УДК 004.056.5

К. Ф. Шакиров [1], И. Д. Пелымская [1], А. С. Асманова [1]

[1] ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», г. Москва, Российская Федерация

ВЛИЯНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ НА БЛОКЧЕЙН-СИСТЕМЫ

Аннотация. В статье рассматривается влияние квантовых вычислений на блокчейн-системы, описываются различные механизмы консенсуса, такие как Proof-of-Work и Proof-of-Stake. Также анализируется потенциальная уязвимость этих систем перед квантовыми алгоритмами Шора и Гровера. Статья подчеркивает необходимость разработки квантовых криптографических алгоритмов для обеспечения долгосрочной безопасности блокчейн-систем в условиях быстрого развития технологий.

Ключевые слова: блокчейн-системы, квантовые вычисления, механизмы консенсуса, квантовая угроза, алгоритм Шора, алгоритм Гровера.

K. F. Shakirov [1], I. D. Pelymskaya [1], A. S. Asmanova [1],

[1] Plekhanov Russian University of Economics, Moscow, Russian Federation

THE IMPACT OF QUANTUM COMPUTING ON BLOCKCHAIN SYSTEMS

Absract. The article examines the impact of quantum computing on blockchain systems, describes various consensus mechanisms such as Proof-of-Work and Proof-of-Stake. The potential vulnerability of these systems to Shor and Grover's quantum algorithms is also analyzed. The article highlights the need to develop quantum cryptographic algorithms to ensure the long-term security of blockchain systems in the context of rapid technology development.

Keywords: blockchain systems, quantum computing, consensus mechanisms, quantum threat, Shor's algorithm, Grover's algorithm.

Введение. В этой статье проведен анализ криптографических алгоритмов и их математической сложности. Одна из задач рассмотреть различные способы применения блокчейна, а также квантовые вычисления и технологии, которые могут повлиять на работу этих систем. В современном мире технологии блокчейн-системы получили большое распространение и используются в разных сферах деятельности. Общество чаще всего их ассоциируют с криптовалютами, что верно. На данном этапе развития тема криптовалют особенно популярна, но не многие знают, что блокчейн активно применяется и в других сферах. Преимущество, которое делает эту технологию столь популярной, объясняется их возможностью передачи информации без привлечения третьей стороны. Помимо этого, процессы, проходящие в данном распределенном реестре, обеспечивают сохранность данных благодаря механизмам консенсуса. Они представляют собой алгоритм для достижения согласия между узлами сети о том, что транзакция действительна [1].

Механизмы консенсуса. Одними из самых распространенных механизмов достижения консенсуса являются Proof-of-Work и Proof-of-Stake. Механизм консенсуса Proof-of-Work, позволяющий сети, где ресурсы и данные распределены между многими узлами, достичь соглашения о состоянии данных за счет решения каждым участником сети сложной вычислительной задачи. Этот процесс необходим для создания нового блока транзакций и добавления его в блокчейн. Данный механизм является достаточно затратным, так как использует много вычислительных ресурсов. Альтернативой ему является механизм Proof-of-Stake, принцип работы которого заключается в блокировании (стейкинге) участниками своих токенов в качестве залога, чтобы претендовать на право создания нового блока и владения им. И чем больше токенов застейковано, тем выше вероятность быть выбранным. Такая процедура достижения консенсуса достаточно энергоэффективная и масштабируема, в отличие от предыдущего алгоритма. Но до недавнего времени эти механизмы и классические криптографические элементы обеспечивали должную безопасность, но с развитием квантовых

вычислений и технологий ситуация может сильно измениться. Есть риск того, что со значительным увеличением мощности вычислительных машин данные алгоритмы потеряют свой первоначальный статус и популярность. В настоящее время существует так называемая квантовая угроза. Но если вовремя рассмотреть данную проблему и начать продумывать варианты внедрения квантовых новшеств в блокчейн-системы, можно обеспечить их бесперебойную и высокоэффективную работу еще на несколько десятков лет.

Квантовые технологии. В действительности квантовые технологии активно набирают свои обороты, несмотря на полярные точки зрения. С одной стороны, это прорыв в технологиях и новые вычислительные возможности, с другой стороны, это серьезный шаг, который существенно и, возможно, революционно повлияет на все сферы жизни. Квантовые технологии представляют собой передовые инновации, базирующиеся на принципах квантовой механики, которые не могут быть интерпретированы в контексте классических физических теорий, таких как законы движения Ньютона, уравнения термодинамики и уравнения Максвелла для электромагнетизма [6, 7].

Квантовые состояния значительно повышают производительность обработки большого количества информации. Данный процесс может быть достигнут, потому что используется меньшее количество квантовых битов – кубитов, кодирующих больший объем данных. Для сравнения в классическом компьютере для кодирования определенного объема информации требуется 2^n бит, тогда как в квантовом достаточно n кубит. А также кубиты могут находиться в суперпозиции состояний и быть запутанными друг с другом, то есть они находятся сразу в состояниях 0 и 1[8-9]. Используя эти свойства, ученые Питер Шор и Гровер, разработали архитектуру и алгоритмы, которые способны улучшить производительность блокчейн-систем.

Квантовый алгоритм Шора. Квантовый алгоритм Шора, разработанный Питером Шором в 1994 году, представляет собой одно из наиболее значительных достижений в области квантовых вычислений. Этот алгоритм предназначен для решения задачи факторизации больших целых чисел, что имеет важное значение для криптографии и безопасности информации. Рассмотрим основные принципы работы алгоритма Шора, его важность для криптографии и приведем пример его применения [2]. Для начала необходимо вспомнить основное понятие факторизации – это процесс разложения числа на простые множители. Например, число 15 можно разложить на множители 3 и 5. Что касается самого алгоритма, то он состоит из двух частей: классической и квантовой. Под классической частью понимается следующее: выбирается случайное число a, которое является взаимно простым с факторизируемым числом N. Далее вычисляется наибольший общий делитель (НОД) чисел a и N с помощью алгоритма Евклида, и если НОД не равен 1, то, значит, найден нетривиальный делитель числа N, который также отличен от самого числа. Следующим шагом вычисляется порядок – r числа a по модулю N, то есть наименьшее положительное число r, такое что $a^r \equiv 1 \pmod N$. Квантовая часть включает в себя эффективное вычисление порядка r, применение квантового преобразования Фурье (QFT) для определения периода функции $f(x) = a^x \bmod N$. Таким образом измерение квантовой системы дает значение, позволяющее определить период r. Проверить результат работы можно следующим образом:

1. Если r четное и $a^{r/2} \not\equiv -1 \pmod N$, то можно найти делители N с помощью алгоритма Евклида;
2. Если условия не выполняются, процесс повторяется с другим случайным числом a.

На примере данный алгоритм можно представить так – рассмотрим факторизацию числа N = 15 с использованием алгоритма Шора.

1. Выбираем случайное число a = 2;
2. Вычисляем порядок r числа 2 по модулю 15;
3. Применяем квантовую часть алгоритма для определения периода функции $f(x) = 2^x \bmod 15$;

4. Получаем период r = 4;
5. Проверяем условия: r четное и $2^{r/2} \not\equiv -1 \pmod{15}$;
6. Находим делители N: $\gcd(2^{r/2} - 1, 15) = 5$ и $\gcd(2^{r/2} + 1, 15) = 3$.

Таким образом, число 15 факторизуется на простые множители 3 и 5.

Алгоритм Шора имеет огромное значение для криптографии, так как многие современные криптосистемы, такие как RSA, основаны на сложности факторизации больших чисел. Если квантовый компьютер с достаточным количеством кубитов будет создан, он сможет эффективно факторизовать большие числа, но при этом он поставит под угрозу безопасность этих криптосистем. Но благодаря использованию принципов квантовой механики алгоритм Шора потенциально может значительно ускорить процесс факторизации по сравнению с классическими методами. Это открывает новые возможности для развития криптографических систем, способных противостоять угрозам со стороны квантовых вычислений [3].

Квантовый алгоритм Гровера. Второй алгоритм, который был разработан Ловом Гровером в 1996 году и предназначен для решения задачи неструктурированного поиска. Рассмотрим множество элементов, среди которых требуется найти определенные элементы, удовлетворяющие заданному условию. Классический подход предполагает последовательную проверку каждого элемента, что в худшем случае требует проверки всех элементов. Эту задачу для наглядности можно описать на примере стога сена, в котором спрятано несколько иголок. Задача состоит в том, чтобы найти все иглы. В классическом случае, если стог сена не упорядочен, то придется проверять каждый элемент по очереди, пока не найдете иголку. В худшем случае, если иголок всего одна, вам придется проверить все элементы стога. Алгоритм Гровера позволяет найти хотя бы одну иголку в стоге сена квадратно быстрее, чем любой классический алгоритм. Если описывать более структурно, то квантовый алгоритм Гровера начинается с инициализации квантового состояния, которое представляет все возможные элементы исследуемого множества. Это состояние обычно формируется как равномерная суперпозиция всех элементов, что достигается с помощью операций Адамара. Далее вводится оракул, который играет ключевую роль в алгоритме.

Оракул представляет собой квантовую операцию, которая "отмечает" те состояния, которые соответствуют искомым элементам. Это достигается путем применения фазового сдвига к состояниям, удовлетворяющим условию поиска, оставляя неизменными остальные состояния. После применения оракула алгоритм переходит к инверсии относительно среднего. Эта операция представляет собой унитарное преобразование, которое увеличивает амплитуду вероятности состояний, отмеченных оракулом, и уменьшает амплитуду остальных состояний. Инверсия относительно среднего эффективно выделяет искомые состояния, повышая их вероятность измерения. Шаги применения оракула и инверсии относительно среднего повторяются определенное количество раз, оптимальное число которых составляет приблизительно квадратный корень из числа элементов множества. Это количество итераций обеспечивает максимальную вероятность успешного измерения искомого состояния. В заключительной стадии алгоритма производится измерение квантового состояния. В результате измерения с высокой вероятностью будет получен один из искомых элементов, что и является конечной целью алгоритма Гровера. Таким образом, квантовый алгоритм Гровера эффективно решает задачу неструктурированного поиска, демонстрируя квадратичное ускорение по сравнению с наилучшими классическими алгоритмами [4].

Алгоритм Гровера хорошо применим для задач оптимизации, цель которых состоит в нахождение экстремума (максимума или минимума) некоторой целевой функции. Особенно он актуален в случаях, когда пространство для поиска достаточно велико. Классические методы, как полный перебор, метод ветвей и границ, градиентного спуска и подобные им, могут быть вычислительно затратными и неэффективными. Преимущества данного алгоритма в том, что он позволяет найти оптимальное решение за время, пропорциональное квадратному корню от

размера пространства поиска, что значительно быстрее обычного перебора. Алгоритм Гровера также достаточно гибкий, поэтому его можно адаптировать для разных задач оптимизации.

Есть и некоторые ограничения, с которыми можно столкнуться в процессе применения этого алгоритма. На данный момент алгоритм может найти локальный, но не глобальный оптимум. И, помимо этого, он эффективен только когда у нас много данных с которыми необходимо работать, в случаях, когда набор информации невелик лучше использовать классические методы. Пример работы алгоритма можно рассмотреть на попытке взлома симметричных шифров, таких как AES, DES и blowfish, которые используют один и тот же ключ для шифрования и дешифрования данных. Классических подход к взлому симметричного шифра – полный перебор возможных ключей, что достаточно долго. В свою очередь алгоритм Гровера позволяет ускорить полный перебор в квадрат раз, что делает некоторые симметричные шифры уязвимыми. Для шифра AES-128, использующего 128-битный ключ, существует 2^{128} возможных ключей, и известный и привычный полный перебор займет колоссальное время выполнение этой операции. А квантовый алгоритм найдет ключ примерно за 2^{64} итераций, что значительно быстрее.

Вывод. При введении алгоритма Гровера и других высокоэффективных методов необходимо предотвратить возможность утечки данных и для этого необходимо использовать более длинные ключи, например AES-256, что снижает риск квантовых атак. Также следует заниматься разработкой новых криптографических алгоритмов, которые будут безопасны даже при квантовых вычислениях. С одной стороны квантовые вычисления представляют собой серьезную угрозу для существующих блокчейн-систем, с другой – открывают новые возможности для их развития и усовершенствования. Рассмотрение и реализация этих технологий позволит обеспечить долгосрочную устойчивость и эффективность блокчейн-систем в условиях быстро меняющейся вычислительной среды [5].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Орлова И.В. Квантовые вычисления: принципы и алгоритмы // Наука и техника. – Москва, 2023. – С. 5-17.
2. Смирнова А.Н. Постквантовая криптография и безопасность: Теория и практика // ИТ-Издательство. – Санкт-Петербург, 2022. – С. 34-39.
3. Сафарли А.Х. Технология блокчейн, как акселератор развития цифровизации в финансовом секторе экономики // Теоретическая и прикладная экономика. – 2022. – № 4. – С. 22-26. DOI: 10.25136/2409-8647.2022.4.39463
4. Крэндалл Р., Померанс К. Простые числа: Криптографические и вычислительные аспекты / под ред. В. Н. Чубарикова ; пер. А. В. Бегунца [и др.]. — М. : УРСС: Книжный дом «ЛИБРОКОМ», 2011. — 664 с.
5. Борисова В.В., Дегтярев Д.В. Реализация алгоритма квантовой факторизации Шора // Вестник АмГУ. – 2023. – Выпуск 103. – С. 3-9.
6. Маслов И.О., Бачило А.О., Черкесова Л.В. Повышение быстродействия квантового алгоритма Гровера путем применения инверсии вокруг среднего // Молодой исследователь Дона.
7. Аллабердиев К.Дж. Влияние квантовых вычислений на информационные системы // Международный научный журнал «Всемирный ученый». – Выпуск №30. – Том 1.
8. Гареев А., Уривский А., Кулик С. Квантовые технологии: кому и зачем это нужно? // Конференция МГУ им. М.В. Ломоносова. – 2021.
9. Ваулин А.Е. Квантовая вычисления и криптология // Хабр. – 17.07.2020.
10. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография: учебное пособие. – М.: МГУ им. М.В. Ломоносова, факультет ВМК. – 106 с.
11. Золотарёв Я. Как машинное обучение помогает в работе квантовых компьютеров // Журнал Яндекс Образование. – 20.04.2023.

12. Росляков И. Как работает квантовая логика и шифрование // КОД журнал Яндекс Практикума.

13. Шнайдер Джош, Смоллей Иэн. Что такое квантовая криптография? // IBM.

14. Internet Engineering Task Force (IETF). Hybrid Public Key Encryption: RFC 9180. — 2022.

15. National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4). U.S. Department of Commerce.

16. International Organization for Standardization. Blockchain and distributed ledger technologies — Vocabulary: ISO 22739:2024. — 2024.

17. Bill White, Gregg Arquero, Ritu Bajaj, Anne Dames, Gloria Ho, Richard Kisley, Henrik Lyksborg, Navya Ramanjulu, Jacob Ruwald and Charu Tejwani – Transitioning to Quantum-Safe Cryptography on IBM Z 22.12.2025.

REFERENCES

1. I.V. Orlova – Quantum computing: Principles and Algorithms // Moscow, Science and Technology, 2023, pp. 5-17.

2. A.N. Smirnova – Post-Quantum cryptography and security: Theory and practice // St. Petersburg, IT Publishing House, 2022, pp. 34-39.

3. Safarli A.H. – Blockchain technology as an accelerator for the development of digitalization in the financial sector of the economy // Theoretical and applied economics. – 2022. – No. 4, From 22-26. DOI: 10.25136/2409-8647.2022.4.39463

4. Crandall R., Pomerance K. Prime numbers: Cryptographic and computational aspects / edited by V. N. Chubarikov ; translated by A.V. Begunts [and others]. Moscow : URSS: LIBROCOM Book House, 2011. — 664 p.

5. Borisova V.V., Degtyarev D.V. Implementation of the Shor quantum factorization algorithm // Bulletin of the AmSU. Issue 103, 2023. pp. 3-9

6. Maslov I.O., Bachilo A.O., L.V. Cherkesova Improving the performance of Grover's quantum algorithm by applying inversion around the average // Young Researcher of the Don. UDC 004.056.5

7. Allaberdiev K.J. – The influence of quantum computing on information systems // International Scientific Journal "World Scientist" Issue No. 30, Volume 1

8. Arsen Gareev, Alexey Urivsky, Sergey Kulik – Quantum technologies: who needs it and why? // Lomonosov Moscow State University Conference on July 1, 2021

9. Vaulin A.E. – Quantum computing and cryptology // Habr 07/17/2020

10. D.A.Kronberg, Yu.I.Ozhigov, A.Yu.Chernyavsky – Quantum Cryptography Textbook of Lomonosov Moscow State University, Faculty of Higher Education, pp. 5-106

11. Yaroslav Zolotarev – How machine learning helps in the work of quantum computers // Yandex Education Magazine 04/20/2023

12. Igor Roslyakov – How Quantum Logic and Encryption work // Yandex Practicum CODE Magazine

13. Josh Schneider, Ian Smalley – What is Quantum Cryptography? // IBM

14. Engineering Task Force (IETF). Hybrid Public Key Encryption: RFC 9180. — 2022

15. National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4). U.S. Department of Commerce

16. International Organization for Standardization. Blockchain and distributed ledger technologies — Vocabulary: ISO 22739:2024. — 2024

17. Bill White, Gregg Arquero, Ritu Bajaj, Anne Dames, Gloria Ho, Richard Kisley, Henrik Lyksborg, Navya Ramanjulu, Jacob Ruwald and Charu Tejwani – Transitioning to Quantum-Safe Cryptography on IBM Z 22.12.2025

Информация об авторах

Кирилл Фаридович Шакиров – старший преподаватель с в/о, кафедра «Информатика», РЭУ им. Г.В. Плеханова, г. Москва, e-mail: shakirov.kf@rea.ru

Ирина Дмитриевна Пелымская – бакалавр, РЭУ им. Г.В. Плеханова, г. Москва, e-mail: irapelymsckaya@gmail.com

Анастасия Сергеевна Асманова – бакалавр, РЭУ им. Г.В. Плеханова, г. Москва, e-mail: anastasiyaasmanova@gmail.com

Authors

Kirill Faridovich Shakirov – Senior Lecturer at the Department of Computer Science, Plekhanov Russian University of Economics, Moscow, e-mail: shakirov.kf@rea.ru

Irina Dmitrievna Pelymskaya – Bachelor's degree, Plekhanov Russian University of Economics, Moscow, e-mail: irapelymsckaya@gmail.com

Anastasia Sergeevna Asmanova – Bachelor's degree, Plekhanov Russian University of Economics, Moscow, e-mail: anastasiyaasmanova@gmail.com

Для цитирования

Шакиров К.Ф., Пелымская И.Д., Асманова А.С. Влияние квантовых вычислений на блокчейн-системы // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2026. – №1. – С. 1-5 – Режим доступа: http://ismm-irgups.ru/toma/129-2026, свободный. – Загл. с экрана. – Яз. рус., англ.

For citations

Shakirov K.F., Pelymskaya L.D., Asmanova A.S. The impact of quantum computing on blockchain systems // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2026. No. 1. P. 1-5.