UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

“CATEGORIZACIÓN DE PROTOCOLOS DE SEGURIDAD EN CRIPTOMONEDAS PARA MITIGAR ATAQUES INFORMÁTICOS: UNA REVISIÓN SISTEMÁTICA”

AUTOR:

JESÚS DAVID HOLGUÍN MENDOZA

TUTOR:

Msg. JOE LLERENA IZQUIERDO

Abril 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, Jesús David Holguín Mendoza, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor

Nombre: Jesús David Holguín Mendoza
CI. 0950641688.

Firma:
(Tutor): Ing. Joe Llerena Izquierdo, MSig.
C.I.: 0914884879

CATEGORIZACIÓN DE PROTOCOLOS DE SEGURIDAD EN CRIPTOMONEDAS PARA MITIGAR ATAQUES INFORMÁTICOS: UNA REVISIÓN SISTEMÁTICA

Jesús Holguín-Mendoza [1][0000-0001-9990-3880], and Joe Llerena-Izquierdo [1][0000-0001-9907-7048]

[1]Universidad Politécnica Salesiana, Guayaquil, Ecuador
jholguinm@est.ups.edu.ec, jllerena@ups.edu.ec

Abstract. In this article, a systematic investigation was carried out about the security protocols of the different cryptocurrencies, studying their processes and their vulnerabilities, in addition to opening a door to researchers who seek topics related to consensus algorithms which make the protocols of cryptocurrencies. The objective is to categorize the security protocols that the different cryptocurrency systems have to mitigate risks in transactions. The role played by different security protocols such as proof of work (PoW) or proof of stake (PoS) among others and their effectiveness in the block chain and the security they provide. The exploratory method was used to identify the most important studies for conducting the research. A search string was used with the main keywords and inclusion and exclusion criteria were determined for the choice of the primary studies and as results we have the categorization of the main consensus protocols.

Keywords: Cryptocurrency, Security, Attacks, Blockchain.

Resumen. En el presente artículo se realizó una investigación sistemática acerca de los protocolos de seguridad de las diferentes criptomonedas estudiando sus procesos y sus vulnerabilidades, además de abrir una puerta a investigadores que busquen temas referentes a algoritmos de consensos los cuales hacen que se cumplan los protocolos de criptomonedas. El objetivo es categorizar los protocolos de seguridad que tienen los distintos sistemas de criptomonedas para mitigar los riesgos en las transacciones. El papel que juegan los diferentes protocolos de seguridad como prueba de trabajo (PoW) o prueba de participación (PoS) entre otros y su eficacia en la cadena de bloque y la seguridad que estos brindan. Se utilizó el método exploratorio para identificar los estudios más importantes para la realización de la investigación. Se utilizó una cadena de búsqueda con las principales palabras claves y se determinaron criterios de inclusión y exclusión para la elección de los estudios primarios y como resultados tenemos la categorización de los principales protocolos de consenso.

Palabras Claves: Criptomoneda, Seguridad, Ataques, Cadena de Bloques.

1 Introducción

Un protocolo de seguridad es un conjunto de normas que rigen dentro de la transferencia de transacciones de criptomonedas para garantizar integridad y seguridad dentro de la red. Los protocolos de consenso están relacionados con la seguridad mediante el uso de la criptografía la cual se basa en algoritmos para realizar el cifrado o codificación de datos para brindar seguridad y confidencialidad a ellos[1]. Las monedas criptográficas son monedas digitales de intercambio que emplea la criptografía para reforzar la integridad de las transacciones. El control de estas monedas se ejerce por una base de datos de transacciones financieras descentralizada conocida como cadena de bloques[2].

Las monedas criptográficas tienen como principales características la garantía de seguridad, integridad y la transparencia de su contabilidad. Violar la seguridad que manejan las criptomonedas a un nivel matemático sería posible, pero llevar esta violación a cabo representaría mucha dificultad gracias a los algoritmos de consenso que dan respuestas para mitigación de ataques y usan, por ejemplo, algoritmos criptográficos para que la integridad de la cadena de bloque no se vea interrumpida por atacantes[3].

El uso de las monedas criptográficas representa distintos beneficios tales como:

- Evitar el pago a intermediarios al ser descentralizadas.
- Disminuir el tiempo de transacción a cuestión de minutos.
- No existe la necesidad de un intermediario de confianza para llevar a cabo las transacciones.

La creación de la primera moneda criptográfica fue dada en el año 2009 por un desarrollador con el pseudónimo de Satoshi Nakamoto llamándolas bitcoin[4], este desarrollador se basó en la función criptográfica SHA-256 y añadiendo una prueba de trabajo para la creación de esta, a raíz del surgimiento de la primera criptomoneda comenzó la creación de diversas monedas digitales utilizando protocolos criptográficos, las criptomonedas que han logrado sobresalir de entre más de siete mil monedas que se han creado hasta la actualidad son las que han aportado con innovaciones y han sabido valorizar y ubicar en el mundo del comercio digital.

Entre las principales criptomonedas tenemos: Bitcoin, Ethereum, Tether, XRP, Chainlink, Bitcoin cash, Binance coin, Litecoin, Polkadot, Cardano.

En la actualidad el bitcoin se ha convertido en la criptomoneda más potencial por su seguridad, confiabilidad y transparencia puesto a que utiliza el protocolo de consenso Prueba de Trabajo (PoW)[4], el cual apareció por primera vez en 1993 y se desarrolló para impedir ataques de denegación de servicios, envíos masivos de e-mails y de más abusos de servicios. En 2009 Bitcoin incluyó la innovación de utilizar la prueba de trabajo como un algoritmo de consenso que se usa para validar transacciones, es necesario que haya un consenso en la red de Bitcoin para que todos los nodos de la red estén viendo la misma información, es decir, los mismos bloques y consecuentemente las mismas transacciones[5]. El bitcoin ofrece innovación por su sistema descentralizado peer-to-peer que da la apertura a que dos partes puedan reali-

zar una transferencia sin depender de entidades financieras centralizadas, dando un uso independiente[6].

Ethereum fue creada por Vitalik Buterin en el año 2015 con la idea de tener una amplia variedad de aplicaciones descentralizadas para el uso de la plataforma que acoge la misma tecnología de Bitcoin con su cadena de bloques.

La cadena de bloques que es el registro único de la criptomoneda se está abriendo paso para ser una tecnología adoptada por el comercio electrónico en la actualidad[7]. La red de criptomonedas maneja un registro público en el que cualquier persona puede acceder y validar la legalidad de alguna transacción por sí mismo, esto genera confiabilidad ya que puede ver de manera íntegra la información que se agrega al registro público[8].

En el siguiente esquema mostramos un detalle de cómo funciona dicho sistema.

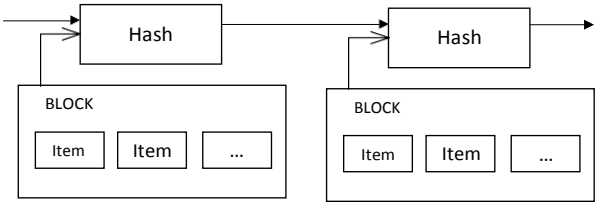

Fig. 1. Mapa sobre la cadena de bloques

2 Metodología

La presente investigación busca evidencias sobre la categorización de los protocolos de seguridad de las diferentes criptomonedas para mitigar los ataques informáticos, es por esto que se ha desarrollado una revisión sistemática, obteniendo así mayores fuentes de información de un punto de vista académico para la elaboración de este artículo.

2.1 Proceso de mapeo sistemático

A continuación, mostramos mediante esquema gráfico el proceso del mapeo sistemático.

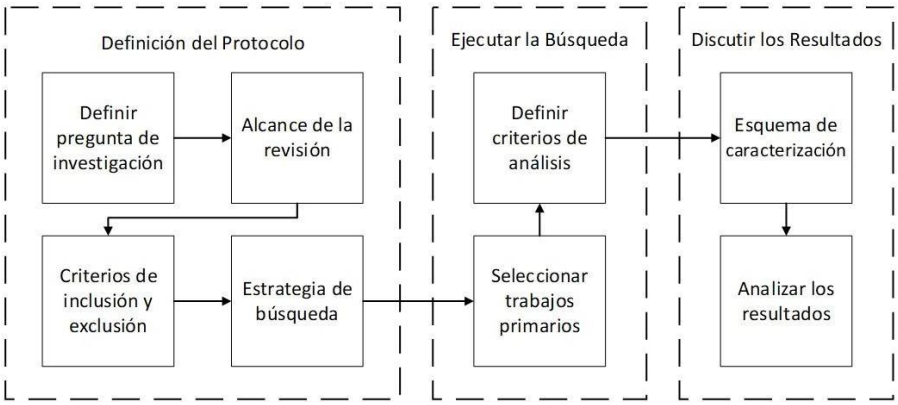

Fig. 2. Esquema del proceso de mapeo sistemático

2.2 Preguntas de investigación

El presente estudio busca solucionar la pregunta a investigación que detallamos a continuación: ¿Qué interés se ha expuesto en las investigaciones anteriores sobre la categorización de protocolos de seguridad para las criptomonedas?

2.3 Alcance de revisión

La presente investigación tuvo un periodo de búsqueda de los artículos publicados entre el año 2015 hasta el año 2021, usando como base de datos los siguientes sitios:

- IEEE
- SCOPUS
- WEB OF SCIENCE

Se tomaron en cuenta además otras búsquedas que llevan mucha relación con la investigación. En las bases de datos antes mencionadas se utilizó la siguiente cadena de búsqueda: (criptocurrency AND security AND attacks).

2.4 Criterios de inclusión

Se escogieron los artículos que cumplen con los siguientes criterios de inclusión:

- Se incluyeron todos los estudios que tienen relación directa con el tema de investigación.
- Además, se incluyeron estudios que estén publicados en revistas o conferencias.
- Se incluyeron estudios en idioma: inglés, español.

2.5 Criterios de exclusión

En esta investigación se tomaron en cuenta los siguientes criterios de exclusión:

- Se excluyeron todos los estudios que no tengan una pregunta formulada de investigación.
- Se excluyeron aquellos estudios como debates u opiniones que no presenten evidencias de su criterio.
- Se excluyeron estudios que su principal aporte no esté relacionado directamente con la seguridad de las criptomonedas.

2.6 Estrategias de búsqueda

En nuestra investigación implementamos 3 filtros para la elección de los estudios primarios que utilizaremos, las cuales se pueden verificar en la siguiente tabla:

Table 1. Estrategia de búsqueda.

Filtro 1	Revisión de título.
Filtro 2	Revisión del Resumen o Abstracto.
Filtro 3	Lectura y análisis completo del contenido.

2.7 Selección de estudios primarios

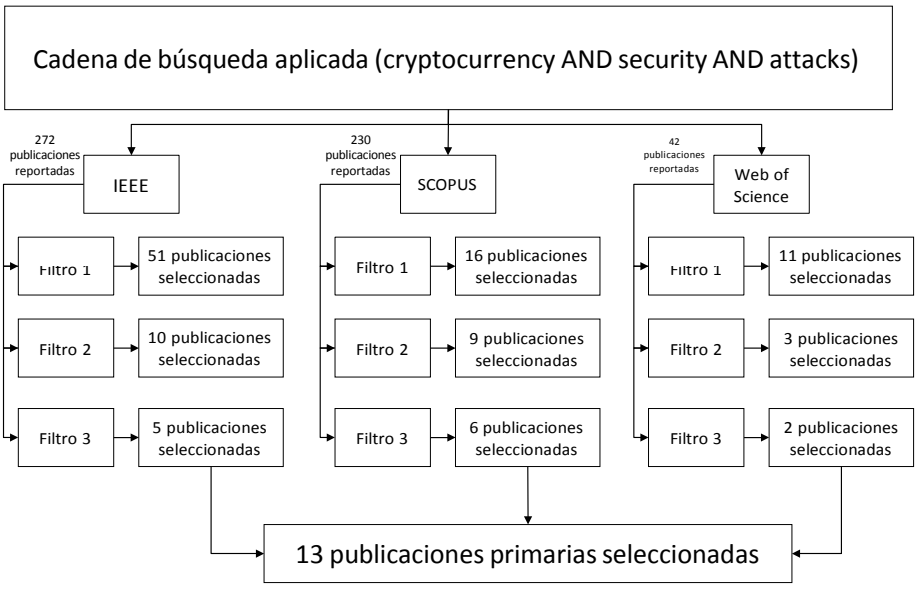

Fig. 3. Esquema de selección de estudios primarios

Después de haber aplicado la estrategia de búsqueda y culminando con el filtro 3, quedaron como resultados de esta búsqueda 13 publicaciones primarias, las cuales se someterán a un análisis.

2.8 Definición de los criterios de análisis

Se analizaron los estudios primarios bajo los siguientes criterios de análisis:

- **Criterio 1.** Protocolos de consenso: Se busca saber que la información dada en estos estudios comprenda no solo las distintas criptomonedas si no también sus protocolos aplicados en la cadena de bloque.
- **Criterio 2.** Vulnerabilidades: Se busca saber si los protocolos de consenso tienen vulnerabilidades ante amenazas o ataques informáticos para brindar una puerta a futuros estudios de investigación.

3 Resultados

En esta etapa presentaremos los análisis realizados a los estudios primarios discutiendo los resultados obtenidos.

3.1 Análisis de los estudios primarios

Table 2. Identificación de estudios primarios

Título	Autores	Año	Ref.	Protocolos de consensos estudiados
A Landscape of Cryptocurrencies	Zhaofang Li, Qinghua Lu, Shiping Chen, Yue Liu, Xiwei Xu	2019	[9]	PoW, PoS, PBFT, DPoS, Pol, Tangle, dBFT, PoA
A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS	Cristian Lepore, Michela Ceria, Andrea Visconti, Udai Pratap Rao, Kaushal Arvindbhai Shah, Luca Zanolini	2020	[10]	BFT, Pow. PoS, Pure PoS
A Survey on Security and Privacy Issues of Bitcoin	Mauro Conti, E. Sandeep Kumar, Chhagan Lal, Sushmita Ruj	2018	[11]	PoW
A survey on the security of blockchain systems	Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wenc	2017	[12]	PoW, PoS, PBFT, DPoS
A systematic literature review of blockchain cyber security	Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo	2019	[13]	Systematic literature review
Availability analysis of a permissioned blockchain with a lightweight consensus protocol	Amani Altarawneh, Fei Sun, Richard R. Brooks, Owulakemi Hambolu, Lu Yu, Anthony Skjellum	2020	[14]	PoW, PoS, PBFT, DPoS, Pol, Tangle, dBFT, PoET, RAFT
Contextualizing Consensus Protocols in Blockchain A Short Survey	Golam Bashar, Graham Hill, Subroto Singha, Praneeth MArella, Gaby G. Dagher, Jidong Xiao	2019	[15]	PoW, PoS, PoB, PoAc, PoI, PoA, PoET, PoL
Countering Block Withholding Attack Efficiently	Suhyeon Lee, Seungjoo Kim	2019	[16]	PoW
Impacts of Consensus Protocols and Trade Network Topologies on Blockchain System Performance	Xianhua Wei, Aiya Li, Zhou He	2020	[17]	PoW, PoS, DPoS
Security Issues and Vulnerabilities	Kevin Jonathan, Anny Kartika	2019	[18]	PoW, PoS

On A Blockchain System: A Review	Sari			
Security of Cryptocurrencies in blockchain technology State-of-art, challenges and future prospects	Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar	2020	[1]	PoW, PoS, PBFT, DPoS, Ripple, Tendermint
The Best of Both Worlds A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance	Matthias Baudlet, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi	2020	[19]	PoW, PoS
The Use of Blockchain in Financial Area A Systematic Mapping Study	Maicon Azevedo da Luz, Kleiner Farias	2020	[20]	PoW, PoS, PBFT

3.2 Discusión por criterios

Esta sección tiene como objetivo responder a nuestra pregunta de investigación ¿Qué interés se ha expuesto en las investigaciones anteriores sobre la categorización de protocolos de seguridad para las criptomonedas?, así que se presentarán las discusiones para los criterios antes expuestos.

Criterio 1

Después de una extensa lectura hemos encontrados que los dos protocolos de consenso más mencionados en los estudios primarios son Prueba de Trabajo (PoW) y Prueba de Participación (PoS), los cuales son utilizados en la dos principales criptomonedas en el mundo, estos algoritmos son muy conocidos por su alto nivel de seguridad y confiabilidad los cuales está preparados para mitigar todas las amenazas y ataques conocidos y a su vez cada día van evolucionando para mitigar los ataques informáticos[1][9][10][14][15][17][18].

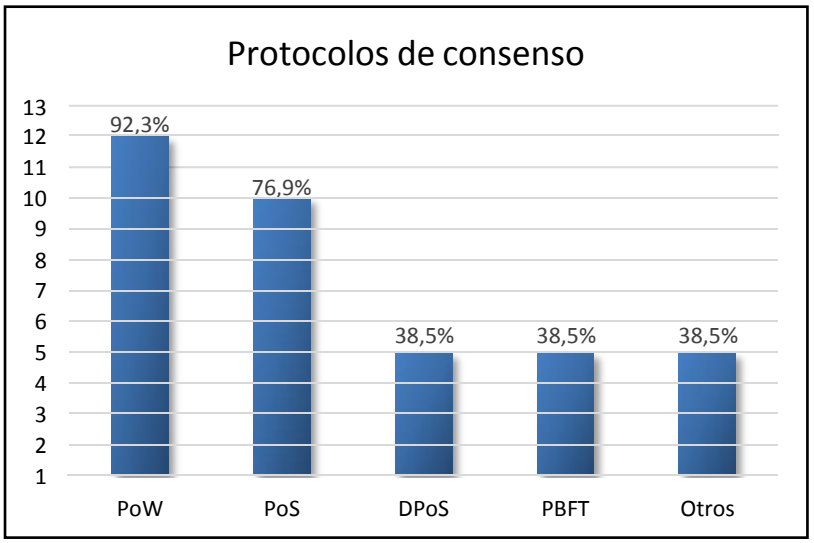

Fig. 4. Número de estudios en los que aparecen los principales protocolos de consenso

Criterio 2

Este análisis ofreció un resultado positivo frente al nivel de seguridad que ofrecen estos protocolos. La mayoría de criptomonedas emplean los algoritmos de Prueba de Trabajo (PoW), Prueba de Participación (PoS) y Tolerancia Práctica a Fallas Bizantinas (PBFT). Se utilizan en la cadena de bloques brindando confiabilidad y que poseen la capacidad de proteger y mitigar las amenazas y ataques evitando, por ejemplo, transacciones fraudulentas.

Sin embargo, los protocolos de consenso tienen vulnerabilidades que pueden violentar las criptomonedas. En este análisis los estudios[1][18], describen el porcentaje de umbral de ataque de los principales protocolos de consenso, los cuales se mencionan a continuación: Prueba de Trabajo (PoW) tiene hasta un 25% de umbral de ataque, los algoritmos Tolerancia Práctica a Fallos Bizantinos (PBFT) y Prueba de Participación Delegada (DPoS) presentan hasta un 33% de umbral de ataque, mientras que el algoritmo Prueba de Participación (PoS) tiene hasta un 51% de umbral de ataque. Entre las principales vulnerabilidades que se presentan en estos protocolos de consenso tenemos el ataque del 51% y el problema de nada en juego.

4 Discusión

Se llevó a cabo una extensa investigación en las diferentes plataformas de bibliotecas de búsqueda empleando palabras claves y una cadena de búsqueda con los cuales encontramos los artículos más relacionados a nuestro tema y los protocolos usados en las criptomonedas principales, estos protocolos aplican un alto nivel de seguridad con lo cual establecimos que son adecuados para ellas. En los últimos 5 años se han hecho muchas investigaciones sobre los protocolos de consenso, pero pocas hablan sobre una categorización, no obstante, se lograron extraer los más importantes, esto brinda una brecha para nuevas y futuras investigaciones.

Los protocolos de consenso juegan un papel importante en las criptomonedas ya que son los responsables de que se ejecuten todos los procesos de las transacciones en las diferentes criptomonedas nuestro estudio categoriza al protocolo de consenso PoW como el eficaz puesto que utiliza una prueba criptográfica muy segura pero que a su vez requiere de mucha capacidad computacional. PoS tiene un menor consumo energético con relación a PoW pero tiene un mayor umbral de ataque, seguido de los protocolos de consenso DPoS y PBFT.

5 Conclusión

Por medio del presente trabajo concluimos que los protocolos de consenso de las criptomonedas integra procesos seguros, brindando estabilidad a los usuarios gracias a su fiabilidad, veracidad, y transparencia en las transacciones que se emiten. La cadena de bloques, un sistema descentralizado que permite prescindir de otros intermediarios reduciendo así los costos de gastos y la inseguridad que se tiene al momento de hacer alguna transacción en la actualidad.

Existen muchos protocolos de consenso que se están estudiando aún y otros que tienen muy poco tiempo en el mercado de las criptomonedas o no han tenido trans-

cendencia no obstante dentro de un tiempo posterior se podrían hacer nuevas investigaciones referentes a nuevos protocolos de consenso que existieran.

Referencias

[1] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," *J. Netw. Comput. Appl.*, vol. 163, no. December 2019, p. 102635, 2020, doi: 10.1016/j.jnca.2020.102635.

[2] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of proof of work (POW) blockchains security network on selfish mining," *2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018*, pp. 126–130, 2018, doi: 10.1109/ISRITI.2018.8864381.

[3] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin Concepts, Threats, and Machine-Learning Security Solutions," *IEEE Access*, vol. 6, pp. 67189–67205, 2018, doi: 10.1109/ACCESS.2018.2874539.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Artif. Life*, vol. 23, no. 4, pp. 552–557, 2017, doi: 10.1162/ARTL_a_00247.

[5] Y. Liu *et al.*, "An efficient method to enhance Bitcoin wallet security," *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identification, ASID*, vol. 2017-Octob, pp. 26–29, 2018, doi: 10.1109/ICASID.2017.8285737.

[6] Y. Liu, X. Liu, L. Zhang, C. Tang, and H. Kang, "An efficient strategy to eliminate malleability of bitcoin transaction," *2017 4th Int. Conf. Syst. Informatics, ICSAI 2017*, vol. 2018-Janua, no. Icsai, pp. 960–964, 2017, doi: 10.1109/ICSAI.2017.8248424.

[7] A. Meynkhard, "Fair market value of bitcoin: Halving effect," *Invest. Manag. Financ. Innov.*, vol. 16, no. 4, pp. 72–85, 2019, doi: 10.21511/imfi.16(4).2019.07.

[8] C. Wang, X. Chu, and Y. Qin, "Measurement and Analysis of the Bitcoin Networks: A View from Mining Pools," pp. 180–188, 2020, doi: 10.1109/bigcom51056.2020.00032.

[9] Z. Li, Q. Lu, S. Chen, Y. Liu, and X. Xu, "A Landscape of Cryptocurrencies," *ICBC 2019 - IEEE Int. Conf. Blockchain Cryptocurrency*, pp. 165–166, 2019, doi: 10.1109/BLOC.2019.8751469.

[10] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of pow, pos and pure pos," *Mathematics*, vol. 8, no. 10, pp. 1–26, 2020, doi: 10.3390/math8101782.

[11] M. Conti, S. Kumar E, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *arXiv*, vol. 20, no. 4, pp. 3416–3452, 2017.

[12] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.

[13] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo,

"A systematic literature review of blockchain cyber security," *Digit. Commun. Networks*, vol. 6, no. 2, pp. 147–156, 2020, doi: 10.1016/j.dcan.2019.01.005.

[14] A. Altarawneh, F. Sun, R. R. Brooks, O. Hambolu, L. Yu, and A. Skjellum, "Availability analysis of a permissioned blockchain with a lightweight consensus protocol," *Comput. Secur.*, vol. 102, 2021, doi: 10.1016/j.cose.2020.102098.

[15] G. Bashar, G. Hill, S. Singha, P. Marella, G. G. Dagher, and J. Xiao, "Contextualizing consensus protocols in blockchain: A short survey," *Proc. - 1st IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2019*, pp. 190–195, 2019, doi: 10.1109/TPS-ISA48467.2019.00031.

[16] S. Lee and S. Kim, "Countering Block Withholding Attack Efficiently," *INFOCOM 2019 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2019*, pp. 330–335, 2019, doi: 10.1109/INFCOMW.2019.8845116.

[17] X. Wei, A. Li, and Z. He, "Impacts of consensus protocols and trade network topologies on blockchain system performance," *Jasss*, vol. 23, no. 3, pp. 1–20, 2020, doi: 10.18564/jasss.4289.

[18] K. Jonathan and A. K. Sari, "Security Issues and Vulnerabilities on A Blockchain System: A Review," *2019 2nd Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2019*, pp. 228–232, 2019, doi: 10.1109/ISRITI48646.2019.9034659.

[19] M. Baudlet, D. Fall, Y. Taenaka, and Y. Kadobayashi, "The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance," *2020 2nd Conf. Blockchain Res. Appl. Innov. Networks Serv. BRAINS 2020*, pp. 17–24, 2020, doi: 10.1109/BRAINS49436.2020.9223280.

[20] M. A. Da Luz and K. Farias, "The use of blockchain in financial area: A systematic mapping study," *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3411564.3411579.