Blockchain y control de acceso en la Industria 5.0: Una revisión de los desafíos y oportunidades

R.A.Ibarra-García
CINVESTAV Unidad Guadalajara
Zapopan 45019, México
ricardo.ibarra@cinvestav.mx

A.Díaz-Pérez
CINVESTAV Unidad Guadalajara
Zapopan 45019, México
adiaz@cinvestav.mx

J.L.González-Compeán
CINVESTAV Unidad Tamaulipas
Ciudad Victoria 87130, México
joseluis.gonzalez@cinvestav.mx

***Resumen*—Blockchain ha surgido como una solución emergente para mejorar la transparencia y la descentralización en los sistemas de control de acceso dentro del contexto de la Industria 5.0, caracterizada por entornos interconectados y sistemas ciberfísicos. Sin embargo, a pesar de sus ventajas evidentes, como la mejora de la trazabilidad y la inmutabilidad de los registros, su adopción enfrenta desafíos considerables tales como problemas de escalabilidad y elevados costos computacionales, los cuales dificultan su implementación a gran escala. Este artículo realiza una revisión de la literatura actual, comparando distintos enfoques como el uso de contratos inteligentes, sistemas distribuidos y soluciones híbridas que integran blockchain con tecnologías tradicionales de control de acceso. Además, se exploran los desafíos pendientes y las oportunidades para el desarrollo de sistemas de control de acceso dinámicos y eficientes. Esta revisión proporciona una visión integral del estado de la investigación en blockchain aplicado al control de acceso, destacando su potencial para fortalecer la ciberseguridad en la Industria 5.0 y proponiendo direcciones futuras para investigación y desarrollo.**

***Palabras clave*—blockchain, control de acceso, industria 5.0, ciberseguridad, sistemas ciberfísicos**

I. Introducción

La Industria 5.0 se caracteriza por una convergencia acelerada de tecnologías avanzadas como los sistemas ciberfísicos, el Internet de las Cosas (IoT), la inteligencia artificial (IA) y la conectividad a gran escala [1]. En este contexto, el control de acceso a los sistemas y datos juega un papel fundamental para garantizar la seguridad y la integridad de los procesos industriales y de los flujos de información [2]. Sin embargo, los métodos tradicionales de control de acceso centralizados presentan limitaciones significativas en términos de escalabilidad, transparencia y resiliencia ante ataques. A medida que el número de usuarios y dispositivos crece, estos sistemas enfrentan problemas de rendimiento debido a la concentración de control en una única autoridad central. Además, la falta de transparencia dificulta la auditoría y el monitoreo efectivo de los accesos, lo que puede generar riesgos de seguridad. Por último, la centralización los hace vulnerables a fallos o ataques dirigidos, ya que un único punto de fallo puede comprometer el acceso a todo el sistema [3], [4].

Blockchain se ha convertido en una solución eficaz para mitigar los problemas de centralización y falta de transparencia en los sistemas de control de acceso. Concretamente, la blockchain ofrece ventajas en estos escenarios, tales como [4]–[6]:

- **Descentralización:** Elimina la necesidad de un intermediario central, reduciendo los puntos únicos de fallo y aumentando la confiabilidad del sistema.
- **Inmutabilidad:** Los registros almacenados en la blockchain no pueden ser modificados o alterados, lo que garantiza la integridad de los datos.
- **Transparencia:** Todas las acciones relacionadas con el control de acceso son visibles y verificables, lo que permite auditorías precisas.

A pesar de estas ventajas, la implementación de blockchain en sistemas de control de acceso no está exenta de desafíos. Entre los más significativos se encuentran [7], [8]:

- **Escalabilidad:** Los sistemas basados en blockchain aún enfrentan dificultades para manejar grandes volúmenes de transacciones en tiempo real, lo que puede limitar su aplicabilidad en entornos industriales a gran escala.
- **Costos computacionales:** El mantenimiento de una red blockchain puede implicar altos costos en términos de recursos computacionales y energéticos.

En este artículo, se presenta una revisión de las propuestas más relevantes en la literatura para la integración de blockchain en sistemas de control de acceso, haciendo énfasis en:

- El uso de *contratos inteligentes* para la gestión dinámica de permisos y autorizaciones.
- Sistemas de *control de acceso distribuidos*, que aprovechan las ventajas de la blockchain para mejorar la seguridad y la resiliencia.
- Soluciones *híbridas*, que combinan la blockchain con tecnologías tradicionales para abordar sus limitaciones inherentes.

Además, se identifican los principales desafíos que aún deben resolverse para lograr una implementación exitosa en la Industria 5.0, así como las oportunidades futuras para la investigación y el desarrollo en este campo. Este análisis busca ofrecer una visión integral del estado del arte y proporcionar un punto de partida para futuros estudios sobre el control de acceso en entornos industriales avanzados.

ISSN: 3061-8991

II. Blockchain y control de acceso: Preliminares

En esta sección se introducen los conceptos fundamentales que forman la base de la integración de blockchain con los sistemas de control de acceso, con un enfoque en los modelos más relevantes de control de acceso en la industria actual. Estos conceptos son clave para comprender el desarrollo de propuestas que buscan mejorar la seguridad y eficiencia de los sistemas en la Industria 5.0.

A. Blockchain: Principios fundamentales

Blockchain es una arquitectura compuesta de diversas tecnologías que, en conjunto, permiten su funcionamiento descentralizado, seguro e inmutable, lo cual permite hacer registros que almacenan transacciones en bloques encadenados cronológicamente, garantizando la integridad y seguridad de los datos sin necesidad de una autoridad central. En un entorno de blockchain, cada nodo de la red mantiene una copia del libro mayor, lo que elimina el riesgo de un punto único de fallo y aumenta la resistencia contra ataques externos [9], [10].

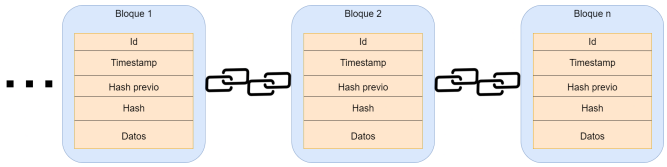

Fig. 1. Representación de una blockchain.

La Figura 1 representa la estructura simplificada de una blockchain. Esta se organiza como una secuencia de bloques enlazados, donde cada bloque contiene los siguientes elementos que aseguran la integridad, seguridad y cronología de los datos:

- **Id**: Es un identificador único del bloque, que lo distingue de otros bloques dentro de la cadena. Generalmente está relacionado con el número de bloque en la secuencia.
- **Timestamp**: Esta es la marca de tiempo que registra el momento exacto en que el bloque fue creado o validado. Es importante para mantener el orden cronológico entre los bloques.
- **Hash previo**: Este campo contiene el hash criptográfico del bloque anterior en la cadena. Es lo que enlaza cada bloque con el anterior, formando una cadena inmutable. Si algún bloque previo es alterado, el hash previo en el bloque siguiente cambiaría, rompiendo la cadena y permitiendo detectar cualquier intento de manipulación.
- **Hash**: Es el hash generado para el bloque actual, calculado a partir de toda la información contenida en el bloque, incluidos los datos. Cualquier alteración en los datos del bloque cambiaría este valor, asegurando así la inmutabilidad de la información.
- **Datos**: Esta sección contiene la información que se quiere almacenar en el bloque. Puede ser información transaccional, contratos inteligentes o cualquier dato que se desee registrar de manera segura y transparente.

Cada bloque está enlazado con el anterior mediante el *hash previo*, lo que garantiza que la cadena sea inmutable y segura. Si un bloque es alterado, todos los bloques siguientes se verán afectados, haciendo evidente cualquier intento de manipulación. La combinación del *hash* y el *hash previo* asegura la integridad y la seguridad de los datos en una blockchain, mientras que el *timestamp* garantiza la secuencia temporal correcta de los eventos.

El consenso entre los nodos se logra a través de diferentes mecanismos (como *Proof-of-Work* o *Proof-of-Stake* [11]) que aseguran que las transacciones sean verificadas y validadas de manera descentralizada. Esta arquitectura ofrece ventajas como la descentralización, transparencia e inmutabilidad [5], [7] que son fundamentales en la implementación de sistemas de control de acceso.

B. Contratos inteligentes

Los contratos inteligentes, o *smart contracts*, son programas informáticos que se ejecutan automáticamente cuando se cumplen condiciones predefinidas. Estos contratos se almacenan en la blockchain y permiten que las partes involucradas en una transacción realicen acuerdos sin necesidad de intermediarios. Una vez que se activan las condiciones establecidas, el contrato inteligente se ejecuta por sí solo, de manera transparente, irreversible y segura [12].

En el contexto del control de acceso, los contratos inteligentes permiten ejecutar reglas de acceso de forma automática, eliminando la necesidad de intervención manual. Esto reduce el tiempo de espera en las decisiones de autorización, lo que mejora el rendimiento en entornos dinámicos como la Industria 5.0, garantizando que solo los usuarios con los derechos apropiados accedan a los recursos correspondientes. Además, al estar registrado en la blockchain, cada ejecución de un contrato inteligente queda almacenada de forma inmutable, lo que facilita las auditorías y el seguimiento de eventos de acceso.

C. Control de acceso: Modelos y tipologías

El control de acceso es un mecanismo importante en los sistemas de seguridad informática para regular qué entidades pueden acceder a qué recursos dentro de un sistema. Existen varios modelos que determinan cómo se gestiona el acceso, dependiendo de las políticas y estructuras organizacionales.

La Figura 2 representa una estructura simplificada de un **sistema de control de acceso a recursos**. En este sistema, múltiples usuarios intentan acceder a un conjunto de recursos protegidos, y su capacidad para hacerlo depende de los permisos y las credenciales que posean. Los componentes principales se describen a continuación:

- **Usuarios (Usuario 1, Usuario 2, Usuario n)**: Cada usuario tiene una llave que simboliza sus credenciales o permisos de acceso. Solo podrán acceder a los recursos si sus credenciales son válidas y coinciden con los requisitos de seguridad del sistema.
- **Llaves de acceso**: Las llaves representan los mecanismos de autenticación que cada usuario debe proporcionar para

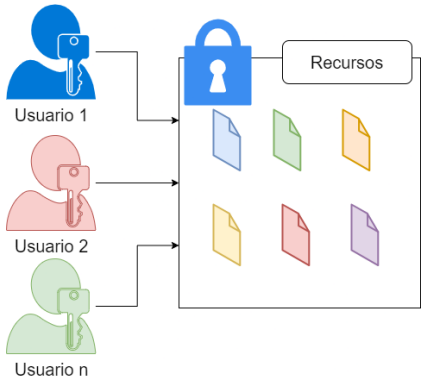

Fig. 2. Representación del control de acceso a recursos.

acceder a los recursos. Estos mecanismos pueden incluir contraseñas, atributos, tokens de seguridad, o certificados digitales que garanticen la autenticidad del usuario.

- **Recursos**: Los recursos, representados por archivos de diferentes colores, simbolizan los activos o datos a los que los usuarios desean acceder. Estos pueden incluir archivos, datos sensibles o servicios a los que se accede de manera controlada.
- **Cerradura y control de acceso**: El ícono de un candado representa el sistema de control de acceso que protege los recursos. Este sistema garantiza que solo los usuarios con las credenciales correctas puedan acceder a los recursos, bloqueando el acceso a quienes no tienen los permisos necesarios.

En resumen, el sistema de control de acceso descrito en la figura asegura que solo los usuarios autorizados puedan acceder a los recursos específicos para los cuales han sido previamente autorizados, mejorando la seguridad y la gestión de la información en entornos controlados.

1) Control de acceso basado en roles: El modelo de *Control de acceso basado en roles* (RBAC) asigna permisos a los usuarios en función de sus roles dentro de una organización. Cada rol tiene un conjunto específico de permisos que le otorgan acceso a ciertos recursos o funciones dentro del sistema. Este enfoque es ampliamente utilizado debido a su simplicidad y facilidad de administración en entornos grandes [13]. Sin embargo, su rigidez puede limitar su aplicabilidad en entornos dinámicos y distribuidos, como la Industria 5.0.

2) Control de acceso basado en atributos: El *Control de acceso basado en atributos* (ABAC) introduce mayor flexibilidad al definir permisos en función de los atributos del usuario, del recurso al que se desea acceder y del contexto. Los atributos pueden incluir propiedades como la ubicación, la hora del día, o el nivel de seguridad requerido. Este enfoque permite una toma de decisiones más dinámica y granular, ideal para entornos altamente interconectados y ciberfísicos [14]. ABAC es particularmente útil en sistemas complejos donde las políticas de acceso requieren ser ajustadas frecuentemente.

3) Control de acceso basado en políticas: El *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) es un modelo de control de acceso que combina técnicas de cifrado con políticas basadas en atributos para asegurar el acceso a los datos. En este esquema, los datos están cifrados bajo una política que especifica qué atributos debe tener un usuario para poder descifrar la información. CP-ABE es particularmente útil en escenarios donde la confidencialidad de los datos debe ser garantizada incluso cuando se comparten a través de una red abierta [15].

D. Integración de blockchain con control de acceso

La integración de blockchain en los sistemas de control de acceso busca aprovechar las ventajas de la descentralización y la seguridad inherentes a la blockchain para mejorar la eficiencia y fiabilidad de estos sistemas. A continuación, se describen los enfoques más comunes para esta integración:

1) Soluciones distribuidas: La descentralización ofrecida por blockchain permite la creación de soluciones distribuidas para el control de acceso, donde múltiples nodos participan en la toma de decisiones sobre los permisos de acceso. Esto elimina los riesgos asociados a los sistemas centralizados, como los puntos únicos de fallo, y mejora la resiliencia general del sistema [16]. En entornos industriales, estas soluciones distribuidas pueden ser vitales para garantizar el acceso seguro a los datos y sistemas críticos.

2) Sistemas híbridos: Algunas propuestas combinan la blockchain con sistemas de control de acceso tradicionales para crear soluciones híbridas. Estos sistemas utilizan blockchain para gestionar la verificación de identidades y almacenar los registros de acceso de manera inmutable, mientras que los sistemas tradicionales se encargan de la autenticación y autorización en tiempo real [17]. Este enfoque permite aprovechar los beneficios de la blockchain sin incurrir en los costos computacionales que implican algunas soluciones puramente basadas en blockchain.

III. Revisión de Literatura

En esta sección, se presentan cinco trabajos recientes que investigan la integración de blockchain con sistemas de control de acceso en diferentes aplicaciones y sectores (ver Tabla I). A continuación se ofrece un resumen de las contribuciones y limitaciones de cada uno de estos estudios.

Priyanka Kamboj, Shivang Khare y Sujata Pal [18] proponen un modelo RBAC que utiliza contratos inteligentes en la plataforma de blockchain Ethereum. La contribución principal es el uso de blockchain para gestionar de forma segura las comunicaciones y autorizaciones de usuarios, eliminando la necesidad de una autoridad centralizada. El modelo propuesto resiste ataques como *man-in-the-middle*, lo que mejora la seguridad en escenarios organizacionales. Además, se probaron las funcionalidades en la red de prueba de Ethereum (Ropsten) para evaluar el costo, la verificación y la autenticación de usuarios.

Contribuciones:

- El uso de **contratos inteligentes** para gestionar permisos de usuario basados en roles, eliminando la dependencia de una autoridad central.

TABLA I
ANÁLISIS CUALITATIVO DE ARTÍCULOS SELECCIONADOS.

Artículo	Enfoque Principal	Ventajas	Desafíos	Experimentación
Kamboj et al. [18]	Autenticación de usuarios usando contratos inteligentes basados en roles	Automatización del control de acceso, mayor seguridad, sin intermediarios	Afectado por escalabilidad y costo de transacciones	Pruebas en Ethereum, evaluando tiempos de autenticación y costos de transacción
Pancari et al. [19]	Comparación de Ethereum y Hyperledger para acceso basado en atributos en IoT	Evaluación de seguridad y rendimiento entre ambas plataformas	La elección práctica depende del entorno	Simulaciones comparativas de latencia y consumo de gas; Hyperledger tuvo mejor rendimiento en redes privadas
Mishra et al. [20]	Compartición de datos médicos con blockchain y CP-ABE optimizado	Mejor rendimiento en cifrado, menor sobrecarga y tiempos de procesamiento	Ataques de retroceso y protección de datos aún son retos	Pruebas de rendimiento en cifrado y tiempos de procesamiento, con mejoras significativas
Banerjee et al. [21]	Control de acceso con CP-ABE multi-autoridad y blockchain en IIoT	Control granular, mayor seguridad y trazabilidad	Sobrecarga computacional y complejidad en gestión distribuida	Evaluación en red privada con mejoras en trazabilidad y seguridad, pero mayor sobrecarga computacional
Wang et al. [22]	Mejora en control de acceso en SWIM con CP-ABE, nube y blockchain	Acceso seguro con soporte a usuarios ligeros	Capacidad computacional limitada en dispositivos ligeros	Simulaciones en dispositivos ligeros, tiempos de procesamiento aceptables con limitaciones en dispositivos de baja capacidad

- Implementación y evaluación del modelo en un entorno real utilizando la red de prueba Ethereum, demostrando su viabilidad.
- La propuesta mejora la **seguridad** al resistir ataques de intermediarios y facilitar la verificación automática de autenticación.

El trabajo de Stefan Pancari *et al.* [19] compara dos plataformas blockchain populares, Ethereum y Hyperledger Fabric, en el contexto de control de acceso basado en atributos (ABAC) para entornos IoT de hogares inteligentes. La comparación se realiza mediante la implementación de contratos inteligentes específicos para ABAC en ambas plataformas y su evaluación bajo diferentes criterios, como seguridad, rendimiento y escalabilidad.

Contribuciones:

- Propuesta de un contrato inteligente original para Ethereum y modificación de un contrato preexistente en Hyperledger Fabric para controlar el acceso en redes IoT domésticas.
- Evaluación de las ventajas y limitaciones de ambas plataformas en cuanto a su capacidad para gestionar el acceso de manera eficiente y segura.

Anil Kumar Mishra y Yogomaya Mohapatra [20] presentan un sistema híbrido de compartición de datos médicos basado en blockchain y cifrado de políticas de atributos (CP-ABE). La propuesta aborda problemas de seguridad comunes en los registros médicos personales (PHR), como el acceso no autorizado y la manipulación de datos. El sistema utiliza blockchain para garantizar la integridad y trazabilidad de los datos, mientras que los contratos inteligentes facilitan el control de acceso y la búsqueda segura en los registros cifrados.

Contribuciones:

- Propuesta de un esquema descentralizado para compartir datos médicos basado en blockchain y CP-ABE, que mejora la privacidad y la eficiencia.
- Implementación de un mecanismo de auditoría de datos y verificación mediante blockchain, garantizando la integridad de los registros.
- Uso de almacenamiento híbrido on-chain/off-chain para reducir los problemas de escalabilidad de la blockchain.

Soumya Banerjee *et al.* [21] presenta un esquema de control de acceso basado en blockchain y en el cifrado basado en políticas de atributos (CP-ABE) en entornos de IIoT. La propuesta aborda el problema de los puntos únicos de fallo que suelen aparecer en sistemas con una única autoridad de control de atributos, utilizando múltiples autoridades para gestionar los atributos. Además, el uso de una blockchain de permisos (Hyperledger Fabric) proporciona un medio seguro y auditable para gestionar los accesos y garantizar la integridad de los registros.

Contribuciones:

- Implementación de un esquema multi-autoridad para gestionar atributos y mitigar problemas de confianza centralizada.
- Uso de contratos inteligentes para reducir la carga de comunicación y cómputo en los usuarios durante el acceso a los datos.

Qing Wang *et al.* [22] presenta un esquema de control de acceso basado en el cifrado de políticas de atributos (CP-ABE) y la fusión de blockchain y computación en la nube para el SWIM (System Wide Information Management). La solución aborda los problemas de seguridad en el intercambio de información dentro del sistema de gestión del tráfico aéreo (ATM). Se proponen algunas mejoras, como el uso de múltiples autoridades para evitar la dependencia de una sola autoridad central, y se emplea blockchain para auditar y registrar el acceso a los datos, lo que garantiza la inmutabilidad de los registros.

Contribuciones:

- Introducción de un esquema multi-autoridad basado en CP-ABE que garantiza un control de acceso distribuido

y seguro en el entorno SWIM.
- Uso de blockchain para registrar de manera auditable las solicitudes de acceso, mejorando la supervisión y la seguridad.
- Implementación de computación subcontratada para reducir la carga computacional en dispositivos con recursos limitados.

IV. Análisis y comparación

Para visualizar la comparación entre los cinco artículos seleccionados, se ha generado un diagrama de radar que evalúa los siguientes criterios: seguridad, escalabilidad, privacidad, eficiencia computacional y latencia. Cada artículo tiene una línea única en el gráfico que refleja su rendimiento en cada una de estas áreas, en una escala del 1 al 5, donde 5 es la mejor puntuación.

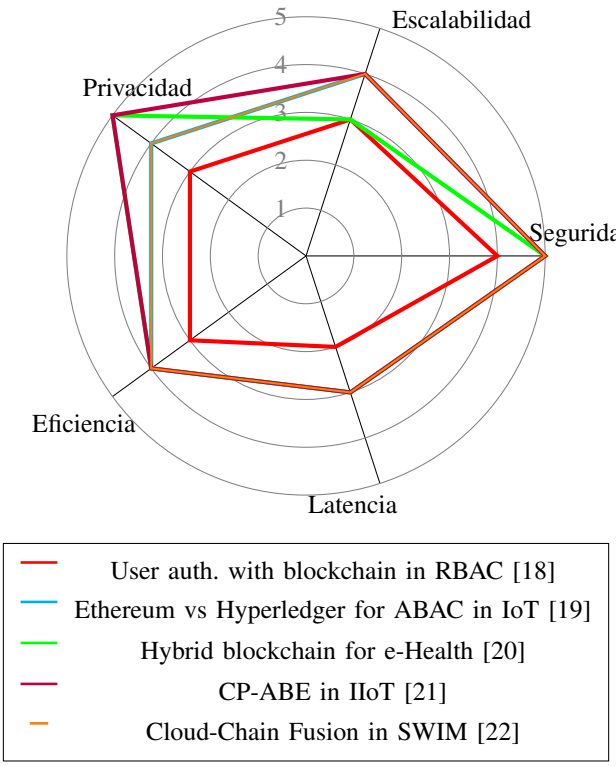

Fig. 3. Comparación de los artículos en términos de Seguridad, Escalabilidad, Privacidad, Eficiencia y Latencia.

La Figura 3 muestra una comparación clara entre cinco artículos en términos de seguridad, escalabilidad, privacidad, eficiencia y latencia. Ethereum vs Hyperledger for ABAC in IoT y CP-ABE in IIoT sobresalen en seguridad con puntuaciones máximas de 5, destacando su enfoque robusto en protección de datos, mientras que Hybrid blockchain for e-Health es líder en privacidad, garantizando una alta protección de datos personales. User auth. with blockchain in RBAC tiene puntuaciones moderadas en escalabilidad y eficiencia, pero su latencia es la más baja, lo que sugiere problemas de rendimiento en tiempo real. Por otro lado, Cloud-Chain Fusion in SWIM y CP-ABE in IIoT son soluciones equilibradas con buenas puntuaciones en todas las categorías, lo que indica que son opciones versátiles y bien balanceadas para su implementación.

V. Desafíos y oportunidades futuras en la Industria 5.0

La Industria 5.0 representa un cambio de paradigma que va más allá de la automatización y digitalización de los procesos industriales que caracterizaban a la Industria 4.0. En esta nueva era, se busca una mayor integración entre los seres humanos y las máquinas, con un enfoque en la personalización y la sostenibilidad [23]. En este contexto, blockchain y el cifrado basado en atributos (CP-ABE) juegan un papel fundamental para garantizar la seguridad, la privacidad y la escalabilidad en los sistemas de control de acceso.

A. Desafíos actuales en la integración de blockchain con sistemas de control de acceso

La integración de blockchain con esquemas de control de acceso basados en atributos, como CP-ABE, enfrenta una serie de desafíos técnicos que deben ser abordados para su adopción generalizada en la Industria 5.0. Algunos de los principales desafíos incluyen:

- **Escalabilidad**: Aunque blockchain ofrece una solución descentralizada y segura para el control de acceso, su rendimiento puede verse comprometido en aplicaciones a gran escala debido a las limitaciones inherentes en la capacidad de procesamiento y el consumo de recursos computacionales. La integración con CP-ABE también aumenta la complejidad debido al procesamiento de claves y atributos.
- **Latencia**: El tiempo necesario para verificar y autorizar las solicitudes de acceso en un entorno basado en blockchain puede ser un problema crítico en la Industria 5.0, donde la inmediatez de las decisiones es clave. La combinación de blockchain con CP-ABE introduce una capa adicional de complejidad que podría incrementar la latencia en el proceso de acceso.
- **Privacidad**: Aunque CP-ABE es eficaz para garantizar la privacidad en los sistemas de control de acceso, la combinación con blockchain podría comprometerla debido a la naturaleza pública de algunas cadenas de bloques. Se requiere una investigación adicional para desarrollar mecanismos que garanticen que los datos cifrados sigan siendo privados en una infraestructura.

B. Oportunidades futuras hacia la Industria 5.0

A pesar de los desafíos mencionados, la integración de blockchain y CP-ABE ofrece oportunidades prometedoras para la evolución de la Industria 5.0. Entre las principales oportunidades destacan:

- **Sistemas de control de acceso descentralizados**: La Industria 5.0 necesitará sistemas más resilientes y adaptativos. La combinación de blockchain y CP-ABE proporciona una infraestructura robusta para gestionar el acceso

a recursos distribuidos en tiempo real, eliminando los riesgos asociados con los puntos únicos de fallo.

- **Privacidad y seguridad mejoradas**: La capacidad de blockchain para garantizar la inmutabilidad y la trazabilidad de los datos, junto con la flexibilidad de CP-ABE para gestionar permisos dinámicos basados en atributos, crea un marco sólido para la protección de la información sensible en entornos industriales interconectados.
- **Automatización inteligente**: Los contratos inteligentes integrados en blockchain permiten la automatización de procesos de control de acceso de manera segura y eficiente. Esto, combinado con el cifrado basado en atributos, permite una gestión del acceso altamente personalizable y adaptada a las necesidades individuales de los usuarios en la Industria 5.0.

En resumen, aunque la integración de blockchain y CP-ABE en la Industria 5.0 enfrenta desafíos significativos, sus ventajas en términos de seguridad, privacidad y automatización presentan una gran oportunidad para el futuro de los sistemas industriales. La investigación y el desarrollo continuarán avanzando para optimizar estas tecnologías y garantizar su adopción en los próximos años.

VI. Conclusiones

La integración de blockchain y el control de acceso presenta un enfoque prometedor para abordar los desafíos de seguridad, privacidad y escalabilidad en la Industria 5.0. A lo largo del artículo, se ha discutido cómo blockchain puede garantizar la inmutabilidad y trazabilidad de los datos, mientras que soluciones como CP-ABE ofrecen flexibilidad en la gestión de permisos dinámicos. Sin embargo, persisten desafíos relacionados con la escalabilidad y la latencia que deben resolverse para su adopción en entornos industriales a gran escala.

A pesar de estas limitaciones, las oportunidades que brindan estas tecnologías, como la creación de sistemas de control de acceso descentralizados y la mejora de la privacidad, son significativas. La Industria 5.0 requerirá sistemas más resilientes, automatizados y personalizados, y la combinación de blockchain con CP-ABE ofrece una vía clara para cumplir con estas expectativas.

En conclusión, la continua investigación y desarrollo en la integración de estas tecnologías permitirá optimizar sus capacidades y contribuir a la evolución de entornos industriales seguros y eficientes en la era de la Industria 5.0.

Referencias

[1] J. Leng, W. Sha, B. Wang, P. Zheng, C. Zhuang, Q. Liu, T. Wuest, D. Mourtzis, and L. Wang, "Industry 5.0: Prospect and retrospect," *Journal of Manufacturing Systems*, vol. 65, p. 279–295, October 2022.

[2] B. Leander, A. Causevic, T. Lindstrom, and H. Hansson, "A questionnaire study on the use of access control in industrial systems," in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 2020 june, p. 1–8, IEEE, September 2021.

[3] D. Wu, X. Huang, X. Xie, X. Nie, L. Bao, and Z. Qin, "Ledge: Leveraging edge computing for resilient access management of mobile iot," *IEEE Transactions on Mobile Computing*, vol. 20, p. 1110–1125, March 2021.

[4] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, p. 2841–2866, May 2021.

[5] R. Saha, G. Kumar, M. Conti, T. Devgun, T.-h. Kim, M. Alazab, and R. Thomas, "Dhacs: Smart contract-based decentralized hybrid access control for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 18, p. 3452–3461, May 2022.

[6] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, "the transparency challenge of blockchain in organizations," *Electronic Markets*, vol. 32, p. 1779–1794, March 2022.

[7] A. Aldoubaee, N. H. Hassan, and F. A. Rahim, "A systematic review on blockchain scalability," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023.

[8] M. Oliveira, S. Chauhan, F. Pereira, C. Felgueiras, and D. Carvalho, "Blockchain protocols and edge computing targeting industry 5.0 needs," *Sensors*, vol. 23, p. 9174, Nov. 2023.

[9] N. Ul Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Industrial Electronics Magazine*, vol. 13, p. 106–118, December 2019.

[10] R. K. Raman and L. R. Varshney, "Coding for scalable blockchains via dynamic distributed storage," *IEEE/ACM Transactions on Networking*, vol. 29, p. 2588–2601, December 2021.

[11] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, October 2017.

[12] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, p. 475–491, April 2020.

[13] J. Xu, Y. Yu, Q. Meng, Q. Wu, and F. Zhou, "Role-based access control model for cloud storage using identity-based cryptosystem," *Mobile Networks and Applications*, vol. 26, p. 1475–1492, January 2020.

[14] L. Karimi, M. Aldairi, J. Joshi, and M. Abdelhakim, "An automatic attribute-based access control policy extraction from access logs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, p. 2304–2317, July 2022.

[15] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based cloud storage system with cp-abe-based access control and revocation process," *The Journal of Supercomputing*, vol. 78, p. 7700–7728, January 2022.

[16] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, and H. Xu, "Bacs: A blockchain-based access control scheme in distributed internet of things," *Peer-to-Peer Networking and Applications*, vol. 14, p. 2585–2599, June 2020.

[17] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," *IEEE Transactions on Services Computing*, p. 1–1, 2020.

[18] P. Kamboj, S. Khare, and S. Pal, "User authentication using blockchain based smart contract in role-based access control," *Peer-to-Peer Networking and Applications*, vol. 14, p. 2961–2976, April 2021.

[19] S. Pancari, A. Rashid, J. Zheng, S. Patel, Y. Wang, and J. Fu, "A systematic comparison between the ethereum and hyperledger fabric blockchain platforms for attribute-based access control in smart home iot environments," *Sensors*, vol. 23, p. 7046, August 2023.

[20] A. K. Mishra and Y. Mohapatra, "Hybrid blockchain based medical data sharing with the optimized cp-abe for e-health systems," *International Journal of Information Technology*, vol. 16, p. 121–130, December 2023.

[21] S. Banerjee, B. Bera, A. K. Das, S. Chattopadhyay, M. K. Khan, and J. J. Rodrigues, "Private blockchain-envisioned multi-authority cp-abe-based user access control scheme in iiot," *Computer Communications*, vol. 169, p. 99–113, March 2021.

[22] Q. Wang, L. Zhang, X. Lu, and K. Wang, "A multi-authority cp-abe scheme based on cloud-chain fusion for swim," in *2022 IEEE Intl Conf on Parallel; Distributed Processing with Applications, Big Data; Cloud Computing, Sustainable Computing; Communications, Social Computing; Networking (ISPA/BDCloud/SocialCom/SustainCom)*, p. 213–219, IEEE, December 2022.

[23] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, p. 69160–69199, 2022.