DOI: 10.58168/CISMP2024_357-361
УДК 004.9

ПОДХОД К ОЦЕНКЕ УРОВНЯ ИСХОДНОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН-СИСТЕМЫ ДЛЯ СМАРТ-КОНТРАКТОВ

А.А. Кривоногов[1], К.В. Стародубов[2], А.В. Прокофьев[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. Статья посвящена вопросу обеспечения устойчивости блокчейн-систем и их влиянию на функционирование смарт-контрактов, осуществляющих автоматизацию сложных процессов. Предложен подход к определению исходной устойчивости блокчейн-системы, который включает в себя оценку эксплуатационных и технических характеристик блокчейн-системы с использованием метода прямой экспертной оценки. Проведена апробация предложенного подхода на примере блокчейн-системы Ethereum.

Ключевые слова: характеристики блокчейн-системы, прямая экспертная оценка, уровень устойчивости, технология, консенсус.

APPROACH TO ASSESSING THE INITIAL SUSTAINABILITY LEVEL OF A BLOCKCHAIN SYSTEM FOR SMART CONTRACTS

A.A. Krivonogov[1], K.V. Starodubov[2], A.V. Prokofyev[3], Y.Y. 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 is devoted to the issue of sustainability of blockchain systems and their impact on the functioning of smart contracts that automate complex processes. An approach to determining the initial stability of a blockchain system is proposed, which includes the assessment of operational and technical parameters of the blockchain system using the method of direct expert evaluation. The proposed approach is tested on the example of the blockchain Ethereum.

Keywords: blockchain system parameters, direct expert assessment, sustainability level, technology, consensus.

В последние годы блокчей-системы и смарт-контракты переживают стремительный рост и широкое внедрение в различных отраслях, в том числе в финансовой и банковской сфере, а также в области военной промышленности.

С повсеместным развитием данных технологий особую актуальность и остроту приобретает вопрос обеспечения устойчивости блокчейн-систем [1, 2].

Необходимость определения исходной устойчивости блокчейн-системы является особенно важной для возможности принятия решения о функционировании в рамках нее смарт-контрактов [2]. Смарт-контракты позволяют автоматизировать сложные процессы и обеспечивать прозрачность выполнения транзакций, но они могут работать эффективно только в случае, если сама блокчейн-система является устойчивой [6]. В статье описывается подход к определению исходной устойчивости блокчейн-системы, в которой предполагается функционирование смарт-контракта.

Под исходной устойчивостью понимается обобщенный параметр блокчейн-системы, зависящий от ее технических особенностей и эксплуатационных характеристик. Так, параметр исходной устойчивости блокчейн-системы определяется с использованием метода прямой экспертной оценки [3] на основании эксплуатационных и технических характеристик, приведенных в таблице 1 [1, 4].

Таблица 1 – Эксплуатационные и технические характеристики блокчейн-системы

Технические особенности и эксплуатационные характеристики системы	Уровень устойчивости		
	Низкий	Средний	Высокий
1. По используемому типу блокчейн-системы	Инклюзивный	Федеративный (консорциум)	Эксклюзивный
2. По используемому алгоритму консенсуса	Proof-of-Work, Proof-of-Stake	Proof-of-Authority, Raft и др.	Proof-of-Elapsed-Time, семейство Byzantine Fault Tolerant
3. По используемому языку описания и улучшения блокчейн-системы	PHP, JavaScript, Python	Java, Rust	C++, Go, Simplicity
4. По количеству узлов в блокчейн-системе	От 1 до 10	От 11 до 100	От 101 и более
5. По используемым механизмам обеспечения конфиденциальности	Не применяются в рамках блокчейн-системы	Возможность использования гомоморфного шифрования и/или обфускации кода	Возможность использования интерактивного/ неинтерактивного доказательства с нулевым разглашением (ZKP/NIZKP)
6. По используемому языку программирования смарт-контракта	Solidity, JavaScript	Java, Vyper, Rust, C#	Низкоуровневые языки программирования (байт-код) (например, Michelson и др.)
7. По использованию	Использование	Использование как	Использование

механизма «оракулов» в блокчейн-системе (программные/аппаратные)	недоверенных источников внешних данных	доверенных, так и недоверенных источников внешних данных	ограниченного пула доверенных источников внешних данных
8. Число обрабатываемых транзакций в секунду (TPS)	До 100 TPS	От 101 до 1000 TPS	От 1001 и более
9. Использование сертифицированного СКЗИ и ГОСТ-криптографии в блокчейн-системе	Не реализовано в блокчейн-системе	–	Реализовано в блокчейн-системе
10. Возможность динамического обновления смарт-контракта	Не реализовано (смарт-контракты являются частью блокчейн-системы)	Реализовано за счёт обращения к ограниченному кругу участников (централизованный способ)	Реализовано (в том числе при использовании Proxy-контрактов)

По результатам определения каждой из эксплуатационных и технических характеристик из таблицы 1 для конкретно исследуемой блокчейн-системы далее определяется исходный уровень устойчивости блокчейн-системы:

- Блокчейн-система имеет высокий уровень исходной устойчивости, если не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему уровню устойчивости и при этом ни одна из характеристик не должна соответствовать уровню «низкий»;
- Блокчейн-система имеет средний уровень исходной устойчивости, если не менее 70% характеристик соответствуют уровню не ниже «средний», а остальные – низкому уровню устойчивости;
- Блокчейн-система имеет низкий уровень исходной устойчивости, если не выполняются соответствующие условия по п. 1 и 2.

Условия определения исходного уровня устойчивости для исследуемой блокчейн-системы приведены в таблице 2.

Таблица 2 – Условия определения уровня исходной устойчивости блокчейн-системы

Общий уровень исходной устойчивости блокчейн-системы	Уровень устойчивости по характеристикам		
	Низкий	Средний	Высокий
Высокий уровень исходной устойчивости	0%	$\sum \leq 30\%$	$\sum \geq 70\%$
Средний уровень исходной устойчивости	$\sum \leq 30\%$	$\sum \geq 70\%$	$\sum < 70\%$
Низкий уровень исходной устойчивости	$\sum < 70\%$	$\sum < 70\%$	$\sum > 0\%$

Таким образом, по результатам оценки уровень исходной устойчивости исследуемой блокчейн-системы принимает одно из трех возможных значений (низкий, средний или высокий), которым соответствуют числовые показатели (от 1 до 3 соответственно).

С целью апробации предложенного подхода в рамках статьи определяется уровень исходной устойчивости блокчейн-системы Ethereum. Ethereum представляет собой универсальную, открытую и децентрализованную программную систему, построенную на основе блокчейна [5]. Она является одной из наиболее популярных и ведущих блокчейн-систем, которая поддерживает смарт-контракты, обеспечиваемые протоколом консенсуса [2, 5].

Для определения уровня исходной устойчивости блокчейн-системы Ethereum следует обратиться к перечню эксплуатационных и технических характеристик из табл. 1 и применить их к блокчейн-системе Ethereum. Эксплуатационные и технические характеристики для блокчейн-системы Ethereum приведены в табл. 3.

Таблица 3 – Эксплуатационные и технические характеристики блокчейн-системы Ethereum

Технические особенности и эксплуатационные характеристики системы	Принимаемое значение
1. По используемому типу блокчейн-системы	Инклюзивный
2. По используемому алгоритму консенсуса	Proof-of-Stake
3. По используемому языку описания и улучшения блокчейн-системы	C++, Go
4. По количеству узлов в блокчейн-системе	От 101 и более
5. По используемым механизмам обеспечения конфиденциальности	Не применяются в рамках блокчейн-системы
6. По используемому языку программирования смарт-контракта	Solidity
7. По использованию механизма «оракулов» в блокчейн-системе	Использование недоверенных источников внешних данных
8. Число обрабатываемых транзакций в секунду (TPS)	До 100 TPS
9. Использование сертифицированного СКЗИ и ГОСТ-криптографии в блокчейн-системе	Не реализовано в блокчейн-системе
10. Возможность динамического обновления смарт-контракта	Реализовано

Исходя из данных, приведенных в табл. 3, и условий определения уровня исходной устойчивости, приведенных в табл. 2, можно сделать вывод о том, что блокчейн-система Ethereum имеет низкий уровень исходной устойчивости и параметр принимает значение, равное 1.

Выводы

Использование предлагаемого подхода позволяет с достаточной точностью и на основе экспертного мнения определить уровень исходной устойчивости блокчейн-системы. Данный параметр также может быть использован в качестве одного из ключевых составных параметров при оценке устойчивости смарт-контракта, функционирующего в конкретно рассматриваемой блокчейн-системе.

Список литературы

1. 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.

2. 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.

3. Зверев Е., Никифоров А. Экспертная выборка: формирование для большой совокупности // МСФО и МСА в кредитной организации. 2019. № 2(72). – С. 68-74.

4. 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. Т. 15. № 4. – С. 613-628.

5. Фролов А.В. Создание смарт-контрактов Solidity для блокчейна Ethereum. Практическое руководство. - М.: ЛитРес: Самиздат, 2019. – 240 с.

6. Андрианов А.С., Вечеркин В.Б., Прохоров М.А., Цветков А.Ю. Разработка подхода к автоматизации процесса первичной обработки исходных данных для анализа устойчивости автоматизированных систем специального назначения в условиях деструктивных воздействий // Известия ТулГУ. Технические науки. 2018. №10. – С. 463-472.

References

1. 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.

2. 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.

3. Zverev E., Nikiforov A. Expert sampling: formation for a large population // IFRS and ISA in credit organization. 2019. № 2(72). – pp. 68-74.

4. Kornienko A.A., Nikitin A.B., Diasamidze S.V., Kuzmenkova E.Yu. Modeling of computer attacks on the distributed information system // Proceedings of St. Petersburg University of Railway Engineering. 2018. T. 15. № 4. – pp. 613-628.

5. Frolov A.V. Creating Solidity smart contracts for Ethereum blockchain. A practical guide. - M.: LitRes: Samizdat, 2019. – 240 p.

6. Andrianov A.S.; Vecherkin V.B.; Prokhorov M.A.; Tsvetkov A.Yu. Development of the approach to the automation of the initial data processing for the stability analysis of the automated systems of special purpose in the conditions of destructive influences // Izvestiya TulSU. Technicheskie nauki. 2018. №10. – pp. 463-472.