Mundo Fesc, 11 (21), pp. 156-165 Enero-Junio, 2021, ISSN 2216-0353, 2216-0388

Uso y Aplicaciones de la Integración Entre Computación Cuantica y Blockchain: Revisión Sistemática Exploratoria

Use snd Applications of Integration Between Quantic Computation and Blockchain: Exploratory Systematic Review

[a]Fredy Andrés Aponte-Novoa, [b]Daladier Jabba-Molinares, [c]Pedro Mario Wightman-Rojas

aMagister en Software Libre, fredy.aponte@usantoto.edu.co, faponte@uninorte.edu.co, orcid: 0000-0003-3773-4414, Investigador Grupo de Investigación y Desarrollo de Ingeniería en Nuevas Tecnologías (GIDINT), Universidad Santo Tomás, Tunja, Estudiante de doctorado en Ingeniería de Sistemas y Computación, Universidad del Norte, Barranquilla, Colombia.

b PhD In Computer Science and Engineering, djabba@uninorte.edu.co, orcid:0000-0001-5876-2559, Docente Tiempo Completo Departamento de Ingeniería de Sistemas, Universidad del Norte, Barranquilla, Colombia.

c PhD In Computer Science and Engineering, pwightman@uninorte.edu.co, orcid:0000-0002-7641-2090, Docente Tiempo Completo Departamento de Ingeniería de Sistemas, Universidad del Norte, Barranquilla, Colombia.

Recibido: Julio 18 de 2020 **Aceptado:** Noviembre 19 de 2020

Forma de citar: F.A. Aponte-Novoa, D. Jabba-Molinares, P.M. Wightman-Rojas "Uso y Aplicaciones de la Integración Entre Computación Cuantica y Blockchain: Revisión Sistemática Exploratoria", *Mundo Fesc,* vol. 11, no. 21, pp. 156-165, 2021

Resumen

Las tecnologías Blockchain en conjunto con la computación cuántica es un nuevo campo de investigación, el cual enfoca sus esfuerzos en la identificación y mitigación de los problemas que traerá consigo la madurez y adopción de las técnicas propias de la computación cuántica, al consultar publicaciones científicas sobre estos temas, específicamente en la base de datos Scopus se puede identificar que desde hace 30 años se realizan investigaciones sobre computación cuántica, teniendo un crecimiento en la última década y un mayor interés en los últimos tres años, por otra parte casi tres lustros después aparecen las publicaciones relacionadas con Blockchain presentando un lento interés en sus inicios en contraste con su gran interés en los últimos 3 años. Además, los resultados de la consulta en esta base de datos de las dos temáticas en conjunto reflejan que solo desde el año 2018 se presentan publicaciones científicas, particularmente para el año 2019 Computación Cuántica presenta 833 publicaciones, Blockchain 3760 y estas dos temáticas en conjunto solo 5 publicaciones, lo que presenta un 0,60% y 0,13%, respecto a cada tema por separado respectivamente. Este documento presenta una revisión sistemática exploratoria (Scoping Review) de la bibliografía relacionada el estudio de la computación cuántica junto con la tecnología Blockchain con el objetivo de identificar sus áreas de estudio, aplicación y tecnologías complementarias.

Palabras clave: Ataques cuánticos, Cadena de bloques, Computación Cuántica, Mitigación postcuántica

Autor para correspondencia:

*Correo electrónico: fredy.aponte@usantoto.edu.co

Abstract

Blockchain technologies in conjunction with quantum computing is a new field of research, which focuses its efforts on the identification and mitigation of the problems that will lead to the maturity and adoption of quantum computing techniques, when consulting scientific publications on These issues, specifically in the Scopus database, can identify that for 30 years research has been carried out on quantum computing, having a growth in the last decade and a greater interest in the last three years, on the other hand almost three decades later they appear Blockchain related publications presenting a slow interest in their beginnings in contrast to their great interest in the last 3 years. In addition, the results of the consultation in this database of the two themes together reflect that only since 2018 are scientific publications presented, particularly for the year 2019 Quantum Computing presents 833 publications, Blockchain 3760 and these two themes together only 5 publications, which presents 0.60% and 0.13%, regarding each subject separately respectively.

This document presents an exploratory systematic review (Scoping Review) of the literature related to the study of quantum computing together with Blockchain technology with the objective of identifying its areas of study, application and complementary technologies.
Keywords: Quantum attacks, Blockchain, Quantum Computing, Post-quantum mitigation

Introducción

La tecnología blockchain (cadena de bloques) se considera como uno de los paradigmas de la informática disruptivos más importantes posterior a internet [1][2] , sus características únicas la convierten en un conjunto de técnicas ideal para registrar, verificar y administrar transacciones. La operación básica de blockchain consiste en la administración segura del libro contable compartido, donde las transacciones se verifican y almacenan en una red que no tiene una autoridad central. Un blockchain puede ser público o privado, permitiendo la configuración de permisos de lectura o escritura. Los algoritmos empleados como funciones hash criptográficas, permiten que blockchain funcione, habilitando la realización de transacciones, y protegiendo a su vez la integridad y el anonimato de la cadena [3]. La combinación de la red peer to peer, consiste en un algoritmo criptográfico que permite el almacenamiento distribuido y un mecanismo de consenso descentralizado; haciendo de blockchain una tecnología ideal para el registro de transacciones de manera segura y verificable, además evitando el doble gasto efectivo [4] [5].

Terminado la primera década del Siglo XXI, Blockchain se ha convertido en una tecnología innovadora, la cual presenta mucho interés, registrando un incremento continuo en la cantidad de estudios y publicaciones que se asocian a su temática. Una de sus principales características es la seguridad, fortaleciendo significativamente sectores financieros, turísticos, médicos, entre otros. A pesar de su oferta innovadora, actualmente enfrenta una amenaza potencial relacionada a un posible ataque informático cuántico, que podría comprometer significativamente las condiciones de seguridad que propone esta tecnología; mostrando hasta el momento pocos estudios que definan como tratar este tema [6].

El poder de cómputo de los computadores cuánticos y las capacidades que presentan sus algoritmos existentes se convierten en una amenaza para la gran mayoría de sistemas criptográficos de clave publica existentes [7]. La computación cuántica emplea diversos fenómenos cuánticos, como lo son la superposición y el “entanglement” (“enredo”), para la representación de datos clásicos en un contexto cuántico, y de esta manera operarlos de manera que provoquen resultados interpretables [8]. Algunos

Pronósticos presumen que para el año 2026 la probabilidad de contar con computadores cuánticos es del 15% y para el año 2031 del 50% [9].

Así como el estado de los computadores clásicos esta dado por los bits, en computación cuántica se usan los Qubits, los cuales tienen dos estados base (0 y 1). No obstante, mientras se realizan los cálculos, el estado es una combinación lineal de los estados base, en donde cada uno de estos tiene una probabilidad asociada de ser medido [10].

Casi todas las implementaciones actuales de blockchain poseen dependencia directa con las firmas digitales de clave pública, lo que las convierte en blanco a los ataques de los computadores cuánticos [11]. Actualmente existen algunas soluciones que adoptan la criptografía post-cuántica, pero estás no garantizan una solución completamente segura a las amenazas de la computación cuántica[6] [12] [10]. Un caso particular de estas soluciones es la llamada "quantum-secured blockchain" (QB) (blockchain con seguridad cuántica), en la que se implementa la autenticación de mensajes de seguridad incondicionales, basados en la metodología de distribución de claves cuánticas, lo que hace a QB inmune a los ataques de los computadores cuánticos [13].

Un ejemplo de esta amenaza, son los algoritmos cuánticos propuestos por Shor (1994), los cuales se enfocan en encontrar logaritmos discretos y factorizar números enteros en un computador cuántico, algoritmos capaces de quebrantar la seguridad de los algoritmos RSA (Rivest, Shamir y Adleman Algorithm), DSA (Digital Signature Algorithm) y ECDSA (Elliptic Curve Digital Signature Algorithm) [14]. Otra característica clave de blockchain que se ve amenazada ante un ataque cuántico son los esquemas de firma digital empleados para la autenticación de transacciones en la mayoría de redes blockchain [15].

Desde su propuesta por Satoshi Nakamoto en el año 2008, blockchain ha sido la columna vertebral de la criptomoneda Bitcoin [16], esta experiencia exitosa ha llamado la atención de muchas organizaciones en investigar como emplear la tecnología blockchain para construir aplicaciones descentralizadas. Actualmente existen alrededor de 1300 tipos de criptomonedas sobre blockchain en todo el mundo, además algunas estimaciones afirman que el mercado de criptomonedas vale alrededor de 150 mil millones de dólares. Por tal motivo, el estudio de la seguridad en sistemas blockchain, específicamente los ataques actuales y futuros tanto en sistemas clásicos y cuánticos recobran gran importancia [12].

El presente documento busca analizar el estado de información existente publicada sobre estudios que asocien la tecnología de blockchain con computación cuántica, permitiendo la identificación de los problemas, las áreas de aplicación y las tecnologías complementarias asociadas. Para esto se plantea una revisión sistemática exploratoria (Scoping Review) la cual se considera como una forma de síntesis de conocimiento que aborda una pregunta de investigación exploratoria, dirigida a mapear conceptos clave, tipos de evidencia y vacíos en la investigación relacionada con un área o campo definido, mediante la búsqueda, selección y síntesis sistemática del conocimiento existente [17].

Metodología

Para el desarrollo del artículo se empleó la declaración PRISMA, la cual es un conjunto de elementos para la presentación de informes en revisiones sistemáticas y de metaanálisis. Esta declaración se puede utilizar como base para informes de revisiones sistemáticas de diferentes tipos de

investigaciones. El principal objetivo al emplear la metodología establecida por PRISMA es mejorar los informes de revisiones realizados por investigadores garantizando la objetividad de las búsquedas y sistematizando el proceso de modo que pueda ser replicable. [18].

Esta declaración comprende de una lista de chequeo de 27 elementos junto un diagrama de flujo de cuatro fases, los ítems de la lista incluyen los elementos que se consideran esenciales para la presentación de informes de una revisión sistemática [18].

La metodología para la presente revisión toma como base las fases que componen el diagrama de flujo empleado por la declaración PRISMA [18], y que se enuncian a continuación (Figura 1):

Figura 1. Fases definidas por el protocolo de la metodología PRISMA para el desarrollo de revisiones sistemáticas exploratorias.

Consulta e identificación

Para iniciar se realizó una consulta general en la base de datos Scopus, para identificar las tendencias de publicaciones realizando tres búsquedas independientes con las palabras *"blockchain", "quantum computing"* y *'"quantum computing" AND blockchain'*.

Las consultas específicas se realizaron el día 29 de octubre de 2019 en las bases de datos "IEEE Xplore Digital Library", "Science Direct", "Scopus", "Springer Link", "Taylor & Francis" y "Web of Science", usando los términos de búsqueda "*quantum computing*" *AND blockchain*". Estas búsquedas contemplaron todos los tipos de publicación, subáreas, tipo de acceso y año de publicación.

Filtrado

Como primera tarea de esta fase se identificaron y eliminaron los registros duplicados, posteriormente se excluyeron los capítulos de libros, así como y documentos diferentes a artículos de investigación, artículos de revisión y actas de congreso con el objetivo de garantizar que las publicaciones analizadas hayan cumplido con el proceso de evaluación asegurando la calidad de la información.

Elección / Inclusión

En esta fase excluyen algunos artículos teniendo en cuenta la pertinencia de los mismos con el trabajo realizado.

Análisis

Se realiza un análisis de los trabajos que estudian la computación cuántica y blockchain en conjunto para identificar temas de estudio, áreas de aplicación y tecnologías complementarias.

Discusión

Con los hallazgos de la fase anterior se identifica un área potencial de desarrollo e investigación empleando la computación cuántica y blockchain.

Resultados

Inicialmente, al analizar las generalidades en las publicaciones sobre los temas de computación cuántica, blockchain y la integración entre ambos, puede notarse que las publicaciones sobre computación cuántica

iniciaron desde el año 1989 y empezaron a incrementarse hacia el año 2000, en donde el mayor número de artículos se registra en el año 2019 con 833 registros. Por su parte, a pesar de que las publicaciones que incluyen blockchain iniciaron 14 años después (2003), han incrementado de manera significativa alcanzando en el 2018 un total de 2821 y en lo corrido del año 2019 un total de 3760 publicaciones registradas (Figura 2).

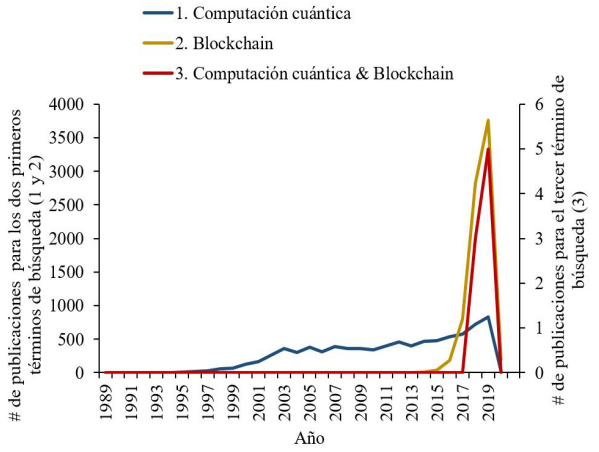

Figura 2. Número de publicaciones por año registradas en la base de datos de SCOPUS, con tres (3) términos de búsqueda distintos.

La Figura 2 muestra adicionalmente como la cantidad de publicaciones que incluyen ambas tecnologías empezaron a registrarse desde el 2018, alcanzando 3 publicaciones en ese año y 5 publicaciones en lo corrido del año 2019.

Al analizar los países que más están publicando específicamente en el tema de computación cuántica, se resalta a Estados Unidos y China con un número elevado de publicaciones, presentando 2813 y 1189 publicaciones respectivamente, Colombia específicamente presenta solo 24 publicaciones al respecto. Con respecto al tema de Blockchain también se observa el liderazgo de China y Estados Unidos con 1575 y 1370 publicaciones. Al analizar los registros con ambos términos de búsqueda ("quantum computing" AND blockchain), se identifica a China en primer lugar con tres (3) publicaciones asociadas seguida de Australia, Austria, Francia, Alemania, India, Israel, Singapur y Reino Unido con (1) publicación asociada cada uno.

Al realizar la consulta específica con ambos términos de búsqueda en las seis (6) bases de datos definidas previamente, puede notarse que registraron 209 resultados en total; siendo los artículos, la tipología de publicación que se registra con mayor frecuencia (37,3%) (Tabla 1).

Tabla 1. Tabla resumen de los resultados de las consultas realizadas clasificadas por tipología de la publicación y detalladas por cada una de las bases de datos analizadas.

Base de datos	Actas de Congresos	Artículos de investigación / revisión	Capítulos de libro	Otros
IEEE Xplore Digital Library	4	5		1
Science Direct		26	11	13
Scopus	2	6		
Springer Link		23	96	3
Taylor & Francis		11		
Web of Science	1	7		

Posterior a la búsqueda bibliográfica se excluyeron los 107 resultados referentes a capítulos de libro, los 17 referentes a otros, obteniendo un total de 85 registros de las tipologías actas de congreso y artículos científicos. De estos registros se identificaron 10 registros duplicados que fueron eliminados, quedando con un total de 75 resultados.

A los 75 registros restantes se les realizó una revisión de título y resumen para excluir los artículos que no son pertinentes con el objetivo de la presente revisión; excluyendo 62 artículos adicionales y obteniendo 13 artículos resultantes para el análisis del presente trabajo.

La Figura 3 presenta el diagrama de flujo establecido en la metodología PRISMA, en donde se detalla el proceso de selección de información.

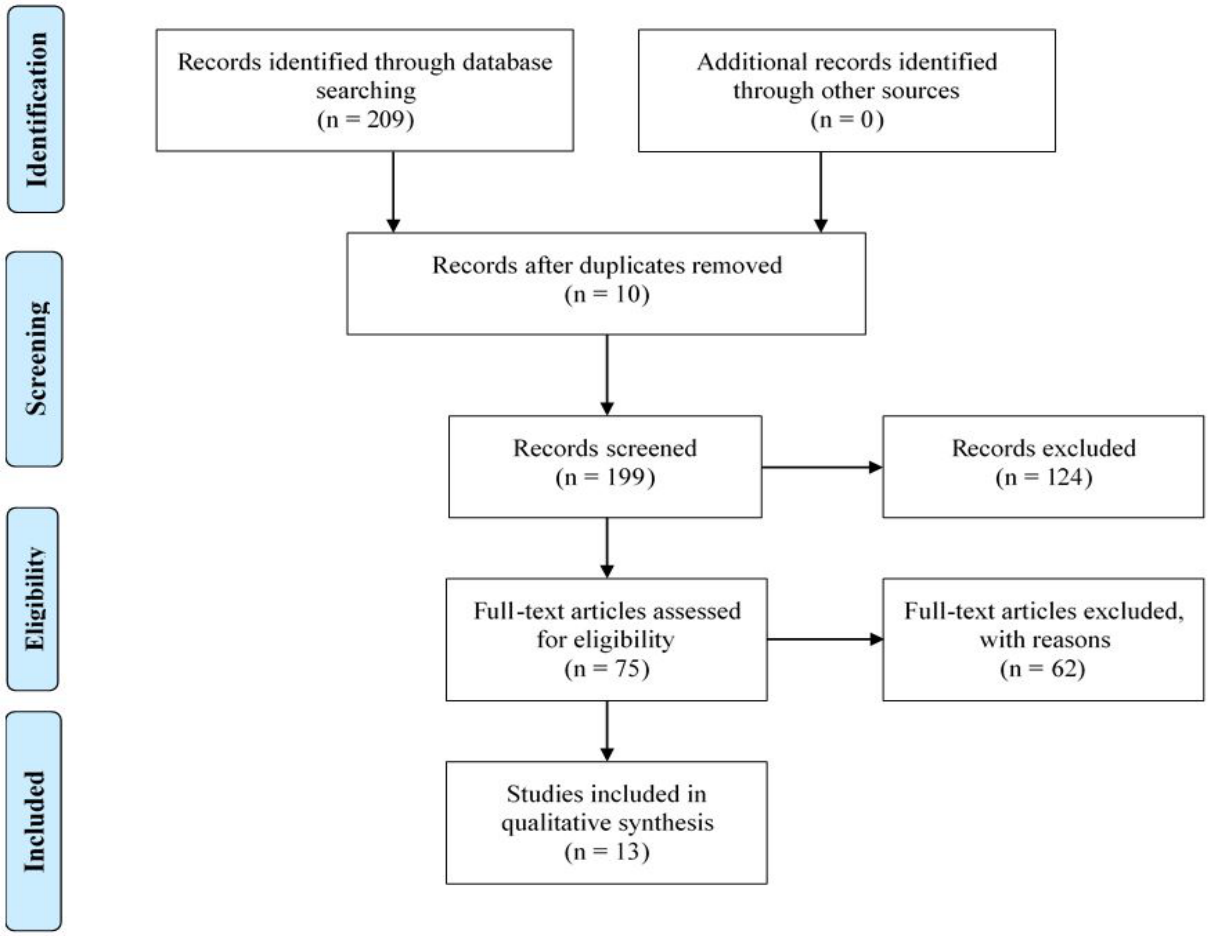

Figura 3. Diagrama de Flujo de la revision, siguiendo el protocolo definido por PRISMA

La Figura 4 muestra la cantidad de artículos elegibles para el estudio junto con su porcentaje de selección teniendo en cuenta la pertinencia de estos para el presente trabajo, es de resaltar que aunque los resultados obtenidos en las bases de datos, Scopus (8), Web of Science (8) y IEEE Xplore Digital Library (9) son bajos en comparación con los de las otras bases de datos su porcentaje de selección es mayor, el cual está dado por 75%, 63% y 56% respectivamente.

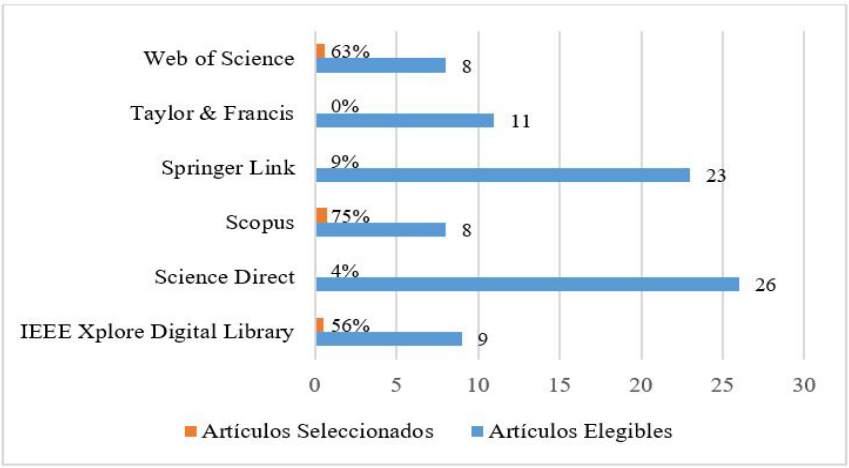

Figura 4. Artículos elegibles vs artículos seleccionados pata el estudio

Al analizar las temáticas en las que se enfocan los artículos incluidos en el análisis, en los que se hace vínculo claro entre la tecnología de blockchain y puede notarse que el 26% se enfoca en el desarrollo o aplicación de algoritmos, seguidos por el estudio de criptomonedas y de esquemas de firma digital (18% cada uno). Por su parte, el 12% de los estudios se han enfocado en la generación de claves y los procesos de minería, seguido por el estudio de contratos inteligentes (6%), mientras que el análisis de las funciones unidireccionales (OWF), el diseño de hardware y el algoritmo consenso son los que menos han sido estudiados hasta el momento (3% cada uno). En algunos de estos estudios resalta el uso de árboles bonsáis, la fibra óptica y las redes neuronales.

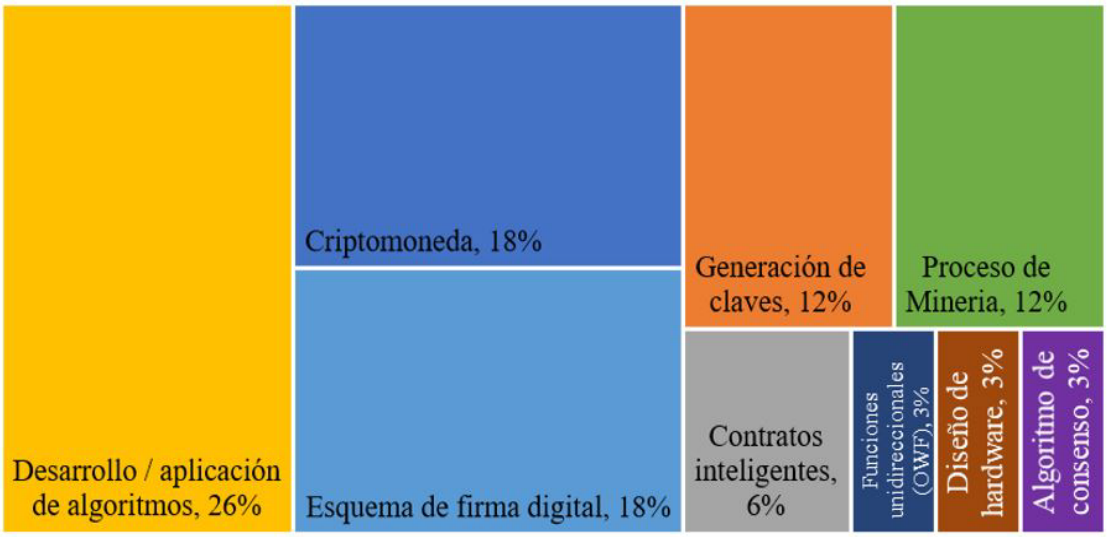

Figura 5. Enfoque de estudio de las publicaciones incluidas en el análisis, que consideran un vínculo claro entre la tecnología blockchain y la computación cuántica

Discusión

Se han propuesto algunas estrategias de mitigación post-quantum, como lo son: la criptografía cuántica resistente, cadena de bloques post-cuántica [12], Hashing cuántico [19] y la máquina del tiempo en red cuántica [20]. Gracias al surgimiento de los computadores cuánticos: IBM de 50 Qbits y Google de 72 Qbits, recientemente está evolucionando el Quantum Blockchain en el cual se reemplazan las funciones criptográficas estándar de hash por funciones criptográficas cuánticas de hash [20].

Yu-Long Gao et al, presentan por primera vez el termino Blockchain Post-Cuántica (PQB), el cual hace referencia a una nueva tecnología segura de blockchain que adopta la criptografía post-cuántica y la tecnologia blockchain tradicional, en otras palabras PQB además de tener las ventajas propias de blockchain, también puede resistir efectivamente los ataques de la computación cuántica [6].

Entre los diferentes temas tratados en los artículos analizados sobresale el desarrollo o aplicación de algoritmos, trabado en nueve de los 13 trabajos [6], [21], [12], [10], [22], [23], [24], [25], [26], en dos de estos se emplean los árboles bonsai para generar las claves sub-públicas y subprivadas [6], [12]. Otros algoritmos estudiados son Shor [12], Grover [12], [23], Lenstra [25] y consenso basado en votos [27]. De estos trabajos pueden destacarse Krendelev y Sazonova (2018) quienes proponen un algoritmo de función hash resistente a la computación cuántica,

el cual utiliza el problema algorítmicamente insoluble de encontrar una solución a un sistema de ecuaciones polinómicas en enteros. Este algoritmo fue desarrollado para aumentar la resistencia a los ataques de las computación cuántica en la tecnología blockchain, pero puede usarse en cualquier aplicación donde se necesita una función hash [22]. Ablayev et al. (2018) consideran la idea natural de aplicar el algoritmo de búsqueda cuántica de Grover a la tecnología general de blockchain (para minería), en el documento se dedican a desarrollar y probar esta idea para la tecnología blockchain [23]. Por su parte, Anada et al. (2019) se basan en la versión modificada del algoritmo de Lenstra, mediante el cual una segunda clave pública relacionada y las cadenas de identidad se integran en el módulo RSA [25]; mientras que Sun et al. (2019), adoptaron un algoritmo de consenso basado en votos para lograr el consenso en la cadena de bloques [27].

Otro tema de gran interés en estos estudios es las firmas digitales, presente en seis de estos artículos [6], [21], [12], [10], [28], [27], Gao et al. (2018) y Li et al. (2019) estudian un esquema de firma basado en la red de blockchain [6], [12]. Por su parte Cai et al. (2019) proponen un contrato inteligente basado en la firma cuántica ciega ligera (Light-Weighted Quantum Blind Signature) [21].

No menos importante, también con presencia en seis artículos se encuentra en estudio el tema de las criptomonedas [6], [10], [29], [28], [23], [26], de estos trabajos sobresale el presentado por Gao et al. (2018) en donde presentan la definición de BlockChain Post-Cuántica (PQB) y proponen un esquema de criptomoneda seguro basado en PQB [6]. Por otra parte, Stewart et al. (2018) realizan una descripción general de los posibles impactos que podría tener la aparición de computacion cuantica en Bitcoin y proponen un protocolo para la transición del esquema de firma actual de Bitcoin a uno resistente a los cuánticos, el esquema propuesto requiere modificaciones al protocolo de Bitcoin [10].

Otro trabajo muy interesante es el de Jogenfors (2019), en el cual se presenta Quantum Bitcoin como la primera moneda cuántica distribuida inspirada en Bitcoin y la mecánica cuántica, moneda que tiene entre otras caracteristicas, una verificación local inmediata de las transacciones, lo cual es una mejora importante sobre el Bitcoin clásico ya que no se necesita el método computacionalmente intensivo y que consume mucho tiempo para registrar todas las transacciones en la cadena de bloques; aunque esta moneda tiene varias ventajas interesantes sobre los sistemas de pago existentes, su principal inconveniente es que requiere un computador cuántico para funcionar [29]. Este mismo documento presenta un novedoso proceso de mineria cuántica en dos etapas.

Conclusiones

Las publicaciones que tienen relación con la computación cuántica y blockchain son un campo aun poco explorado el cual ha comenzado a despertar interés en los últimos tres años en algunos pocos países, para el caso particular de Colombia aun no presenta publicaciones sobre estas temáticas, por otra parte todos los trabajos presentados en el análisis tienen como foco principal el estudio de los problemas que acarreara la computación cuántica en los sistemas computacionales, específicamente en la tecnología blockchain. Debido a que actualmente no se cuenta con el suficiente poder de cómputo en los computadores cuánticos y su uso está enfocado más la investigación, las soluciones presentadas en estas investigaciones son aún muy teóricas y no 100% seguras, además los problemas que se presagian cuando la computación cuántica

logre su madurez convierte a la computación cuántica y blockchain como un campo muy interesante para la investigación.

Referencias

[1] M. Pilkington, "Blockchain technology: Principles and applications," *Res. Handbooks Digit. Transform.*, pp. 225–253, 2016.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Applied Innovation Review," *Appl. Innov. Rev.*, no. 2, pp. 5–20, 2016.

[3] D. Wessel, "The Hutchins Center Explains: How blockchain could change the financial system (part 1) | Brookings Institution," *Brookings*, p. 1, 2016.

[4] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current Trends in Sustainability of Bitcoins and Related Blockchain Technology," *Sustainability*, vol. 9, 2017.

[5] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, 2018.

[6] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, Apr. 2018.

[7] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, pp. 303–332, 1999.

[8] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Comput. Surv.*, vol. 32, no. 3, pp. 300–335, 2000.

[9] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Secur. Priv.*, vol. 16, no. 5, pp. 38–41, 2018.

[10] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: A slow defence for Bitcoin against a fast quantum computing attack," *R. Soc. Open Sci.*, vol. 5, no. 6, Jun. 2018.

[11] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018.

[12] 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.

[13] E. O. Kiktenko et al., "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018.

[14] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[15] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger*, vol. 3, pp. 1–21, 2018.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/

s10838-008-9062-0stem," *J. Gen. Philos. Sci.*, vol. 39, no. 1, pp. 53–67, 2008.

[17] H. L. Colquhoun et al., "Scoping reviews: time for clarity in definition, methods, and reporting," *J. Clin. Epidemiol.*, vol. 67, no. 12, pp. 1291–1294, Dec. 2014.

[18] A. Liberati et al., "The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration," *PLoS Med.*, vol. 6, no. 7, p. e1000100, Jul. 2009.

[19] M. Jin and C. D. Yoo, "Quantum hashing for multimedia," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 982–994, 2009.

[20] D. Rajan and M. Visser, "Quantum Blockchain Using Entanglement in Time," *Quantum Reports*, vol. 1, no. 1, pp. 3–11, 2019.

[21] Z. Cai, J. Qu, P. Liu, and J. Yu, "A Blockchain Smart Contract Based on Light- Weighted Quantum Blind Signature," *IEEE Access*, vol. 7, pp. 138657–138668, 2019.

[22] S. Krendelev and P. Sazonova, "Parametric hash function resistant to attack by quantum computer," *Proc. 2018 Fed. Conf. Comput. Sci. Inf. Syst. FedCSIS 2018*, vol. 15, pp. 387–390, 2018.

[23] F. M. Ablayev, D. A. Bulychkov, D. A. Sapaev, A. V. Vasiliev, and M. T. Ziatdinov, "Quantum-Assisted Blockchain," *Lobachevskii J. Math.*, vol. 39, no. 7, pp. 957–960, 2018.

[24] W. Dai, "Quantum-computing with AI & blockchain: modelling, fault tolerance and capacity scheduling," *Math. Comput. Model. Dyn. Syst.*

[25] H. Anada, T. Yasuda, J. Kawamoto, J. Weng, and K. Sakurai, "RSA public keys with inside structure: Proofs of key generation and identities for web-of-trust," *J. Inf. Secur. Appl.*, vol. 45, pp. 10–19, 2019.

[26] T. Lee, M. Ray, and M. Santha, "Strategies for quantum races," *Leibniz Int. Proc. Informatics, LIPIcs*, vol. 124, no. 51, pp. 1–21, 2019.

[27] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic," *Entropy*, vol. 21, no. 9, p. 887, Sep. 2019.

[28] A. Behera and G. Paul, "Quantum to classical one-way function and its applications in quantum money authentication," *Quantum Inf. Process.*, vol. 17, no. 8, pp. 1–24, 2018.

[29] J. Jogenfors, "Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics," *ICBC 2019 - IEEE Int. Conf. Blockchain Cryptocurrency*, pp. 245–252, 2019.