African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Blockchain, archivage sécurisé et protection des données dans le cloud : analyse croisée des enjeux techniques et juridiques liés à l'intégrité et à la souveraineté de l'information

Blockchain, Secure Archiving and Data Protection in the Cloud: A Cross-Analysis of the Technical and Legal Challenges Related to Information Integrity and Sovereignty.

Auteur 1 : Abir OMRI.
Auteur 2 : Kawtar AZIZ.
Auteur 3 : Soumaya AKKOUR.

Abir OMRI (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

Kawtar AZIZ (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

AKKOUR Soumaya (Professeure de l'Enseignement Supérieur)
Faculté des Sciences Juridiques et Politiques de Settat
Université Hassan 1er de Settat

Déclaration de divulgation : **L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.**

Conflit d'intérêts : **L'auteur ne signale aucun conflit d'intérêts.**

Pour citer cet article : **OMRI .A, AZIZ .K & AKKOUR .S (2025) « Blockchain, archivage sécurisé et protection des données dans le cloud : analyse croisée des enjeux techniques et juridiques liés à l'intégrité et à la souveraineté de l'information », African Scientific Journal « Volume 03, Num 33 »
Pp: 1310 – 1321.**

DOI : 10.5281/zenodo.18099525

AFRICAN SCIENTIFIC JOURNAL
MANAGEMENT AND ECONOMIC DEVELOPMENT

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Résumé

La blockchain est fréquemment présentée comme une technologie disruptive capable de transformer les mécanismes traditionnels de sécurisation, de traçabilité et d'intégrité de l'information. En parallèle, l'usage croissant du cloud computing soulève des interrogations profondes quant à la protection des données personnelles et à la souveraineté numérique. Cet article propose une analyse technique et juridique croisée de la blockchain appliquée à deux problématiques clés : l'archivage sécurisé des documents numériques et la protection des données dans les environnements cloud. L'étude examine les garanties offertes par la technologie blockchain en matière d'intégrité, de traçabilité et d'immutabilité des données, tout en confrontant ces promesses aux exigences du droit de la protection des données (notamment le RGPD). À travers une grille de lecture combinant architecture technique (registre distribué, smart contracts, chiffrement) et enjeux normatifs (responsabilité, droit à l'oubli, territorialité des données), nous discutons la capacité réelle de la blockchain à répondre aux défis actuels en matière de conformité, de sécurité et de gouvernance des informations numériques. Cette réflexion s'inscrit dans une perspective interdisciplinaire mobilisant le droit des technologies, la cybersécurité, et l'ingénierie des systèmes d'information.

Mots clés : blockchain, cloud computing, archivage électronique, protection des données, RGPD, intégrité, souveraineté numérique, analyse juridique, cybersécurité.

Abstract:

Blockchain is frequently presented as a disruptive technology capable of transforming traditional mechanisms for securing, tracing, and ensuring the integrity of information. At the same time, the growing use of cloud computing raises significant concerns regarding the protection of personal data and digital sovereignty. This article offers a combined technical and legal analysis of blockchain applied to two key issues: the secure archiving of digital documents and data protection in cloud environments. The study examines the guarantees provided by blockchain technology in terms of data integrity, traceability, and immutability, while confronting these promises with data protection law requirements (notably the GDPR). Using an analytical framework that combines technical architecture (distributed ledger, smart contracts, encryption) with normative issues (liability, right to erasure, data territoriality), we discuss the actual capacity of blockchain to address current challenges relating to compliance, security, and the governance of digital information. This reflection is grounded in an interdisciplinary perspective drawing on technology law, cybersecurity, and information systems engineering.

Keywords: blockchain, cloud computing, electronic archiving, data protection, GDPR, integrity, digital sovereignty, legal analysis, cybersecurity.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Introduction

À l'ère de la transformation numérique accélérée, les organisations publiques et privées produisent et stockent des volumes croissants de données sensibles, stratégiques ou patrimoniales. La dématérialisation des procédures, la transition vers des services numériques et l'adoption massive du cloud computing modifient profondément les modèles traditionnels de gestion documentaire, de protection des données et de gouvernance de l'information. Si le cloud offre des avantages indéniables en matière de flexibilité, de coûts et d'évolutivité, il soulève également des défis critiques liés à la confidentialité, à la localisation des données, à leur intégrité, et à leur accessibilité à long terme. La centralisation des services dans des datacenters souvent situés hors des juridictions nationales interroge non seulement la souveraineté numérique, mais aussi la conformité aux normes juridiques comme le Règlement général sur la protection des données (RGPD).

Dans ce contexte, la blockchain, technologie émergente fondée sur des registres distribués et une architecture de sécurité décentralisée, suscite un intérêt croissant. Connue initialement pour son usage dans les cryptomonnaies comme le Bitcoin, elle est aujourd'hui perçue comme une infrastructure transversale susceptible de réinventer des pans entiers de l'économie numérique, notamment dans les domaines de la traçabilité, de l'archivage électronique, de la preuve numérique, et de la protection des données. Grâce à ses propriétés d'immutabilité, de transparence contrôlée, et de résistance à la falsification, la blockchain pourrait répondre aux exigences techniques de l'archivage sécurisé et aux obligations juridiques relatives à la conservation, à la confidentialité, et à l'intégrité des données.

Toutefois, cette promesse technologique se heurte à plusieurs zones d'ombre. D'une part, les mécanismes de fonctionnement de la blockchain notamment le minage, les smart contracts, ou le consensus distribué introduisent de nouvelles complexités juridiques et techniques : quid de la responsabilité des acteurs décentralisés ? comment concilier immutabilité des registres et droit à l'oubli ? quelle compatibilité avec les principes fondamentaux du RGPD, tels que la finalité, la minimisation ou la portabilité des données ? D'autre part, l'intégration de la blockchain dans les architectures cloud pose des questions d'interopérabilité, de scalabilité, et de gouvernance multi-niveaux.

Dès lors, une analyse croisée des apports et des limites de la blockchain s'impose, en tant que technologie d'archivage sécurisé et comme levier potentiel de renforcement de la protection des données dans les environnements cloud. Cette réflexion nécessite une approche interdisciplinaire articulant les dimensions techniques (architecture distribuée, hachage cryptographique, enregistrement horodaté, etc.) et les dimensions juridiques (cadre réglementaire, obligations de conformité, souveraineté informationnelle).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

L'objectif de cet article est ainsi double :

Évaluer les apports de la blockchain dans la sécurisation, la traçabilité et l'intégrité des données numériques, notamment dans les processus d'archivage électronique certifié.

Analyser dans quelle mesure la blockchain peut contribuer à renforcer la protection des données à caractère personnel dans le cloud, en cohérence avec les exigences du droit de l'Union européenne et des cadres nationaux.

L'article s'articule en plusieurs parties : une première section présentera les fondements techniques et les promesses de la blockchain en matière de sécurisation des données ; la seconde analysera les implications juridiques de l'usage de cette technologie dans un contexte de cloud computing, à l'aune du RGPD et des jurisprudences récentes ; la dernière section proposera une discussion critique sur les conditions de mise en œuvre, les limites opérationnelles, et les recommandations pour une adoption responsable et juridiquement conforme.

1. La blockchain comme technologie d'archivage sécurisé : revue de littérature technique et juridique

L'idée d'utiliser la blockchain comme support d'archivage sécurisé a émergé dès le début des années 2010, dans le sillage de l'essor des registres distribués. Elle est fondée sur une hypothèse centrale : les propriétés d'immutabilité, de traçabilité horodatée et de résilience du réseau permettraient de répondre aux exigences croissantes en matière de conservation, d'authenticité et de sécurité des documents électroniques. Toutefois, cette hypothèse a rapidement suscité des interrogations juridiques, notamment quant à la valeur probatoire, à la responsabilité des acteurs, et à la compatibilité avec les normes existantes d'archivage légal.

1.1 Blockchain et archivage : principes et premières applications

Dans la littérature technique, plusieurs auteurs (Yaga et al., 2018 ; Zheng et al., 2017) ont mis en avant les capacités de la blockchain à fournir un registre immuable, dans lequel chaque entrée est liée cryptographiquement à la précédente. Cela garantit une intégrité forte des données enregistrées, tout en assurant une traçabilité complète des modifications ou tentatives d'altération. Ces caractéristiques ont été explorées pour des cas d'usage variés : archives notariales, certification universitaire, actes fonciers, ou logs de cybersécurité.

Des projets pilotes comme Archangel (National Archives UK, 2019) ont tenté de démontrer la faisabilité de l'archivage certifié via blockchain pour des institutions publiques, en combinant stockage hors-chaîne des documents et ancrage on-chain de leur empreinte numérique (hash). D'autres études, comme celles de Fenu et Marchesi (2018), ont expérimenté des modèles de preuve d'existence (proof of existence) fondés sur le hachage des documents archivés, sans les exposer directement dans la chaîne.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

1.2 Approches juridiques : entre promesse d'authenticité et limites réglementaires

Du côté des juristes, la blockchain a suscité un débat sur sa valeur juridique comme outil d'archivage. Pour certains auteurs (Germain, 2019 ; Pélissier, 2020), les propriétés techniques de la blockchain pourraient renforcer la fiabilité probatoire des documents numériques, en particulier en matière de non-répudiation et de preuve d'antériorité. Ces auteurs s'interrogent toutefois sur sa reconnaissance effective par les juridictions, dans un contexte où le cadre légal de l'archivage reste centré sur des notions comme le tiers de confiance ou l'archivage à valeur probante tel que défini dans le Code civil ou les normes NF Z42-013.

La CNIL (2018), dans son analyse de la blockchain, reconnaît le potentiel d'usage comme outil d'archivage mais souligne des incertitudes concernant la conformité avec les obligations du RGPD, notamment le droit à l'effacement, la limitation des finalités, et la minimisation des données. De même, l'ANSSI (2019) rappelle que la sécurité d'un système ne repose pas uniquement sur ses caractéristiques cryptographiques, mais aussi sur la maîtrise de son environnement juridique, contractuel et organisationnel.

1.3 Vers une hybridation normative et technique

La littérature contemporaine (Chauvet & Michaut, 2021 ; Debois, 2022) converge vers une approche hybride de l'archivage blockchain : les documents sont conservés dans des bases de données classiques ou sur des serveurs cloud certifiés (off-chain), tandis que leur empreinte cryptographique, leur métadonnée temporelle, ou leur preuve de validité est enregistrée dans la blockchain (on-chain). Ce modèle permettrait de concilier les exigences techniques de traçabilité avec les normes juridiques d'accessibilité, de mise à jour, et d'effacement.

Cependant, plusieurs points restent débattus :

- Quelle interopérabilité entre les systèmes de conservation réglementaire (SAE, coffre-fort numérique) et les blockchains ?
- Peut-on conférer à une blockchain le statut de système d'archivage à valeur probante ?
- Quelles conditions de gouvernance et de certification pour un usage juridiquement admissible dans le secteur public ou les contentieux ?

2. Blockchain et protection des données dans le cloud : perspectives juridiques et tensions normatives — Revue de littérature

La rencontre entre technologies distribuées (blockchain) et services externalisés (cloud computing) suscite une reconfiguration profonde des normes encadrant la protection des données à caractère personnel. Cette section propose une revue critique des travaux académiques et rapports institutionnels portant sur les interactions entre architecture décentralisée, sécurité des données, et conformité réglementaire, en particulier à l'aune du Règlement général sur la protection des données (RGPD).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

2.1 Données personnelles et blockchain : une tension conceptuelle persistante

De nombreux auteurs (Finck, 2018 ; Zyskind & Nathan, 2015) soulignent la difficulté d'appliquer les concepts juridiques traditionnels à l'univers blockchain. Le RGPD repose sur une chaîne de responsabilité centralisée : un responsable de traitement identifié, un traitement déterminé, des droits clairement définis (accès, rectification, effacement, etc.). Or, la blockchain repose sur une logique opposée : décentralisation, absence d'intermédiaire, immutabilité des données.

Finck (2019) introduit la notion de « regulatory mismatch » pour décrire cette discordance entre droit positif et innovation technologique. La qualification de données personnelles dans une blockchain publique est discutée, notamment en cas de pseudonymisation : les adresses publiques (hash) permettent-elles ou non l'identification indirecte d'une personne physique ? La CNIL (2018) considère qu'une donnée pseudonymisée sur une blockchain peut être qualifiée de donnée personnelle, rendant le RGPD applicable.

2.2 Cloud et blockchain : vers un cumul de responsabilités ?

La littérature récente (Brooks & Dierksmeier, 2021 ; Popescu & Gheorghe, 2020) met en lumière la **complexité du régime de responsabilité** dans les architectures hybrides cloud + blockchain. En pratique, les données sont souvent stockées hors chaîne (off-chain) dans des serveurs cloud, tandis que les métadonnées (hash, pointeurs, smart contracts) sont inscrites on-chain.

Cette dualité pose plusieurs problèmes :

- **Qui est le responsable de traitement ?** Le fournisseur de service cloud ? Le développeur du smart contract ? Le validateur de bloc ?
- **Quel fondement juridique pour le traitement ?** Certains auteurs évoquent une « co-responsabilité distribuée », mais son applicabilité reste floue.
- **Comment garantir l'effectivité des droits de l'utilisateur final ?** Le droit à l'effacement (art. 17 RGPD) semble difficilement compatible avec l'immutabilité des blockchains.

Des propositions doctrinales émergent : recours au chiffrement fort et à la gestion des clés privées pour rendre les données inaccessibles plutôt qu'effacées (Pulle & Höhn, 2021), ou encore stockage des données sensibles off-chain avec effacement contrôlé.

2.3 Souveraineté numérique et territorialité des traitements

Plusieurs études (De Filippi, 2016 ; Pagallo, 2020) insistent sur le fait que la blockchain, par nature transfrontalière, remet en cause les modèles traditionnels de localisation des données. Dans le cloud, la question de la juridiction compétente est déjà litigieuse ; elle est exacerbée en blockchain par l'absence de centre d'hébergement ou d'ancrage territorial.

La Cour de justice de l'Union européenne (CJUE), notamment à travers les arrêts Schrems I et II, a rappelé que tout transfert de données vers des pays tiers devait garantir un niveau de protection « essentiellement équivalent » à celui prévu par le droit européen. Or, dans un système distribué, il est quasiment impossible d'identifier la localisation exacte des données ou des nœuds.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Cela conduit plusieurs auteurs à proposer la création de blockchains souveraines, gérées par des consortiums nationaux ou régionaux, permettant une gouvernance conforme aux exigences du RGPD (Reyna et al., 2018 ; Husain et al., 2021).

3. Discussion croisée : vers une grille d'analyse intégrée droit/technologie pour l'archivage et la protection des données via blockchain

L'analyse croisée des travaux doctrinaux et techniques permet de faire émerger une grille de lecture interdisciplinaire visant à évaluer la pertinence du recours à la blockchain dans des contextes à haute exigence juridique : l'archivage électronique à valeur probante et la protection des données personnelles dans les environnements cloud. Cette section propose une synthèse structurée autour de quatre dimensions critiques : intégrité, conformité, gouvernance et efficacité opérationnelle.

3.1 Intégrité des données : une réponse technique robuste mais juridiquement encadrée

Sur le plan technique, la blockchain constitue une réponse particulièrement robuste à l'exigence d'intégrité des enregistrements, telle qu'imposée par les normes d'archivage (ex. : norme NF Z42-013, ISO 14641). Grâce à son architecture décentralisée, son horodatage distribué et sa structure de hachage cryptographique, elle rend pratiquement impossible toute altération non détectée des documents ou des métadonnées enregistrées.

Cependant, sur le plan juridique, l'intégrité probatoire ne repose pas uniquement sur la sécurité du système, mais aussi sur la capacité à garantir la traçabilité, l'authenticité de la source, et la conservation dans le temps selon des durées légales. Ainsi, un registre blockchain ne peut être reconnu comme équivalent à un système d'archivage électronique (SAE) que s'il respecte des exigences complémentaires : identifiabilité des auteurs, gouvernance contrôlée, documentation des procédures de conservation.

Synthèse : la blockchain offre un socle technologique pertinent, mais doit être combinée à des dispositifs juridiques de qualification probatoire, notamment pour son usage en matière de preuve ou de conservation à long terme.

3.2 Conformité au RGPD et droit à l'effacement : tensions et pistes de compatibilité

L'un des débats les plus vifs dans la littérature juridique concerne la compatibilité entre l'immutabilité de la blockchain et certains droits fondamentaux consacrés par le RGPD, notamment le droit à l'effacement (article 17), le droit à la rectification (article 16), et le principe de minimisation des données (article 5).

La blockchain, par définition, ne permet pas la suppression rétroactive d'un enregistrement. Or, le RGPD impose la possibilité d'effacer une donnée lorsqu'elle devient obsolète, inexacte ou non justifiée. Plusieurs solutions techniques et juridiques ont été proposées :

- L'anonymisation forte des données stockées (inaccessibilité équivalente à un effacement).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

- Le stockage off-chain des données sensibles, avec inscription dans la blockchain d'un identifiant ou d'un hash, ce qui permet de supprimer les données sources tout en maintenant l'intégrité de la preuve.
- L'intégration de smart contracts de gestion de droits (ex. : smart GDPR) qui permettent d'automatiser certaines demandes d'accès, de rectification ou de désactivation.

Mais ces solutions doivent être encadrées juridiquement : l'anonymisation doit être irréversible, l'effacement doit être documenté, et la responsabilité des différents acteurs (développeur, opérateur, hébergeur) doit être précisée dans des clauses contractuelles ou des codes de conduite reconnus.

Synthèse : la tension entre immutabilité et effacement peut être partiellement résolue par une architecture hybride et une programmation éthique des smart contracts, mais nécessite une interprétation constructive du RGPD.

3.3 Gouvernance des registres distribués : vers une régulation contextuelle

Une autre limite souvent soulignée concerne la gouvernance des blockchains, particulièrement dans les réseaux publics ou sans autorité centrale identifiable. Du point de vue juridique, toute activité de traitement de données suppose l'identification d'un responsable de traitement, ou à tout le moins d'un core group d'opérateurs exerçant une responsabilité conjointe.

La littérature récente (Finck, 2020 ; Kuner et al., 2021) propose des modèles de gouvernance multi-niveaux : dans les blockchains d'entreprise (privées ou consortium), il est possible de contractualiser les responsabilités via des SLA, des politiques de sécurité, ou des normes ISO. Dans les blockchains publiques, la régulation pourrait reposer sur des mécanismes de soft law, des certifications d'usage, ou la création de nœuds d'arbitrage éthique intégrés à l'infrastructure.

Dans le cadre du cloud, cette gouvernance distribuée pourrait également s'inscrire dans les politiques d'interopérabilité cloud/blockchain (Cloud Security Alliance, 2022) afin d'assurer une continuité juridique dans l'ensemble de la chaîne de traitement.

Synthèse : la blockchain nécessite un réexamen de la notion de responsabilité numérique, fondé sur une approche dynamique, collective et contextualisée.

3.4 Efficacité et soutenabilité : la blockchain est-elle réellement applicable aux grands volumes ?

Enfin, au-delà des principes, la question de l'applicabilité opérationnelle de la blockchain dans un contexte de cloud massif et de traitement à grande échelle reste posée. L'empreinte énergétique, les limites de scalabilité, les coûts de transaction, et la latence d'enregistrement sont souvent incompatibles avec les exigences de réactivité et de performance des infrastructures cloud modernes.

Cela a conduit à explorer des alternatives : blockchains permissionnées, architectures multicouches (layer-2), ou ancrage périodique dans la blockchain publique d'un condensé de logs produits par

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

le cloud. De plus, la blockchain pourrait jouer un rôle de registre de preuve ou de métaregistre d'audit, et non de base de données principale.

Synthèse : la blockchain ne remplace pas les infrastructures cloud, mais peut les compléter comme un outil de traçabilité, de certification ou de contrôle d'intégrité, dans une logique de complémentarité ciblée.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Conclusion

La blockchain, en tant que technologie de registre distribué, a été saluée pour sa capacité à transformer les modes de sécurisation, de certification et de traçabilité des données numériques. Lorsqu'elle est appliquée à des domaines critiques tels que l'archivage électronique à valeur probante ou la protection des données personnelles dans le cloud, elle suscite à la fois des espoirs importants et des interrogations majeures. D'un point de vue technique, ses propriétés d'immutabilité, d'horodatage décentralisé et de résistance à la falsification offrent des garanties solides en matière d'intégrité et de preuve. Toutefois, sur le plan juridique, son intégration dans les systèmes d'information soulève des tensions notables avec les normes existantes, notamment celles issues du droit européen de la protection des données, tel que le RGPD.

L'analyse menée dans cet article montre que la blockchain ne peut être appréhendée comme une technologie neutre ou juridiquement inoffensive. Bien au contraire, elle implique une reconfiguration profonde des notions classiques de responsabilité, de consentement, d'effacement ou de preuve. Les principes d'autonomie technique et de décentralisation qui sous-tendent son fonctionnement entrent parfois en conflit avec les exigences de contrôle, de finalité et de transparence imposées aux traitements de données à caractère personnel. Par exemple, l'immutabilité d'un registre blockchain semble a priori incompatible avec le droit à l'effacement, tandis que l'anonymat partiel des transactions complexifie l'identification d'un responsable de traitement clairement défini.

Face à ces tensions, plusieurs solutions techniques et juridiques émergent. L'architecture hybride, combinant stockage off-chain effaçable et ancrage on-chain sécurisé, semble aujourd'hui la plus prometteuse. De même, le recours à des smart contracts éthiquement paramétrés, le développement de blockchains permissionnées avec gouvernance contractuelle, et la mise en place de standards interopérables entre infrastructures cloud et chaînes de blocs sont autant de pistes permettant d'aligner innovation technologique et sécurité juridique. Ces mécanismes ne sauraient toutefois suffire sans un cadre réglementaire évolutif, un dialogue interdisciplinaire entre ingénieurs, juristes et autorités de contrôle, et une doctrine juridique apte à intégrer la pluralité des modèles émergents.

En définitive, la blockchain ne doit pas être considérée comme une solution de substitution aux infrastructures juridiques existantes, mais comme un outil complémentaire pouvant renforcer, sous conditions, la confiance numérique. Son intégration réussie dans les domaines de l'archivage sécurisé et de la protection des données dans le cloud dépendra de sa capacité à s'inscrire dans une gouvernance responsable, conforme aux droits fondamentaux des personnes et à la souveraineté informationnelle des États. Pour la recherche juridique, cette technologie constitue une opportunité unique de repenser les équilibres entre sécurité, innovation et régulation, dans une société où la donnée devient le socle des interactions sociales, économiques et institutionnelles.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

BIBLIOGRAPHIE

(1) Bhatia, S., & Wright, A. (2019). *Blockchain is already here. What does that mean for records management and archives?* Journal of Archival Organization, 16(1), 75–84.

(2) Abid, M. et Douari, A. (2023). Comportement et performance des banques face à l'asymétrie d'information. Revue internationale de comptabilité, finance, audit, gestion et économie , 4 (2-1 (2023)), pp-217.

(3) Bhatia, S., Douglas, E. K., & Most, M. (2020). *Blockchain and records management: Disruptive force or new approach?* Records Management Journal, 30(3), 277–286. https://doi.org/10.1108/RMJ-08-2019-0040

(4) Brokeman, L., & Dierksmeier, C. (2021). Data responsibility and blockchain in cloud environments. *Journal of Business Ethics, 170*(3), 491–506.

(5) Mustapha, A. (2024). la responsabilité sociétale des entreprises comme vecteur d'innovation en sciences de l'éducation. **مجلة القانون والأعمال الدولية , 4**(52).

(6) Chauvet, M., & Michaut, C. (2021). Blockchain et archivage numérique : quelles convergences ? *Revue du droit des technologies, 5*(2), 35–49.

(7) CNIL. (2018). *Blockchain et RGPD : quels impacts ?* Commission nationale de l'informatique et des libertés. https://www.cnil.fr

(8) De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*, (7), 1–13.

(9) Debois, T. (2022). L'archivage électronique à l'épreuve de la blockchain. *Revue générale du droit des technologies de l'information, 36*(1), 71–90.

(10) Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review, 4*(1), 17–35.

(11) Finck, M. (2019). *Blockchain Regulation and Governance in Europe*. Cambridge University Press.

(12) Fenu, G., Marchesi, L., & Pinna, A. (2018). The use of blockchain in archival certification: Towards a new trust paradigm. *Computer Law & Security Review, 34*(5), 1165–1177.

(13) Francis, A. (2018). Underscoring archival authenticity with blockchain technology. *Insights: UKSG*, 31(5), 1–6. https://doi.org/10.1629/uksg.470

(14) Germain, C. (2019). Preuve et immutabilité en droit des contrats : que peut la blockchain ? *Revue Lamy Droit civil, 167*(4), 22–27.

(15) Haque, A. B. H., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR-compliant blockchains: A systematic literature review. *arXiv*.

(16) Husain, W., Hasan, R., & Rahman, A. (2021). Towards GDPR-compliant permissioned blockchains. *Future Generation Computer Systems, 125*, 155–171. https://doi.org/10.1016/j.future.2021.06.028

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

(17) Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. (2021). The GDPR: Understanding the EU General Data Protection Regulation. *International Data Privacy Law, 11*(1), 1–20.

(18) Nguyen, T. B., Sun, K., Lee, G. M., & Guo, Y. (2019). GDPR-compliant personal data management: A blockchain-based solution. *arXiv*.

(19) Onik, F. R., et al. (2023). Olympus: a GDPR compliant blockchain system. *International Journal of Information Security*, 22(4), 1–18. https://doi.org/10.1007/s10207-023-00782-z

(20) Pagallo, U. (2020). *The Law of Smart Contracts: Technology, Philosophy and Regulation*. Springer.

(21) Park, S. O., & Belen-Saglam, R. (2022). A systematic literature review of the tension between the GDPR and public blockchain systems. *arXiv*.

(22) Pélissier, M. (2020). La valeur probatoire des registres blockchain : une révolution annoncée ? *Revue Lamy Droit de l'immatériel, 165*(6), 29–38.

(23) Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *arXiv*.

(24) Popescu, D., & Gheorghe, S. (2020). Blockchain and GDPR compliance: A synthesis of legal and technical issues. *European Journal of Law and Technology, 11*(2), 1–22.

(25) Shastri, S., Wasserman, M., & Chidambaram, V. (2019). GDPR Anti-Patterns: How design and operation of modern cloud-scale systems conflict with GDPR. *arXiv*.

(26) Spandusky, D. (2018). Decentralizing privacy: Using blockchain to protect personal data. In *IEEE Security and Privacy Workshops* (pp. 180–184). IEEE.

(27) Stanford Law Review (2024). Adaptive governance for blockchain networks. *Stanford Journal of Blockchain Law & Policy*.

(28) SAHABNA, L., Mustapha, ABID, & DOUARI, A. (2025). La communication interculturelle dans l'entrepreneuriat féminin immigré : état de la recherche et perspectives théoriques. Revue scientifique africaine , 3 (31), 307-307.

(29) Stancic, H., & Bralic, V. (2020). Digital archives relying on blockchain: Overcoming the limitations of data immutability. *Archives and Manuscripts*, 47(3), 321–340.

(30) Truong, N. B., Sun, K., & Lee, G. (2019). GDPR-compliant personal data management using blockchain. *arXiv*.

(31) Wright, R. (2022). A systematic review on blockchain-based access control systems in cloud computing. *Journal of Cloud Computing*, 13(1), 1–20. https://doi.org/10.1186/s13677-024-00697-7

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

(32) Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. NIST. https://doi.org/10.6028/NIST.IR.8202

(33) Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE.