پیشنهاد پژوهشی

ادغام رمزنگاری کوانتومی با بلاک‌چین به عنوان راهکاری برای مقابله با تهدیدات امنیتی آینده

هدی جنتی

فروردین ۱۴۰۴

۱. مقدمه

فناوری بلاک‌چین به واسطه‌ی ساختار غیرمتمرکز، شفافیت بالا و قابلیت اطمینان در امنیت، جایگاه ویژه‌ای در حوزه‌هایی نظیر سیستم‌های مالی، مدیریت زنجیره تأمین و رأی‌گیری الکترونیکی یافته است. امنیت این فناوری عمدتاً بر پایه‌ی الگوریتم‌های رمزنگاری سنتی مانند RSA و ECC بنا شده است. با این حال، ظهور رایانش کوانتومی و توان بالقوه‌ی آن در شکستن این الگوریتم‌ها، تهدیدی جدی برای پایداری امنیتی بلاک‌چین به شمار می‌آید.

در این میان، رمزنگاری کوانتومی که بر اصول فیزیک کوانتومی استوار است، به عنوان راهکاری نوین و مقاوم در برابر حملات کوانتومی مطرح می‌شود. این فناوری با فراهم‌کردن امکان توزیع کلیدهای رمزنگاری‌شده به‌صورت کاملاً ایمن، می‌تواند بستر مطمئنی برای حفظ امنیت بلاک‌چین در برابر تهدیدات آینده ایجاد کند.

ترکیب رمزنگاری کوانتومی با بلاک‌چین، افق‌های تازه‌ای برای تقویت امنیت اطلاعات در صنایع مختلف می‌گشاید. از جمله کاربردهای برجسته‌ی این فناوری تلفیقی می‌توان به موارد زیر اشاره کرد:

- بانکداری و امور مالی: حفاظت از تراکنش‌ها و داده‌های حساس در برابر حملات احتمالی رایانش کوانتومی.
- سازمان‌های دولتی و نهادهای حساس: تأمین امنیت اطلاعات محرمانه و حیاتی در برابر تهدیدات پیچیده و نوظهور.
- شبکه‌های اینترنت اشیا: تضمین امنیت ارتباطات و تبادل داده میان دستگاه‌های متصل در محیط‌های توزیع‌شده

۲. مطالعات پیشین

تحقیقات متعددی در زمینه استفاده از رمزنگاری کوانتومی برای امنیت بلاک‌چین انجام شده است که هر یک جنبه‌ای از این موضوع را بررسی کرده‌اند. برخی پژوهش‌ها به پیاده‌سازی و بهینه‌سازی الگوریتم‌های امضای

دیجیتال پساکوانتومی پرداخته‌اند و نشان داده‌اند که این الگوریتم‌ها می‌توانند امنیت بلاک‌چین را در برابر حملات کوانتومی تضمین کنند[1].

گروهی دیگر از مطالعات، سیستم‌های بلاک‌چین مقاوم در برابر محاسبات کوانتومی را مورد بررسی قرار داده و چالش‌های مربوط به پیاده‌سازی این فناوری را تحلیل کرده‌اند. این پژوهش‌ها همچنین مقایسه‌ای جامع از عملکرد و ویژگی‌های الگوریتم‌های رمزنگاری پساکوانتومی ارائه داده‌اند [2,3].

همچنین، تحقیقات دیگری به تحلیل آسیب‌پذیری‌های بلاک‌چین در برابر حملات کوانتومی پرداخته و راهکارهایی برای افزایش امنیت این سیستم‌ها پیشنهاد کرده‌اند. علاوه بر این، برخی مطالعات به بررسی فرصت‌ها و چالش‌های ناشی از ترکیب بلاک‌چین و محاسبات کوانتومی پرداخته و راهکارهایی برای بهره‌گیری از ویژگی‌های کوانتومی جهت تقویت امنیت بلاک‌چین ارائه داده‌اند [4,5,6.7.8.9.10].

۳. دلایل انجام طرح

بیشتر تحقیقات کنونی بر روی کاربرد توزیع کلید کوانتومی (QKD) متمرکز شده‌اند و به بررسی چگونگی تأمین امنیت در کانال‌های ارتباطی پرداخته‌اند. با این حال، در بسیاری از این مطالعات، استفاده از الگوریتم‌های رمزنگاری کوانتومی برای امضاهای دیجیتال، رمزنگاری داده‌ها و هش‌ها در بلاک‌چین مورد توجه قرار نگرفته است.

علاوه بر این، حریم خصوصی کاربران و انجام تراکنش‌های کاملاً امن در کاربردهایی مانند بانکداری و تراکنش‌های مالی همچنان در برابر حملات کوانتومی آسیب‌پذیر هستند. این نقطه ضعف‌ها نشان‌دهنده نیاز به توسعه روش‌های جدید برای تأمین حریم خصوصی در بلاک‌چین کوانتومی است. ترکیب تکنیک‌های مختلف رمزنگاری کوانتومی، می‌تواند امنیت بیشتری برای حفاظت از اطلاعات حساس و جلوگیری از حملات کوانتومی فراهم آورد.

در نهایت، اگرچه تحقیقات زیادی در برخی جنبه‌ها انجام شده، هنوز فضای زیادی برای پژوهش در زمینه‌های عملی و پیاده‌سازی این الگوریتم‌ها در سیستم‌های بلاک‌چین وجود دارد. این مسائل باید در تحقیقات آینده به طور جدی‌تر بررسی شوند.

۴. اهداف تحقیق

هدف اصلی این تحقیق، توسعه روش‌های ترکیبی از رمزنگاری کوانتومی و کلاسیک برای تأمین امنیت بلاک‌چین در برابر تهدیدات رایانش کوانتومی است. در این راستا، اهداف خاص تحقیق به شرح زیر می‌باشند:

۱. تحلیل آسیب‌پذیری بلاک‌چین در برابر حملات کوانتومی: شناسایی و ارزیابی نقاط ضعف بلاک‌چین‌های فعلی در برابر تهدیدات ناشی از رایانش کوانتومی، به‌ویژه در زمینه‌های امضای دیجیتال، رمزنگاری داده‌ها و هش‌ها.

۲. ترکیب الگوریتم‌های کلاسیک و پساکوانتومی برای تأمین امنیت بلاک‌چین: ارائه مدل‌های ترکیبی که در آن از الگوریتم‌های کلاسیک و پساکوانتومی به‌طور همزمان برای افزایش امنیت بلاک‌چین استفاده می‌شود. این روش‌ها باید قادر باشند در برابر حملات کوانتومی مقاوم باشند و در عین حال از کارایی بالایی برخوردار باشند.

۳. حفظ حریم خصوصی کاربران در بلاک‌چین‌های پساکوانتومی: توسعه‌ی روش‌های ترکیبی برای تأمین حریم خصوصی کاربران در بلاک‌چین‌های پساکوانتومی، به‌ویژه در کاربردهای حساس مانند بانکداری و تراکنش‌های مالی.

٤. ارائه‌ی مدل‌های امنیتی ترکیبی برای بلاک‌چین پساکوانتومی: طراحی و پیشنهاد مدل‌های امنیتی که بتوانند از ترکیب الگوریتم‌های کلاسیک و پساکوانتومی برای مقابله با تهدیدات کوانتومی استفاده کنند و در عین حال از کاربردهای عملی آن‌ها در بلاک‌چین اطمینان حاصل کنند.

۵. مراحل تحقیق

این پژوهش شامل چهار مرحله اساسی است.

مرحله اول - بررسی منابع موجود: در مرحله اول، مقالات و تحقیقات پیشین در زمینه رمزنگاری کوانتومی و بلاک‌چین به‌طور جامع بررسی خواهند شد. این مرحله شامل تحلیل پروتکل‌های شناخته‌شده رمزنگاری کوانتومی مانند BB84و E91، که پایه‌گذار بسیاری از الگوریتم‌های توزیع کلید کوانتومی هستند، خواهد بود. همچنین،

چالش‌های امنیتی موجود در بلاک‌چین در برابر تهدیدات ناشی از رایانش کوانتومی مورد بررسی قرار می‌گیرند. این تحقیق شامل شناسایی آسیب‌پذیری‌های بلاک‌چین‌ها در زمینه امضاهای دیجیتال، هش‌ها و فرآیند انتقال کلیدها خواهد بود. با تحلیل مقالات مرتبط، شکاف‌های تحقیقاتی شناسایی شده و نیاز به ادغام رمزنگاری کوانتومی و کلاسیک مشخص می‌شود.

مرحله دوم – طراحی سیستم: در این مرحله، سیستم امنیتی ترکیبی برای بلاک‌چین طراحی خواهد شد. این سیستم شامل ادغام الگوریتم‌های توزیع کلید کوانتومی (QKD) با فرآیند انتقال کلید در بلاک‌چین است. استفاده از QKD باعث می‌شود که کلیدهای انتقالی به‌طور ایمن و مقاوم در برابر حملات کوانتومی جابجا شوند. علاوه بر این، از الگوریتم‌های رمزنگاری مقاوم به کوانتوم (PQC) استفاده خواهد شد، مانند lattice-based cryptography که در برابر تهدیدات رایانش کوانتومی مقاوم است. این الگوریتم‌ها برای تأمین امنیت امضاهای دیجیتال و هش‌ها در بلاک‌چین‌های کوانتومی طراحی می‌شوند. در واقع هدف از این مرحله طراحی یک چارچوب امنیتی است که بتواند به‌طور همزمان از ویژگی‌های رمزنگاری کلاسیک و کوانتومی بهره‌برداری کند. سپس، یک چارچوب امنیتی ترکیبی طراحی خواهد شد که در آن، مکانیزم‌های رمزنگاری سنتی بلاکچین با روش‌های مقاوم در برابر کوانتوم ادغام شوند. این چارچوب، ضمن حفظ تمرکززدایی بلاکچین، از تهدیدات رایانش کوانتومی جلوگیری می‌کند.

مرحله سوم – تحلیل کارایی: در این مرحله عملکرد آن از جنبه‌های مختلف تحلیل خواهد شد. این ارزیابی شامل بررسی سرعت پردازش، مصرف منابع و سطح امنیت سیستم در برابر حملات کوانتومی است. علاوه بر این، مدل پیشنهادی با بلاک‌چین‌های کلاسیک که از الگوریتم‌های رمزنگاری سنتی استفاده می‌کنند مقایسه خواهد شد تا مقاومت آن در برابر حملات کوانتومی اندازه‌گیری شود. در این مرحله، شاخص‌هایی همچون زمان تأخیر، کارایی در مقیاس‌های بزرگ و مصرف انرژی نیز ارزیابی خواهد شد. هدف این تحلیل‌ها، به‌دست آوردن نتایج دقیق در خصوص مزایا و معایب مدل ترکیبی نسبت به سیستم‌های بلاک‌چین موجود است.

نتایج مورد انتظار

با ترکیب تکنیک‌های رمزنگاری کوانتومی و کلاسیک، انتظار می‌رود این پژوهش راهکارهایی برای افزایش امنیت بلاکچین در برابر تهدیدات آینده ارائه دهد. مهم‌ترین نتایج مورد انتظار عبارت‌اند از:

- افزایش امنیت: مقاوم‌سازی بلاکچین در برابر حملات کامپیوترهای کوانتومی و حفظ حریم خصوصی.
- ارزیابی عملکرد: ارائه شاخص‌هایی برای سنجش کارایی رمزنگاری کوانتومی در بلاکچین.
- بهینه‌سازی پردازش: کاهش تأخیرهای محاسباتی با ترکیب بهینه رمزنگاری کلاسیک و کوانتومی.
- کاربردپذیری گسترده: بررسی تأثیر این مدل بر افزایش اعتمادپذیری بلاکچین در حوزه‌هایی مانند مالی، سلامت و اینترنت اشیا.

References

[1] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero and M. Polsinelli, "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," in *IEEE Transactions on Industrial Informatics*, vol. 21, no. 2, pp. 1674-1683, Feb. 2025.

[2] Preethi, M. M. Ulla, R. Sapna and K. G. Mohan, "Implementing Post-Quantum Cryptography Algorithm in Blockchain," *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*, Bangalore, India, 2023, pp. 1-7.

[3] Preethi, M. M. Ulla, R. Sapna and K. G. Mohan, "Implementing Post-Quantum Cryptography Algorithm in Blockchain," *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*, Bangalore, India, 2023, pp. 1-7.

[4] M. G. Selvaraj, C. Mulay, K. Durai, …, Quantum Blockchain: Trends, Technologies, and Future Directions," *IET Quantum Communication*, vol. 5, no.4, pp. 516-542, 2024.

[5] W. Cui, T. Dou and S. Yan, "Threats and Opportunities: Blockchain meets Quantum Computation," *2020 39th Chinese Control Conference (CCC)*, Shenyang, China, pp. 5822-5824, 2020.

[6] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, A. Erbad, "A Survey and Comparison of Post-Quantum and Quantum Blockchains," *IEEE Communications Surveys & Tutorials*, vol. 26, iss. 2, 2024.

[7] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.

[8] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on postquantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[9] M. C. Semmouni, A. Nitaj, and M. Belkasmi, "Bitcoin security with post quantum cryptography," in *Networked Systems* (Lecture Notes in Computer Science). Cham, Switzerland: Springer Int., 2019, pp. 281–288.

[10] Z. Yang, T. Salman, R. Jain, and R. D. Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Trans. Quant. Eng.*, vol. 3, pp. 1–16, 2022.