# ANEXO A. REVISIÓN SISTEMÁTICA

En este anexo, se presentan las fases que se desarrollaron de acuerdo con la metodología PRISMA versión 2020 explicadas en el contexto de la investigación realizada, en cada una de ellas se explican los métodos de inclusión y exclusión de artículos, con el objetivo obtener un conjunto reducido de artículos que realmente tengan relevancia en la investigación

## Contenido

## 1. Revisión sistemática

En primer lugar, se escogieron las bases de datos que se tomaron como referencia para realizar la búsqueda de los artículos de interés, las cuales fueron Scopus y ScienceDirect, a las cuales la Universidad del Cauca brinda acceso. La revisión sistemática fue realizada utilizando la metodología *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* versión 2020, conocida por su sigla en inglés con el nombre de PRISMA.

La metodología PRISMA es usada para documentar revisiones sistemáticas, fue lanzada en el año 2009 haciendo referencia a cuatro fases: Identificación, presentación, elegibilidad e inclusión. En el caso de esta investigación, fue utilizada la versión de PRISMA 2020 que, a diferencia de la versión anterior, une las fases de presentación y elegibilidad en una sola denominada fase de detección. Como resultado, en esta nueva versión se cuenta solo con tres fases, las cuales son: fase de identificación, fase de detección y fase de inclusión [1].

A continuación, se presentan las fases que se desarrollaron de acuerdo con la metodología PRISMA versión 2020 explicadas en el contexto de la investigación realizada, en cada una de ellas se explican los métodos de inclusión y exclusión de artículos, con el objetivo obtener un conjunto reducido de artículos que realmente tengan relevancia en la investigación.

### 1.1. Fase de identificación

Se seleccionaron dos cadenas para realizar la búsqueda en la base de datos, las cuales contienen palabras clave que fueron consideradas importantes en la investigación. Debido a que el proyecto está enfocado en el transporte compartido usando *Blockchain,* la primera cadena fue la siguiente: ***“Blockchain AND transportation AND system AND shared”.*** Por otra parte, el segundo enfoque del proyecto es la autenticación de usuarios, por lo que la segunda cadena seleccionada

fue: ***"Blockchain AND identity AND authentication".*** Las dos cadenas mencionadas se denominarán en adelante cadena 1 y cadena 2 respectivamente.

La búsqueda fue filtrada por tipo de documento, excluyendo tipos como conferencias, noticias, libros, entre otros. Y solo se seleccionaron los correspondientes a artículos y revisiones.
Para la cadena 1 se encontraron 14 documentos en la base de datos Scopus y 2279 en la base de datos ScienceDirect. Para la segunda cadena, fueron encontrados 302 documentos en Scopus y 1485 en ScienceDirect.

**1.2. Fase de detección**

Teniendo en cuenta que la cantidad de resultados obtenidos al consultar las cadenas seleccionadas en las bases de datos fue demasiado grande para realizar una revisión completa de todos los artículos, se determinó como primer criterio de elegibilidad el descarte por título, el cual brinda una idea general del contenido de cada artículo. Luego de aplicar dicho criterio se obtuvieron los siguientes resultados.

De la cadena 1 resultaron 6 artículos de la base de datos de Scopus y en la base de datos ScienceDirect 11 artículos, para un total de 17 artículos. De la cadena 2 resultaron 135 artículos de la base de datos de Scopus y en la base de datos ScienceDirect 77 artículos. Pero, 9 de estos 77 artículos estaban repetidos en la base de datos Scopus, por lo que quedaron en total, entre las dos bases de datos, 203 artículos.

Posteriormente, se aplicó el segundo criterio de elegibilidad que consistió en la revisión del "abstract" (resumen) de cada artículo seleccionado, teniendo en cuenta los siguientes criterios:

1. Para la cadena 1 se descartaron aquellos artículos que no se basaran en sistemas de transporte compartido, sin importar el tipo de medio usado.

2. Para la cadena 2, se descartaron aquellos artículos que no se refirieron a la autenticación de usuarios, es decir aquellos que mencionan autenticación basada en *Blockchain,* pero sin enfatizar en identidad o en seres humanos.

Luego de aplicar los criterios mencionados, para la cadena 1 se encontró solamente 1 artículo correspondiente a la base de datos de ScienceDirect, esto debido a que los resultados encontrados no presentaron un sistema de movilidad compartido y, en los casos donde los documentos tratan de transporte compartido no estaban basados en la tecnología *Blockchain* que es uno de los criterios de la cadena.

Para la cadena 2 se encontraron 68 artículos en la base de datos de Scopus y 39 en ScienceDirect para un total de 107 artículos seleccionados considerando el *abstract*. Luego de realizar el proceso de filtrado por título y *abstract*, se detectó que aún había un número elevado de artículos para continuar con la tercera fase de la metodología PRISMA, por tanto, fue aplicado un tercer filtro que consistió en revisar si los artículos contenían un desarrollo software o algún tipo de algoritmo que explicara de manera clara cuál ha sido el proceso de implementación del sistema propuesto. Adicionalmente a ello, se realizó una revisión de las conclusiones, para determinar si los autores habían logrado los objetivos que se propusieron con sus respectivos proyectos.
Al aplicar el filtro mencionado, se obtuvieron los siguientes resultados:

De la cadena 1 se descartó el único artículo que se tenía hasta ese proceso.

De la cadena 2, en la base de datos Scopus, quedaron 11 artículos después del proceso de descarte y en la base de datos ScienceDirect quedaron 14, para un total de 25 artículos entre las dos bases de datos, estos fueron los artículos que pasaron a la etapa de inclusión, que es la tercera fase de la metodología PRISMA.

### 1.3. Fase de inclusión

Se realizó una lectura detallada de los artículos seleccionados hasta esta etapa (25 en total), los cuales se dividieron en grupos de acuerdo con la temática que abarcan. Los grupos fueron: medicina, movilidad y autenticación.

#### 1.3.1. Trabajos relacionados

La revisión sistemática realizada permitió identificar tecnologías, métodos, sistemas y diferentes puntos de vista que fueron la base para el planteamiento de la solución propuesta en el presente trabajo. De acuerdo con los resultados obtenidos en la fase de inclusión, se presentan a continuación, los trabajos más relevantes de cada grupo identificado.

##### 1.3.1.1. Medicina, tele-salud y entidades prestadoras de servicios.

El primer grupo corresponde a artículos en el área de la medicina, esta área históricamente ha manejado inmensas cantidades de datos que no se almacenan de manera segura, por lo cual no se tiene un adecuado control de acceso. Con la llegada de la era digital, esta información empezó a migrar a bases de datos y a la Internet, pero seguía siendo "hackeada" o interceptada cuando se enviaba de manera remota. Una de las opciones para introducir seguridad en esta área ha sido la tecnología *Blockchain*, debido a las ventajas que brinda con respecto a privacidad y anonimato.

- En el artículo ***A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records (EHR) ([2])*** se diseña un modelo de autenticación para pacientes y gestión de las historias médicas por medio de credenciales verificables (*Verifiable credential, VC*) e identificadores descentralizados (*Decentralized identifier, DID*) basados en la tecnología *Blockchain*. Estos identificadores son generados por un algoritmo que aloja los datos en la *Blockchain* Indi de *Hyper Ledger*.

La importancia de este artículo radica en la descentralización de los datos médicos sensibles alojados en la Blockchain, puesto que los pacientes necesitan que la información que existe en sus historias médicas sea sólo accesible por ellos y por los médicos y entidades que le brindan el seguimiento a su condición médica. El equipo de trabajo en el artículo logra proponer un modelo basado en Blockchain para autenticación de pacientes y entidades conservando la privacidad y la gestión del consentimiento para el acceso a los registros EHR mediante VC y DID.

- El artículo ***A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems ([3])*** propone un sistema de autenticación y gestión de identidad para sistemas de salud electrónicos (*e-health*) basado en *Blockchain* que trata de solventar los problemas de seguridad y privacidad que introducen los sistemas de información en línea.

  Este artículo es importante debido a que el sistema PBBIMUA propuesto por los autores utiliza un nuevo mecanismo de distribución de claves para la autenticación y gestión en sistemas de salud electrónicos. Estas claves se obtienen a través de algoritmos de cifrado partiendo de los datos biométricos personales que, a su vez, se alojan en la *Blockchain*. Este mecanismo puede brindar una base en cuanto al manejo de datos biométricos en el proceso de autenticación de la solución propuesta en este trabajo.
- El artículo ***Health-ID A Blockchain-Based Decentralized Identity Management for Remote Healthcare ([4])*** brindó una solución en el contexto de la pandemia por Covid19, durante la cual, muchos servicios *e-health* tuvieron auge, pero los usuarios tenían que confiar en el manejo que los proveedores de estos servicios le daban su información de identidad. Por ello, los autores del artículo proponen un sistema de gestión de identidad descentralizada donde pacientes y proveedores de atención médica se identifican y autentican de manera transparente, segura y descentralizada mediante identificadores de salud (HealthID) que se almacenan en la *Blockchain* Ethereum.
- El artículo ***A decentralized framework for device authentication and data security in the next generation internet of medical things ([5])*** presenta un

protocolo de autenticación basado en técnicas criptográficas clonables (Physical Unclonable Function, PUF) las cuales, debido a su compleja matemática son difíciles de replicar. Junto a esta técnica criptográfica, este artículo usa *Blockchain* para el intercambio de datos seguros en la red. La asignación de dichas claves (técnica criptográfica) se hace según la distancia Hamming entre los nodos y, cada par de entidades que se comunican deben tener la misma clave, además se analiza la seguridad de su propuesta respecto a algunos ataques como sybyl, suplantación de identidad, reproducción entre otros.

#### 1.3.1.2. Vehículos y movilidad

El segundo grupo corresponde a artículos que se centran en la movilidad y vehículos en el contexto de los ITS. Este ámbito ha sido influido por el Internet y los dispositivos *IoT*, haciendo que se compartan datos con otros vehículos o con sistemas inteligentes de control de transporte.

- El artículo ***EASBF An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles ([6])*** propone un esquema de autenticación basado en *Blockchain* para *Fog computing* (computación de niebla) segura en el Internet de vehículos, además, usa criptografía de curva elíptica, función hash unidireccional y un algoritmo de consenso Práctica Tolerancia a Fallos Bizantinos (*Practical Byzantine Fault Tolerance, PBFT*) para garantizar confidencialidad, anonimato, privacidad e integridad.
- En el artículo ***Towards blockchain-IoT based shared mobility Car-sharing and leasing as a case study ([12])*** se presenta una arquitectura de alto nivel para promover la movilidad compartida combinando el uso compartido de vehículos con el arrendamiento de estos a través de una plataforma *Blockchain - IoT*. Cabe resaltar que en este artículo se propone un enfoque híbrido para disminuir el consumo de recursos junto a un puntero hash que permite a los usuarios el derecho al olvido en la plataforma.

- En ***Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing ([7])*** se propone un sistema de autenticación en grupo con *Blockchain* basado en el intercambio de secretos y en un proxy mecánico. En este artículo se cuenta con una entidad de confianza, vehículos comunes, vehículos proxy y unidades de carretera (RSU). Un vehículo proxy y una RSU realizan el proceso de autenticación mutua, luego varios vehículos pueden conectarse a un vehículo proxy formando grupos de autenticación.

#### 1.3.1.3. Autenticación

El tercer grupo de artículos se centra en la autenticación, ya sea de usuarios o de dispositivos IoT, dado que los datos que se almacenan en los sistemas de información en internet deben permanecer privados y los usuarios deben tener la garantía de que nadie pueda suplantar su identidad.

- En el artículo ***A zero-knowledge-proof-based digital identity management scheme in blockchain ([8])*** se mejora el sistema tradicional centralizado de administración de identidad (Digital Identity Management System, DIMS) con ayuda de los contratos inteligentes y algoritmos de prueba de conocimiento cero (Zero Knowledge Protocol, ZKP). Consiste en un sistema de reclamo que se desvincula de la identidad del usuario, el cual puede revelar selectivamente sus atributos.
- El artículo ***PTAS Privacy-preserving Thin-client Authentication Scheme in blockchain-based PKI ([9])*** presenta un esquema de autenticación de cliente ligero que le permite al usuario recuperar su información privada. Además, garantiza la seguridad mediante un nuevo modelo denominado PTAS(m-1). Este artículo también utiliza una autoridad de certificación que actúa como un tercero de confianza.
- ***AuthChain A decentralized blockchain-based authentication system ([10])*** es un artículo que trata de solucionar el problema de la centralización de la

información del usuario en servicios en línea. Debido a que los usuarios dependen de la gestión de identidad y autenticación de su proveedor de servicios, esto hace que las credenciales de usuario estén expuestas a riesgos como fugas información y ataques de hackers. Para dar solución al problema planteado, los autores del artículo proponen un sistema denominado *"Authchain*". *"Authchain*" es un sistema de autenticación seguro y descentralizado, alojado en la *Blockchain* Ethereum, para proveedores de servicios en línea, en el que sus usuarios pueden autenticarse disminuyendo la posibilidad de ataques y fugas de datos.

- En el artículo ***A secure end-to-end verifiable e-voting system using blockchain and cloud server ([11])*** se propone específicamente una técnica criptográfica para la elección de un voto autenticado modificando el sistema existente DRE-ip. En este artículo el proceso de registro y autenticación de votantes se realiza utilizando el algoritmo de Fuzzy Vault y un cifrado biométrico.

### 1.3.2. Resumen de evaluación de los trabajos relacionados

En la Tabla 1 se muestra un resumen de los criterios que se consideraron importantes respecto a los trabajos relacionados, en donde se puede observar que sólo tres de las soluciones de los trabajos relacionados están enfocadas en transporte, pero ninguno se centra en el carpooling, aunque la mayoría de artículos realiza una autenticación de usuarios (solo tres realizan autenticación de dispositivos), no realizan autenticación o manejo de datos biométricos. Solo un artículo está enfocado en transporte y realiza autenticación de usuarios y es el único amigable con el medio ambiente, pero no realiza autenticación o manejo de datos biométricos ni pruebas de seguridad.

| **Criterio / Propuesta** | **[40]** | **[41]** | **[42]** | **[43]** | **[44]** | **[21]** | **[45]** | **[46]** | **[47]** | **[48]** | **[49]** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Enfocado en transporte** | | | | | ✔ | ✔ | ✔ | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Autenticación de usuarios** | ✔ | ✔ | ✔ | | | ✔ | | ✔ | ✔ | ✔ | ✔ |
| **Autenticación de dispositivos** | | | | ✔ | ✔ | | ✔ | | | | |
| **Manejo de datos biométricos** | | ✔ | ✔ | | | | | | | | ✔ |
| **Amigable con el medio ambiente** | | | | | | ✔ | | | | | |
| **Pruebas de seguridad** | ✔ | ✔ | | | ✔ | | ✔ | ✔ | ✔ | | ✔ |
| **Uso de métodos de encriptación** | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ |

Tabla 1. Resumen de evaluación de los trabajos relacionados.

**Referencias**


[1] Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Salsear, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McKenzie, J. E. "PRISMA 2020 *explanation and elaboration: updated guidance and exemplars for reporting systematic reviews*", BMJ, p. 160, marzo de 2021. Disponible: https://doi.org/10.1136/bmj.n160

[2] M. T, K. Makkithaya y N. V G, "*A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records", Cogent Engineering*, vol. 9, n.º 1, marzo de 2022. Doi: https://doi.org/10.1080/23311916.2022.2035134

[3] X. Xiang, M. Wang and W. Fan, "*A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems*," in IEEE Access, vol. 8, pp. 171771-171783, 2020, doi: 10.1109/ACCESS.2020.3022429.

[4] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi y K. N. Qureshi, "Health-ID: *A Blockchain Based Decentralized Identity Management for Remote Healthcare", Healthcare,* vol. 9, n.º 6, p. 712, junio de 2021. Doi: https://doi.org/10.3390/healthcare9060712

[5] K. P. Satamraju y B. Malarkodi, "*A decentralized framework for device authentication and data security in the next generation internet of medical things", Computer Communications,* vol. 180, pp. 146–160, diciembre de 2021. doi: https://doi.org/10.1016/j.comcom.2021.09.012

[6] M. S. Eddine, M. A. Ferrag, O. Friha y L. Maglaras, "EASBF: *An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles", Journal of Information Security and Applications*, vol. 59, p. 102802, junio de 2021. Doi: https://doi.org/10.1016/j.jisa.2021.102802

[7] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan and Y. Zhang, "*Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge*

*Computing," in IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221-4232, April 2020, doi: 10.1109/TVT.2020.2969722.

[8] X. Yang y W. Li, *"A zero-knowledge-proof-based digital identity management scheme in blockchain", Computers & Security*, vol. 99, p. 102050, diciembre de 2020. Doi: https://doi.org/10.1016/j.cose.2020.102050

[9] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong y X. Lin, "PTAS: *Privacy-preserving Thin-client Authentication Scheme in blockchain-based PKI", Future Generation Computer Systems*, vol. 96, pp. 185–195, 2019. doi: https://doi.org/10.1016/j.future.2019.01.026

[10] S. Y. Lim, P. T. Fotsing, O. Musa y A. Almasri, "*AuthChain: A Decentralized Blockchain-based Authentication System", International Journal of Engineering Trends and Technology*, pp. 70–74, octubre de 2020. Doi: https://doi.org/10.14445/22315381/cati1p212

[11] S. Panja y B. Roy, *"A secure end-to-end verifiable e-voting system using blockchain and cloud server", Journal of Information Security and Applications*, vol. 59, p. 102815, 2021. doi: https://doi.org/10.1016/j.jisa.2021.102815

[12] S. Auer, S. Nagler, S. Mazumdar y R. R. Mukkamala, "*Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study", Journal of Network and Computer Applications*, vol. 200, p. 103316, abril de 2022. Doi: https://doi.org/10.1016/j.jnca.2021.103316