call.value(amount) [6].

2) Злоупотребление tx.origin.

Когда видимость неправильно настроена для некоторых ключевых функций (например, некоторых конфиденциальных функций с модификатором public), дополнительный контроль разрешений имеет значение. Однако могут возникнуть проблемы, когда в контрактах используется устаревший tx.origin (особенно tx.origin==owner) для проверки вызывающих объектов на предмет управления разрешениями. Это имеет отношение к уязвимости контроля доступа в NCC Group. Когда пользователь U вызывает вредоносный контракт A, который намеревается переадресовать вызов контракту B. Контракт B основан на уязвимой проверке личности (например, require(tx.origin == owner) для фильтрации вредоносного доступа. Поскольку tx.orign возвращает адрес U (т. е. адрес владельца), вредоносный контракт A успешно выдает себя за U.

3) Неожиданный возврат.

В смарт-контракте некоторые операции могут, к сожалению, завершиться неудачно. Это может привести к двум основным последствиям: (1) «газ» (то есть плата за выполнение операции на платформе Ethereum) транзакции тратится впустую; (2) транзакция будет отменена, т.е. отказ в обслуживании (DoS). Атака типа «отказ в обслуживании» также называется «DoS с возвратом». Злоумышленник может намеренно вызвать сбой некоторых операций с целью DoS. Например, некоторые функции рекурсивно отправляют эфиры множеству пользователей. Если один из этих вызовов завершится ошибкой, вся транзакция будет отменена. Злоумышленник может намеренно провалить эту транзакцию, чтобы осуществить атаку типа «отказ в обслуживании».

4) Злоупотребление самоуничтожением.

Эта уязвимость позволяет злоумышленникам принудительно отправлять эфир, не активируя его резервную функцию. Обычно контракты содержат важную логику в резервной функции или выполнении расчетов на основе баланса контракта. Однако это можно обойти с помощью метода контракта самоуничтожения, который позволяет пользователю указать получателя для отправки избыточного эфира. То есть уязвимый контракт может быть использован для перевода всех денег на счет злоумышленника при отключении службы.

Таблица 3

Типы уязвимостей смарт-контрактов

Table 3

Types of Smart Contract Vulnerabilities

Уязвимости	**Механизм уязвимости**
Повторный вход	Рекурсивный вызов функции из резервной функции
Целочисленное переполнение/незаполнение	При выполнении сложения, вычитания или сохранении пользовательского ввода с целочисленными переменными, которые содержат ограничения по значениям, может произойти переполнение/недостаточное значение
Зависимость порядка транзакции	Несогласованные заказы транзакций относительно времени вызовов
Ограничение глубины стека вызовов	Превышение лимита на количество вызовов контрактного метода
Зависимость временной метки блока	Эта уязвимость возникает, когда контракт использует временную метку блока как часть условий для выполнения критической операции (отправки эфира) и используется вредоносным майнером
Аутентификация через tx.origin	Эта уязвимость возникает, когда контракт использует для авторизации tx.origin, что может быть скомпрометировано фишинговой атакой
DoS с неограниченными операциями	Эта уязвимость вызвана неправильным программированием с неограниченными операциями в контракте
Короткий адрес	EVM не проверяет валидность адресов

Уязвимости	Механизм уязвимости
Самоуничтожение/самоубийственный контракт	Контракт может быть уничтожен неавторизованными пользователями
Не проверено и не удалось отправить	Отправляйте эфиры без проверки условий
Необеспеченный баланс	Баланс эфира в контракте подвергается краже анонимным абонентом из-за модификатора public
Жадный контракт	Блокировка контрактного фонда или баланса эфира на неопределенный срок
Блудный контракт	Утечка средств или баланса эфира произвольным пользователям
Неправильно обработанные исключения	Когда в смарт-контракте вызывается исключение из другого контракта, и вызывающая сторона не управляет им должным образом
Перерасход «газа»	Выполнение кода контракта потребляет больше «газа» без необходимости

ЗАКЛЮЧЕНИЕ

Проведенный выше анализ, показывает, что помимо уязвимостей смарт-контрактов, связанных с платформами, где они реализуются, также имеют место уязвимости, связанные с программированием смарт-контрактов (уязвимости исходного кода), которые возникают вследствие недостаточности компетенций разработчика. В свою очередь, это авторы связывают с отсутствием единой и понятной методологии проектирования и разработки защищенных смарт-контрактов, а также средств верификации первых. Авторы полагают, что подобная методология и, основанные на ней, технологии могут быть разработаны с использованием теории системно-объектного моделирования [7,8]. Технология системно-объектного моделирования [9] может стать удобным инструментом для проектирования и верификации защищенных смарт-контрактов. Также, следует отметить, что технология системно-объектного имитационного моделирования позволяет симулировать выполнение смарт-контракта, и как следствие, позволит проверить его на адекватность, генерируемых им транзакций.

Список литературы

1. Алага А. и др. Целевая локализация с использованием мультиагентного глубокого обучения с подкреплением и проксимальной оптимизацией политик // Компьютерные системы будущего. – 2022. – Т. 136. – С. 342-357.
2. Ауэр П., Чеза-Бьянки Н., Фишер П. Анализ конечного времени задачи о многоруком бандите // Машинное обучение. – 2002. – Т. 47. – С. 235-256.
3. Байгин М. и др. Блокчейн-подход к интеллектуальным грузоперевозкам с использованием UHF RFID // Экспертные системы с приложениями. – 2022. – Т. 188. – С. 116030.
4. Бентахар Дж., Дроуэл Н., Садики А. Количественное групповое доверие: двухэтапный подход к проверке // Материалы 21-й Международной конференции по автономным агентам и мультиагентным системам. – 2022. – С. 100-108.
5. Беррихилл Р., Венерис А. ASTRAEA: децентрализованный блокчейн-оракул //Технические сводки IEEE по блокчейну. – 2019.
6. Чжан Ф. и др. Городской глашатай: аутентифицированный поток данных для смарт-контрактов // Материалы конференции aCM sIGSAC 2016 года по компьютерной и коммуникационной безопасности. – 2016. – С. 270-282.
7. Маторин С.И., Жихарев А.Г. Системно-объектный подход как основа общей теории систем // Научные ведомости БелГУ. Сер. Экономика. Информатика. – 2019. – Т. 46, № 4. – С. 717-730.
8. Matorin S.I., Zhikharev A.G. Accounting for system-wide regularities in the system-object modeling of organizational knowledge // Scientific and Technical Information Processing. – 2019. – Vol. 46, № 6. – P. 1-9.
9. Zhikharev A.G. Formalization of Knowledge by Tools of System-Object Simulation // Lecture Notes in Networks and Systems. – 2022. – Vol. 330. – P. 390- 399.

References

1. Alagha A. et al. Target localization using multi-agent deep reinforcement learning with proximal policy optimization //Future Generation Computer Systems. – 2022. – T. 136. – P. 342-357.
2. Auer P., Cesa-Bianchi N., Fischer P. Finite-time analysis of the multiarmed bandit problem // Machine learning. – 2002. – T. 47. – P. 235-256.
3. Baygin M. et al. A blockchain-based approach to smart cargo transportation using UHF RFID // Expert Systems with Applications. – 2022. – T. 188. – P. 116030.
4. Bentahar J., Drawel N., Sadiki A. Quantitative group trust: A two-stage verification approach // Proceedings of the 21st International Conference on Autonomous Agents and Multiagent Systems. – 2022. – P. 100-108.
5. Berryhill R., Veneris A. ASTRAEA: A decentralized blockchain oracle // IEEE Blockchain Technical Briefs. – 2019.
6. Zhang F. et al. Town crier: An authenticated data feed for smart contracts // Proceedings of the 2016 aCM sIGSAC conference on computer and communications security. – 2016. – P. 270-282.
7. Matorin S.I., Zhikharev A.G. System-object approach as the basis of the general theory of systems // Nauchnye Vedomosti BelSU. Ser. Economy. Computer science. - 2019. - T. 46, No. 4. - P. 717-730.
8. Matorin S.I., Zhikharev A.G. Accounting for system-wide regularities in the system-object modeling of organizational knowledge // Scientific and Technical Information Processing. – 2019. – Vol. 46, № 6. – P. 1-9.
9. Zhikharev A.G. Formalization of Knowledge by Tools of System-Object Simulation // Lecture Notes in Networks and Systems. – 2022. – Vol. 330. – P. 390- 399.

Жихарев Александр Геннадиевич, доктор технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем
Киданов Владислав Викторович, аспирант кафедры прикладной информатики и информационных технологий, Белгородский государственный национальный исследовательский университет
Фефелов Олег Сергеевич, магистрант кафедры информационных и робототехнических систем

Zhikharev Alexander Gennadievich, Doctor of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Automated Systems Software
Kidanov Vladislav Viktorovich, post-graduate student of the Department of Applied Informatics and Information Technologies
Fefelov Oleg Sergeevich, Master student of the Department of Information and Robotic Systems