MDPI

Article

Integridad de los datos Biometricos en firmas digitales descentralizadas

Devin Llerena [1,*]

Pontificia Universidad Católica del Ecuador, Esmeraldas, Ecuador; devinllerena23@gmail.com

Abstract

La creciente adopción de firmas digitales y sistemas de identidad en entornos electrónicos ha incrementado la necesidad de garantizar la integridad y la seguridad de los datos biométricos utilizados en estos procesos. Sin embargo, el uso de biometría introduce desafíos críticos, ya que los datos biométricos no pueden ser reemplazados si se ven comprometidos y son vulnerables a manipulación, suplantación o reconstrucción cuando no se protegen adecuadamente. En entornos descentralizados, la gestión de las plantillas biométricas requiere mecanismos específicos, ya que no existe una entidad central encargada de supervisar su generación, almacenamiento y verificación. En este contexto, las tecnologías descentralizadas han surgido como una alternativa para reducir la dependencia de infraestructuras centralizadas y reforzar la verificabilidad de la información. Frente a este escenario, el objetivo de este estudio es analizar de forma sistemática las limitaciones, fortalezas y tendencias de los enfoques propuestos para garantizar la integridad de los datos biométricos en firmas digitales descentralizadas. La investigación se desarrolló mediante una revisión sistemática de la literatura, siguiendo las guías metodológicas de Kitchenham, el proceso PRISMA . Los resultados muestran que las soluciones integran principalmente biometría humana, como huella dactilar y reconocimiento facial, y en menor medida biometría de voz e iris, combinadas con arquitecturas basadas en blockchain. y que la integridad se apoya sobre todo en técnicas criptográficas consolidadas, mientras que enfoques avanzados, como pruebas de conocimiento cero y compromisos criptográficos, presentan una adopción limitada. También se identifican desafíos relacionados con costos, latencia, variabilidad biométrica y riesgos de privacidad. No obstante, persisten brechas técnicas y operativas relacionadas con la escalabilidad, los costos, la variabilidad biométrica y la protección de la privacidad, que limitan su aplicación práctica a gran escala. Estos hallazgos muestran la necesidad de continuar desarrollando y evaluando mecanismos que equilibren integridad, privacidad y usabilidad en sistemas de firma digital descentralizados.

Received:
Revised:
Accepted:
Published:

Citation: Lastname, F.; Lastname, F.; Lastname, F. Integridad de los datos biométricos en firmas digitales descentralizadas. *Future Internet* **2025**, *1*, 0. https://doi.org/

Keywords: biometría; firmas digitales; blockchain; integridad; privacidad

1. Introduction

La transformación digital impulso la necesidad de métodos de seguridad robustos que garanticen la seguridad y confianza en entornos electrónicos. Por ello las firmas digitales se convirtieron en un pilar esencial para asegurar la integridad y no repudio de la información. Por otro lado, las tecnologías descentralizadas, como blockchanin surgieron como una alternativa prometedora para implementar mecanismos de identidad digital distribuidos y verificables. En este contexto, los datos biométricos representan un gran avance al ofrecer una autenticación basada en características únicas, fortaleciendo la confianza en los procesos digitales [1,2]. A pesar de que la biometría y las técnicas criptográficas han avanzado bastante, La integración de datos biométricos en sistemas digitales presenta desafíos técnicos relevantes. Las plantillas biométricas siguen siendo vulnerables a ataques donde alguien puede reconstruir o hasta suplantar la identidad, sobre todo cuando esos datos se guardan o se envían sin buenos mecanismos de descentralización o anonimización. En sistemas de firma digital pasa algo parecido, porque si la plantilla se altera un poco, ya se compromete todo el proceso y pueden darse casos de fraude o accesos que no deberian pasar[3]. Además, no todos los sistemas generan ni validan las plantillas biométricas del mismo modo, lo que complica evaluar su integridad y limita la compatibilidad entre plataformas[3]. Todo esto se vuelve mas complicado en infraestructuras descentralizadas, porque no existe una entidad que supervise ese proceso, asi que se necesita asegurar que los datos sean verificables, inmutables y resistentes a cualquier manipulacion, algo que aún no esta del todo resuelto [3].

La importancia de este tema se encuentra en el potencial para redefinir lo que es la seguridad digital contemporánea, en especial dentro del ámbito global donde la protección de la identidad y la privacidad se ve limitada por la fragilidad de los mecanismos de autenticación tradicionales [4,5], la dependencia de sistemas centralizados que funcionan como puntos únicos de fallo, y la dificultad para garantizar la integridad y la privacidad de los datos de identidad incluidos los biométricos en escenarios reales [4]. A esto se suman problemas como el rastreo constante por parte de proveedores centralizados, la posibilidad de ataques fuera de línea cuando se comprometen bases de datos, la falta de control del usuario sobre su propia información, los errores en el reconocimiento biométrico que pueden excluir a individuos legítimos y los riesgos de manipulación de registros críticos en sectores sensibles como la salud[3]. Estas limitaciones ponen en evidencia que los modelos actuales no siempre son confiables, ni escalables, ni adecuados para contextos globales donde la identidad digital debe ser segura, verificable y resistente a manipulación.

Se han explorado distintas soluciones, incluyendo el cifrado homomórfico y el almacenamiento distribuido; sin embargo, la mayoría de estas propuestas aborda únicamente componentes aislados del problema, lo que impide una protección completa frente a amenazas como los ataques fuera de línea que pueden producirse cuando un servidor o base de datos es comprometido. En este contexto, ciertos registros sensibles, como los relacionados con la salud o las transacciones críticas, pueden verse alterados si no existen mecanismos sólidos de inmutabilidad. A esto se suma que la biometría no siempre funciona como un identificador totalmente confiable, porque puede fallar en condiciones reales o ser manipulada en algunos casos, lo que afecta directamente la integridad del proceso de autenticación. En relación con la protección de las plantillas biométricas, el usar directamente la template biométrica para la autenticación es considerado un punto débil, y los sistemas centralizados de datos biométricos están expuestos a que cualquier fallo o ataque comprometa toda la base completa, debido a que reúnen todas plantillas en un mismo punto, cualquier fallo o ataque compromete toda la base completa. Si un atacante logra acceder al servidor central, obtiene de una sola vez un volumen grande de datos que no pueden ser cambiados ni reemplazados, como sí ocurre con una contraseña. Esto convierte a estos sistemas en

objetivos muy atractivos y amplifica el impacto de cualquier filtración o manipulación de la biometría almacenada.

El uso de datos biométricos como semilla de una clave privada es muy peligroso , por que si un atacante obtiene los datos biométricos, podría reconstruir la clave privada y acceder a los fondos o servicios[6]. Esta falta de claridad ha dado lugar a una diversidad de enfoques en la literatura, donde pueden encontrarse sistemas híbridos basados en cifrado homomórfico y blockchain, como los descritos por Tavares et al. [7], asi como protocolos mas complejos como DAMFA, propuesto por Mir, Roland y Mayrhofer [4]. En conjunto, estos trabajos muestran que todavia no existe un marco metodologico unificado para determinar que tecnicas son mas adecuadas ni como evaluar su efectividad en sistemas distribuidos, lo que dificulta avanzar hacia estandares comunes [6,8]. A partir de este panorama distintos estudios recientes han comenzado a explorar soluciones que buscan superar estas limitaciones. En el trabajo de Varma et al. [9] se propone un modelo para compartir datos biométricos de manera segura mediante blockchain. Las evaluaciones realizadas por los autores reportan una precisión de autenticación que supera el 98 % y una disminución importante en la tasa de falsa aceptacion (FAR) frente a enfoques convencionales.Estos hallazgos evidencian de forma cuantitativa la eficacia de las tecnologías descentralizadas para reforzar la integridad y fiabilidad de los datos biométricos en entornos de firma digital.Estos resultados respaldan la idea de que las arquitecturas descentralizadas pueden fortalecer la integridad y la fiabilidad de los datos biométricos en entornos de firma digital. Por otro lado, tambien hay un estudio importante de Griffin [5] que se centra en cómo usar datos biometricos en la creacion de firmas electronicas seguras. El autor propone los protocolos BAKE y BESAKE, que basicamente mezclan una contraseña con un dato biometrico para lograr una autenticacion multifactor mas fuerte, capaz de resistir ataques como phishing o man in the middle. En estos esquemas la informacion biometrica no se revela durante el intercambio, lo que ayuda a mantener la integridad y la confidencialidad de las credenciales. Ademas, el trabajo muestra que este tipo de firmas puede funcionar en entornos descentralizados, ya que los protocolos no dependen de una PKI centralizada y se adaptan bien a sistemas basados en blockchain o DLT. Esto permite crear canales seguros, autenticacion mutua y reducir el riesgo de repudio en transacciones digitales.

Otro trabajo relevante es el de Hassen et al. [10] abordan la problemática de la vulnerabilidad de las claves privadas tradicionales en entornos IoT integrados con tecnologías blockchain. A diferencia de los enfoques que se basan en el almacenamiento de secretos, los autores proponen un esquema de firma digital basado en identidad difusa (FIBS), en el cual la clave privada se obtiene de forma dinámica a partir de biometría multimodal, combinando la huella dactilar y las venas del dedo. El funcionamiento de la propuesta comienza con una fase de preprocesamiento biométrico que incluye la mejora de la imagen, la detección de regiones de interés y la extracción de características mediante filtros de Gabor y análisis de componentes principales, lo que permite fusionar los rasgos en una identidad biométrica única. Esta identidad se incorpora directamente en el proceso criptográfico de generación de firmas, de modo que la autenticación y la firma de transacciones se realizan sin necesidad de almacenar claves privadas en dispositivos o servidores externos. Para mantener la integridad de los datos biométricos, el esquema utiliza un mecanismo de verificación tolerante a errores, en el que una firma generada con una identidad biométrica puede ser validada con capturas posteriores dentro de un umbral predefinido, evitando la exposición de los datos biométricos en bruto. Además, la propuesta se apoya en la naturaleza descentralizada de la blockchain para el registro y la validación de certificados y transacciones, incorporando contratos inteligentes que refuerzan la integridad del entorno distribuido mediante la verificación del software y del comportamiento de los nodos IoT. Aunque el enfoque implica un aumento en el tamaño de la clave derivada, los resultados

experimentales demuestran su viabilidad práctica y su resistencia criptográfica, lo que lo posiciona como una alternativa relevante para garantizar la integridad de los datos biométricos en esquemas de firma digital descentralizados. [10].

En los sistemas de autenticación biométrica descentralizados, Lee et al. [11] proponen el sistema BDAS (Blockchain-based Distributed Biometric Authentication System) para abordar las vulnerabilidades presentes en los esquemas tradicionales, como la fuga de información y la dependencia de servidores centrales. La propuesta se basa en la segmentación de la plantilla biométrica tras la captura y la extracción de características, lo que evita su almacenamiento en un solo repositorio y reduce el riesgo de ingeniería inversa. El sistema divide la plantilla biométrica en varios fragmentos que se distribuyen entre distintos nodos de una red blockchain. Durante la autenticación, un contrato inteligente localiza los fragmentos necesarios, que son recuperados y fusionados para realizar la verificación biométrica. La integridad y confidencialidad de la información se preservan tanto por la fragmentación de los datos como por el registro auditable de cada operación en la blockchain, eliminando puntos únicos de falla. Aunque el enfoque introduce una mayor latencia respecto a sistemas convencionales, los resultados evidencian una disponibilidad robusta, posicionando a BDAS como una alternativa viable para fortalecer la integridad de los datos biométricos en entornos de autenticación descentralizados [11].

Alzahab et al. [12] presentan una aplicación descentralizada denominada BiometricIdentity, orientada a reducir las vulnerabilidades de los sistemas de identidad biométrica centralizados mediante el uso de la blockchain de Ethereum. La propuesta incorpora el esquema de compromiso difuso (Fuzzy Commitment Scheme), lo que permite gestionar la variabilidad inherente de los datos biométricos sin almacenar directamente las plantillas en la cadena de bloques. El sistema funciona a partir de la generación de un compromiso criptográfico durante la fase de enrolamiento, en la cual las características biométricas se combinan con una clave aleatoria mediante códigos de corrección de errores. En esta etapa, únicamente se registran en la blockchain valores derivados e irreversibles. Durante la autenticación, una nueva captura biométrica permite reconstruir y verificar la clave sin exponer la plantilla original. La integridad y la confidencialidad de la información se preservan mediante un enfoque híbrido, donde los datos sensibles se procesan fuera de la cadena y la blockchain actúa como un registro inmutable y auditable. Aunque existen limitaciones de escalabilidad que requieren optimización fuera de la cadena, la propuesta resulta viable para garantizar la integridad de los datos biométricos en sistemas de identidad descentralizados. [12].

Jian Yun et al. [13] proponen Bio-Rollup, una arquitectura biométrica descentralizada que combina una blockchain de dos capas con pruebas de conocimiento cero para abordar las vulnerabilidades de los sistemas biométricos centralizados, especialmente en términos de integridad, privacidad y escalabilidad. La propuesta evita el almacenamiento directo de los datos biométricos y permite verificar el proceso de autenticación de forma criptográfica sin exponer información sensible. El sistema funciona a partir de la generación de resúmenes biométricos obtenidos del reconocimiento, los cuales se protegen mediante funciones hash y se transmiten a través de canales cifrados. La integridad del proceso se garantiza mediante pruebas criptográficas off-chain basadas en SNARKs, que permiten validar transacciones y consultas sin revelar los datos originales. Además, el uso de estructuras de Merkle facilita auditorías ligeras y verificables. Al separar el procesamiento del almacenamiento en la cadena principal y apoyarse en contratos inteligentes, Bio-Rollup mejora la eficiencia operativa y refuerza su resiliencia frente a ataques, lo que lo convierte en una opción viable para preservar la integridad de los datos biométricos en sistemas de autenticación descentralizados. [13].

Lai et al. [14] presentan BioZero, un protocolo de autenticación biométrica descentralizada orientado a cadenas de bloques públicas, diseñado para superar las limitaciones de los esquemas basados en claves asimétricas y reducir riesgos como el robo de claves y los ataques Sybil. La propuesta introduce un modelo de identidad biométrica vinculada directamente al usuario mediante credenciales soul-bound, lo que evita la dependencia de proveedores de identidad centralizados. El funcionamiento del sistema integra la biometría a través de compromisos criptográficos, en los que los rasgos biométricos se transforman en valores comprometidos que se almacenan en la blockchain, manteniendo ocultos los datos originales. Durante la autenticación, una nueva captura biométrica permite generar una prueba criptográfica que valida la similitud entre muestras sin revelar la información en texto plano. La integridad del proceso se asegura mediante pruebas de conocimiento cero, que permiten verificar la autenticación dentro de un umbral definido sin exponer los datos biométricos ni requerir su almacenamiento directo. Gracias a este enfoque, BioZero alcanza una verificación eficiente y escalable, y se posiciona como una alternativa viable para preservar la integridad de los datos biométricos en sistemas de autenticación descentralizados [14]. Los principales antecedentes analizados, junto con sus enfoques técnicos y los aportes específicos de cada propuesta, se sintetizan en la Tabla 1, con el objetivo de ofrecer una visión comparativa que justifica y contextualiza las soluciones revisadas.

Table 1: Antecedentes relevantes sobre biometría y arquitecturas descentralizadas.

Autor (Año)	**Propuesta**	**Descripción y aporte**
Varma et al. (2020) [9]	Computación distribuida y base de datos centralizada (Aadhar)	Propone un sistema de votación electrónica basado en la infraestructura Aadhar que utiliza huellas dactilares para la autenticación, reportando una precisión superior al 98 % y una reducción significativa de la FAR mediante la selección de las huellas más confiables.
Griffin (2019) [5]	BAKE / BESAKE	Presenta un enfoque de firma electrónica en el que la biometría participa en la construcción y activación del proceso de firma, reduciendo la dependencia de infraestructuras centralizadas tradicionales mediante autenticación multifactor basada en datos biométricos.
Hassen et al. (2020) [10]	FIBS	Diseña un esquema de firma digital donde rasgos biométricos multimodales apoyan la autenticación y la derivación dinámica de material criptográfico, evitando el almacenamiento directo de secretos y fortaleciendo la seguridad del proceso.
Lee et al. (2021) [11]	BDAS	Explora un sistema de autenticación biométrica con soporte blockchain enfocado en la protección de plantillas, preservando su integridad mediante técnicas de fragmentación y almacenamiento distribuido.

Continued on next page

Table 1: Antecedentes relevantes sobre biometría y arquitecturas descentralizadas. (Continued)

Alzahab et al. (2024) [12]	Biometric	Presenta una aplicación descentralizada de autenticación biométrica basada en fuzzy commitment y blockchain, garantizando la integridad de los datos biométricos a través de compromisos criptográficos verificables.
Yun et al. (2024) [13]	Bio-Rollup	Propone una arquitectura de dos capas que integra técnicas criptográficas avanzadas para proteger la biometría, permitiendo la verificación de autenticación mediante pruebas de conocimiento cero y mejorando la escalabilidad con un enfoque tipo rollup.
Lai et al. (2024) [14]	BioZero	Introduce un protocolo eficiente de autenticación biométrica descentralizada en blockchain abierta que combina compromisos criptográficos y pruebas de conocimiento cero para reforzar la identidad biométrica autosoberana y preservar la privacidad.

A pesar de los avances existentes, aún no se cuenta con una revisión sistemática que permita una visión clara y organizada de los enfoques para asegurar la integridad de los datos biométricos en firmas digitales descentralizadas. La informacion disponible esta muy dispersa, cada estudio usa tecnicas distintas y no hay un analisis que compare sus resultados, sus limites o sus verdaderas fortalezas. Esta falta de claridad dificulta saber que tan efectivas son las soluciones actuales, que vacios siguen abiertos y hacia donde deberia avanzar la investigacion en este campo.

Frente a este panorama , este estudio se centra en responde la pregunta de investigación: ¿Cuales son las limitaciones, fortalezas y tendencias actuales de los enfoques propuestos para garantizar la integridad de los datos biometricos en firmas digitales descentralizadas? De esta manera, la investigación busca el examinar como se están enfrentando los desafíos técnicos y conceptuales relacionados con la integridad de los datos biométricos, centrándonos en lo que respecta a su almacenamiento, transmisión y validación dentro de sistemas distribuidos. El estudio se delimitó a artículos científicos publicados entre 2009 y 2025, recuperados de bases de datos indexadas como Scopus, IEEE Xplore y Web of Science. lo que permite contar con una visión actualizada de la literatura disponible sobre el tema. Este estudio ayuda a entender, de una forma más clara y directa, cómo funcionan los sistemas que identifican a las personas usando sus propias características, cómo se integran en plataformas distribuidas y cómo se usan en procesos de verificación digital que necesitan protección matemática y criptográfica. También explica qué medidas hacen falta para cuidar la información sensible que manejan estos sistemas y muestra, de manera sencilla, los problemas técnicos, las limitaciones y las dudas conceptuales que todavía dificultan su uso. En conjunto, este trabajo sintetiza el estado actual de la investigación y permite identificar tendencias y vacíos que orientan el desarrollo de soluciones más robustas en entornos descentralizados.

La estructura del artículo es la siguiente:

En la Sección 1 se describe el contexto general del estudio, la problemática abordada y los antecedentes que motivan la investigación. La Sección 2 detalla la metodología empleada para el mapeo sistemático, incluyendo el proceso de búsqueda, los criterios de inclusión

y exclusión y el análisis de los estudios seleccionados. En la Sección 3 se presentan los principales resultados, junto con una discusión sobre las limitaciones, fortalezas y tendencias identificadas en las propuestas relacionadas con la integridad de los datos biométricos en firmas digitales descentralizadas. Finalmente, la Sección 4 expone las conclusiones generales y plantea posibles líneas de trabajo futuro orientadas a mejorar la seguridad y la verificación de datos biométricos en sistemas distribuidos.

2. Materials and Methods

2.1. Research Questions and Scope

El presente trabajo corresponde a una revisión sistemática de la literatura, desarrollada siguiendo las guías de Kitchenham y los lineamientos de PRISMA 2020, con el fin de asegurar un proceso claro y ordenado de búsqueda, selección y síntesis de la información. Se adoptó un diseño documental con enfoque cualitativo, ya que el estudio se basa exclusivamente en fuentes secundarias y en el análisis interpretativo de los trabajos seleccionados. El alcance es descriptivo y exploratorio, dado que busca identificar, clasificar y analizar los enfoques y soluciones reportados en la literatura, lo que permite ofrecer una visión estructurada del estado actual del conocimiento y detectar vacíos o tendencias relevantes para futuras investigaciones. El alcance del estudio se delimitó mediante el marco PICo, presentado en la Tabla 2, el cual permitió definir la Población, el Interés y el Contexto de la revisión. A partir de esta delimitación se formuló la pregunta central:

> *¿Cuales son las limitaciones, fortalezas y tendencias actuales de los enfoques propuestos para garantizar la integridad de los datos biometricos en firmas digitales descentralizadas?*

Con base en las recomendaciones de Kitchenham, se formularon preguntas adicionales que apoyan la extracción y organización de la información:

RQ1: ¿Qué enfoques han sido propuestos en la literatura científica para integrar datos biométricos en firmas digitales descentralizadas?
RQ2: ¿Qué técnicas y principios criptográficos se utilizan para garantizar la integridad de los datos biométricos en firmas digitales en entornos descentralizados?
RQ3: ¿Cuáles son las principales limitaciones y desafíos técnicos que enfrenta la implementación de sistemas biométricos en firmas digitales descentralizadas?

Table 2: Esquema PICo — Elementos, términos concretos y definiciones

Elemento	Definición	Alcance Operativo
P — Población	Entornos descentralizados	Plataformas basadas en tecnologías distribuidas como blockchain, identidades autosoberanas (SSI) y registros distribuidos (DLT) que soportan procesos de autenticación, verificación y gestión de información sin intermediarios.
I — Intervención	Mecanismos de integridad y protección de datos en sistemas de firma digital.	Técnicas y métodos orientados a garantizar que los datos utilizados en la firma digital no sean alterados, manipulados o comprometidos durante su procesamiento o verificación en entornos descentralizados.
Co — Contexto	Sistemas que emplean datos biométricos.	Ambientes donde datos como huella, rostro, iris o voz se integran para verificación o vinculación en firmas digitales

2.2. Estrategia de búsqueda

La estrategia de búsqueda se basó en los elementos definidos en el marco PICo presentado previamente Tabla 2. A partir de la Población, el Interés y el Contexto se elaboró una matriz de términos relacionados, donde cada componente fue desglosado en sinónimos, expresiones equivalentes y acrónimos usados en la literatura sobre biometría, seguridad y sistemas descentralizados. Estos términos derivados sirvieron como base para la construcción de las cadenas booleanas aplicadas en cada base de datos. En esta etapa se evitaron definiciones conceptuales del PICo, enfocándose únicamente en los términos operativos necesarios garantizar búsquedas amplias, precisas y reproducibles. La Tabla 3 presenta el conjunto de términos derivados para cada elemento.

Table 3: Variant terms derivados del esquema PICo utilizados en la estrategia de búsqueda

Elemento PICo	Variant Terms / Equivalencias léxicas
P — Población	electronic, connection, relation, system, disperse, Distribute, Scatter , Decentralized, Self-Sovereign Identity, Web of trust, GPG, PGP
I — Intervención	digitall, Electronic* sing*, singed, authentication, verification , certification, validation, authorization
Co — Contexto	Biometric*, FaceID, Fingerprint, dactylogram, IRIS , eye , Voice, Keystroke dynamics

Las cadenas se elaboraron uniendo los términos de forma iterativa con operadores booleanos, siguiendo el criterio:

Población **AND** Intervención **AND** Contexto.

Estas combinaciones se adaptaron a la sintaxis y operadores propios de cada base de datos. Se realizaron búsquedas piloto y revisiones manuales para depurar términos y asegurar la recuperación de literatura relevante. Las búsquedas finales se efectuaron en Web of Science, Scopus e IEEE Xplore, y las cadenas utilizadas en cada plataforma se presentan en la Tabla 4, garantizando coherencia y comparabilidad en el proceso PRISMA.

Table 4: Cadenas de búsqueda empleadas en las bases de datos consultadas

Base de datos	Cadena de búsqueda
Scopus y Web of Science	((electronic OR connection OR system) AND (Disperse OR Distribute OR Scatter OR Decentralized)) OR (Self-Sovereign Identity OR Web of trust OR GPG OR PGP) (digital OR Electronic*) AND (sing* OR sign OR signed) OR (authentication OR verification OR validation) OR (authorization) (Biometric* OR FaceID OR Fingerprint OR dactylogram OR IRIS OR eye OR Voice OR Keystroke dynamics)
IEEE Xplore	electronic OR connection OR system AND Disperse OR Distribute OR Scatter OR Decentralized OR Self-Sovereign Identity OR Web of trust OR GPG OR PGP digital OR Electronic* AND sing* OR sign OR signed OR authentication OR verification OR validation OR authorization Biometric* OR FaceID OR Fingerprint OR dactylogram OR IRIS OR eye OR Voice OR Keystroke dynamics

2.3. Selección de Artículos

El proceso de selección de estudios siguió la estructura del diagrama PRISMA 2020, organizada en las etapas de identificación, cribado, elegibilidad e inclusión. En la fase de identificación, todos los registros obtenidos desde las bases de datos fueron exportados y se eliminaron duplicados mediante herramientas automáticas complementadas con una verificación manual. Durante el cribado de títulos y resúmenes se aplicó un filtro conceptual basado en el marco PICo, comprobando que cada registro guardara correspondencia básica con los elementos definidos para la Población, el Interés y el Contexto. Este paso permitió excluir estudios sin relación con entornos descentralizados, biometría o procesos de firma digital. El cribado se realizó mediante revisión por pares ciegos utilizando la plataforma Rayyan. Una vez completada la fase de screening, las discrepancias entre revisores fueron discutidas y resueltas por consenso, sin necesidad de intervención externa, garantizando así coherencia en la clasificación de los estudios. En la fase de elegibilidad, los trabajos preseleccionados fueron revisados a texto completo aplicando los criterios de inclusión y exclusión establecidos en la Tabla 5, considerando aspectos como el tipo de tecnología analizada, la pertinencia con el enfoque del estudio, el idioma, la fecha de publicación y la disponibilidad del contenido.

Table 5: Criterios de inclusión y exclusión aplicados en la revisión sistemática.

Criterio	**Criterios de Inclusión**	**Criterios de Exclusión**
Población	Estudios que trabajen con entornos descentralizados aplicados a procesos de firma digital, identidad digital o gestión de información segura.	Estudios centrados en sistemas centralizados, biometría sin relación con firmas digitales, o contextos no tecnológicos.
Intervención	Propuestas, mecanismos o métodos orientados a garantizar la integridad o protección de datos biométricos.	Trabajos que utilicen únicamente métodos tradicionales sin tratar integridad biométrica, o que aborden criptografía general sin incluir biometría.
Tipo de dato biométrico	Estudios que utilicen datos biométricos humanos empleados para autenticación o procesos de firma digital.	Estudios centrados en el diseño o evaluación de dispositivos físicos de captura biométrica, sin analizar la gestión o integridad de los datos biométricos en procesos de firma digital.

Continued on next page

Table 5: Criterios de inclusión y exclusión aplicados en la revisión sistemática. (Continued)

Resultados	Deben presentar aportaciones claras, como enfoques, desafíos, ventajas o análisis vinculados a integridad, seguridad o manejo de datos biométricos en contextos descentralizados.	Artículos que trabajen biometría en ámbitos no relacionados con autenticación, firmas digitales o seguridad.
Tipo de estudio	Artículos primarios revisados por pares que describan arquitecturas, frameworks, protocolos, técnicas criptográficas o sistemas aplicables.	
Relevancia temática	Correspondencia con los tres elementos del marco PICo.	
Disponibilidad	Acceso al texto completo para la revisión y extracción de datos.	
Periodo	Publicaciones entre 2009 y 2025, debido al desarrollo reciente de biometría y sistemas descentralizados.	
Idioma	Publicaciones en inglés.	
Acceso limitado		Imposibilidad de obtener el texto completo del estudio.
Duplicación		Estudios duplicados o versiones extendidas o reducidas del mismo trabajo.
Periodo excluido		Publicaciones anteriores a 2009.
Idioma no permitido		Trabajos escritos en idiomas distintos del inglés.
Calidad metodológica		Reportes con deficiencias importantes en claridad, transparencia, coherencia o descripción técnica.

La selección de estudios se llevó a cabo mediante revisión por pares con dos evaluadores independientes en la plataforma Rayyan, utilizando el modo ciego para minimizar sesgos. Las discrepancias se resolvieron mediante discusión y acuerdo entre los revisores. En la fase de full-text screening, los artículos fueron evaluados a texto completo y se registraron las razones de exclusión, siguiendo las indicaciones de PRISMA. Finalmente, solo se incorporaron a la síntesis cualitativa los estudios que cumplían con todos los criterios definidos, asegurando la trazabilidad y reproducibilidad del proceso.

2.4. Quality Assessment

La evaluación de calidad metodológica se realizó después de la selección a texto completo y antes de la extracción de datos, siguiendo las guías de Kitchenham (2007) para revisiones sistemáticas en ingeniería. El objetivo fue valorar el rigor y la transparencia de los estudios incluidos y detectar posibles sesgos que pudieran afectar la interpretación de los resultados sobre integridad de datos biométricos en entornos descentralizados.

Se aplicó un instrumento de evaluación adaptado al dominio de biometría y tecnologías descentralizadas, considerando las dimensiones establecidas por Kitchenham: (1) Claridad de la información, (2) Calidad del diseño del estudio, (3) amenazas a la validez, (4) integracion biometria-descentralizacion , y (5) transparencia general del estudio. La Tabla 6 presenta los criterios aplicados.

Table 6: Criterios de evaluación de calidad aplicados a los estudios incluidos.

Criterio	Descripción
Claridad de la información	El estudio explica claramente qué datos o conceptos utiliza y para qué sirven dentro del sistema que analiza.
Calidad del diseño del estudio	Describe de forma sencilla y ordenada cómo se hizo el estudio, qué partes lo componen y qué decisiones metodológicas se tomaron.
Amenazas a la validez	El estudio reconoce factores que pueden afectar la validez de los resultados obtenidos.
Integración biometría–descentralización	Explica de forma clara cómo se combinan los sistemas descentralizados con los datos biométricos y por qué esta integración aporta mejoras en seguridad o integridad.
Transparencia del estudio	Menciona las limitaciones, posibles problemas y el alcance real del enfoque propuesto.

La evaluación de calidad de los estudios se realizó mediante una escala trivalente, asignando 1 punto cuando el criterio era cumplido, 0.5 puntos cuando se cumplía de forma parcial y 0 puntos cuando no se cumplía. La puntuación total se obtuvo a partir de la suma de los criterios evaluados, permitiendo clasificar los estudios según su nivel de calidad metodológica.

2.5. Extracción de datos

El proceso de extracción de datos se realizó siguiendo las guías metodológicas de Kitchenham para revisiones sistemáticas. Para cada estudio incluido después de la evaluación a texto completo, se aplicó un formulario estructurado de extracción diseñado específicamente para esta revisión (Tabla 7), el cual fue probado previamente en una fase piloto con un conjunto reducido de artículos para asegurar claridad y consistencia en

su aplicación. La extracción fue realizada por un único revisor, registrando de manera sistemática la información relevante de cada estudio. Este procedimiento buscó garantizar uniformidad en la captura de datos y reducir posibles sesgos derivados del análisis. Los datos extraídos incluyeron: (1) el sistema biométrico utilizado, (2) el entorno descentralizado empleado, (3) la técnica criptográfica asociada, (4) los mecanismos de protección aplicados a los datos biométricos, (5) los desafíos identificados en cada propuesta y (6) las limitaciones reconocidas por los autores. Estas variables permitieron caracterizar de manera estructurada el estado del arte sobre integridad biométrica en sistemas de firma digital descentralizada.

Table 7: Matriz de extracción de datos para los estudios incluidos.

Parámetro	Descripción
Sistema biométrico	Tipo de biometría empleada (Iris, huella dactilar, voz).
Entorno descentralizado	Tipo de infraestructura distribuida utilizada.
Técnica criptográfica	Métodos criptográficos aplicados (ZKP, fuzzy commitment, cifrado homomórfico).
Protección de datos biométricos	Medidas empleadas para resguardar los datos biométricos (cifrado, anonimización, plantillas, etc.).
Desafíos identificados	Problemas técnicos o limitaciones prácticas mencionados en la propuesta.
Limitaciones	Restricciones reconocidas por los autores respecto al enfoque o a su aplicabilidad.

2.6. Análisis de datos

El análisis de los datos extraídos se realizó mediante una síntesis narrativa, siguiendo las recomendaciones de Kitchenham para revisiones sistemáticas en ingeniería. Dado que los estudios incluidos presentan una notable diversidad en cuanto a tipos de biometría, arquitecturas descentralizadas, técnicas criptográficas y mecanismos de protección, no fue posible aplicar un metaanálisis cuantitativo. Por ello, se optó por una integración descriptiva y estructurada de los hallazgos, complementada con el uso de estadística descriptiva para resumir y comparar las características de los estudios analizados.

Los estudios fueron organizados en función de las preguntas de investigación planteadas, lo que permitió agrupar la evidencia según: (1) el sistema biométrico utilizado, (2) el entorno descentralizado empleado, (3) las técnicas criptográficas integradas en cada propuesta, (4) los métodos de protección de datos biométricos, (5) los desafíos señalados y (6) las limitaciones reconocidas por los autores. Dentro de cada dimensión se identificaron patrones recurrentes y variaciones metodológicas relacionadas con la integridad de los datos biométricos en sistemas de firma digital. Asimismo, se realizó un análisis transversal asociando la calidad metodológica de los estudios según los criterios definidos en la Tabla 6 con la solidez y consistencia de los enfoques propuestos. Este contraste permitió valorar hasta qué punto los trabajos más completos o transparentes ofrecen soluciones más robustas o coherentes dentro del ámbito descentralizado. Finalmente, los resultados se integraron en una síntesis narrativa que responde de manera conjunta a las preguntas de investigación y al marco PICo, proporcionando una visión general y crítica del estado actual de las soluciones orientadas a proteger la integridad de los datos biométricos en firmas digitales descentralizadas.

3. Results

3.1. Study Selection

La estrategia de búsqueda permitió identificar inicialmente 110 registros; posteriormente, tras descartar los duplicados y aplicar los criterios de inclusión y exclusión durante las fases de selección y revisión a texto completo, se incluyeron finalmente 10 estudios en la presente revisión sistemática. El proceso de selección de estudios se resume en el diagrama PRISMA presentado en la Figura 1

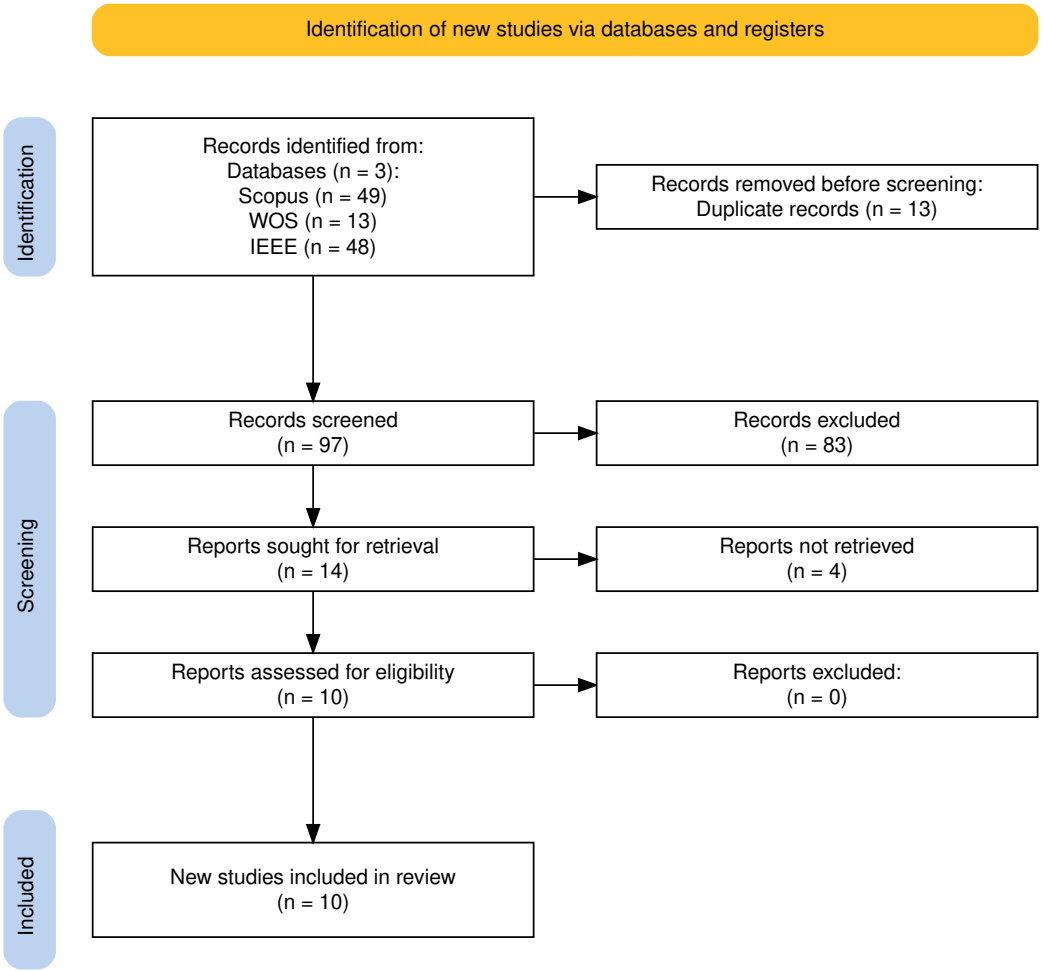

Figure 1. PRISMA 2020 flow diagram of the study selection process.

Table 8. Razones de exclusión de los estudios tras la revisión a texto completo.

Categoría	Referencias Excluidas	Número de Estudios
Without access	A01,A05, A20, A43	4

3.2. Data Availability

Los materiales utilizados durante la revisión sistemática se encuentran disponibles en una carpeta compartida en línea: Repositorio de datos y materiales de la revisión.

3.3. Quality Assessment

Los resultados de la evaluación de calidad muestran que, tras aplicar los criterios C1–C5, la mayoría de los estudios incluidos presenta una calidad metodológica alta. En esta evaluación se consideró la Claridad de la información (C1), Calidad del diseño del estudio (C2), Amenazas a la validez(C3) , Integración biometría–descentralización(C4) y Transparencia del estudio(C5). Los trabajos con una puntuación normalizada inferior a 0.5 fueron descartados, mientras que los estudios aceptados se clasificaron en calidad baja, buena y excelente. Los resultados indican que solo un número reducido de estudios alcanzó una calidad baja (T.R entre 0.1 y 0.7). En estos casos, las limitaciones se relacionan principalmente con una descripción poco detallada de los mecanismos de integridad biométrica o con un uso parcial de tecnologías descentralizadas. Por otra parte, un número menor de trabajos fue clasificado como de calidad buena (T.R entre 0.7 y 0.9), caracterizados por una implementación técnica adecuada, aunque con restricciones en el alcance o en la integración de la biometría dentro del sistema propuesto. La mayoría de los estudios aceptados alcanzó una calidad excelente (T.R $\geq$ 0.9). Estos trabajos se distinguen por definir claramente sus objetivos, emplear biometría humana de forma explícita, integrar tecnologías descentralizadas y presentar arquitecturas o evaluaciones técnicas bien estructuradas. Estos resultados muestran que la literatura más reciente en el área tiende a ofrecer propuestas más maduras y metodológicamente sólidas, como se resume en la Tabla 9.

Table 9. Distribución de los estudios según el nivel de calidad metodológica.

Nivel de calidad	Referencias	Número de estudios
Baja	A055, A36	2
Buena	A015	1
Excelente	A09, A08, A17, A13, A60, A95	6
Rechazado	A12	1

3.4. Characteristics of Included Studies

En relación con las modalidades biométricas, el reconocimiento facial y la huella dactilar son las técnicas más utilizadas, cada una presente en el 50 %e los estudios (n = 5), observándose que varios trabajos emplean más de una modalidad biométrica [4,9,15–17]. La biometría de voz aparece en el 20 % (n = 2) de los artículos[5,15] , mientras que el iris es considerado en el 10 % (n = 1).

Respecto a las tecnologías descentralizadas, el 70 % de los estudios (n = 7) adopta arquitecturas basadas en blockchain[3,4,7,9,15,16,18] siendo Ethereum la plataforma más mencionada (n = 4)[3,4,7,18]. Adicionalmente, el uso de soluciones de almacenamiento distribuido, como IPFS, se reporta en el 30 % de los casos (n = 3)[3,15,18]. En cuanto al uso de firmas digitales y enfoques criptográficos, los estudios muestran una combinación de esquemas tradicionales y mecanismos biométricos. Se identifican propuestas que emplean protocolos biométricos para la derivación de claves, como BAKE/BESAKE [5] , así como el uso de identificadores descentralizados (DIDs) y credenciales verificables en el 30 % de los estudios (n = 3)[3,4,15]. Los esquemas criptográficos tradicionales, como RSA-SHA256 y certificados X.509, aparecen en el 20 % (n = 2) de los artículos[5,7].

Para garantizar la integridad de los datos biométricos, el hashing es la técnica criptográfica más frecuente, reportada en el 80 % de los estudios, incluyendo variantes como el hashing perceptual [3–5,7,9,15,16,18]. Asimismo, se reporta el uso de Pruebas de Conocimiento Cero (ZKP) en el 30 %de los casos (n = 3)[3,4,15] y Cifrado Homomórfico en dos estudios[16,18].

En relación con la protección de los datos biométricos, el 40 % de los artículos (n = 4) emplea almacenamiento distribuido o fragmentación de claves[3,4,15,18] , mientras que

tres estudios optan por almacenamiento local en dispositivos del usuario[3,4,7]. Desde el punto de vista metodológico, los estudios experimentales y simulaciones representan el 60 % (n = 6)[4,9,16–19] , mientras que las pruebas de concepto y propuestas arquitectónicas constituyen el 40 % restante [3,5,7,15].La distribución porcentual de estas características se resume en la Figura 2.

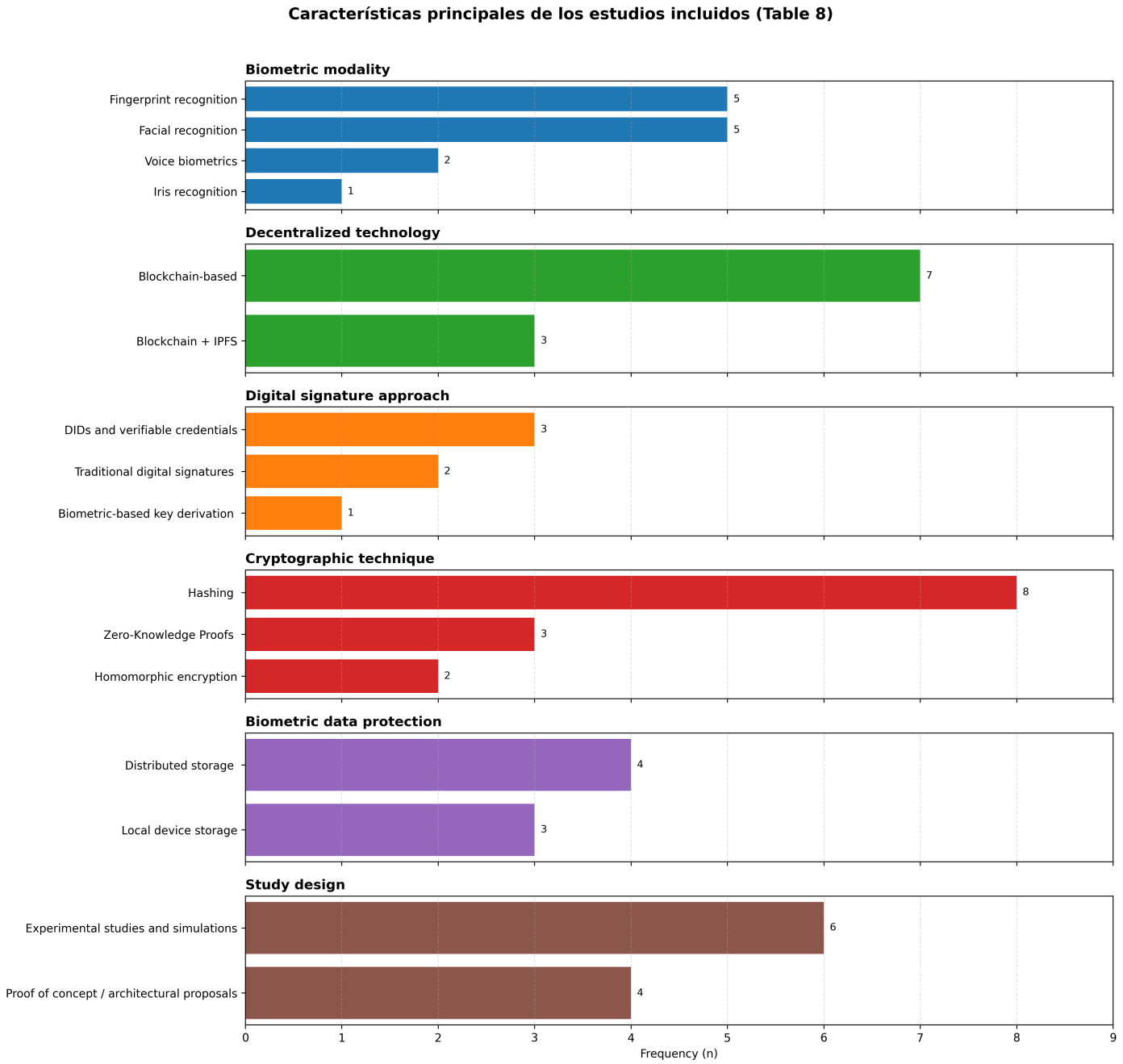

Figure 2. Percentage of studies reporting each characteristic (N=10).

3.5. Synthesis of Results According to Research Questions

A continuación se presentan los hallazgos organizados en función de las RQs establecidas.

RQ1. ¿Qué enfoques han sido propuestos en la literatura científica para integrar datos biométricos en firmas digitales descentralizadas?

Se identificó que la integración de datos biométricos en sistemas de firmas y autorizaciones descentralizadas se estructura bajo tres enfoques arquitectónicos principales.

I. Establecimiento de canales y claves seguras

En la comparación de las propuestas dentro de este enfoque, se observa que tanto Griffin [5] como Lu et al. [16] posicionan la biometría como una capa de seguridad previa, aunque con aplicaciones distintas. Griffin propone una estructura donde la muestra biométrica permite a dos partes remotas establecer una conexión cifrada directamente, eliminando la necesidad de infraestructuras de certificados externos para validar la comunicación de un contrato. Por su parte, Lu et al. implementan esta arquitectura como una puerta de enlace de autenticación en un entorno de aprendizaje distribuido, donde la validación biométrica es el requisito funcional que autoriza a un nodo local para acceder a datos privados y participar en la actualización de un modelo global. Mientras Griffin se enfoca en la creación del vínculo de comunicación para firmas legales, Lu et al. utilizan la arquitectura para proteger el acceso a activos de información en procesos de computación industrial.

La arquitectura funcional de este enfoque se apoya en el uso de sensores biométricos para capturar muestras, las cuales constituyen el punto de partida de una interacción entre dos partes sin intermediarios centralizados. La información obtenida a partir del rasgo biológico capturado se utiliza para generar los elementos necesarios que permiten establecer un canal de comunicación seguro.. En este modelo, los componentes principales incluyen el dispositivo de captura local y un protocolo de intercambio que emplea la información biométrica para asegurar la sesión antes de que se produzca cualquier acto formal de firma o transferencia de datos. Los estudios señalan que la biometría actúa como el componente inicial de autenticación que asegura la infraestructura de comunicación y permite validar la identidad antes del intercambio de información sensible en la red.

II. Evidencia de intención y sello de integridad inmutable

Al comparar a los autores de este paradigma, Orofino Giambastiani et al. [15], Jose et al. [9] y Griffin [5] coinciden en el uso de la biometría como un sustituto funcional de la firma manuscrita para garantizar la integridad de un evento. Orofino Giambastiani describe una arquitectura aplicada a registros médicos donde la firma biométrica del profesional valida hitos clínicos específicos, asegurando su presencia y vigilancia activa. Jose et al. proponen una estructura para el sufragio electrónico donde la huella dactilar del votante autoriza la emisión del voto tras ser contrastada con una base de datos de identidad nacional. Griffin complementa este enfoque sugiriendo que las muestras biológicas pueden documentar formalmente la aceptación de términos contractuales, sirviendo como evidencia de consentimiento que se almacena junto al documento firmado.

Este enfoque arquitectónico se despliega en el punto de acción donde se requiere vincular la voluntad física de un individuo con un registro digital persistente. Los componentes fundamentales incluyen el hardware (Escáneres de iris, Cámaras para reconocimiento facial, Micrófonos) de captura biométrica integrado en el proceso de autorización y una red descentralizada que registra la asociación entre el rasgo biológico y la transacción.

En este contexto, el acto de proporcionar la muestra biométrica constituye en sí mismo la autorización de la operación, generando un registro que se vincula de forma permanente a una cadena de bloques para asegurar que la acción sea auditable y resistente al

repudio.Aunque los dominios de aplicación difieren, los estudios coinciden en mantener la biometría como prueba directa de la participación del sujeto en el acto registrado.

III. Factor de Identidad Soberana (SSI) y recuperación de activos

Mir et al. [4], Wang y De Filippi [3] y Tavares et al. [7] proponen sistemas que eliminan la dependencia de proveedores de identidad siempre en línea, aunque con matices técnicos. Mir et al. presentan una arquitectura donde la biometría permite al usuario interactuar con múltiples agentes personales para recuperar el control de su capacidad de firma sin que ninguna entidad única posea la información completa.Wang y De Filippi analizan este modelo en contextos humanitarios, donde la biometría permite vincular a una persona con sus derechos y beneficios de forma persistente, haciendo posible que la identidad sea transportable incluso cuando la autoridad emisora original deja de existir. Por su parte, Tavares et al. proponen una arquitectura que conecta documentos de identidad físicos con billeteras de la red Ethereum y emplean la biometría para verificar que el poseedor de los activos digitales sea el titular legítimo del documento original. Mir et al. se centran en los mecanismos de recuperación técnica de la identidad, mientras que Wang y Tavares resaltan aspectos relacionados con la soberanía individual y la movilidad global.

La arquitectura funcional de este enfoque sitúa al usuario en el centro de la gestión de su identidad y utiliza la biometría como el medio para ejercer control sobre sus propios atributos y credenciales. Entre sus componentes principales se incluyen billeteras digitales, identificadores descentralizados y agentes de identidad personales que operan de manera distribuida. En este modelo, la biometría se emplea como mecanismo para desbloquear el acceso a la identidad digital del usuario o para recuperar capacidades de firma que no se encuentran almacenadas en un servidor central.

RQ2. ¿Qué técnicas y principios criptográficos se utilizan para garantizar la integridad de los datos biométricos en firmas digitales en entornos descentralizados?

A partir de la revisión de la literatura, se identificó que la integridad de los datos biométricos en sistemas de firmas digitales descentralizadas se garantiza mediante la aplicación de distintos principios y técnicas criptográficas, los cuales pueden agruparse en cuatro enfoques principales según su función dentro del proceso de seguridad.

I. Protocolos de intercambio de claves

Griffin (2018) reporta el uso de protocolos de Intercambio de Claves Autenticadas por Contraseña (PAKE) y su variante biométrica (BAKE) para establecer canales de comunicación seguros que protegen la confidencialidad de las credenciales durante su transferencia[5]. En esta arquitectura, la biometría se integra mediante la extracción de "secretos débiles" a partir de muestras procesadas por sensores locales, los cuales alimentan un intercambio de claves Diffie-Hellman[5]. La función principal de esta técnica es permitir que partes remotas establezcan un vínculo cifrado de forma directa, eliminando la dependencia de Infraestructuras de Claves Públicas (PKI) externas y evitando ataques de intermediario (man-in-the-middle)[5]. Como ventaja, se reporta una reducción considerable en los costos de gestión de certificados, aunque Griffin advierte que la seguridad del sistema sigue ligada a la entropía del secreto extraído.

II. Anclaje criptográfico mediante hashing y estampado en blockchain

Esta tecnica constituye el pilar de la inmutabilidad en la mayoría de los estudios analizados. Orofino Giambastiani et al. (2023) y Tavares et al. (2018) emplean funciones de hash criptográfico para generar identificadores únicos de los registros biométricos, los cuales se almacenan en la blockchain mientras los datos originales permanecen fuera de la red (off-chain)[7,15]. De forma similar, Jose et al. (2020) reportan el uso de códigos hash para verificar si las imágenes esteganográficas que contienen datos de identidad han sido alteradas durante el proceso de votación[9]. En estos sistemas, la arquitectura funcional se basa en una separación estricta: los datos sensibles se sitúan en sistemas de almacenamiento

direccionables por contenido, como el Sistema de Archivos Interplanetario (IPFS), y solo el hash resultante se registra on-chain como una prueba de existencia inmutable[15,18]. Esta configuración permite que cualquier modificación en el dato original invalide el vínculo con la cadena de bloques, garantizando así que la información no haya sido adulterada. No obstante, Orofino Giambastiani et al. señalan como limitación técnica la latencia actual en la subida y descarga de redes de almacenamiento logico-decentralizadas, lo que obliga a usar bases de datos intermedias para el procesamiento en tiempo real[15].

III. Compromisos criptográficos y pruebas de conocimiento cero (ZKP)

El uso de Compromisos Criptográficos y Pruebas de Conocimiento Cero (ZKP) se identifica como un principio avanzado para preservar la integridad sin comprometer la privacidad. Mir et al. (2022) integran Funciones Pseudoaleatorias Oblivious de Umbral (TOPRF) y esquemas de intercambio de secretos de Shamir (TSS) para fragmentar las capacidades de firma entre múltiples agentes personales[4]. En su flujo operativo, la biometría actúa como el factor de desbloqueo que permite reconstruir la clave privada solo cuando se alcanza un umbral determinado de agentes autorizados, protegiendo al sistema contra ataques de diccionario offline[4]. Wang y De Filippi (2020) y Mir et al. (2022) coinciden en que el uso de ZKP permite al usuario demostrar la posesión de una credencial biométrica válida ante un verificador (como un proveedor de servicios) sin revelar el dato biológico subyacente, asegurando que la identidad sea portable y resistente al repudio[3,4]. Una limitación reportada en la arquitectura de Mir et al. es que la seguridad se ve comprometida si el número de agentes corrompidos supera el umbral crítico establecido.

IV. Técnicas de enmascaramiento y ruido diferencial

La integridad de los datos procesados en el extremo (edge computing) se refuerza mediante técnicas de enmascaramiento y ruido diferencial. Lu et al. (2022) reportan una arquitectura de aprendizaje federado donde se añade ruido gaussiano a los parámetros del modelo (gradientes) antes de ser cargados al servidor central[16]. Esta técnica de privacidad diferencial evita que atacantes externos infieran la distribución de los datos biométricos privados a partir de las actualizaciones del sistema[16]. Sin embargo, los autores observan una limitación técnica inherente: la adición de ruido excesivo para mejorar la protección de la privacidad puede provocar una disminución en la precisión diagnóstica del sistema[16]. Por su parte, Tavares et al. (2018) integran firmas RSA-SHA256 para vincular billeteras de Ethereum con atributos de identidad certificados por autoridades oficiales (X.509), asegurando que el puente entre el mundo físico y digital mantenga la legitimidad de la titularidad de forma desintermediada[7]. Estas técnicas configuran un ecosistema donde la integridad biométrica no depende de un único almacén central, sino de la robustez matemática del anclaje on-chain y el control de acceso en el extremo.

RQ3. ¿Cuáles son las principales limitaciones y desafíos técnicos que enfrenta la implementación de sistemas biométricos en firmas digitales descentralizadas?

I. Rendimiento y viabilidad económicas

Se observa que la eficiencia de las firmas biométricas está condicionada por la latencia de confirmación y los costos operativos de transacción (gas fees). Mir et al. (2022) reportan valores monetarios específicos para el registro de credenciales, con costos estimados de 0.069USD en la redNamecoiny 0.0225 USD en la red de prueba Ethereum Rinkeby[4].

Estos autores detallan que las tarifas pueden oscilar entre 0 y 0.01 NMC o hasta 0.000424 ETHER dependiendo de la prioridad de procesamiento, lo que genera disparidades notables en los tiempos de confirmación: mientras Namecoin requiere aproximadamente dos horas para alcanzar 12 confirmaciones, en Ethereum el proceso se reduce a alrededor de tres minutos, una vez completada la sincronización inicial del nodo que puede extenderse hasta aproximadamente tres horas y se realiza solo durante la fase de configuración, sin afectar la agilidad de las firmas posteriores [4].

Wang y De Filippi (2020) coinciden en que los costos en cadenas públicas basadas en prueba de trabajo (PoW) resultan elevados y prohibitivos para el uso masivo, a diferencia de las redes privadas de prueba de autoridad (PoA) que operan con costo cero por transacción o redes laterales donde las tarifas son despreciables[3]. Por su parte, Orofino Giambastiani et al. (2023) reportan que las velocidades de carga en redes como IPFS impiden el registro de datos biométricos en tiempo real y califican el almacenamiento masivo directamente en cadena como técnicamente impráctico debido al tamaño extremo de bloque que requeriría[15]. Finalmente, Tavares et al. (2018), aunque no proveen costos exactos de gas para su solución, informan que los procesos tradicionales de identidad tienen costos de $15 a $20 USD por trámite, señalando que la ineficiencia y los tiempos de respuesta de varios días en sistemas convencionales persisten como un factor de comparación crítico para la viabilidad de las alternativas descentralizadas[7].

II. Precisión y estabilidad de los sistemas biométricos

La precisión y estabilidad de los sistemas biométricos constituyen una limitación técnica recurrente en entornos descentralizados, debido a la naturaleza inherentemente variable de los rasgos biológicos utilizados para la autenticación y la firma digital. A diferencia de los factores basados en conocimiento, los datos biométricos no son invariantes en el tiempo y están sujetos a degradación progresiva, lo que afecta directamente la fiabilidad del reconocimiento y compromete la integridad de los mecanismos criptográficos que dependen de ellos[3].

Desde la perspectiva de la estabilidad temporal, la literatura evidencia que los rasgos biométricos se ven alterados por cambios físicos inevitables. Wang y De Filippi (2020) reportan que las tasas de error en escaneos de iris pueden oscilar entre el 2.5% y el 20%[3], mientras que factores como el envejecimiento, lesiones, desgaste físico o condiciones ambientales afectan la calidad de huellas dactilares y reconocimiento facial. Estas variaciones introducen un compromiso directo entre seguridad y usabilidad: umbrales estrictos incrementan la tasa de falso rechazo (FRR), excluyendo usuarios legítimos, mientras que configuraciones más permisivas elevan el riesgo de falsa aceptación (FAR).[3]

Esta problemática se intensifica en escenarios de gran escala, como sistemas de votación electrónica o infraestructuras nacionales de identidad. Jose et al. (2020) enfatizan la dificultad de mantener tasas FAR y FRR cercanas a cero en contextos poblacionales amplios[9], donde incluso pequeñas desviaciones estadísticas se traducen en fallos masivos. Para mitigar estos efectos, se han propuesto estrategias como múltiples intentos de captura o la selección del "mejor dedo", logrando precisiones superiores al 99%, aunque a costa de mayor latencia operativa y una infraestructura de soporte más compleja[9].

los estudios identifican un conflicto estructural entre robustez y precisión en el procesamiento biométrico. Cheng et al. (2010) demuestran que, en esquemas basados en Modulación por Cuantización (QIM), el aumento del tamaño del paso de cuantificación mejora la resistencia frente a perturbaciones y ataques, pero degrada significativamente el rendimiento de detección de las huellas biométricas[19]. De manera similar, en técnicas de extracción de características basadas en transformadas wavelet o contourlet, los coeficientes de baja frecuencia aportan estabilidad global, mientras que los de alta frecuencia, necesarios para una identificación precisa, resultan altamente sensibles al ruido introducido durante la transmisión o el procesamiento.

La incorporación de mecanismos de preservación de la privacidad añade una capa adicional de complejidad. En arquitecturas de aprendizaje federado, Lu et al. (2022) reportan que la adición de ruido diferencial gaussiano para proteger los gradientes del modelo evita ataques de inversión de información, pero provoca una caída apreciable en la precisión diagnóstica cuando el nivel de ruido es elevado[16]. Este efecto se ve reforzado

por el desequilibrio de clases característico de los sistemas descentralizados, donde los eventos anómalos son escasos frente a los accesos legítimos, reduciendo la sensibilidad del sistema ante situaciones críticas.

estos hallazgos indican que la biometría no constituye un factor suficientemente estable para operar de forma aislada en esquemas de firma digital descentralizada. Dado que el compromiso de una plantilla biométrica es irreversible y que en entornos descentralizados no existe una autoridad central encargada de su supervisión, las propuestas más robustas tienden a relegar la biometría a un rol complementario, utilizándola principalmente como prueba de vivacidad o como mecanismo de desbloqueo de claves protegidas por hardware seguro, en lugar de emplearla como semilla criptográfica directa.

III. Seguridad y privacidad

Los estudios identifican riesgos inherentes al carácter público e irreversible de la biometría, los cuales introducen desafíos estructurales para la seguridad y la privacidad en sistemas de firma digital descentralizados. Wang y De Filippi (2020) advierten que, a diferencia de una contraseña o una clave criptográfica, el rasgo biológico no puede ser revocado ni reemplazado una vez comprometido[3]. Esta irreversibilidad convierte a la biometría en un factor de seguridad frágil, ya que la exposición de la identidad física implica una pérdida permanente del control sobre la identidad digital asociada.

A estas limitaciones se suman las amenazas de suplantación (*spoofing*), ampliamente documentadas en distintas modalidades biométricas. Se ha reportado que las huellas dactilares pueden ser copiadas mediante técnicas de levantamiento físico, mientras que el reconocimiento facial y de iris es vulnerable a ataques basados en fotografías, videos o lentes de contacto especializados. Estas vulnerabilidades afectan directamente la confianza en los sistemas biométricos, al demostrar que el "algo que eres" puede ser replicado sin interacción directa con el usuario legítimo[3].

Mir et al. (2022) señalan que el almacenamiento de datos de referencia biométrica o plantillas en proveedores de identidad genera puntos únicos de falla altamente atractivos para atacantes[4]. La centralización de esta información facilita ataques fuera de línea, como los ataques de diccionario, en los que un adversario puede intentar reconstruir las credenciales sin ser detectado en tiempo real. Asimismo, el uso de parámetros compartidos en arquitecturas distribuidas amplía el riesgo de ataques de inversión de modelo que comprometen la privacidad del usuario[4].

En entornos descentralizados, los dispositivos finales representan otra superficie de ataque crítica. Los smartphones y dispositivos portátiles están expuestos a malware, pérdida o robo físico, y en ausencia de una autoridad central, la pérdida del dispositivo puede implicar la pérdida irreversible de claves privadas y activos asociados. Ante este escenario, la literatura coincide en la necesidad de incorporar capas adicionales de protección, como la anonimización, la fragmentación de capacidades criptográficas y los mecanismos de verificación sin revelación, para mitigar los riesgos derivados del uso directo de biometría y preservar la privacidad del usuario.

IV. Barreras tecnológicas y resistencia de los usuarios

La dependencia de la infraestructura tecnológica y la resistencia de los usuarios constituyen barreras relevantes para la adopción de firmas digitales biométricas en entornos descentralizados. Diversos estudios coinciden en que estas limitaciones no son únicamente técnicas, sino que derivan de una fragilidad operativa en la interacción entre el usuario, el hardware disponible y los protocolos criptográficos, lo que genera una brecha entre la seguridad teórica de los modelos descentralizados y su aplicación práctica[3].

Los modelos de identidad autosoberana (SSI) dependen en gran medida de la disponibilidad de dispositivos capaces de gestionar de forma segura claves privadas y credenciales digitales. Wang y De Filippi (2020) señalan que la adopción de estos sistemas está condi-

cionada por la penetración de smartphones y la conectividad constante, lo cual resulta incierto en contextos de vulnerabilidad[3]. En escenarios reales, la ausencia de dispositivos adecuados obliga a recurrir a esquemas de custodia o tutoría que reducen el grado de descentralización. Además, el cumplimiento de normativas de protección de datos exige el uso de hardware especializado para el procesamiento local de biometría, incrementando los costos y dificultando su despliegue masivo.

Un desafío crítico adicional es la gestión y recuperación de claves. En ausencia de una autoridad central, la pérdida del dispositivo físico puede implicar la pérdida irreversible de la identidad digital, lo que introduce un punto único de falla a nivel del usuario y afecta la confianza en el sistema. Asimismo, los mecanismos de revocación de credenciales en entornos descentralizados suelen ser complejos o poco eficientes, lo que limita la capacidad de corrección ante errores o compromisos de seguridad[3,4].

Las tasas de error en la captura biométrica pueden excluir a usuarios legítimos en aplicaciones críticas, mientras que la necesidad de gestionar múltiples factores de seguridad incrementa la carga cognitiva y la probabilidad de errores operativos. A nivel institucional, Orofino Giambastiani et al. (2023) destacan que la inmutabilidad de los registros biométricos genera resistencia entre profesionales, quienes perciben un aumento del riesgo legal y de responsabilidad[15]. estas barreras evidencian que la integración biométrica en firmas descentralizadas aún enfrenta el desafío de equilibrar la seguridad criptográfica con la fragilidad operativa del entorno del usuario, lo que explica la adopción limitada y la necesidad de enfoques híbridos en implementaciones actuales.

4. Discussion

Los resultados de esta revisión sistemática permiten contrastar los enfoques propuestos en estudios previos con las tendencias generales observadas en los trabajos analizados. Los principales antecedentes revisados se resumen en la Tabla 1, mientras que esta sección se centra en examinar las similitudes, diferencias y vacíos identificados a partir de los resultados obtenidos. En relación con las similitudes, se observa una coincidencia clara entre los enfoques individuales y los patrones generales identificados. La mayoría de los estudios analizados adopta arquitecturas descentralizadas basadas en blockchain, en línea con propuestas como BDAS [11], BiometricIdentity [12] y BioZero [14], donde la descentralización se emplea como un mecanismo para reforzar la integridad y la trazabilidad de los datos biométricos [4,7,15,18]. En este contexto, la biometría se incorpora principalmente como un factor de autenticación o como un insumo para la generación de material criptográfico [4,5,8,10]. Este enfoque es coherente con los resultados que evidencian un uso frecuente de la huella dactilar y del reconocimiento facial [9,15–17], así como con la adopción de protocolos de derivación de claves biométricas [5,8,14]. De manera similar, los mecanismos criptográficos identificados en los antecedentes también se reflejan en los resultados de la revisión.

El uso amplio de funciones hash como técnica de anclaje criptográfico aparece tanto en propuestas tempranas como en soluciones más recientes, lo que explica que el hashing sea la técnica más frecuente en los estudios incluidos [4,7,9,10,18]. En la misma línea, la incorporación de pruebas de conocimiento cero en trabajos recientes coincide con la tendencia hacia esquemas que priorizan la verificación sin revelación, orientados a preservar la privacidad sin afectar la integridad de los datos [4,8,13,14]. Sin embargo, también se identifican diferencias relevantes.

Aunque algunos antecedentes proponen mecanismos avanzados de fragmentación [11,12], así como esquemas de almacenamiento distribuido o arquitecturas de múltiples capas [8,13]. Sin embargo, los resultados generales muestran que estas soluciones todavía no son predominantes,principalmente debido a limitaciones prácticas asociadas a su imple-

mentación y operación a gran escala. Una proporción significativa de los estudios continúa utilizando almacenamiento local o enfoques híbridos [3,4], lo que sugiere que la adopción de esquemas completamente descentralizados para la protección de datos biométricos sigue siendo limitada en la práctica [3,15]. Esta situación evidencia una brecha entre propuestas conceptualmente sólidas y su implementación efectiva [3,7].

Otra diferencia relevante está relacionada con la madurez técnica de las soluciones. Si bien algunas propuestas recientes incorporan técnicas avanzadas de escalabilidad y privacidad, como los rollups [13] o la computación homomórfica parcial [14,18], los resultados de la revisión indican que estos enfoques aún se mantienen como líneas emergentes de investigación y no como soluciones ampliamente consolidadas. Esta situación explica su menor frecuencia relativa frente a técnicas más tradicionales y mejor comprendidas.Finalmente, los desafíos reportados en propuestas previas de la literatura, como las descritas por Lai et al. [14] y Abo Alzahab et al. [12], se confirman de forma consistente a nivel global en los resultados de esta investigación. A partir del análisis conjunto de los estudios incluidos, se observa que problemas relacionados con el rendimiento, la latencia, los costos operativos y la variabilidad inherente de los sistemas biométricos persisten como barreras técnicas relevantes [4,7]. A pesar de los avances observados, estos factores continúan limitando la adopción a gran escala de firmas digitales descentralizadas basadas en biometría [3,7]. Esta situación evidencia que, aunque existe un consenso creciente sobre la utilidad de integrar biometría y descentralización para garantizar la integridad de los datos, aún persiste una brecha entre las propuestas más avanzadas y su aplicación generalizada, lo que refuerza la necesidad de estudios que evalúen de forma comparativa la viabilidad, escalabilidad y robustez de estas soluciones en escenarios reales.

5. Conclusions

Los resultados de esta revisión sistemática muestran que los enfoques propuestos para integrar datos biométricos en firmas digitales descentralizadas se basan principalmente en la combinación de biometría humana con arquitecturas distribuidas. En estos sistemas, la biometría se utiliza de forma recurrente como mecanismo de autenticación y como vínculo entre la identidad del usuario y los procesos de firma o validación. Las tecnologías descentralizadas se emplean para reducir la dependencia de infraestructuras centralizadas y para reforzar la verificación de las operaciones digitales mediante propiedades como la inmutabilidad y la trazabilidad.

En relación con las técnicas y principios criptográficos utilizados para garantizar la integridad de los datos biométricos, se observa que la mayoría de las propuestas se apoya en mecanismos consolidados, especialmente funciones hash y el registro de evidencias en libros mayores distribuidos. Estas técnicas continúan siendo la base práctica más utilizada para asegurar que la información no sea alterada una vez registrada. Al mismo tiempo, se identifican propuestas orientadas a mejorar la privacidad y la escalabilidad, como compromisos criptográficos y pruebas de conocimiento cero, aunque su adopción aún es limitada y se concentra principalmente en trabajos más recientes.

Se evidencia la presencia de limitaciones y desafíos técnicos persistentes. Entre los más relevantes se identifican los problemas de rendimiento y latencia, los costos operativos asociados a infraestructuras descentralizadas, la variabilidad inherente de los sistemas biométricos y los riesgos derivados de la exposición de datos sensibles que no pueden ser reemplazados si se ven comprometidos. Estas limitaciones continúan afectando la viabilidad y la adopción a gran escala de las soluciones propuestas.

el análisis realizado permite comprender las limitaciones, fortalezas y tendencias actuales de los enfoques propuestos para garantizar la integridad de los datos biométricos en firmas digitales descentralizadas. Como principales fortalezas, se identifica el uso combinado de

biometría humana y tecnologías descentralizadas para reforzar la integridad y la verificación de los procesos digitales. En cuanto a las tendencias, se observa un interés creciente por integrar mecanismos orientados a mejorar la privacidad y la escalabilidad, aunque su aplicación práctica aún es limitada. De forma general, el área avanza hacia soluciones más completas y mejor fundamentadas, aunque persisten brechas entre las propuestas técnicas y su aplicación práctica a gran escala, lo que justifica la necesidad de continuar investigando y evaluando estas soluciones en contextos reales.

References

1. Khranovskyi, M.; Kernytskyy, A. Blockchain and Biometrics: Challenges and Solutions. *Computer Design Systems. Theory and Practice* **2024**, *6*, 189–198. Received: 25 Mar 2024; Revised: 01 Apr 2024; Accepted: 05 Apr 2024.
2. Ghafourian, M.; Sumer, B.; Vera-Rodríguez, R.; Fierrez, J.; Tolosana, R.; Morales, A.; Kindt, E. Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis. *arXiv preprint arXiv:2302.10883* **2024**, [arXiv:cs.CV/2302.10883].
3. Wang, F.; De Filippi, P. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain* **2020**, *2*, 28. https://doi.org/10.3389/fbloc.2019.00028.
4. Mir, O.; Roland, M.; Mayrhofer, R. Decentralized, Privacy-Preserving, Single Sign-On. *Security and Communication Networks* **2022**, *2022*, 1–18. https://doi.org/10.1155/2022/9983995.
5. Griffin, P.H. Biometric Electronic Signature Security. In Proceedings of the Advances in Human Factors in Cybersecurity; Ahram, T.Z.; Nicholson, D., Eds., Cham, 2019; Vol. 782, *Advances in Intelligent Systems and Computing*, pp. 15–22. https://doi.org/10.1007/978-3-319-94782-2_2.
6. Qin, Y.; Zhang, B. Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal. *Applied Sciences* **2023**, *13*, 1–20. Received: 12 June 2023; Revised: 11 July 2023; Accepted: 11 July 2023; Published: 12 July 2023, https://doi.org/10.3390/app13148117.
7. Tavares, M.; Guerreiro, A.; Coutinho, C.; Veiga, F.; Campos, A. WalliD: Secure Your ID in an Ethereum Wallet. In Proceedings of the 2018 International Conference on Intelligent Systems (IS). IEEE, 2018, pp. 813–820. https://doi.org/10.1109/IS.2018.8710547.
8. Sarier, N.D. Efficient biometric-based identity management on the Blockchain for smart industrial applications. *Pervasive and Mobile Computing* **2021**, *71*, 1–18. https://doi.org/10.1016/j.pmcj.2020.101322.
9. Varma, C.S.P.; Rahul, D.S.; Jose, J.; Samhitha, B.K.; Cherukullapurath Mana, S. Aadhar Card Verification Based Online Polling. In Proceedings of the Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020), India, 2020; pp. 479–483.
10. Hassen, O.A.; Abdulhussein, A.A.; Darwish, S.M.; Othman, Z.A.; Tiun, S.; Lotfy, Y.A. Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IoT Blockchain Network. *Symmetry* **2020**, *12*, 1699. https://doi.org/10.3390/sym12101699.
11. Lee, Y.K.; Jeong, J. Securing biometric authentication system using blockchain. *ICT Express* **2021**, *7*, 322–326. https://doi.org/10.1016/j.icte.2021.08.003.
12. Abo Alzahab, N.; Rafaiani, G.; Battaglioni, M.; Cavalli, A.; Chiaraluce, F.; Baldi, M. BiometricIdentity dApp: Decentralized biometric authentication based on fuzzy commitment and blockchain. *SoftwareX* **2024**, *28*, 101932. https://doi.org/10.1016/j.softx.2024.101932.
13. Yun, J.; Lu, Y.; Liu, X.; Guan, J. Bio-Rollup: a new privacy protection solution for biometrics based on two-layer scalability-focused blockchain. *PeerJ Computer Science* **2024**, *10*, e2268. https://doi.org/10.7717/peerj-cs.2268.
14. Lai, J.; Wang, T.; Zhang, S.; Yang, Q.; Liew, S.C. BioZero: An Efficient and Privacy-Preserving Decentralized Biometric Authentication Protocol on Open Blockchain. *arXiv preprint arXiv:2409.17509* **2024**, [arXiv:cs.CR/2409.17509].
15. Orofino Giambastiani, R.; Sáenz, R.; Lahitte, G.; Umaran, J. Technology Optimization for Patient Safety: A Blockchain-Based Anesthesia Record System Architecture. *Frontiers in Blockchain* **2023**, *6*, 1116124. Published: 13 July 2023, https://doi.org/10.3389/fbloc.2023.1116124.

16. Lu, S.; Gao, Z.; Xu, Q.; Jiang, C.; Zhang, A.; Wang, X. Class-Imbalance Privacy-Preserving Federated Learning for Decentralized Fault Diagnosis With Biometric Authentication. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 9101–9111. https://doi.org/10.1109/TII.2022.3190034.
17. Muraleedharan, R.; Osadciw, L.A.; Yan, Y. Resource Optimization in Distributed Biometric Recognition Using Wireless Sensor Network. *Multidimensional Systems and Signal Processing* **2009**, *20*, 165–182. https://doi.org/10.1007/s11045-008-0073-0.
18. Qureshi, A.; Megías, D. Blockchain-based P2P Multimedia Content Distribution Using Collusion-Resistant Fingerprinting. In Proceedings of the Proceedings of the APSIPA Annual Summit and Conference (APSIPA ASC 2019), Lanzhou, China, 2019; pp. 1606–1615.
19. Cheng, G.; Ling, H.; Zou, F.; Li, P. An Improved QIM Based Anti-Collusion Fingerprinting Scheme. In Proceedings of the Proceedings of the IEEE International Conference. IEEE, 2010, pp. 1865–1868.