DOI: 10.58168/CISMP2024_71-77
УДК 004.9

ОЦЕНКА СОСТОЯНИЙ БЛОКЧЕЙН-СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ МАРКОВСКИХ ПРОЦЕССОВ

А.А. Кривоногов[1], К.В. Стародубов[2], Р.В. Дорошенко[3], Ю.Ю. Громов[4]

[1]ФГАОУ ВО «Московский политехнический университет»
[2]ФГБОУ ВО «МИРЭА - Российский технологический университет»
[3] ООО «Региональные Системы Комплексной Безопасности»
[4]ФГБОУ ВО «Тамбовский государственный технический университет»

Аннотация. В статье рассмотрено применение марковских процессов для оценки состояний блокчейн-системы. Определены особенности использования модели марковского процесса в контексте определения множества возможных состояний блокчейн-системы, а также выявляются ключевые аспекты надежности и устойчивости ее функционирования. Проведена апробация предложенного подхода путем моделирования и определения состояний блокчейн-системы Ethereum при реализации деструктивных воздействий за счет вызова дефекта повторного входа.

Ключевые слова: смарт-контракты, моделирование деструктивных воздействий, граф переходов состояний, модель марковского процесса, метода противодействия.

ASSESSING STATES OF BLOCKCHAIN SYSTEM USING MARKOV PROCESSES

A.A. Krivonogov[1], K.V. Starodubov[2], R.V. Doroshenko[3], Yu. Yu. Gromov[4]

[1]Moscow Polytechnic University
[2] Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University
[3] LLC "Regional Systems of Comprehensive Security"
[4] Federal State Budgetary Educational Institution Tambov State Technical University

Abstract. The article considers the application of Markov processes to assess the states of a blockchain system. The peculiarities of using the Markov process model in the context of determining the set of possible states of the blockchain system are defined, and the key aspects of reliability and stability of its functioning are identified. The proposed approach is tested by modeling and determining the states of the Ethereum blockchain system when destructive influences are implemented by calling a reentrancy defect.

Keywords: smart contracts, modeling of destructive influences, state transition graph, Markov process model, countermeasure methods.

В современном мире технологий, блокчейн-системы и смарт-контракты становятся все более перспективными инструментами для различных сфер

деятельности. Смарт-контракты обеспечивают прозрачность, надежность и автоматизацию различных процессов, таких как управление активами, проведение голосований, управление цепочками поставок, регистрация интеллектуальной собственности и другие транзакции [1]. Однако для их успешного функционирования необходимо обеспечить надежность и устойчивость блокчейн-системы, которая должна быть способна выдерживать различные нагрузки и деструктивные воздействия со стороны злоумышленников, включая кибератаки и другие формы вмешательства, чтобы гарантировать непрерывность и целостность транзакций [2].

В этом контексте применение марковских процессов является ключевым инструментом и может быть использован в качестве подхода для обеспечения надежности функционирования и оценки состояний блокчейн-системы. Марковские процессы позволяют моделировать и анализировать поведение системы в различных условиях, включая вероятность возникновения ошибок, время восстановления после сбоев и общую стабильность блокчейн-системы [6]. Использование такого математического метода позволяет удобно описывать появление случайных событий в виде вероятностей переходов из одного состояния системы в другое, поскольку считается, что при переходе из одного состояния в другое система не учитывает обстоятельства того, как она попала в него [4, 7].

Для инициирования процесса моделирования состояний блокчейн-системы в качестве исходных данных следует определить три множества, описывающие модель блокчейн-системы с точки зрения возможной реализации деструктивных воздействий [5]:

- множество дефектов, характерных для блокчейн-системы и функционирующих в рамках нее смарт-контактов: $V = \{v_1, v_2, \ldots, v_n\}$, где $n \in \mathrm{N}$;
- множество деструктивных воздействий, характерных для блокчейн-системы и функционирующих в рамках нее смарт-контактов: $Th = \{th_1, th_2, \ldots, th_z\}$, где $z \in \mathrm{N}$;
- множество действий злоумышленника, реализующие деструктивные воздействия на блокчейн-систему и функционирующие в рамках нее смарт-контракты: $Int = \{int_1, int_2, \ldots, int_k\}$, где $k \in \mathrm{N}$.

Поскольку время $T = \{t_m\}$, где $m = \overline{1, \infty}$, то такая последовательность является марковской цепью. Если для каждого шага вероятность перехода блокчейн-системы и функционирующих в рамках нее смарт-контактов из любого состояния S_i в любое состояние S_j не зависит от того, когда и как она попала в состояние S_j, то состояние является случайным и характеризуется вероятностью P_{ij} [3]. Также необходимо представить множество состояний системы $S = \{S_j\}$, где $j = \overline{1, \infty}$.

Модель марковского процесса представляется в виде графа, в котором состояния (или вершины) связаны между собой связями (т.е. переходами из одного состояния в другое) [4, 5]. В конкретный момент времени система переходит в одно из состояний из множества S. Каждый переход

характеризуется вероятностью перехода P_{ij}, которая показывает, как часто после попадания в i-е состояние осуществляется переход в j-е состояние. При этом для каждого состояния сумма вероятностей всех переходов из него в другие состояния должна быть всегда равна 1. Пример графа переходов состояний при реализации деструктивных воздействий за счет вызова дефекта отказа в обслуживании с ограничением газа в блоке (или DoS with block gas limit) приведен на рис. 1.

Рисунок 1 – Пример графа переходов состояний блокчейн-системы

В соответствии с рисунком 1 и по результатам анализа исходных данных о дефекте определено множество возможных состояний $S = \{S_1, S_2, \ldots, S_6\}$, где: S_1 – первоначальное состояние блокчейн-системы, в рамках которой корректно функционирует смарт-контракт, а сама система обрабатывает все возникающие в ней исключения, S_2 – увеличение лимита газа в блоках, созданных злоумышленником, S_3 – медленная обработка блоков блокчейн-системы (нагрузка сети), S_4 – реализация двойного расходования, S_5 – снижение общей производительности и возникновение сбоев в блокчейн-системе, S_6 – отказ в обслуживании блокчейн-системы в целом.

Так, в случае, если блокчейн-система переходит из первоначального состояния в промежуточные, а затем возвращается в исходное состояние, то это свидетельствует о том, что в блокчейн-системе корректно настроены механизмы защиты. В противном случае при реализации деструктивных воздействий со стороны злоумышленника система не вернется в исходное состояние, вследствие чего потребуется внесение соответствующих изменений как в смарт-контракт, так и в блокчейн-систему, что, в некоторых случаях, может привести к разветвлению цепочек блоков и их последующей параллельной работе (или форку системы).

С целью апробации предложенного подхода в рамках статьи осуществлено моделирование деструктивных воздействий на блокчейн-систему Ethereum при реализации дефекта повторного входа. Дефект повторного входа является наиболее часто реализуемым в смарт-контрактах в блокчейн-системах на основе Ethereum. На основании анализа дефекта повторного входа определено множество возможных состояний блокчейн-системы Ethereum $S = \{S_1, S_2, \ldots, S_6\}$, где: S_1 – первоначальное состояние блокчейн-системы, в рамках которой корректно функционирует смарт-контракт, а сама система обрабатывает все возникающие в ней исключения, S_2 – блокирование

взаимодействия пользователей со смарт-контрактом, S_3 – разрушение отдельных управляющих блоков блокчейн-системы, S_4 – блокирование цифровых активов в смарт-контакте, S_5 – кража цифровых активов из смарт-контакта, S_6 – отказ в обслуживании блокчейн-системы в целом.

Состояния блокчейн-системы $S_2,\ldots,S_6$ характеризуют действия злоумышленника. Учитывая тот факт, что организационно-технические возможности злоумышленника заранее не известны, то в качестве распределения времени пребывания в том или ином состоянии целесообразным является использование равномерного распределения. Граф переходов состояний с вероятностями переходов блокчейн-системы из одного состояния в другое при реализации деструктивных воздействий за счет вызова дефекта повторного входа приведен на рис. 2.

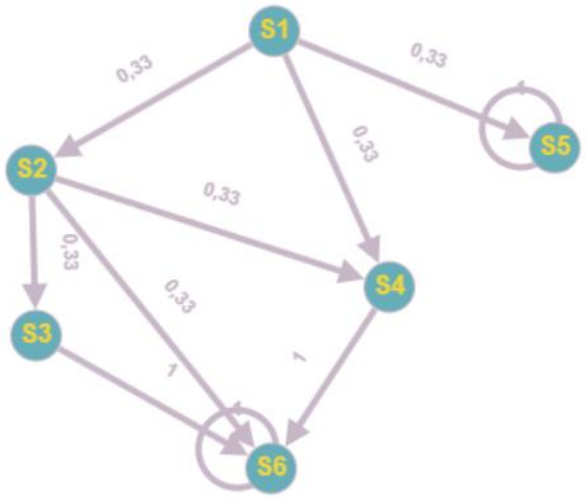

Рисунок 2 – Граф переходов состояний блокчейн-системы при реализации дефекта повторного входа

Для определения возможности перехода блокчейн-системы в исходное состояние S_1 необходимо определить множество мер и методов противодействия $Pr = \{pr_1,\ldots, pr_n\}$, где: pr_1 – применение автоматизированных средств анализа для определения смарт-контракта с функцией *call.value()* и использование вместо нее функций *send()* или *transfer()*; pr_2 – использование в блокчейн-системе узлов в режиме «холодного» резервирования для их экстренного поднятия в целях распределения нагрузки на систему в случае большого числа вредоносных запросов; pr_3 – вызов функции *selfdestruct()* для прекращения функционирования целевого смарт-контракта в блокчейн-системе. Граф переходов состояний при реализации деструктивных воздействий за счет вызова дефекта повторного входа с применяемыми мерами и методами противодействия приведен на рис. 3.

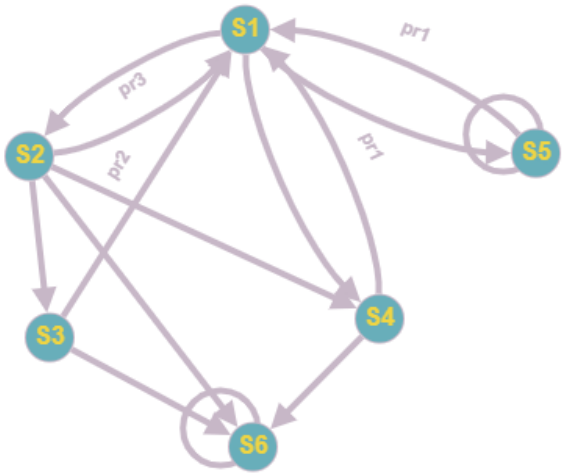

Рисунок 3 – Граф переходов состояний при реализации дефекта повторного входа с применяемыми мерами и методами противодействия

Из рис. 3 видно, что в некоторых случаях при реализации мер и методов противодействия блокчейн-система возвращается в исходное состояние S_1. При этом чем глубже злоумышленник преодолевает каждое из состояний системы S, тем, как правило, меры и методы противодействия становятся более трудными и нетривиальными в реализации.

По результатам анализа построенных графов переходов состояний при реализации дефекта повторного входа необходимым является определение наиболее вероятных цепочек переходов состояний для возможности формулирования дополнительных рекомендаций по улучшению как смарт-контракта, так и блокчейн-системы. На рис. 4 приведены наиболее вероятные цепочки переходов состояний блокчейн-системы при реализации дефекта повторного входа.

Рисунок 4 – Наиболее вероятные цепочки переходов состояний при реализации дефекта повторного входа

Из рис. 4 очевидно, что только цепочка (2) позволяет блокчейн-системе вернуться в исходное состояние, а для цепочек (1) и (3) потребуется формирование дополнительных рекомендаций.

Выводы

Использование предлагаемого подхода позволяет получить граф и цепочки переходов для различных состояний блокчейн-системы при реализации деструктивных воздействий за счет вызова дефекта со стороны злоумышленника, что в конечном итоге позволит учесть все недостатки и

разработать устойчивый смарт-контракт, тем самым обеспечивая неизменяемость и целостность той блокчейн-системы, в рамках которой он осуществляет свое функционирование. Кроме того, результаты исследования позволят разработать более эффективные механизмы защиты и поддержки функционирования блокчейн-системы, повысить ее устойчивость к различным видам деструктивных воздействий, а также оптимизировать процессы по восстановлению после сбоев.

Список литературы

1. Репин М.М., Кривоногов А.А. Проблемы обеспечения информационной безопасности смарт-контрактов в системах на основе технологии распределенных реестров. – М.: ООО «Издательство ТРИУМФ», 2020. – 115 с.

2. Кривоногов А.А., Репин М.М., Федоров Н.В. Методика анализа уязвимостей и определения уровня безопасности смарт-контрактов при размещении в системах распределенных реестров // Вопросы кибербезопасности. – 2020. – №4(38). – С. 56-65.

3. Цырульник В.Ф., Магазев А.А. Применение одной марковской модели безопасности для повышения надежности и выбора оптимальной конфигурации // Прикладная математика и фундаментальная информатика. 2019. № 1(6) – С. 25-32.

4. Щеглов К.А., Щеглов А.Ю. Марковские модели угрозы безопасности информационной системы // Приборостроение. 2015. Т. 58, №12. – С. 957-965.

5. Горохова В. Ф. Оптимизация выбора средств защиты от атак с использованием поглощающих марковских цепей // Системы управления, информационные технологии и математическое моделирование: сб. тр. по материалам IV Всероссийской научно-практической конференции с международным участием: в 2 т. Т. 1. 2022. – С. 126-134.

6. Токарев В.Л. Скрытые марковские модели в задаче обнаружения атак на компьютерные сети // Чебышевский сборник. 2021. №5 (81). – С. 391-399.

7. Корниенко А. А., Никитин А. Б., Диасамидзе С. В., Кузьменкова Е. Ю. Моделирование компьютерных атак на распределенную информационную систему // Известия Петербургского университета путей сообщения. 2018. №4. – С. 613-626.

References

1. Repin M.M., Krivonogov A.A. Problems of information security of smart contracts in systems based on distributed registers technology. – M.: LLC «Publishing house TRIUMF», 2020. – 115 p.

2. Krivonogov A.A., Repin M.M., Fedorov N.V. Methodology for analyzing vulnerabilities and determining the security level of smart contracts when placed in distributed registry systems // Cyber security issues. – 2020. – pp. 56-65.

3. Tsyrulnik, V.F., Magazev, A.A. Application of one Markov hazard-free model for reliability improvement and optimal configuration selection // Applied Mathematics and Fundamental Informatics. 2019. № 1(6) – pp. 25-32.

4. Shcheglov K.A., Shcheglov A.Yu. Markov models of the security threat of the information system // Instrumentation. 2015. T. 58, №12. – pp. 957-965.

5. Gorokhova V. F. Optimization of the choice of means of protection against attacks using absorbing Markov chains // Control Systems, Information Technologies and Mathematical Modeling: proceedings of the IV All-Russian Scientific and Practical Conference with International Participation: in 2 vol. T. 1. 2022. – pp. 126-134.

6. Tokarev, V.L. Hidden Markov models in the task of detecting attacks on computer networks // Chebyshev Collection. 2021. №5 (81). – pp. 391-399.

7. Kornienko A. A., Nikitin A. B., Diasamidze S. V., Kuzmenkova E. Yu. Modeling of computer attacks on distributed information system // Izvestiya of St. Petersburg University of Railway Engineering. 2018. №4. – pp. 613-626.