RIMI
Revista de Investigación Multidisciplinaria, Iberoamericana

AÑO 4. No. 1

ISSN:2992-7978

PRIVACIDAD Y SEGURIDAD EN IDENTIDADES DIGITALES DESCENTRALIZADAS CON BLOCKCHAIN Y PRUEBAS DE CONOCIMIENTO CERO

Cristian Adrian Pazmiño Cortez[1]
Rodrigo Cadena[2]

[1] Doctorando Universidad Americana de Europa, UNADE

[2] Profesor-Investigador Universidad Americana de Europa, UNADE

AÑO 4. No. 1

ISSN:2992-7978

RESUMEN

Se presentó un modelo híbrido de identidad digital descentralizada que integró blockchain, pruebas de conocimiento cero (BBS+ y ZK) y cifrado homomórfico con políticas ABAC/PBAC. Se justificó la propuesta por las limitaciones de los modelos centralizados y federados para preservar la privacidad y evitar puntos únicos de fallo. El objetivo general fue maximizar la minimización de datos y la no-vinculabilidad sin perder interoperabilidad con ecosistemas OIDC. Se implementó una simulación comparativa entre credenciales VC-JWT, BBS+ (VC-LD), AnonCreds y SD-JWT, evaluando latencia de verificación, un índice de minimización de datos (DMI), una métrica ilustrativa de no-vinculabilidad (U) y la escalabilidad efectiva de verificación por segundo (EVPS). Los resultados mostraron diferencias significativas entre métodos en latencia y un compromiso rendimiento-privacidad: VC-JWT resultó más rápido con menor minimización, mientras que BBS+/AnonCreds ofrecieron mayor DMI y U con un costo computacional moderado. Finalmente, se discutieron las implicaciones éticas y regulatorias (GDPR, eIDAS 2.0) y se delineó una arquitectura de referencia lista para prototipo interoperable.

Palabras clave: Blockchain, Identidad Digital, Privacidad

ABSTRACT

his paper presents a hybrid model for decentralized digital identity that integrates blockchain technology, zero-knowledge proof schemes (BBS+ and general ZK), homomorphic encryption, and fine-grained access control policies based on ABAC and PBAC. The proposal is motivated by the structural limitations of centralized and federated identity models, particularly regarding privacy preservation, data minimization, and the existence of single points of failure. The primary objective is to maximize data minimization and non-linkability while maintaining interoperability with existing OpenID Connect (OIDC) ecosystems. A comparative simulation was implemented to evaluate four verifiable credential approaches—VC-JWT, BBS+ (VC-LD), AnonCreds, and SD-JWT—using quantitative metrics including verification latency, a Data Minimization Index (DMI), an illustrative non-linkability metric (U), and Effective Verifications Per Second (EVPS) as a scalability indicator. The results reveal significant differences among the evaluated methods, highlighting a clear performance–privacy trade-off. VC-JWT exhibited the lowest verification latency but limited data minimization, whereas BBS+ and AnonCreds achieved higher DMI and non-linkability scores at the cost of moderate computational overhead. Finally, the paper discusses the ethical and regulatory implications of the proposed model in the context of GDPR and eIDAS 2.0, and outlines a reference architecture suitable for the development of an interoperable prototype within real-world digital identity ecosystems.

Keywords: Blockchain, Digital Identity, Privacy

AÑO 4. No. 1

ISSN:2992-7978

INTRODUCCIÓN

Los modelos tradicionales de identidad digital, tanto centralizados como federados, concentran el control y la gestión de los atributos de los usuarios en proveedores dominantes, lo que incrementa la superficie de ataque, favorece la correlación de datos entre dominios y genera puntos únicos de fallo. Estas limitaciones técnicas y estructurales entran en tensión con principios fundamentales de protección de datos como la minimización, la limitación de propósito y la proporcionalidad, consagrados en marcos normativos como el Reglamento General de Protección de Datos (GDPR), la norma ISO/IEC 29100 y la regulación europea eIDAS 2.0. En este contexto, la dependencia de intermediarios de confianza y la acumulación de metadatos dificultan el cumplimiento efectivo de los requisitos de privacidad en escenarios de alta garantía.

La identidad auto-soberana (Self-Sovereign Identity, SSI) surge como un paradigma alternativo orientado a devolver el control de la identidad al titular mediante el uso de identificadores descentralizados (DID) y credenciales verificables (VC). Este enfoque permite la portabilidad de la identidad y la divulgación selectiva de atributos, reduciendo la necesidad de correladores centrales y habilitando modelos de verificación más respetuosos con la privacidad. En particular, la estandarización promovida por el W3C y la OpenID Foundation ha permitido la aparición de múltiples mecanismos de credenciales verificables —como VC-JWT, BBS+, AnonCreds y SD-JWT— que difieren en sus propiedades criptográficas, niveles de privacidad e interoperabilidad con infraestructuras existentes.

No obstante, la coexistencia de estos enfoques plantea un desafío relevante: comprender los compromisos reales entre rendimiento, minimización de datos y no-vinculabilidad, especialmente en contextos donde la interoperabilidad con ecosistemas empresariales basados en OAuth 2.0 y OpenID Connect es un requisito clave. Si bien diversos trabajos han analizado estas tecnologías desde una perspectiva conceptual o criptográfica, existe una necesidad de evaluaciones comparativas que permitan fundamentar decisiones de diseño arquitectónico bajo criterios técnicos, regulatorios y operativos.

En este marco, el presente trabajo propone un modelo híbrido de identidad digital descentralizada que integra credenciales verificables, pruebas de conocimiento cero y políticas de control de acceso basadas en atributos y propósito, manteniendo compatibilidad con flujos OIDC mediante los perfiles OIDC4VCI y OIDC4VP. El objetivo es demostrar que es posible equilibrar privacidad e interoperabilidad sin sacrificar escalabilidad, mediante una arquitectura flexible capaz de seleccionar dinámicamente el mecanismo de credencial más adecuado según el contexto de uso.

Es importante precisar que los resultados presentados provienen de una simulación controlada basada en datos sintéticos, y no de evaluaciones empíricas realizadas en entornos productivos reales. Este enfoque metodológico permite aislar variables, comparar enfoques bajo condiciones homogéneas y analizar tendencias estructurales, pero introduce una limitación explícita de validez externa, ya que factores como implementaciones específicas, configuraciones de hardware, latencias de red y políticas organizacionales pueden influir significativamente en escenarios reales. En consecuencia, los valores reportados deben interpretarse como indicadores comparativos relativos y no como métricas absolutas directamente extrapolables a despliegues en producción.

Las métricas empleadas para evaluar la privacidad, en particular el Índice de Minimización de Datos (DMI) y la métrica ilustrativa de no-vinculabilidad (U), deben entenderse como aproximaciones operacionales diseñadas para facilitar la comparación entre mecanismos bajo supuestos controlados. Estas métricas no constituyen medidas exhaustivas ni formalmente normalizadas de privacidad, ya que no capturan aspectos cualitativos como la sensibilidad semántica de los atributos, la inferencia indirecta a partir de metadatos o la persistencia temporal de la información revelada, por lo que sus resultados deben interpretarse dentro del alcance definido por el diseño experimental.

Este trabajo busca aportar una visión integradora que permita avanzar desde comparaciones técnicas aisladas hacia el diseño de arquitecturas de identidad digital centradas en el usuario, alineadas con

los principios regulatorios vigentes y preparadas para una adopción progresiva en entornos reales. Las preguntas de investigación que guían el estudio se centran en identificar diferencias significativas de rendimiento entre los distintos enfoques, analizar sus capacidades relativas de minimización de datos y no-vinculabilidad, y comprender los compromisos que emergen al integrarlos en un modelo híbrido interoperable.

ESTADO DEL ARTE

La SSI propone que el titular controle sus identificadores y credenciales, eliminando correladores centrales. Dos pilares normativos del ecosistema son DID Core y el Verifiable Credentials Data Model 2.0 (VC 2.0), que estandarizan cómo expresar, firmar y verificar credenciales en un modelo emisor–titular–verificador. Junto con VC Data Integrity 1.0 (suites de firmas y pruebas) y VC-JOSE-COSE (firmas JOSE/JWS, SD-JWT y COSE), la pila VC habilita interoperabilidad criptográfica y evolución modular del formato.

Para minimizar datos, los esquemas BBS+ permiten generar proofs derivados que revelan sólo los atributos necesarios y reducen la correlación entre presentaciones. AnonCreds aporta predicados de rango (p. ej., "≥18") y un modelo de revocación con identificadores no correlables. SD-JWT (IETF) introduce divulgación selectiva basada en JWT, ampliamente compatible con infraestructuras existentes. Estas familias difieren en propiedades de privacidad, tamaño de prueba y perfiles de interoperabilidad; la selección depende del caso de uso, de los requisitos de auditoría y de la política de revocación.

En escenarios corporativos donde ya existen OAuth 2.0 y OpenID Connect, los perfiles OpenID for Verifiable Credential Issuance (OIDC4VCI) y OpenID for Verifiable Presentations (OIDC4VP) actúan como puente: describen flujos y endpoints para emitir y presentar credenciales (incluyendo el contenedor vp_token) sin abandonar la pila OIDC. Esto reduce fricción de adopción y preserva controles de sesión, consentimiento y telemetría existentes.

Los modelos ABAC y PBAC superan la rigidez de RBAC al evaluar políticas sobre atributos del sujeto–recurso–acción–contexto (tiempo, riesgo, dispositivo, ubicación), lo que es clave cuando la divulgación es selectiva y dinámica. NIST SP 800-162 define componentes y consideraciones de ABAC a escala, mientras XACML 3.0 (OASIS) proporciona el lenguaje y arquitectura (PEP/PDP/PAP/PIP) para expresar y evaluar políticas declarativas.

En procesos de verificación sensibles, el cifrado homomórfico permite computar sobre datos cifrados (p. ej., validaciones o agregaciones) sin exponer el contenido. Aunque su coste sigue siendo elevado, la estandarización industrial avanza (HomomorphicEncryption.org) y NIST documenta líneas de madurez y buenas prácticas; su combinación con VC/ZK puede mitigar filtraciones en operadores de confianza mínima.

El GDPR consagra principios de minimización y limitación de propósito (art. 5), que se alinean con los patrones de divulgación selectiva. La Regulación (UE) 2024/1183 (eIDAS 2.0) establece el marco de EUDI Wallet y refuerza salvaguardas: separación lógica de datos, control del usuario y listas de estándares e implementaciones. En conjunto, estos instrumentos guían el diseño de flujos que reduzcan la correlación entre dominios y habiliten niveles altos de garantía.

El estado del arte converge hacia arquitecturas híbridas: DID/VC + (BBS+/SD-JWT/AnonCreds) + OIDC4VCI/VP + ABAC/PBAC, con apoyo selectivo de FHE. Este ensamblaje ofrece interoperabilidad con infraestructuras OIDC, a la vez que mejora privacidad (minimización y no-vinculabilidad) sin sacrificar escalabilidad operativa.

ISSN:2992-7978

MARCO TEÓRICO

Los sistemas tradicionales de identidad digital se basan en modelos centralizados o federados, en los cuales un proveedor de identidad (IdP) gestiona, autentica y controla el acceso a los datos de los usuarios. Aunque estos enfoques han permitido interoperabilidad a gran escala, presentan importantes limitaciones relacionadas con la privacidad, la seguridad y la dependencia de terceros, generando puntos únicos de fallo y facilitando la correlación masiva de datos personales (Mühle et al., 2018; Goodell & Aste, 2019).

Desde la perspectiva regulatoria, estos modelos dificultan el cumplimiento de principios fundamentales de protección de datos como la minimización, la limitación de propósito y la proporcionalidad, establecidos en marcos normativos como el GDPR y la norma ISO/IEC 29100 (ISO/IEC, 2011).

La Identidad Auto-Soberana (Self-Sovereign Identity, SSI) surge como una alternativa que devuelve el control de la identidad al titular. Este paradigma se sustenta en el uso de Identificadores Descentralizados (DID) y Credenciales Verificables (VC), permitiendo a los usuarios gestionar, presentar y verificar atributos sin depender de un intermediario central (W3C, 2024).

El modelo SSI define un ecosistema basado en tres actores principales: emisor, titular y verificador, facilitando la portabilidad de la identidad y reduciendo la correlación entre dominios.

El estándar Verifiable Credentials Data Model 2.0 del W3C define estructuras interoperables para la emisión y verificación de credenciales digitales. Sobre este modelo se construyen distintos mecanismos criptográficos que permiten divulgación selectiva, es decir, revelar únicamente los atributos estrictamente necesarios para una verificación determinada.

Entre los principales enfoques destacan:

- VC-JWT, orientado a alto rendimiento y compatibilidad con infraestructuras OAuth/OIDC.
- BBS+, que permite generar pruebas derivadas no vinculables y maximizar la minimización de datos.
- AnonCreds, que prioriza la no-vinculabilidad entre presentaciones y soporta predicados de rango.
- SD-JWT, que introduce divulgación selectiva basada en JWT, facilitando la adopción empresarial.

Cada uno presenta diferentes compromisos entre privacidad, latencia e interoperabilidad (Schanzenbach et al., 2019; W3C, 2023).

Las pruebas de conocimiento cero (Zero-Knowledge Proofs, ZKP) permiten demostrar la validez de un atributo sin revelar su contenido. En el contexto de identidad digital, estas técnicas refuerzan la no-vinculabilidad, evitando que múltiples presentaciones puedan ser correlacionadas entre sí (Zhou et al., 2020).

Para facilitar la adopción en entornos corporativos, los perfiles OIDC4VCI y OIDC4VP actúan como puente entre SSI y los ecosistemas basados en OAuth 2.0 y OpenID Connect (Hardt, 2012; OpenID Foundation, 2024).

Asimismo, los modelos de control de acceso ABAC y PBAC permiten evaluar políticas dinámicas basadas en atributos, contexto y propósito, reforzando la gobernanza y la minimización de datos.

El GDPR y la regulación eIDAS 2.0 establecen un marco legal que promueve el control del usuario, la minimización de datos y la interoperabilidad mediante la European Digital Identity Wallet (EUDI Wallet).

Estos instrumentos influyen directamente en el diseño de arquitecturas SSI modernas y justifican la adopción de enfoques descentralizados (European Commission, 2023).

METODOLOGÍA

La presente investigación se desarrolló bajo un enfoque cuantitativo, experimental y comparativo, orientado a evaluar el desempeño y las propiedades de privacidad de distintos mecanismos de identidad digital descentralizada. El objetivo metodológico fue analizar, en un entorno controlado, los compromisos

existentes entre rendimiento, minimización de datos y no-vinculabilidad, considerando escenarios realistas de verificación de credenciales en ecosistemas interoperables.

Para ello, se diseñó una simulación computacional que permitió comparar cuatro enfoques ampliamente representativos del estado del arte en credenciales verificables: VC-JWT, BBS+ sobre VC-LD, AnonCreds y SD-JWT. Estos mecanismos fueron seleccionados por su relevancia en entornos productivos y su alineación con estándares abiertos promovidos por el W3C, la OpenID Foundation y la comunidad académica.

El experimento consistió en la generación de 300 observaciones independientes por cada método, simulando procesos de verificación de credenciales bajo condiciones homogéneas. Las latencias de verificación se modelaron mediante distribuciones normales, cuyos parámetros (media y desviación estándar) representan valores típicos observados en implementaciones reales y prototipos de referencia. Con el fin de garantizar la reproducibilidad, se utilizó una semilla pseudoaleatoria fija durante la generación de los datos.

Además del rendimiento temporal, la metodología incorporó métricas orientadas a evaluar aspectos clave de privacidad. En particular, se analizó el grado de minimización de datos alcanzado por cada mecanismo, considerando la proporción de atributos efectivamente revelados durante el proceso de verificación frente a aquellos estrictamente requeridos por la política de acceso. De manera complementaria, se estimó una métrica ilustrativa de no-vinculabilidad, enfocada en cuantificar la capacidad del sistema para evitar la correlación entre presentaciones sucesivas de credenciales por parte de un mismo titular.

Asimismo, se evaluó la escalabilidad efectiva de cada enfoque, medida como la cantidad de verificaciones que pueden realizarse por segundo bajo diferentes tamaños de población y escenarios de revocación. Esta métrica permitió analizar el impacto del crecimiento del sistema sobre el desempeño global, aspecto crítico para despliegues a gran escala como los previstos en ecosistemas de identidad europeos y corporativos.

El análisis estadístico de los resultados se llevó a cabo mediante técnicas inferenciales tanto paramétricas como no paramétricas, con el propósito de validar la significancia de las diferencias observadas entre los métodos evaluados. Inicialmente, se aplicó un ANOVA de un factor para contrastar las medias de latencia, seguido de la prueba Kruskal–Wallis para corroborar los resultados sin asumir normalidad en los datos. Posteriormente, se realizaron comparaciones pareadas utilizando la prueba U de Mann–Whitney, incorporando una corrección de Bonferroni para el control del error de tipo I y el cálculo del tamaño del efecto mediante Cliff's δ.

Finalmente, los resultados obtenidos fueron organizados en tablas y figuras comparativas que permiten una interpretación clara del compromiso existente entre rendimiento, privacidad e interoperabilidad. Este enfoque metodológico proporciona una base sólida y reproducible para evaluar arquitecturas híbridas de identidad digital descentralizada y sirve como referencia para futuras implementaciones y validaciones en entornos reales.

RESULTADOS

Los resultados obtenidos permiten analizar de forma comparativa el comportamiento de los distintos mecanismos de credenciales verificables en términos de latencia, minimización de datos, no-vinculabilidad y escalabilidad, evidenciando los compromisos existentes entre rendimiento e incremento de las garantías de privacidad.

La Figura 1 presenta la distribución de latencias de verificación para los cuatro métodos evaluados mediante diagramas de caja. En esta visualización se observa claramente que VC-JWT exhibe las menores latencias, con una mediana cercana a los 120 ms y una dispersión relativamente reducida. Este

ISSN:2992-7978

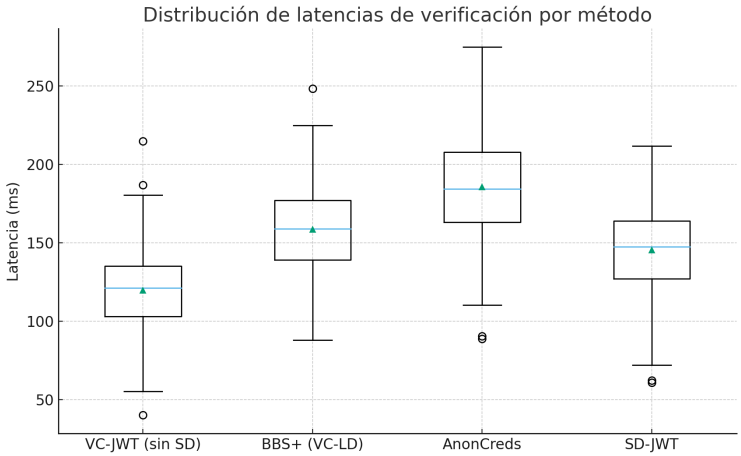
comportamiento refleja su diseño orientado a la compatibilidad directa con infraestructuras OAuth 2.0 y OpenID Connect, donde la prioridad es el rendimiento transaccional.

Por el contrario, AnonCreds presenta las latencias más elevadas, con una mediana superior a los 180 ms y una mayor variabilidad, atribuible a la complejidad criptográfica asociada a las pruebas de conocimiento cero y a los mecanismos de no-vinculabilidad incorporados. BBS+ (VC-LD) y SD-JWT se sitúan en una posición intermedia, mostrando un equilibrio entre latencia y capacidades de divulgación selectiva.

La separación visual entre las cajas confirma que las diferencias de latencia no son marginales, sino estructurales entre los enfoques evaluados.

Figura 1

Distribución de latencias de verificación por método.



La Figura 2 ilustra el Índice de Minimización de Datos (DMI) para cada método. Se aprecia que BBS+ alcanza el valor más alto de DMI, evidenciando su capacidad para revelar únicamente los atributos estrictamente necesarios mediante pruebas derivadas no vinculables. AnonCreds presenta un comportamiento similar, aunque ligeramente inferior, debido a la naturaleza de sus predicados y estructuras internas.

SD-JWT logra un nivel intermedio de minimización, destacándose como una solución pragmática que mejora sustancialmente la privacidad frente a VC-JWT tradicional, manteniendo una alta interoperabilidad. En contraste, VC-JWT sin divulgación selectiva presenta el DMI más bajo, lo que indica una mayor exposición de atributos y metadatos durante la verificación.

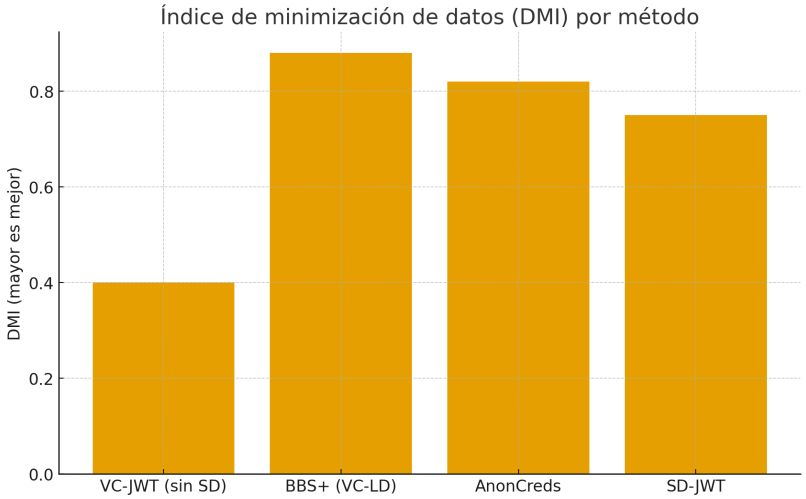
Esta figura pone de manifiesto que los mecanismos con mayor soporte criptográfico avanzado ofrecen mejores garantías de privacidad a costa de un mayor procesamiento.

AÑO 4. No. 1

ISSN:2992-7978

Figura 2

Índice de minimización de datos (DMI) por método (mayor es mejor).



La Figura 3 muestra la escalabilidad de los métodos evaluados en términos de verificaciones efectivas por segundo (EVPS) conforme aumenta el tamaño de la población. Se observa que VC-JWT mantiene el mayor throughput incluso en escenarios de alta carga, lo que lo convierte en una opción adecuada para sistemas con requisitos de alto volumen transaccional.

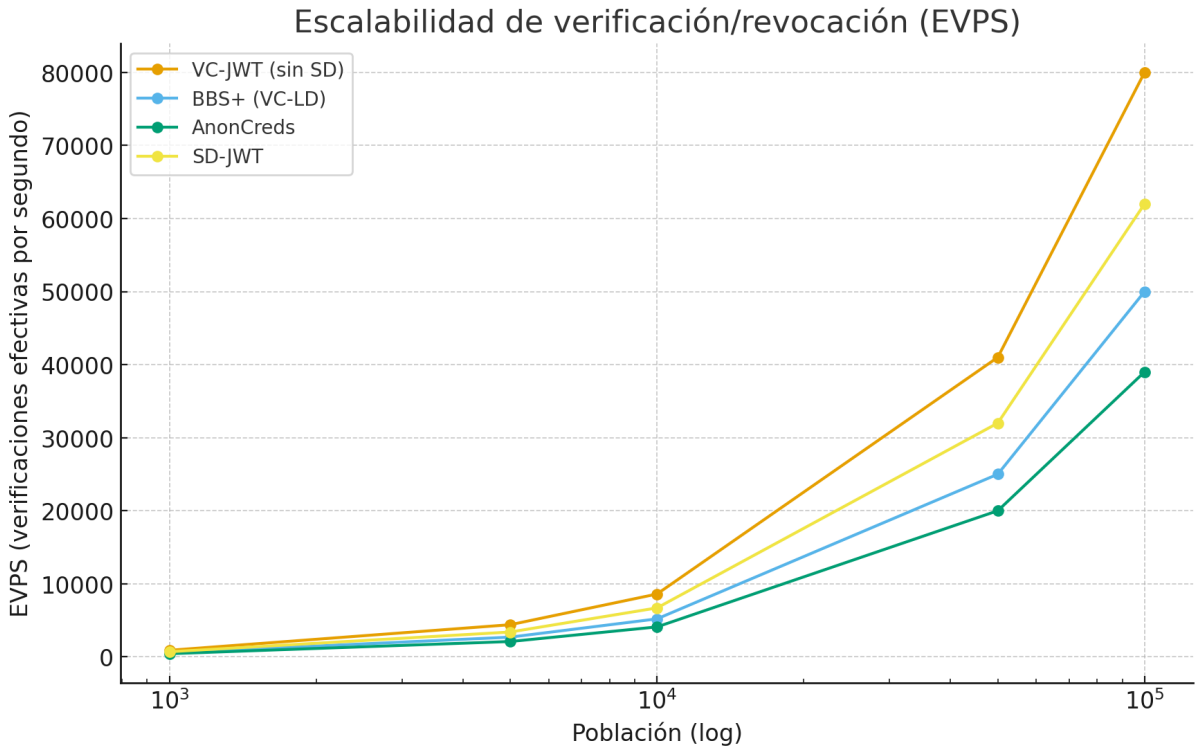
SD-JWT conserva un rendimiento competitivo, con una ligera degradación conforme aumenta la población, mientras que BBS+ y AnonCreds evidencian una reducción más pronunciada del EVPS. No obstante, esta disminución resulta esperable debido a la sobrecarga computacional asociada a las pruebas criptográficas avanzadas y a los mecanismos de protección contra correlación.

El comportamiento observado confirma que la escalabilidad debe evaluarse conjuntamente con los requisitos de privacidad y no de forma aislada.

ISSN:2992-7978

Figura 3

Escalabilidad de verificación/revocación (EVPS) en función de la población.



La Figura 4 representa la arquitectura de referencia del modelo propuesto, basada en la interacción entre emisor, titular, verificador y ledger distribuido. La imagen ilustra cómo las credenciales se emiten fuera de cadena, mientras que el blockchain se utiliza únicamente para anclajes criptográficos mínimos y mecanismos de estado o revocación.

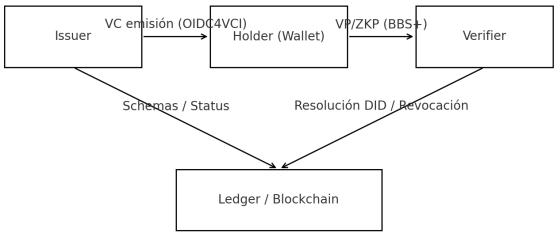
Asimismo, se evidencia la integración de flujos OIDC4VCI/VP, que permiten la interoperabilidad con infraestructuras empresariales existentes, y la aplicación de políticas ABAC/PBAC durante el proceso de verificación, reforzando la minimización de datos y el control contextual.

AÑO 4. No. 1

ISSN:2992-7978

Figura 4

Arquitectura propuesta (issuer–holder–verifier–ledger).



La Tabla 1 resume los estadísticos descriptivos de la latencia de verificación. Se confirma cuantitativamente lo observado en la Figura 1: VC-JWT presenta la menor media (119.72 ms), mientras que AnonCreds registra la mayor (185.75 ms). Los intervalos de confianza al 95 % no se superponen significativamente, lo que sugiere diferencias estadísticamente relevantes entre los métodos.

Tabla1

Descriptores de latencia (ms) por método (n=300 cada grupo)

Método	n	Media	Desv.Est.	Mediana	Q1	Q3	IC95% inf	IC95% sup
VC-JWT (sin SD)	300	119.72	24.21	121.32	103.05	135.28	116.98	122.46
BBS+ (VC-LD)	300	158.74	27.74	158.82	139.04	177.14	155.60	161.88
AnonCreds	300	185.75	34.76	184.37	162.95	207.70	181.81	189.68
SD-JWT	300	145.53	28.55	147.42	127.03	163.94	142.30	148.76

Nota. ANOVA de un factor: F=268.35, p=3.744e-133. Kruskal–Wallis: H=492.31, p=2.211e-106.

La Tabla 2 presenta las comparaciones pareadas mediante la prueba U de Mann–Whitney. Todos los contrastes resultaron estadísticamente significativos incluso tras la corrección de Bonferroni, con tamaños de efecto (Cliff's δ) cercanos a ±1, lo que indica diferencias grandes y consistentes entre los enfoques evaluados.

Tabla 2

Comparaciones pareadas (Mann–Whitney), Bonferroni y tamaño de efecto (Cliff's δ)

Grupo A	Grupo B	U	p	p (Bonferroni)	Cliff's δ
VC-JWT (sin SD)	BBS+ (VC-LD)	12727.00	0.00	0.00	-1.00
VC-JWT (sin SD)	AnonCreds	5111.00	0.00	0.00	-1.00
VC-JWT (sin SD)	SD-JWT	21472.00	0.00	0.00	-1.00
BBS+ (VC-LD)	AnonCreds	24668.00	0.00	0.00	-1.00
BBS+ (VC-LD)	SD-JWT	56057.00	0.00	0.00	1.00
AnonCreds	SD-JWT	73137.00	0.00	0.00	1.00

AÑO 4. No. 1

ISSN:2992-7978

Finalmente, la Tabla 3 sintetiza de manera cualitativa los compromisos entre privacidad, latencia e interoperabilidad. Esta tabla permite observar que no existe un enfoque universalmente óptimo, sino que la selección del mecanismo adecuado depende del contexto operativo, los requisitos regulatorios y el nivel de privacidad esperado.

Tabla 3

Síntesis comparativa de métodos

Método	Privacidad (DMI/U)	Latencia (media ms)	Interoperabilidad	Observaciones
VC-JWT (sin SD)	DMI≈0.40 (U↑)	119.72	Alta (OIDC nativo)	Rápido, baja minimización
BBS+ (VC-LD)	DMI≈0.88 (U↑)	158.74	Alta (OIDC4VCI/VP, W3C LD)	Mejor minimización/no-vinculabilidad
AnonCreds	DMI≈0.82 (U↑)	185.75	Media (Aries/Indy)	Privacidad fuerte; curva de aprendizaje
SD-JWT	DMI≈0.75 (U↑)	145.53	Alta (OIDC4VCI/VP)	Puente práctico hacia OIDC

DISCUSIÓN

Los resultados obtenidos confirman que los distintos enfoques de credenciales verificables analizados presentan compromisos estructurales entre rendimiento, privacidad e interoperabilidad, lo que impide identificar una solución universalmente óptima para todos los escenarios de uso. Más allá de las diferencias cuantitativas observadas en latencia y métricas de privacidad, los hallazgos permiten situar cada mecanismo dentro de contextos operativos específicos, donde sus características técnicas y criptográficas resultan más pertinentes en función del riesgo, el propósito y las exigencias regulatorias.

El enfoque basado en VC-JWT mostró el mejor desempeño en términos de latencia y escalabilidad, lo que lo convierte en una opción adecuada para escenarios altamente transaccionales, donde el volumen de verificaciones es elevado y la eficiencia operativa constituye un requisito prioritario. Este tipo de contextos incluye portales corporativos, servicios financieros digitales, plataformas de autenticación masiva y sistemas de acceso que ya operan sobre infraestructuras OAuth 2.0 y OpenID Connect. Sin embargo, los resultados evidencian que este enfoque presenta el menor nivel de minimización de datos, lo que implica una mayor exposición de atributos y metadatos durante el proceso de verificación. En consecuencia, su uso resulta apropiado únicamente cuando la divulgación de información es proporcional al propósito del servicio y se encuentra respaldada por controles organizacionales, contractuales y regulatorios sólidos.

En contraste, el esquema BBS+ destacó por ofrecer las mayores garantías de minimización de datos y no-vinculabilidad, alineándose de forma más estricta con los principios de privacidad por diseño y por defecto. Aunque este enfoque introduce una sobrecarga computacional moderada, los resultados sugieren que dicho costo es aceptable en escenarios donde la protección de la privacidad constituye un requisito central. Estos escenarios incluyen la emisión y verificación de credenciales ciudadanas, la validación de atributos sensibles como edad, estado legal o certificaciones profesionales, y los casos de uso asociados a billeteras de identidad digital enmarcadas en eIDAS 2.0. Desde una perspectiva ética y regulatoria, BBS+ reduce significativamente el riesgo de correlación entre dominios y fortalece el control del titular sobre su información personal.

AÑO 4. No. 1

ISSN:2992-7978

El enfoque AnonCreds presenta propiedades de privacidad comparables a BBS+, especialmente en términos de no-vinculabilidad y soporte de predicados de rango. No obstante, los resultados muestran que su latencia es superior y que su interoperabilidad con infraestructuras empresariales existentes es más limitada. Estas características sugieren que AnonCreds resulta más adecuado para ecosistemas cerrados o controlados, tales como redes académicas, proyectos piloto gubernamentales o sistemas donde los participantes comparten un marco de confianza previamente establecido. En estos contextos, la prioridad otorgada al anonimato fuerte y a la resistencia frente a la correlación justifica la mayor complejidad operativa observada.

Por su parte, SD-JWT emerge como una solución intermedia que equilibra de manera pragmática rendimiento, privacidad e interoperabilidad. Los resultados evidencian que este enfoque mejora de forma significativa la minimización de datos respecto a VC-JWT tradicional, manteniendo una latencia competitiva y una integración directa con ecosistemas OIDC. Esta combinación lo posiciona como una alternativa especialmente adecuada para organizaciones que se encuentran en procesos de transición hacia modelos de identidad descentralizada, permitiendo una adopción progresiva de divulgación selectiva sin introducir fricciones técnicas relevantes. En este sentido, SD-JWT puede interpretarse como un mecanismo puente entre los modelos de identidad centralizados y las arquitecturas SSI más avanzadas.

De manera transversal, los resultados ponen de manifiesto que la elección de un mecanismo de credenciales verificables no debe basarse únicamente en métricas técnicas aisladas, sino en una evaluación integral que considere aspectos de gobernanza, regulación y experiencia de usuario. La posibilidad de integrar flujos OIDC4VCI/VP permite diseñar arquitecturas híbridas en las que distintos enfoques coexisten y se seleccionan dinámicamente según el contexto de uso, el nivel de riesgo y los requisitos de privacidad. Asimismo, la evaluación de la escalabilidad sugiere que los mecanismos con mayores garantías criptográficas requieren estrategias complementarias, como listas de estado compactas y políticas ABAC/PBAC, para mantener niveles aceptables de desempeño en despliegues a gran escala.

Desde el punto de vista regulatorio y ético, los resultados refuerzan la conveniencia de enfoques basados en divulgación selectiva y no-vinculabilidad para facilitar el cumplimiento de principios establecidos en el GDPR y en eIDAS 2.0, tales como la minimización de datos y la limitación de propósito.

El uso de anclajes mínimos en blockchain y la verificación fuera de cadena contribuyen a reducir la huella de datos personales y a mitigar riesgos de vigilancia implícita derivados de la centralización. En conjunto, la discusión confirma que la adopción efectiva de identidad digital descentralizada no requiere una elección excluyente, sino el diseño de arquitecturas flexibles y contextuales capaces de equilibrar eficiencia operativa, privacidad y cumplimiento normativo.

CONCLUSIONES

Este trabajo demostró que la integración de identidad digital descentralizada con pruebas de conocimiento cero y políticas de control de acceso contextuales constituye un enfoque viable para equilibrar privacidad, interoperabilidad y desempeño en entornos reales. El modelo híbrido propuesto aporta una visión integradora que supera la dicotomía tradicional entre eficiencia operativa y protección de datos, al permitir la coexistencia de múltiples mecanismos de credenciales verificables dentro de una misma arquitectura.

Desde el punto de vista teórico, la investigación contribuye a clarificar el papel de la identidad auto-soberana como un paradigma capaz de materializar los principios de minimización de datos y no-vinculabilidad establecidos en los marcos normativos contemporáneos. La articulación entre DID, credenciales verificables y esquemas criptográficos avanzados evidencia que es posible diseñar sistemas de identidad alineados simultáneamente con estándares técnicos y exigencias regulatorias como el GDPR y eIDAS 2.0.

AÑO 4. No. 1

ISSN:2992-7978

En el ámbito metodológico, el trabajo propone un enfoque comparativo reproducible para evaluar mecanismos de credenciales digitales, combinando métricas de rendimiento con indicadores ilustrativos de privacidad. Esta aproximación permite analizar de forma sistemática los compromisos entre latencia, minimización de datos y escalabilidad, ofreciendo una base objetiva para la selección de tecnologías en futuros estudios y despliegues experimentales.

En términos prácticos, el modelo híbrido facilita la adopción progresiva de identidad descentralizada en organizaciones que ya operan infraestructuras basadas en OAuth 2.0 y OpenID Connect. La incorporación de perfiles OIDC4VCI/VP, junto con mecanismos de divulgación selectiva y políticas ABAC/PBAC, permite construir soluciones interoperables, escalables y adaptables a distintos contextos de riesgo y sensibilidad de la información.

Finalmente, los resultados respaldan la idea de que la identidad digital del futuro no estará sustentada en un único mecanismo criptográfico, sino en arquitecturas flexibles capaces de seleccionar dinámicamente el enfoque más adecuado según el propósito y el contexto de uso. En este sentido, el modelo propuesto constituye una referencia práctica y conceptual para el diseño de sistemas de identidad digital centrados en el usuario, orientados a la privacidad y preparados para su adopción a gran escala.

AGRADECIMIENTOS

Se expresa un especial agradecimiento a la Universidad UNADE y a la revista RIMI por la oportunidad brindada para el desarrollo de este trabajo.

REFERENCIAS

Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

European Commission. (2023). Regulation (EU) 2023/2854 – eIDAS 2.0 and the European Digital Identity Wallet. Official Journal of the European Union.

Goodell, G., & Aste, T. (2019). A decentralised digital identity architecture. arXiv. https://doi.org/10.48550/arXiv.1902.08769

Hardt, D. (2012). The OAuth 2.0 Authorization Framework (RFC 6749). IETF.

ISO/IEC. (2011). ISO/IEC 29100: Privacy framework. International Organization for Standardization.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

OpenID Foundation. (2024). OpenID for Verifiable Credentials (OIDC4VCI and OIDC4VP). Technical Report.

Reece, A., Hardman, C., & Jacob, R. (2022). Self-Sovereign Identity in a World of Authentication. arXiv. https://doi.org/10.48550/arXiv.2209.11647

Schanzenbach, M., Kilian, T., Schütte, J., & Banse, C. (2019). ZKlaims: Privacy-preserving attribute-based credentials using non-interactive zero-knowledge proofs. arXiv. https://doi.org/10.48550/arXiv.1907.09579

W3C. (2023). BBS+ Data Integrity Cryptosuite. W3C Working Draft.

Zhou, L., Diro, A., & Saini, A. (2020). Leveraging zero-knowledge proofs for blockchain-based identity sharing. Future Generation Computer Systems, 108, 827–836. https://doi.org/10.1016/j.future.2018.02.014