ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

حجية الدليل الرقمي الموثقة بالبلوكشين في الإثبات الجنائي

The evidentiary value of Blockchain-Verified digital evidence chain of custody in criminal proceedings

الباحثة: الحمدوني هاجر

جامعة محمد الخامس – الرباط كلية العلوم القانونية والاقتصادية والاجتماعية - أكدال

تحت إشراف الدكتور: مولاي رشيد الإدريسي

أستاذ التعليم العالي جامعة محمد الخامس - الرباط

المستخلص

يتناول هذا المقال اشكالية توظيف تقنية البلوكشين كأداة بديلة لتوثيق سلسلة الحيازة للدليل الرقمي في مجال الاثبات الجنائي، في ظل ما تثيره آليات التوثيق التقليدية القائمة على المحاضر الورقية والسجلات المركزية من قصور على الاستجابة لمتطلبات الحفاظ على سلامة الدليل الرقمي، القابل بطبيعته للنسخ والتعديل، وضمان إمكانية تتبعه بصورة دقيقة وغير قابلة للتلاعب. واعتمدت الدراسة منهجا تحليليا لبحث مدى توافق الخصائص الأساسية للبلوكشين، والمتمثلة في اللامركزية والتوثيق الزمني وعدم القابلية للتغيير وإمكانية التتبع، مع متطلبات سلسلة الحيازة المتعلقة بالدليل الرقمي، مع الاستئناس بالتجارب المقارنة. كما تناولت الدراسة أبرز الإشكالات القانونية التي يثيرها هذا التوظيف فيما يتعلق بتوزيع المسؤولية بين الأطراف التقنية المتدخلة وبإدارة المفاتيح الخاصة كنقطة ضعف بشرية وبتنازع الاختصاص القضائي في الشبكات الرقمية العابرة للحدود، وربطت ذلك بواقع التشريع المغربي الذي وإن شهد تعديلا مهما فيما يخص تنظيم إجراءات التفتيش والحجز الرقمي، إلا أنه لا يزال يفتقر إلى إطار قانوني ينظم توثيق سلسلة الحيازة الرقمية أو يحدد القيمة الثبوتية للسجلات القائمة على البلوكشين. ويخلص المقال إلى أن اعتماد هذه التقنية يمكن أن يسهم في تعزيز موثوقية الدليل الجنائي الرقمي وحجيته الثبوتية شريطة تأطيرها ضمن نموذج تقني وقانوني يقوم على اعتماد شبكات بلوكشين مرخصة والتنصيص التشريعي الصريح على القيمة الثبوتية للسجل الموثق وآليات توزيع المسؤولية وتعزيز التكوين للأطر القضائية، بما من شأنه أن يضمن مواءمة التطور التقني مع متطلبات العدالة الجنائية.

الكلمات المفتاحية

سلسلة الحيازة الرقمية، تقنية البلوكشين، الاثبات الجنائي الرقمي، الدليل الرقمي، الحجية القانونية، آليات توزيع المسؤولية، عدم القابلية للتغيير، التوثيق الزمني للدليل الرقمي.

Abstract

This article addresses the challenge of employing blockchain technology as an alternative tool for documenting the chain of custody for digital evidence in criminal investigations. This challenge arises from the shortcomings of traditional documentation mechanisms based on centralized ledgers and paper records in meetings the requirements for preserving the integrity of digital evidence, which is inherently susceptible to copying and modification, and ensuring its accurate and tamper-prof traceability. The study adopts an analytical approach to examine the compatibility of blockchain's fundamental characteristics including decentralization, data immutability, certified timestamping, and traceability, with the requirements of the digital chain of custody for digital evidence, drawing on comparative experiences. Furthermore, the study analyzes the main legal issues raised by this technological approach, particularly regarding the distribution of responsibility among the technical stakeholders, the management of private keys as a human vulnerability and jurisdictional disputes in cross-border

digital networks. This analysis is placed in the context of the Moroccan legal framework, which despite evolution in the regulation of digital search and seizure procedures, still lacks a specific legal mechanism governing the documentation of the digital chain of custody or determining the probative value of blockchain-based records. The article concludes that the adoption of this technology could contribute to enhancing the reliability and evidentiary value of digital forensic evidence. However, if it is framed within a techno-legal model based on the adoption of licensed blockchain networks, explicit legislative stipulation of the evidentiary value of documented record, and a clear definition of the mechanisms for allocating responsibilities, in order to ensure that technological development is aligned with the requirements of criminal justice.

Keywords:

Digital chain of custody, Blockchain technology, Digital forensic evidence, Digital evidence, legal probative value, liability allocation mechanisms, immutability, Timestamping of digital evidence.

المقدمة

شهد الدليل الجنائي الرقمي تحولا نوعيا في وظيفته القانونية، فلم يعد مجرد وسيلة اثبات استثنائية مرتبطة بالجرائم المعلوماتية، بل غدا في العديد من القضايا الجنائية المعاصرة أحد أهم الأدلة التي يبنى عليها الاقتناع القضائي وتُستخلص من خلالها المسؤولية الجنائية. فقد أضحت سجلات الاتصالات الإلكترونية، ورسائل تطبيقات التراسل الفوري، وبيانات تحديد المواقع الجغرافية، ومختلف محتويات الوسائط الرقمية أهم الأدلة التي يعتمد عليها القضاء الجنائي في استجلاء الحقيقة وتحديد المسؤوليات الجنائية المترتبة عن الأفعال الإجرامية. غير أن الحجية الثبوتية لهذا النوع من الأدلة لم تعد تتوقف على مجرد وجوده أو سلامة إجراءات الحصول عليه، وإنما باتت ترتبط ارتباطا وثيقا بسلامة مساره الإجرائي والتقني منذ لحظة ضبطه إلى غاية تقديمه أمام القضاء بشكل يضمن الحفاظ على أصالته وعدم تعرضه لأي تعديل أو عبث خلال مختلف مراحل التعامل معه.

وفي هذا السياق، تبرز سلسلة الحيازة باعتبارها إحدى أهم الضمانات الإجرائية الرامية إلى المحافظة على سلامة الدليل الجنائي، من خلال توثيق مختلف مراحل جمعه وحفظه ونقله وفحصه التقني إلى غاية تقديمه أمام الجهات القضائية المختصة. والغاية من هذا التوثيق المتسلسل هي دحض أي شبهة تلاعب أو عبث أو استبدال قد تثار بشأن الدليل، وبالتالي صون حجية الدليل. غير أن الأساليب التقليدية المعتمدة في توثيق هذه السلسلة من محاضر ورقية وتوقيعات وأختام، تكشف عن قصور بنيوي حين تطبق على الدليل الرقمي تحديدا. فالملف الرقمي، بخلاف الشيء المادي، قابل للنسخ والتعديل دون ترك أثر ظاهر بالضرورة، كما أن توقيت كل عملية نقل أو معاينة له قلّما يوثق بدقة تقنية يمكن التحقق منها لاحقا بشكل مستقل، ناهيك عن أن السجل الورقي نفسه، الذي من المفترض أن يشهد على سلامة الدليل الرقمي، يبقى عرضة للتزوير أو الضياع أو التلاعب، مما يجعله أضعف من الدليل الذي يوثقه.

وفي خضم هذه التحديات، برزت تقنية البلوكشين أو "سلسلة الكتل" باعتبارها إحدى التقنيات القادرة على توفير مستوى متقدم من الموثوقية والشفافية في مجال توثيق الأدلة الرقمية، وذلك بفضل ما تتميز به من خصائص تقنية تجعلها مؤهلة للقيام بهذا الدور، وفي مقدمتها اللامركزية، والطابع الزمني الموثق للبيانات، وعدم قابلية السجلات للتغيير، وإمكانية تتبع مختلف العمليات المنجزة عليها بصورة دقيقة وشفافة.

غير أن توظيف تقنية البلوكشين في مجال توثيق سلسلة الحيازة الرقمية، وعلى ما ينطوي عليه من إمكانات مهمة لتعزيز موثوقية الدليل الجنائي الرقمي وحجيته الثبوتية، لا يخلو من إشكاليات قانونية مستحدثة تستوجب البحث والتأصيل. فمن جهة، يثار التساؤل بشأن القيمة الثبوتية للسجلات الرقمية الموثقة بهذه التقنية، ومدى انطباق نظرية المحرر الرسمي والعرفي عليها في ظل

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

غياب نصوص قانونية صريحة تحدد طبيعتها القانونية ونطاق الاعتداد بها أمام القضاء. ومن جهة أخرى، تثير الطبيعة التقنية واللامركزية لبعض تطبيقات البلوكشين جملة من الإشكاليات القانونية المرتبطة بتحديد المسؤولية القانونية للأطراف التقنية المتدخلة في تشغيل هذه الأنظمة، فضلًا عن إشكالية إدارة المفاتيح الخاصة باعتبارها إحدى أبرز نقاط الضعف البشرية التي قد تؤثر في فعالية الضمانات التقنية التي توفرها هذه التقنية. فضلا عن الإشكالات المرتبطة بتنازع الاختصاص القضائي عند اعتماد شبكات البلوكشين العابرة للحدود.

ويكتسي هذا الموضوع أهمية خاصة حين يُسقط على التشريع المغربي، إذ يكشف تفحص المنظومة القانونية المغربية عن مفارقة تستحق الوقوف عندها. فبينما تدخل المشرع المغربي عبر القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، والذي حدد النظام القانوني المطبق على المعطيات المتبادلة إلكترونيا وعلى المعادلة بين المحررات الورقية والإلكترونية، ثم عبر القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات، الذي أسس لتجريم الاعتداءات المعلوماتية، وصولا إلى الإصلاح الأخير لقانون المسطرة الجنائية بمقتضى القانون رقم 03.23، الذي نظّم بشكل تفصيلي سلطات التفتيش الرقمي وحجز المعطيات المعلوماتية في المواد 59 و101 و105، فإنه ظل صامتا تماما عن آلية توثيق سلسلة الحيازة ذاتها، أي عن الوسيلة التقنية التي تضمن تتبع الدليل الرقمي وسلامته من لحظة ضبطه إلى حين عرضه على القضاء. والأدهى من ذلك أن المشرع المغربي، حين بادر أخيرا عبر مشروع القانون رقم 42.25 المتعلق بالأصول المشفرة، إلى الاعتراف التشريعي الصريح الأول بتقنية البلوكشين، فعل ذلك بوصفها أداة مالية محضة لتنظيم الأصول المشفرة وخدمات مزوديها، دون أي إشارة لتوظيفها الممكن كأداة إجرائية وإثباتية في المجال الجنائي. وبالتالي فهذه الازدواجية بين تنظيم البلوكشين كموضوع للتقنين المالي، وإغفاله التام كأداة للتقنين الإجرائي في المادة الجنائية، تشكل فراغا تشريعيا حقيقيا يستدعي البحث والمساءلة.

وانطلاقا مما سبق، تتمحور إشكالية هذا المقال حول التساؤل إلى أي مدى يمكن لتقنية البلوكشين، بخصائصها التقنية اللامركزية وغير القابلة للتغيير، أن تشكل بديلا أو مكمّلا فعّالا لسلسلة الحيازة التقليدية في مجال الإثبات الجنائي الرقمي، وما هي الإشكاليات القانونية المستحدثة التي يطرحها هذا التوظيف، لا سيما في ظل الفراغ التشريعي الذي يطبع الموقف المغربي في هذا الخصوص؟

وتكمن أهمية هذا البحث في بعدين متكاملين، بعد نظري يتمثل في محاولة التأصيل المفاهيمي لعلاقة تقنية ناشئة مثل البلوكشين بنظريات قانونية راسخة مثل سلسلة الحيازة ونظرية الإثبات، وهو تقاطع لم يحظ بعد بمعالجة كافية في الفقه القانوني المغربي، وبعد تطبيقي يتمثل في الوقوف على واقع التشريع المغربي وتشخيص فراغه التنظيمي في هذا المجال تحديدا، بما يفتح الباب أمام صياغة مقترحات تشريعية عملية قابلة للتفعيل.

وللإجابة عن هذه الإشكالية، يعتمد المقال مقاربة تحليلية قانونية ومقارنة من خلال بحثين رئيسين، يتناول **المبحث الأول** الإطار المفاهيمي لسلسلة الحيازة الرقمية وتقنية البلوكشين، والقيمة الثبوتية للسجل الموثق بهذه التقنية في ضوء نظرية الإثبات والتجربة القضائية المقارنة، ويرصد المبحث **الثاني** الإشكاليات القانونية المستحدثة التي يطرحها هذا التوظيف، وتشخيص الموقف التشريعي المغربي وفراغه في هذا الخصوص، مع اقتراح نموذج تقني وقانوني ملائم لتفعيل هذه التقنية ضمن منظومة الإثبات الجنائي الوطنية.

المبحث الأول: الإطار المفاهيمي والقيمة الثبوتية لسلسلة الحيازة الرقمية الموثقة بالبلوكشين

يرتكز الدليل الجنائي في جوهره على مبدأ سلامة الأدلة، أي ثقة القاضي بأن الدليل المقدم هو نفسه الدليل الذي تم ضبطه، وأنه لم يغير أو يعبث به أو يزور خلال مراحل جمعه وحفظه والتعامل معه. ولترسيخ هذه الثقة، اعتمدت الأنظمة القانونية مبكرا اليات إجرائية لتنظيم نقل الأدلة وتوثيق مسارها، فيما يعرف بسلسلة الحيازة. وقد استندت هذه الاليات في المقام الأول إلى السجلات الورقية والإجراءات الإدارية التقليدية التي أثبتت فعاليتها في التعامل مع الأدلة المادية.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

إلا أن التطورات التكنولوجية وما صاحبها من انتشار للأدلة الرقمية، بخصائصها التي تختلف اختلافا جذريا عن الأدلة التقليدية، خصوصا فيما يتعلق بسهولة نسخها وإمكانية تعديلها دون ترك أثر مرئي، قد أعادت إحياء النقاش حول مدى كفاية هذه الاليات التقليدية، وأبرزت الحاجة إلى حلول تكنولوجية أكثر ملاءمة لطبيعة الأدلة الرقمية(1225).

في هذا السياق، برزت تقنية سلسلة الكتل أو البلوكشين(Blockchain(1226)) كإحدى أبرز التقنيات لتعزيز موثوقية سلسلة الحيازة، نظرا لتوافق خصائصها مبدئيا مع الشروط التي تقوم عليها هذه السلسلة. غير أن هذا التوافق يستوجب بداية تحديد مفهوم سلسلة الحيازة ووظيفتها والخصائص التقنية للبلوكشين التي تجعل منها أداة مرشحة لتعزيز هذه السلسلة (المطلب الأول)، قبل الانتقال إلى دراسة القيمة الثبوتية التي من الممكن أن يحظى بها السجل الموثق بهذه التقنية في ضوء نظرية الإثبات العامة (المطلب الأول).

المطلب الأول: ماهية سلسلة الحيازة الرقمية وخصائص تقنية البلوكشين ذات الصلة بالإثبات

يتطلب تقييم مدى ملاءمة أي تقنية لتوثيق سلسلة الحيازة فهم مفهوم السلسلة نفسها ووظيفتها القانونية. ولا يمكن تقييم فعالية أي حل تقني قبل تحديد طبيعة المشكلة التي يسعى إلى معالجتها. فبينما قد تبدو سلسلة الحيازة مجرد إجراء تنظيمي لتوثيق تداول الأدلة، إلا أنها تمثل ضمانة قانونية أساسية للحفاظ على سلامة الأدلة ومصداقيتها منذ لحظة ضبطها وحتى تقديمها أمام المحكمة(1227). وتزداد أهمية هذه الضمانة عند التعامل مع الأدلة الرقمية، نظرًا لخصائصها الفريدة التي تثير تساؤلات تتعلق بالأصالة وسلامة المحتوى. لذا، يستلزم هذا الشرط دراسة مفهوم سلسلة الحيازة ووظيفتها أولا، ثم تحديد قيود الآليات التقليدية لتوثيقها في البيئة الرقمية، قبل استعراض الخصائص التقنية لتقنية البلوكشين وقدرتها على تجاوز هذه التحديات.

الفقرة الأولى: مفهوم سلسلة الحيازة ووظيفتها الضامنة لسلامة الدليل الجنائي

تعرف سلسلة الحيازة في الأدبيات المتخصصة في الطب الشرعي الرقمي بكونها تسلسلا من الأحداث يوثق انتقال الدليل الرقمي بين الخبراء المتعاقبين على معالجته، من حيث الزمان والمكان والفاعل والسبب والكيفية في كل مرحلة من مراحل التحقيق(1228). وتمتد هذه السلسلة لتشمل جميع المتدخلين في عمليتي الجمع والتحليل، إلى جانب المعلومات السياقية كترقيم الملف والجهة التي تولت المعالجة.

وتتقاطع هذه المقاربة مع التعريف المعتمد في الأدبيات الأمنية، والذي يصف سلسلة الحيازة بكونها التوثيق المسجل لعمليات جمع الدليل الرقمي ومعالجته ونقله وتخزينه وحمايته، حفاظا على سلامته طوال مدة التحقيق(1229). أما من الناحية الإجرائية، فقد عرفها أحد الباحثين بكونها خارطة طريق تُظهر كيفية جمع الدليل وتحليله والحفاظ عليه تمهيدا لتقديمه أمام المحكمة(1230). ومن الناحية المعيارية الدولية، يبقى المرجعان الأساسيان في هذا المجال هما معيار ISO/IEC 27037:2012 الخاص بتحديد الدليل الرقمي وجمعه والحفاظ عليه، والمبادئ التوجيهية الصادرة عن المعهد الوطني الأمريكي للمعايير والتقنية (NIST)، واللذان يتفقان

(1225) علي طوالبة، "حقوق منتجي ومستخدمي الإنترنت في مواجهة الإجراءات الجنائية"، جامعة اربد الاهلية، الأردن، 2014، ص25.

(1226) Blockchain هي كلمة انجليزية، وتقابلها في اللغة العربية عبارة سلسلة الكتل، وباللغة الفرنسية Chaîne de Blocs.

(1227) محمد شاهين، "الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي"، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ط1، 2018، ص288.

(1228) N. RANA, G. SANSANWAL, K. KHATTER et S. SINGH, *"Taxonomy of Digital Forensics: Investigation Tools and Challenges", arXiv preprint*, 2017.
المتاح على الموقع: https://arxiv.org/pdf/1709.06529 تم الاطلاع عليه بتاريخ 25 يوليوز 2026 على الساعة 15:10.

(1229) *"Chain of Custody in Digital Forensics Explained", KnowledgeHut, 14 mai 2026.*
المتاح على الموقع: https://www.knowledgehut.com/blog/security/chain-of-custody-in-cyber-security
تم الاطلاع عليه بتاريخ 25 يوليوز 2026 على الساعة 15:40

(1230) *Ruan, K. (citant Vacca, J., 20*.5), in "Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics", arXiv preprint1
المتاح على الموقع: https://arxiv.org/pdf/1410.2123 تم الاطلاع عليه بتاريخ 23 ماي 2026 على الساعة 14:00

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

على أن سلسلة الحيازة الرقمية تقوم على التوثيق المتسلسل غير المنقطع لكل عملية تُجرى على الدليل، من لحظة اقتنائه إلى حين تقديمه أمام القضاء(1231).

ولهذا التوثيق وظيفة جوهرية مزدوجة تتمثل من جهة في كونها تتيح **إثبات استمرارية سلامة الدليل**، بمعنى التأكد من أن الدليل المعروض على القضاء هو نفسه الذي تم ضبطه دون تعديل أو استبدال، ومن جهة ثانية، في كونها تتيح **إثبات المساءلة**، بمعنى تحديد هوية كل من تداول الدليل بدقة، بحيث يمكن استدعاؤه للشهادة إن اقتضى الأمر. وقد عبر أحد الباحثين عن هذه الوظيفة المزدوجة بمبدأ مفاده أن كل ما لم يدون يعد بحكم ما لم يحدث، ذلك أن التوثيق الدقيق ضروري للتحقق من أن الدليل المعروض أمام المحكمة أصلي ولم يُعبث به(1232).

الفقرة الثانية: حدود الآليات التقليدية لتوثيق سلسلة الحيازة عند تطبيقها على الدليل الرقمي

يصطدم تطبيق آليات التوثيق التقليدية على الدليل الرقمي بعقبات بنيوية ترتبط بطبيعته، إذ إن هذا الأخير لا يحمل أي تشابه ملموس مع البيانات المخزنة عليه، مما يعقّد عمليات تحديده ومناولته ونقله واسترجاعه(1233). كما تزداد صعوبة إثبات الأصالة اللازمة لسلسلة الحيازة كلما كان مصدر البيانات معزولا جغرافيا أو محدود الإشراف(1234).

وتتجلى هذه الإشكالية بشكل أكثر حدة في بيئات الحوسبة السحابية، حيث لا يكتسب المحقق سيطرة مادية مباشرة على الدليل، بل يقتصر دوره على استخلاص البيانات من أي محطة متصلة بالشبكة، وهو ما يجعل الحفاظ على سلسلة الحيازة تحديا حقيقيا في ظل تعدد الاختصاصات القضائية(1235).

وقد لجأت الممارسة الفنية إلى تدارك هذا القصور جزئيا عبر توظيف تقنيات الاختزال التشفيري (Hashing)، باستخدام خوارزميتي SHA-256 وMD5 لإنتاج بصمة فريدة للدليل في كل مرحلة، تُستخدم للتحقق من عدم العبث به عبر مقارنة القيمة الحالية بالقيمة الأصلية عند التقديم أمام المحكمة(1236). غير أن هذا الحل يبقى محدودا ما دام السجل الذي يوثق حركة هذه البصمات ونقلها بين الأطراف يظل معتمدا على آليات تقليدية قابلة للتلاعب من الجهة المتحكمة فيه.

الفقرة الثالثة: الخصائص التقنية للبلوكشين ذات الصلة بالإثبات

قبل الخوض في الخصائص التقنية لتقنية البلوكشين وعلاقتها بمنطق الإثبات، من الضروري فهم طبيعة هذه التقنية نفسها، إذ يعد ذلك الأساس اللازم لفهم المبادئ التقنية التي تقوم عليها هذه الخصائص. فقد ظهرت تقنية البلوكشين(1237) في البداية

(1231) *"Digital Chain of Custody: ISO 27037 and Best Practices", TrueScreen, 15 mai 2026.*

المتاح على الموقع: https://truescreen.io/articles/digital-chain-of-custody-guide/

تم الاطلاع عليه بتاريخ 24 ماي 2026 على الساعة 12:04

(1232) *Keb Summers & Co.,"Digital Evidence Chain of Custody: Navigating New Realities", Arizona State University (SEFCOM), 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, P 13.*

المتاح على الموقع: https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf

تم الاطلاع عليه بتاريخ 18 ماي 2026 على الساعة 21:05

(1233) *"Law enforcement real time digital information chain of custody assurance system and method", U.S. Patent Documentation, USPTO.*

المتاح على الموقع: https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/10231006

تم الاطلاع عليه بتاريخ 19 ماي 2026 على الساعة 22:05

(1234) *علي محمود أحمد، «الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية، دراسة فقهية مقارنة»، جملة كلية الشريعة والقانون، جامعة الأزهر، مصر، مج2، ع32، 2020، ص11*

(1235) *"Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems", arXiv preprint.*

المتاح على الموقع: https://arxiv.org/pdf/1302.6312 تم الاطلاع عليه بتاريخ 22 ماي 2026 على الساعة 23:14

(1236) *"Digital Forensic Investigation of the ChatGPT Windows Application", arXiv preprint.*

المتاح على الموقع: https://arxiv.org/pdf/2505.23938 تم الاطلاع عليه بتاريخ 24 ماي 2026 على الساعة 00:15

(1237) *وليد حفاف، سمري بوعافية، "دور تقنية سلاسل الكتل (البلوك تشين) في إدارة سلاسل الأحداث: تجارب دول عربية"، جملة دراسات في الاقتصاد وإدارة الأعامل، مج7، ع1، 2024، ص1.*

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

كبنية تحتية تقنية للعملات المشفرة، قبل أن تتوسع تطبيقاتها تدريجيا لتشمل مجالات لا علاقة لها بالمعاملات المالية. ويعود هذا التوسع إلى خصائصها الهيكلية الفريدة، التي جعلتها محط اهتمام متزايد في مختلف المجالات، بما في ذلك الإثبات القانوني(1238). وتعرف هذه التقنية، من الناحية الاصطلاحية، بأنها سجل رقمي موزع يخزن على شكل سلسلة من "الكتل" المرتبطة زمنيا وتشفيريا، بحيث تحتوي كل كتلة على مجموعة من المعاملات أو البيانات، مرتبطة بالكتلة التي سبقتها عبر بصمة تشفيرية فريدة(1239). مما ينشئ سلسلة متصلة يصعب فكها أو التلاعب بها دون المساس بالسلسلة بأكملها. ويكمن الاختلاف الجوهري بين هذا السجل والسجلات الرقمية التقليدية في أنه لا يحفظ في موقع مركزي واحد، بل توزع نسخ متطابقة منه على عدد كبير من أجهزة الحاسوب المعروفة بالعقد المنتشرة عبر الشبكة، بحيث يخضع أي تحديث للسجل لآلية توافق جماعي بين هذه العقد قبل اعتماده وإضافته إلى السلسلة(1240).

وتقوم تقنية البلوكشين على قاعدة بيانات لا مركزية تضاف إليها البيانات فقط دون إمكانية حذفها، اعتمادا على تقنيات التشفير والشبكات الحاسوبية(1241)، وتتوفر على أربع خصائص جوهرية ذات صلة بمنطق الإثبات، وهي:

اللامركزية: توزع وظائف التحقق والتسجيل على شبكة واسعة من العقد المتساوية الحقوق، بدل تركزها في جهة واحدة(1242). وبالتالي فهي تعمل على تقليل الاعتماد على السلطة المركزية، أي لا تخضع لتحكم أو رقابة جهة مركزية، بل تظهر لكل المتعاملين، مما يعزز موثوقية الأدلة الجنائية كما تسمح طبيعتها باسترجاع البيانات التي سبقت معالجتها، مما يسمح بالتحقق منها بشكل كاف ويضمن صحتها ودقتها، وعلى الرغم من أن النظام يمكن أن يكون معقدا(1243).

الطابع الزمني الموثق: تحتوي كل كتلة على طابع زمني وبصمة تشفيرية للكتلة السابقة، بحيث يمكن التحقق بدقة من لحظة كل تسجيل دون إمكانية التلاعب به بأثر رجعي(1244).

عدم القابلية للتغيير: تطبع كل معاملة بطابع زمني وتؤمن بدالة اختزال Hash لا رجعة فيها(1245)، بحيث يغير أي تعديل طفيف في المدخلات قيمة الاختزال بالكامل، وتستدعى بيانات الكتلة السابقة عند توليد كل كتلة جديدة، مما ينتج عنه ترابط تسلسلي يجعل أي تعديل على كتلة واحدة يبطل جميع الكتل اللاحقة ويكشف التلاعب فورا(1246).

إمكانية التتبع: يتيح الترابط التسلسلي إعادة بناء التاريخ الزمني الكامل والشفاف لكل معاملة سُجلت على السلسلة(1247).

المطلب الثاني: القيمة الثبوتية للسجل الموثق بالبلوكشين في ضوء نظرية الإثبات والتجربة القضائية المقارنة

(1238) حنان كامل، «تأثير تطبيقات تقنية بلوكشين في تطوير الخدمات الحكومية الرقمية وآفاق المستقبل»، المجلة العلمية للمكتبات والوثائق والمعلومات، جامعة القاهرة - كلية الآداب، مج7، ع21، 2025، ص191.

(1239) هيثم السيد علي، «إبرام العقود الذكية عرب تقنية البلوكشين»، جملة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة السادات، مج7، ع2، ديسمبر2021، ص9.

(1240) هدى الرحيلي، وهناء الضحوي، «تطوير قطاع الإجيار العقاري بما يتماشى مع التحول الرقمي للمملكة العربية السعودية: دراسة مقترحة لتطبيق تقنية البلوك تشين»، جامعة الملك عبد العزيز، السعودية، جملة دراسات وتكنولوجيا المعلومات، مج1، ع1، 2020، ص4.

(1241) Dong, S., Abbas, K., Li, M., Kamruzzaman, J., "Blockchain technology and application: an overview", PeerJ Computer Science, 29 novembre 2023, DOI: 10.7717/peerj-cs.1705, p 4.

(1242) Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E., "Blockchain for finance: A survey. IET Blockchain", 4(2), 2024, p 106.

(1243) Cheng Li, Liang-Jie Zhang, "A Block chain Based New Secure Multi-Layer Network Model for Internet of Things," IEEEInternational Congress on Internet of Things (ICIOT), 2017, p 34, DOI: 10.1109/IEEE.ICIOT.2017.

(1244) "Blockchain Security: Cryptography, Decentralization, and Consensus", Rapid Innovation, 19 Sep 2024.

المتاح على الموقع: https://www.rapidinnovation.io/post/what-is-blockchain-security

تم الاطلاع عليه بتاريخ 5 يونيو 2026 على الساعة 20:30

(1245) سامي الصالحات، «الوقف وتقنية البلوكشن، قراءة شرعية في الاستثمار والتمويل»، مجلة كلية الشريعة والدراسات الإسلامية، جامعة قطر، مج41، ع1، 2023، ص139.

(1246) Tripathi, G., Ahad, M. A., & Casalino, G. (2023). "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decision Analytics Journal, 9, 100344, 2023, p 15

(1247) Dong, S. et al., supra, p 7.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

يتطلب تقييم القيمة الثبوتية للسجل الموثق بالبلوكشين التمييز بين الكفاءة التقنية والحجية القانونية، فمجرد امتلاك خصائص تقنية متقدمة لا يكفي لمنحه قيمة معترف بها قانونا. ويبقى الانتقال من الجدوى التقنية إلى الاعتراف القانوني رهينا بمدى استيعاب القواعد القانونية القائمة لهذا التطور، واستعداد القضاء لترسيخ آثاره العملية. لذا يستلزم هذا الأمر دراسة مدى قابلية النظريات القانونية التقليدية المنظمة للمحررات لاستيعاب السجل الموثق بالبلوكشين، قبل استعراض التجارب التشريعية والقضائية المقارنة التي تناولت هذه المسألة، وتقييم حدود حجيته والتحديات القانونية التي قد تواجهها.

الفقرة الأولى: إمكانية تطبيق نظرية المحرر الرسمي والعرفي على السجل الرقمي الموثق بالبلوكشين

يثير تكييف السجل الموثق بالبلوكشين ضمن نظرية المحرر التقليدية إشكالية حقيقية في الأنظمة القانونية التي لم تواكب تشريعيا هذا التطور التقني ومنها المغرب، كما سنبينه في المبحث الثاني. فالقانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، رغم كونه أول نص يعادل بين المحرر الورقي والمحرر الإلكتروني، لم يعرف هذا الأخير تعريفا دقيقا واكتفى بقبوله كوسيلة إثبات متى توافرت فيه شروط معينة، صيغت في الأصل بمنطق التوقيع الإلكتروني الفردي الصادر عن جهة معينة، لا بمنطق السجل الموزع جماعيا عبر شبكة لا مركزية كما هو الحال في البلوكشين.

وتزداد هذه الإشكالية تعقيدا حين يتعلق الأمر بالسجلات المبنية على شبكات بلوكشين **عمومية** لا تخضع لأي جهة إصدار رسمية، بخلاف السجلات المبنية على شبكات **خاصة أو مرخصة** التي تنشئها وتشرف عليها جهة رسمية مثل محكمة، نيابة عامة أو مختبر خبرة معتمد، الشيء الذي يكسبها طابع المحرر الرسمي أو شبه الرسمي. وهذا التمييز التقني بين البلوكشين العمومي والخاص يحمل تبعات قانونية جوهرية على مستوى القيمة الثبوتية المحتملة للسجل كما سيتم التطرق له لاحقا.

الفقرة الثانية: تقييم الأنظمة القانونية المقارنة لكفاءة البلوكشين في توثيق الدليل الرقمي

انتقل موضوع القيمة الثبوتية للسجلات الموثقة بتقنية البلوكشين من الدراسة النظرية البحتة إلى موضوع نقاش عملي في العديد من الأنظمة القانونية المقارنة بما فيها من تفسيرات قضائية وتدخلات تشريعية ومبادرات تجريبية ميدانية.

وتُعد التجربة الصينية، وتحديدًا تجربة محكمة هانغتشو للإنترنت، أبرز سابقة عالمية على مستوى التفسير القضائي. ففي حكمها الصادر في 27 يونيو 2018، أقرت هذه المحكمة بتقنية البلوكشين كوسيلة لقبول الدليل، مؤكدة أن شرط إثبات سلسلة الحيازة يظل ملزما حتى في ظل أحدث التقنيات(1248)، مستندة في ذلك إلى ما يوفره البلوكشين من تخزين موزع، ومقاومة التلاعب، وإمكانية التتبع(1249). وقد اعتمدت المحكمة لذلك معيارا وظيفيا مبنيا على ثلاث محاور متمثلة في استقلالية الجهة التي تحتفظ بالدليل، والموثوقية التقنية لعملية الالتقاط، واتساق البصمات التشفيرية المخزنة(1250). وقد تعززت هذه السابقة بتدخل تشريعي من المحكمة العليا في الصين في سبتمبر 2018، بإطلاق أول منصة قضائية وطنية تربط مكاتب التوثيق ومراكز الفحص

(1248) *Don Daugherty, "Using Blockchain in the admission of evidence M Chinese court leads the Way", Godfrey & Khan, 2019.*
المتاح على الموقع:
https://www.gklaw.com/Insights/Using-Blockchain-in-the-Admission-of-Evidence-Chinese-Court-Leads-the-Way.htm
تم الاطلاع عليه بتاريخ 01 يوليوز 2026 على الساعة 18:12

(1249) *Vivien Chan & Co., "Blockchain evidence in internet courts in China:The fast track for evidence collection for online disputes", Lexology, 2020.*
المتاح على الموقع:
https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb
تم الاطلاع عليه بتاريخ 01 يوليوز 2026 على الساعة 12:51

(1250) *Beige Media, "Blockchain Provenance and record in Chine an US".*
المتاح على الموقع:
https://www.beigemedia.org/article/blockchain-evidence-admissibility-china-us-factom-provenance
تم الاطلاع عليه بتاريخ 01 يوليوز 2026 على الساعة 19:35.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

الجنائي والمحاكم ضمن سلسلة تحالف قضائي واحدة(1251)، مع الإشارة إلى أن هذه التجربة نشأت بشكل أساسي في مجال المنازعات المدنية والتجارية وليس في الإجراءات الجنائية.

وعلى النقيض من هذا النهج التفسيري، تبنت الولايات المتحدة(1252) من خلال تشريع ولاية فيرمونت، نهجا تشريعيا صريحا. فبمقتضى المادة 1913 من الباب 12 من مدونة قوانين الولاية، عدل المشرع الفيرمونتي قواعد الإثبات لينص على أن السجل الرقمي المسجل عبر البلوكشين يعد موثقا ذاتيا، شريطة أن يكون مصحوبا بإقرار كتابي محلف صادر عن شخص مؤهل يشهد على تاريخ ووقت دخول السجل إلى السلسلة ويؤكد أنه يشكل جزءا من نشاط منتظم(1253). تكمن الأهمية المنهجية لهذا النموذج في دقته في تحديد الأثر القانوني لهذه التكنولوجيا، فهو يمنح فقط قرينة على صحة السجل شكليا، أي متى وكيف دخلت البيانات إلى النظام دون أن يمتد هذا الافتراض إلى دقة محتواه، تاركا عبء إثبات عدم الدقة على عاتق الطرف المعترض(1254)، وهو تمييز يقدم، من الناحية النظرية، معالجة متوازنة لـ"مشكلة الوسيط" التي سيتم التطرق إليها لاحقا.

وفي أوروبا، مرت فرنسا بمرحلة انتقالية تتجاذب بين الصمت التشريعي والانفتاح القضائي الحذر، إذ أقر الفقه الفرنسي لسنوات عدم وجود أي نص يحدد صراحة الأثر القانوني للبيانات المسجلة على بروتوكول تقني مثل سلسلة الكتل (البلوكشين)، تاركا تقييم قيمتها الثبوتية للسلطة التقديرية للقاضي(1255) (1256)، رغم أن هذه التقنية تستجيب جزئيا لمقتضيات لائحة الاتحاد الأوروبي رقم 2014/910 (eIDAS) بفضل ما توفره من طابع زمني وعدم قابلية التغيير التي توفرها، دون أن ترتقى إلى مستوى الطابع الزمني المؤهل الذي يحمل قرينة قانونية وذلك بسبب غياب مزود خدمة موثوق معتمد(1257)، إلا أن هذا التحفظ بدأ يشهد تحولا عمليا على نطاق محدود، ففي 20 مارس 2025، أصدرت محكمة مرسيليا القضائية حكما، يعد سابقة في القانون الفرنسي، أقرت بموجبه اعتماد الطابع الزمني المنشأ عبر بلوكشين عمومية كوسيلة إثبات في نزاع متعلق بحقوق المؤلف لتصاميم الأزياء، مكيفة إياه ليس كدليل كتابي كامل ومكتف بذاته ولكن كبداية إثبات كتابي يتطلب تأييدا بأدلة أخرى(1258) (1259)، و هو

(1251) *Library of Congress, "China: Supreme Court issues rules on internet courts, allowing for Blockchain evidence", Global Legal Monitor, 21 September 2018.*

المتاح على الموقع:

/ https://www.loc.gov/item/global-legal-monitor/2018-09-21/china-supreme-court-issues-rules-on-internet-courts-allowing-for-blockchain-evidence

تم الاطلاع عليه بتاريخ 01 يوليوز 2026 على الساعة 20:57.

(1252) *عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، دار النهضة العربية للطبع والنشر والتوزيع، مصر، 2005، ط1، ص4.*

(1253) *12 V.S.A § 1913, "Blockchain enabling", Vermont statutes annotated, Justia.*

المتاح على الموقع:https://law.justia.com/codes/vermont/2016/title-12/chapter-81/section-1913

تم الاطلاع عليه بتاريخ 02 يوليوز 2026 على الساعة 16:07

(1254) *Jason TASHEA, "Some states are allowing people and companies to use Blockchain to authenticate documents", ABA Journal, 01 September 2019.*

المتاح على الموقع:

https://www.abajournal.com/magazine/article/best-evidence

تم الاطلاع عليه بتاريخ 02 يوليوز 2026 على الساعة 16:30

(1255) *مبروك نصر الدين، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، دار الهدى، المغرب، ط2، 2010، ص4*

(1256) *Florian, "Preuve par Blockchain et force probante légale", Portail du droit, 17 Décembre 2018,*

المتاح على الموقع:https://www.droit.fr/actualite/1424-preuve-par-blockchain-et-force-probante-legale/

تم الاطلاع عليه بتاريخ 06 يوليوز 2026 على الساعة 22:30

(1257) *Florian, "Preuve par Blockchain et force probante légale", préc.*

(1258) *Murielle Cahen, "La Blockchain comme preuve : une révolution pour le droit d'auteur", Cabinet Murielle Cahen, 26 Juin 2026.*

المتاح على الموقع:

https://www.murielle-cahen.com/a/la-blockchain-comme-preuve-une-revolution-pour-le-droit-dauteur/

تم الاطلاع عليه بتاريخ 07 يوليوز 2026 على الساعة 01:30

(1259) *Tribunal judiciaire de Marseille, jugement du 20 Mars 2025, cité in:Santarelli, "Valeur probatoire Blockchain : 1ère décision du tribunal de Marseille", 24 Novembre 2026.*

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

تكييف يتقاطع مع النموذج الأمريكي في تمييزه بين الأصالة الشكلية والدقة الموضوعية، مع الإشارة إلى أن هذا الحكم صدر عن محكمة ابتدائية في نزاع مدني، وليس عن محكمة النقض أو في سياق جنائي.

فيما يخص الدول العربية، دهب اتجاه فقهي مصري إلى أن تقنية البلوكشين تتمتع بصلاحية قانونية كدليل على غرار وسائل الإثبات الأخرى، ويمكن استخدامها لإثبات الأدلة أمام المحاكم أو الهيئات الرسمية، شريطة استيفاء الشروط القانونية للكتابة والتوقيع الإلكتروني لقبولها كدليل(1260). في المقابل، أكدت دراسات خليجية متخصصة أن الدول العربية، ولا سيما دول الخليج، لا تزال في مرحلة استكشاف التطبيقات الحالية والمستقبلية لأنظمة البلوكشين، مع وجود حاجة ملحة لإجراء دراسة معمقة للجوانب القانونية ووضع أطر تنظيمية وتشريعات مناسبة قبل التوسع في اعتماد هذه الأنظمة(1261). علاوة على ذلك، أوصت دراسات قانونية إماراتية متخصصة بضرورة تطوير الخبرة القضائية في المنازعات المتعلقة بتقنية البلوك تشين داخل المحاكم ومراكز التحكيم، ووضع إجراءات واضحة لحل هذه المنازعات(1262)، وهي توصية تنطبق كذلك على السياق الجنائي قيد الدراسة.

وإلى جانب هذه النماذج التشريعية والقضائية، سجلت عدة مبادرات تطبيقية مرتبطة أساسا بالسياق الأمني، رغم كونها في المرحلة التجريبية فقط ودون سند تشريعي يمنحها حجية معترفا بها قضائيا. ففي الاتحاد الأوروبي مثلا، يستخدم مشروع LAW-GAME تقنية Hyperledger Fabric لبناء شبكات موحدة تدمج أنظمة إدارة الأدلة الرقمية(1263). وفي الولايات المتحدة، تمكن منصة Amber Authenticate كاميرات الشرطة المثبتة على أجسادهم من تسجيل بصمات تشفيرية دورية لمقاطع الفيديوعلى بلوكشين إيثيريوم، وأطلقت كذلك منصة تجارية متخصصة EvidenceTrust، تصرح بامتثالها لقواعد الإثبات الفيدرالية الأمريكية لتوثيق أدلة مسرح الجريمة بإحداثيات جغرافية وطوابع زمنية لحظة التقاطها ميدانيا(1264).

الفقرة الثالثة: عبء الإثبات وإمكانية الطعن في السجل الموثق تقنيا

تثار في مواجهة السجل الموثق بالبلوكشين مشكلة الوسيط Oracle Problem، ومفادها أن عقود السلسلة الذكية لا يمكنها الوصول مباشرة إلى بيانات خارجية، مما يجعل التحدي الجوهري كامنا في كيفية إدخال بيانات موثوقة من خارج السلسلة

المتاح على الموقع: https://www.santarelli.com/blockchain-evidential-value/

تم الاطلاع عليه بتاريخ 07 يوليوز 2026 على الساعة 11:15

(1260) جهاد محمود عبد المبدي، "مدى حجية تقنية البلوك تشين في الإثبات المدني: دراسة تحليلية"، المجلة الدولية للفقه والقضاء والتشريع، مصر، بنك المعرفة المصري، مج4، ع1، 2023، ص 86.

(1261) د. فاطمة السبيعي، "اتجاهات تطبيق تقنية البلوكشين في دول الخليج العربي"، مركز البحرين للدراسات الاستراتيجية والدولية والطاقة، يونيو 2019، ص 15.

(1262) حسام رعون، "الإطار القانوني لدولة الإمارات: دليل شامل لتنفيذ تقنية البلوكشين"، 10 شتنبر 2024.

المتاح على الموقع:

https://www.raalc.ae/ar/news/uaes-legal-landscape-a-comprehensive-guide-to-blockchain-implementation

تم الاطلاع عليه بتاريخ 12 يوليوز 2026 على الساعة 13:40

(1263) CPI OpenFox , "How Blockchain secures chain of custody in an era of AI deepfakes", CPI OpenFox, 22 Janvier 2026.

المتاح على الموقع:

https://www.openfox.com/news/how-blockchain-secures-chain-of-custody-in-an-era-of-ai-deepfakes/

تم الاطلاع عليه بتاريخ 12 يوليوز 2026 على الساعة 13:40

(1264) "Miami startup launches Blockchain platform that makes criminal evidence legally unchallengeable", Morningstar/AccessWire, 5 Mai 2026.

المتاح على الموقع:

https://www.morningstar.com/news/accesswire/1163836msn/miami-startup-launches-blockchain-platform-that-makes-criminal-evidence-legally-unchallengeable

تم الاطلاع عليه بتاريخ 14 يوليوز 2026 على الساعة 18:30

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

إليها(1265). ويختزل ذلك في مبدأ المدخلات الفاسدة تنتج مخرجات فاسدة، الشيء الذي يعني أن البلوكشين لا يوفر آلية للتحقق من صحة البيانات عند إدخالها، فقد يخزن معلومات غير دقيقة ويعرضها لاحقا وكأنها موثوقة(1266).

وقد لخصت إحدى الدراسات الأكاديمية هذه المفارقة، مؤكدة أن التحليل يكشف عن عقبات جوهرية تشمل مخاطر إدخال بيانات معيبة أو احتيالية، وتحديات التحقق من الأنظمة المرخصة، وتضارب الأنظمة عبر الحدود، وغياب بروتوكولات موحدة للفحص الجنائي(1267). كما تبقى إشكالية الأدلة خارج السلسلة قائمة، ذلك أن السجل غير القابل للتغيير يحفظ النتائج لا العمليات، بينما تتمحور المنازعات القانونية غالبا حول هذه العمليات ذاتها(1268).

إذا كان المبحث السابق قد مكن من تأسيس الإطار المفاهيمي لسلسلة الحيازة الرقمية وتقنية البلوكشين وبيان القيمة الثبوتية النسبية التي يمكن أن يحظى بها السجل الموثق بها استنادا إلى التجربة القضائية المقارنة، فإن هذا التأسيس النظري يظل غير مكتمل ما لم يقرن بتحليل الإشكاليات القانونية المستحدثة التي يطرحها التوظيف الفعلي لهذه التقنية. فمن جهة، لا يمكن التسليم بتوظيف البلوكشين في المجال الجنائي دون معالجة إشكاليات المسؤولية القانونية وتنازع الاختصاص التي تفرضها طبيعته التقنية اللامركزية والعابرة للحدود. ومن جهة أخرى، يبقى أي طرح نظري لهذا الموضوع منقوصا ما لم يسقط على واقع تشريعي ملموس، يكشف عن مفارقة دالة بين تقدم نسبي في تنظيم الحجز والتفتيش الرقمي من جهة، وفراغ تام في تأطير البلوكشين كأداة إجرائية إثباتية من جهة أخرى. وهذا بالضبط ما سيُعالجه المبحث الثاني من هذه الدراسة.

المبحث الثاني: الإشكاليات القانونية المستحدثة والموقف التشريعي المغربي

تثير التقنيات الناشئة، بغض النظر عن نضجها وفعاليتها، تحديات قانونية جديدة تفرضها طبيعة تطبيقها العملي. فإدماج تقنية ناشئة في إطار قانوني قائم لا يقتصر على إخضاعها للقواعد الحالية فحسب، بل يتطلب تقييم مدى ملاءمة المفاهيم القانونية التقليدية لاستيعاب بنية تكنولوجية لامركزية وعابرة للحدود. ورغم ما أظهرته الأنظمة القانونية من قدرة على التكيف مع التحولات التكنولوجية المتتالية، فإن هذا التكيف غالبا ما يمر بمرحلة انتقالية تتسم بالغموض وتثير العديد من التساؤلات قبل صياغة الحلول تشريعيا وقضائيا.

من هذا المنطلق، تم اسقاط هذا التصور على واقع التشريع المغربي لتقييم مدى مواكبة قواعده الإجرائية لهذا التطور الجديد، والكشف عن أوجه القصور التي لا تزال تحول دون تنظيمه بشكل صريح. لذا، سيتم دراسة الاشكالات القانونية المستحدثة الناجمة عن توظيف البلوكشين بشكل عام (المطلب الأول)، ثم تحليل موقف التشريع المغربي منها، وتحديد سبل تطوير إطارها القانوني (المطلب الثاني).

المطلب الأول: الإشكاليات القانونية المستحدثة الناجمة عن توظيف البلوكشين في سلسلة الحيازة

إذا كانت الخصائص التقنية للبلوكشين توفر ضمانات موضوعية لسلامة السجل بعد تسجيله(1269)، فإن توظيفها العملي في سياق إجرائي جنائي يفرز ثلاث إشكاليات قانونية مستحدثة تستوجب المعالجة، وتتمثل في إشكالية تحديد المسؤول القانوني عند

(1265) Tarun Kota, "Design and Evaluation of Multi-Agent AI Oracle Systems for Prediction Market Resolution", arXiv preprint. المتاح على الموقع: https://arxiv.org/pdf/2605.30802 تم الاطلاع عليه بتاريخ 6 يوليو2026 على الساعة 10:30.

(1266) G. S. RAMACHANDRAN et al., « Blockchain in Supply Chain: Opportunities and Design Considerations », in Duc A. TRAN, My T. THAI et Bhaskar KRISHNAMACHARI (dir.), Handbook on Blockchain, Springer, 2022, p. 547, DOI : 10.1007/978-3-031-07535-3_17.

(1267) Harris, M., "Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges", Legal Studies in Digital Age, Vol. 2, No. 3, 2023, p 54.

(1268) David B. HOPPE, "Can Cryptographic Certainty Still Fail the Evidentiary Test?", Gamma Law, 14 avril 2026. المتاح على الموقع: https://gammalaw.com/can-cryptographic-certainty-still-fail-the-evidentiary-test/ تم الاطلاع عليه بتاريخ 11 يوليو2026 على الساعة 08:45.

(1269) جليل الساعدي وعامر علي شاه، «حجية عقود البلوك تشين في الاثبات»، مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، العراق، مج4، ع 20، 2023، ص49.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

حدوث خلل تقني، وإشكالية نقطة الضعف البشرية الكامنة في إدارة مفاتيح الوصول للنظام، وإشكالية تنازع الاختصاص القضائي الناجمة عن الطبيعة اللامركزية والعابرة للحدود لبعض هذه الشبكات.

الفقرة الأولى: مسؤولية الأطراف التقنية

يثير اعتماد العقود الذكية لأتمتة تسجيل حركة الدليل الرقمي عبر البلوكشين، إشكالية توزيع المسؤولية القانونية بين عدة أطراف تقنية (المطورون، مشغلو منصات البلوكشين، مشغلو العقود الذكية) يصعب حصرها ضمن الأطر التقليدية للمسؤولية المدنية أو الجنائية. فمن الناحية المبدئية، يميل الفقه القانوني المقارن إلى تحميل مطور العقد الذكي المسؤولية عن الأخطاء البرمجية الكامنة في الكود ذاته، مع استثناء الحالات التي ينجم فيها الضرر عن سوء تطبيق العقد من قبل الجهة المشغلة، كإدخال معطيات خاطئة(1270). وتزداد هذه الإشكالية تعقيدا حين يتعذر تحديد الجهة المسيطرة فعليا على النظام، إذ إن العقود الذكية تعمل غالبا دون إشراف بشري مستمر بعد نشرها، مما يطرح تساؤلا جوهريا حول إمكانية مقاضاة أي طرف أصلا حين يحدث خلل(1271).

وقد رصدت دراسات قانونية متخصصة ثلاثة مستويات محتملة للمسؤولية في هذا السياق، مسؤولية المطورين على أساس نظرية الإهمال متى لم يُلتزم بمعايير العناية المعقولة، مع صعوبة إثبات ذلك في البيئات مفتوحة المصدر ومسؤولية الجهات المشغلة والناشرة للنظام، التي تعد المحور الأساسي للامتثال التنظيمي وضوابط المخاطر ومسؤولية المستخدمين والأطراف المتعاقدة، التي قد تتحمل بعض المخاطر بموجب شروط الاستخدام، مع مراعاة القيود التي تفرضها قواعد حماية المستهلك على شروط الإعفاء الواسعة من المسؤولية. وتبقى مسألة تنازع الاختصاص بين هذه الأطراف الثلاثة من أكثر المسائل التي لم تستقر بعد في قانون البلوكشين، لا سيما في الأنظمة مفتوحة المصدر القائمة على الحوكمة المجتمعية(1272).

ويزداد هذا الإشكال حدة حين يتعلق الأمر بتوثيق سلسلة حيازة دليل جنائي تحديدا، فإذا أفضى خلل برمجي في العقد الذكي المكلف بتسجيل حركة الدليل إلى تسجيل غير دقيق لتوقيت أو هوية أحد المتدخلين(1273)، فمن يتحمل مسؤولية هذا الخلل الإجرائي؟ هل هي مسؤولية الجهة القضائية التي اعتمدت النظام، أم الشركة المطورة له، أم الخبير التقني الذي أشرف على تشغيله؟ هذا التساؤل يستدعي تدخلا تشريعيا صريحا يحسم توزيع الأدوار والمسؤوليات قبل أي اعتماد رسمي لهذه التقنية في الإجراءات الجنائية كما سيتبين في المطلب الثاني.

الفقرة الثانية: نقطة الضعف البشرية وإشكالية إدارة المفاتيح الخاصة

(1270) *Kaulartz, M., Gross, J., Lichti, C., Sandner, P., "Legal Aspects of Blockchain Technology — Liability", Frankfurt School Blockchain Center, 16 décembre 2021.*

المتاح على الموقع:

https://jonasgross.medium.com/legal-aspects-of-blockchain-technology-liability-8f5b433030f

تم الاطلاع عليه بتاريخ 9 يوليو2026 على الساعة 10:40.

(1271) *American Arbitration Association, "Smart Contracts: Legal Risks and Enforceability", ADR.org, 21 mai 2026.*

المتاح على الموقع: https://www.adr.org/news-and-insights/smart-contracts-legal-risks/

تم الاطلاع عليه بتاريخ 6 يوليو2026 على الساعة 10:00.

(1272) *Suyash RAIZADA, "Legal and Compliance Considerations for Smart Contracts: Enforceability, Liability, and On-Chain Governance", Blockchain Council, 30 mai 2026.*

المتاح على الموقع:

https://www.blockchain-council.org/blockchain/legal-compliance-considerations-smart-contracts-enforceability-liability-on-chain-governance/

تم الاطلاع عليه بتاريخ 7 يوليو2026 على الساعة 10:00.

(1273) *شرف شمس الدين، «مخاطر العملات الافتراضية في نظر السياسة الجنائية»، المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة، بعنوان «العملات الافتراضية في الميزان»، الامارات، في الفترة 16-17-2019، ص2*

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

على الرغم من متانة الضمانات التشفيرية التي توفرها بنية البلوكشين، فإن النظام بأكمله يبقى رهينا بعنصر بشري يشكل حلقته الأضعف، وهو إدارة المفاتيح الخاصة التي تخول صلاحية التسجيل أو التعديل أو الوصول إلى السجل(1274). فكما تؤكد الدراسات التقنية المتخصصة، تبقى سرقة المفاتيح الخاصة السبب الجذري المهيمن على معظم حوادث فقدان الأصول الرقمية، إذ تشير إحدى الدراسات إلى أن المفاتيح الخاصة المخترقة تستأثر بما يقارب 43.8% من إجمالي الأموال المسروقة، متجاوزة بذلك ثغرات العقود الذكية وأخطاء مصادر البيانات الخارجية مجتمعة(1275). كما يمكن أن تتعرض هذه المفاتيح للاختراق نتيجة أخطاء في توليدها أو تخزينها أو استخدامها، أو نتيجة سرقتها من قبل جهات خبيثة(1276).

وينسحب هذا الخطر مباشرة على سياق سلسلة الحيازة الجنائية، فحتى لو افترضنا نظاما تقنيا موثوقا من الناحية الخوارزمية، فإن تحكم شخص واحد مثل ضابط الشرطة القضائية، موظف كتابة ضبط أو الخبير التقني بمفتاح الوصول المخول لتسجيل حركة الدليل يعيد إنتاج نفس مكمن الضعف الذي عانت منه الآليات التقليدية، أي إمكانية التلاعب من الجهة المخولة نفسها، وإن كان بصورة أكثر تعقيدا تقنيا. وقد تنبهت بعض الأنظمة القانونية المقارنة لهذا الخطر، فاعتمدت آليات المحافظ متعددة التوقيع التي تستوجب موافقة أكثر من طرف لإتمام أي عملية تسجيل أو تعديل، وهو ما ينصح به كحل تقني للحد من هذا الخطر تحديدا في السياقات ذات الحساسية العالية(1277). ويبقى السؤال القانوني الحاسم في هذا الصدد من يتحمل تبعة فقدان أو سرقة المفتاح الخاص المخول بتوثيق سلسلة الحيازة، هل هي الجهة القضائية التي أوكلت إليها هذه المهمة، أم الشخص الحائز للمفتاح شخصيا، أم الجهة المشغلة للبنية التحتية التقنية؟

الفقرة الثالثة: تنازع الاختصاص القضائي في الشبكات العابرة للحدود

تشكل الطبيعة اللامركزية لبعض شبكات البلوكشين، خصوصا الشبكات العمومية تحديا بنيويا لمفهوم الاختصاص القضائي التقليدي القائم أساسا على معيار الإقليمية. فبخلاف السجل المركزي الذي يحتفظ بنسخة أصلية وحيدة يمكن تحديد موقعها الجغرافي وإخضاعها لسلطة قضائية بعينها، تقوم بنية البلوكشين على وجود عدد لامتناه من النسخ الأصلية المتكافئة في القيمة، موزعة عبر نظام لا يخضع لأي حدود إقليمية محددة سلفا. وقد وصف البلوكشين، من هذا المنظور، بكونه التحدي الأكبر لمبدأ الإقليمية، ذلك أن العملات المشفرة القائمة عليه تعمل بشكل مستقل عن أي سيادة دولة بعينها، مما يخلق احتكاكا بنيويا بين المبادئ المؤسسة للاختصاص القضائي من جهة، والخصائص المميزة للبلوكشين من جهة أخرى(1278).

وتتجلى هذه الإشكالية عمليا على مستويين. فمن جهة، يصعب على المحقق التمييز بين الاختصاص القضائي القائم على مكان الجهاز (السيرفر) المضيف للبيانات، والاختصاص القائم على مكان إقامة المستخدم، والاختصاص القائم على مكان وقوع الضرر، وهي معايير قد تتداخل أو تتنازع في آن واحد. ومن جهة أخرى، فحتى في حال تحديد هوية طرف بعينه، يبقى تتبعه فعليا وإخضاعه لإنفاذ الحكم القضائي رهينا بتعاون قضائي دولي قد لا يكون متاحا أو سريعا بما يكفي لمقتضيات التحقيق الجنائي المستعجل. وقد

(1274) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص2.

(1275) S. KIM, S. YUN et J. JANG, "Secure User-friendly Blockchain Modular Wallet Design Using Android & OP-TEE", arXiv, 22 juin 2025.
المتاح على الموقع: https://arxiv.org/pdf/2506.17988 تم الاطلاع عليه بتاريخ 11 يوليو2026 على الساعة 11:45.

(1276) Blockchain Identity Management Systems", NIST Cybersecurity White Paper (CSWP 9), National Institute of Standards and Technology (NIST), Gaithersburg (MD), 14 janvier 2020.
المتاح على الموقع: https://arxiv.org/pdf/1908.00929 تم الاطلاع عليه بتاريخ 13 يوليو2026 على الساعة 13:45.

(1277) Safeheron Team, "What Are the Main Custody Risks in Crypto Investing", Safeheron, 24 juillet 2025.
المتاح على الموقع: https://safeheron.com/blog/main-custody-risk-crypto-investing-key-risks-protection/
تم الاطلاع عليه بتاريخ 13 يوليو2026 على الساعة 10:00.

(1278) "Cross-Border Evidence Gathering in Criminal Crypto Investigations: A Case Study of the Netherlands", Tilburg Law Review, 28 novembre 2025.
المتاح على الموقع: https://tilburglawreview.com/articles/10.5334/tilr.423
تم الاطلاع عليه بتاريخ 16 يوليو2026 على الساعة 14:45.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

أكدت دراسة قانونية متخصصة في هذا الصدد أن هذا الاحتكاك بين الإقليمية والبلوكشين لا يعني بالضرورة تنازعا حادا دائما، بل قد يتخذ في بعض الحالات طابع التعايش البديل، حيث يمكن لأكثر من جهة قضائية أن تدعي اختصاصا مشروعا على ذات المعطى الرقمي دون تناقض مطلق(1279)، وهو ما يستدعي من المشرع المغربي وضع معايير واضحة لحسم أي لبس محتمل، تحديدا حين يتعلق الأمر بمنصة بلوكشين تستضيف بيانات سلسلة حيازة دليل في قضية جنائية.

المطلب الثاني: الموقف التشريعي المغربي و آفاق التأطير القانوني

تختلف الأنظمة القانونية في سرعة استجابتها للتطورات التكنولوجية، بحسب طبيعة كل مجال ومدى إلحاحه العملي. فقد يتقدم التشريع في جانب من جوانب موضوع ما، بينما يتخلف في جانب آخر لا يقل أهمية. ولتقييم وضع التشريع المغربي في ظل هذا التباين، لا بد من دراسة النصوص القانونية القائمة في مجالات الأدلة الرقمية وعمليات التفتيش والحجز المعلوماتي، لتحديد طريقة وحدود تناولها لتقنية البلوكشين في سلسلة الحيازة. لذا، سيتم أولا استعراض الإطار التشريعي العام للإثبات الرقمي بالمغرب، تمهيدا لتقدير مدى ملاءمته لخصوصيات لهذه التقنية، ووصولا إلى استشراف الاليات التي من شأنها تعزيز انسجامه مع متطلبات هذا التطور.

الفقرة الأولى: الإطار التشريعي العام للإثبات الرقمي بالمغرب

يستند الإطار القانوني المغربي المنظم للإثبات الرقمي إلى ثلاثة نصوص أساسية متعاقبة زمنيا. فقد أرسى القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية النظام القانوني المطبق على المعطيات المتبادلة إلكترونيا، وعلى المعادلة بين المحررات الورقية والإلكترونية والتوقيع الإلكتروني(1280)، وإن ظل هذا القانون، كما بينا في المبحث الأول، صامتا عن تعريف دقيق للمحرر الإلكتروني ذاته(1281). ثم جاء القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات ليؤسس لتجريم الاعتداءات المعلوماتية(1282)، سادا بذلك فراغا تشريعيا كان قائما في المجال المعلوماتي منذ صدوره سنة 2003.

أما أحدث تدخل تشريعي في هذا المجال فيتمثل في القانون رقم 03.23 المغير والمتمم لقانون المسطرة الجنائية، الذي نظم بشكل تفصيلي ولأول مرة بهذا القدر من الدقة سلطات التفتيش الرقمي وحجز المعطيات المعلوماتية. فقد خولت المادة 59، الفقرات 8-14 لضابط الشرطة القضائية إجراء تفتيش رقمي للأجهزة المعلوماتية، وحجز البيانات والآثار الرقمية المفيدة في إظهار الحقيقة، بما فيها تلك المستعادة بعد حذفها أو فك تشفيرها، مع إمكانية إخضاعها لخبرة تقنية بإذن النيابة العام. ووسعت المادة 101 نطاق التفتيش ليشمل كل مكان يحتمل أن يحتوي على أدلة رقمية، بينما فرضت المادة 105 قيودا صارمة لحماية سرية التحقيق وخصوصية المعطيات المحجوزة(1283).

الفقرة الثانية: الفراغ التشريعي الخاص بتوظيف البلوكشين كأداة إجرائية و إثباتية

رغم هذا التقدم النسبي في تنظيم سلطات الحجز والتفتيش الرقمي، يلاحظ أن المشرع المغربي ظل صامتا تماما في القانون 03.23 كما في القانون 53.05، عن آلية توثيق سلسلة الحيازة ذاتها، أي عن الوسيلة التقنية التي تضمن تتبع الدليل الرقمي وسلامته من

(1279) *P. de Hert, C. Parlar & J. Thumfart, Legal Arguments Used in Courts Regarding Territoriality and Cross-border Production Orders: From Yahoo Belgium to Microsoft Ireland, 9 New J. Eur. Crim. L. 326, (2018), p 328.*

(1280) *الظهير الشريف رقم 1.07.129 الصادر في 19 من ذي القعدة 1428 (30 نونبر 2007) بتنفيذ القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية عدد 5584 بتاريخ 6 ديسمبر 2007.*

(1281) *" دور الكتابة والمحررات الإلكترونية في الإثبات وفق التشريع المغربي" ، مجلة مغرب القانون، 9 فبراير 2019.*

https://maroclaw.com/دور-الكتابة-و-المحررات-الإلكترونية-في/ المتاح على الموقع:

تم الاطلاع عليه بتاريخ 29 ماي 2026 على الساعة 23:00.

(1282) *الظهير الشريف رقم 1.03.197 الصادر في 16 رمضان 1424 (11 نونبر 2003) بتنفيذ القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 (22 ديسمبر 2003)، ص. 4284.*

(1283) *القانون رقم 03.23 المغير والمتمم لقانون المسطرة الجنائية، وبالخصوص المواد 59 (الفقرات 8-14)، 101، و105 المتعلقة بالتفتيش الرقمي وحجز المعطيات المعلوماتية.*

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

لحظة ضبطه إلى حين عرضه على القضاء. والمفارقة أن هذا الصمت التشريعي لا يعكس جهلا بتقنية البلوكشين ذاتها، بل إغفالا لتوظيفها الإجرائي تحديدا، ذلك أن المغرب بادر فعلا عبر مشروع القانون رقم 42.25 المتعلق بالأصول المشفرة، إلى الاعتراف التشريعي الصريح الأول بتقنية البلوكشين، الهادف إلى إرساء إطار تشريعي متكامل ينظم تداول الأصول الرقمية والتمويل اللامركزي، بتنسيق بين وزارة الاقتصاد والمالية وبنك المغرب والهيئة المغربية لسوق الرساميل(1284).

غير أن هذا المشروع ينظم البلوكشين حصريا بوصفه تمثيلا رقميا للقيمة المالية مثل العملات المشفرة وتوكنات، ويقترح إخضاع مزودي الخدمات المرتبطة به لنظام ترخيص وإشراف صارم دون أي إشارة أو تلميح لتوظيفه الممكن كأداة توثيق إجرائي في المجال الجنائي. وبذلك يتكرس، على مستوى التشريع المغربي، تمييز جوهري بين تنظيم البلوكشين كموضوع للتقنين المالي قيد الإنجاز، وإغفاله كأداة للتقنين الإجرائي، وهو تمييز يعكس، نمطا عاما في التشريعات المقارنة التي تناولت البلوكشين، إذ تظهر التجارب الخليجية المقارنة أن جل الجهود التشريعية العربية في هذا المجال تتجه أساسا نحو تنظيم البلوكشين في الخدمات المالية والمستندات الرقمية والتجارية، دون التفات يذكر لتوظيفه الإثباتي الإجرائي في المادة الجنائية(1285).

الفقرة الثالثة: نحو تأطير تشريعي ملائم

لقد أبانت دراسة الإشكالية موضوع المقال، عن أهمية التطلع لضبط الثغرة القانونية المرتبطة بسلسلة الحيازة بواسطة تقنية البلوكشين من اجل الارتقاء بالحجية الثبوتية للدليل الرقمي في الاثبات الجنائي. وفي هذا الإطار، يمكن اقتراح مجموعة من المعايير والتوصيات لسد هذه الثغرة التشريعية، أخذا بعين الاعتبار المستجدات القانونية والقضائية المفصلة في المطلب الأول.

فبالنسبة لطبيعة الشبكة، من الارجح التوجه الى اعتماد البلوكشين المرخص أو الخاص، بدلا من النموذج العمومي المفتوح، على غرار المنصة القضائية الصينية التي تربط جهات التوثيق ومراكز الفحص الجنائي والمحاكم ضمن سلسلة تحالف قضائي موحدة تحت إشراف مؤسسي واضح(1286)، وذلك تفاديا لإشكاليات تنازع الاختصاص المرتبطة بالشبكات العمومية اللامركزية بالكامل.

ومن حيث توزيع المسؤولية، يقتضي الأمر تحديدا تشريعيا صريحا للجهة المسؤولة عن أي خلل تقني يطرأ على النظام، مع تفضيل نموذج مسؤولية الجهة المشغلة، أي النيابة العامة أو مؤسسة قضائية معتمدة، باعتبارها الطرف الأقدر على ضمان الرقابة المؤسسية، دون إسقاط إمكانية الرجوع على المطور التقني في حال ثبوت خطأ برمجي صرف.

وفيما يخص إدارة المفاتيح الخاصة، ينصح باعتماد آلية التوقيع المتعدد التي تستوجب موافقة أكثر من جهة (الضابطة القضائية، النيابة العامة، الخبير التقني) لإتمام أي عملية تسجيل، حدا من مخاطر نقطة الضعف البشرية المتمثلة في تحكم شخص واحد بمفتاح الوصول(1287).

ثم هناك نقطة مهمة لا يجب إغفالها، ينبغي أن يتم الحسم تشريعيا في التكييف القانوني للسجل الموثق بالبلوكشين ضمن نظرية المحرر المغربية وفق الفصل 417 من قانون الالتزامات والعقود، بمنحه صراحة قوة ثبوتية توازي المحرر الرسمي متى استوفى شروطا تقنية ومؤسسية محددة ككون الشبكة مرخصة ومشرفا عليها من جهة قضائية معتمدة، تفاديا لأي اجتهاد قضائي متضارب قد ينشأ عن الفراغ الحالي.

(1284) *مشروع القانون رقم 42.25 المتعلق بالأصول المشفرة، الصادر عن وزارة الاقتصاد والمالية بتنسيق مع بنك المغرب والهيئة المغربية لسوق الرساميل(AMMC) ، قيد المصادقة البرلمانية.*

(1285) *د. فاطمة السبيعي، "اتجاهات تطبيق تقنية البلوكشين في دول الخليج العربي" ، مرجع سابق، ص 18*

(1286) *Guodong DU et Meng YU, "A Close Look at Hangzhou Internet Court: Inside China's Internet Courts Series -06", China Justice Observer, 3 November 2019.*

المتاح على الموقع: https://www.chinajusticeobserver.com/a/a-close-look-at-hangzhou-internet-court

تم الاطلاع عليه بتاريخ 26 ماي 2026 على الساعة 21:00.

(1287) *Safeheron Team, "What Are the Main Custody Risks in Crypto Investing", supra note 53.*

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

الخاتمة

يثير دمج التقنيات الرقمية الحديثة في مجال الاثبات الجنائي إشكالية جوهرية حول إمكانية تحقيق التوازن بين مقتضيات اليقين القانوني، باعتباره ركيزة أساسية للأمن القانوني وحسن سير العدالة، وبين الضرورات التي يفرضها التسارع غير المسبوق في التطور التكنولوجي. فإذا كانت الأدلة الجنائية تشكل الركيزة الرئيسية لإثبات الوقائع الجنائية، فإن الحفاظ على سلامتها وأصالتها وسلسلة حفظها وحيازتها، أصبح يقتضي اعتماد آليات تقنية أكثر تطوراً من أي وقت مضى. ونتيجة لذلك، برز نقاش قانوني هام حول مدى إمكانية الاعتماد على التقنيات الناشئة، ولا سيما تقنية البلوكشين، كوسيلة لتعزيز موثوقية الأدلة الجنائية، دون افتراض أن هذه التقنيات قادرة على استبدال الضمانات الإجرائية القائمة والمبادئ القانونية الراسخة. وفي هذا السياق، تتناول هذه الدراسة التفاعل بين الابتكار التكنولوجي ومتطلبات الشرعية الإجرائية في مجال الأدلة الجنائية.

في هذا السياق، تناولت هذه الدراسة التفاعل بين الابتكار التكنولوجي ومتطلبات الشرعية الإجرائية في مجال الأدلة الجنائية، واستكشفت مدى قدرة تقنية البلوكشين، بفضل بنيتها اللامركزية وسجلها غير القابل للتغيير، على تعزيز سلامة وموثوقية واستمرارية سلسلة حيازة الأدلة الرقمية، مع الحفاظ على توافقها مع المبادئ الأساسية التي تحكم الإثبات الجنائي. كما امتدت الدراسة إلى بحث الاشكالات القانونية التي يثيرها توظيف هذه التقنية، لا سيما في ظل غياب إطار تشريعي شامل ينظم الأدلة القائمة على البلوكشين في القانون المغربي، وما يترتب على ذلك من تساؤلات حول حجيتها القانونية وقبولها أمام المحاكم الجنائية، وتوافقها مع الضمانات الإجرائية المعمول بها.

من هذا المنطلق، تسهم هذه الدراسة في النقاش الأكاديمي من خلال تقييم الإمكانات القانونية والعملية لتقنية البلوكشين في تعزيز الإطار الذي ينظم الأدلة الجنائية الرقمية، مع دراسة مدى توافقها مع مبادئ الشرعية الإجرائية واليقين القانوني وحسن سير العدالة. مما سمح باستخلاص جملة من النتائج وتوصيات أهمها:

أولا: النتائج

- سلسلة الحيازة الرقمية تؤدي وظيفة مزدوجة، فهي تضمن سلامة الدليل الرقمي ومساءلة كل من تداولها،
- تعاني الاليات التقليدية من قصور في توثيق سلسلة الحيازة الرقمية عند تطبيقها على الأدلة الرقمية، نظرا لغياب التشابه الملموس بين الدليل ووسيطه المادي، وصعوبة إثبات صحته في بيئات موزعة كالحوسبة السحابية.
- تتوافق تقنية البلوكشين مع متطلبات سلسلة الحيازة وهو ما يفسر الاهتمام المتزايد بتطبيقها في هذا المجال.
- أظهرت التجارب المقارنة أن الاعتراف القضائي بتقنية البلوكشين كآلية توثيق سلسلة الحيازة الرقمية أمر ممكن عمليا، لكن لا يجب أن يكون تلقائيا ومطلقا، إذ يجب احترام شروط استقلالية الجهة التي تحتفظ بالدليل وضمان الموثوقية التقنية لعملية التسجيل واتساق التوقيعات المشفرة.
- يطرح توظيف البلوكشين في سياق إجرائي جنائي، إشكاليات قانونية مستحدثة مرتبطة بمسألة تحديد المسؤولية القانونية عن الخلل التقني وبارتباط إدارة المفاتيح الخاصة بالعنصر البشري وبالنزاعات القضائية في الشبكات العابرة للحدود التي تضع مبدأ الاختصاص الإقليمي في مواجهة مباشرة مع منطق اللامركزية التقنية.
- الموقف التشريعي المغربي يعرف مفارقة جوهرية، بين تنظيم سلطات التفتيش والحجز الرقمي من خلال القانون رقم 3.23، والتزامه الصمت حيال آلية توثيق سلسلة الحيازة نفسها.
- الاعتراف التشريعي الأول والوحيد بتقنية البلوكشين من خلال مشروع القانون رقم 42.25، اقتصر على البعد المالي دون أي اعتبار لاستخدامها المحتمل كأداة إجرائية وإثباتية في المجال الجنائي.

ثانيا: التوصيات

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

- دعوة المشرع المغربي لإضافة أحكام صريحة للقانون 03.23، تنظم آلية توثيق سلسلة الحيازة الرقمية للدليل الرقمي باستخدام وسائل تقنية موثوقة كالبلوكشين مع الحفاظ على مرونة النص في مواجهة التطور التكنولوجي المتسارع.
- حسم الطبيعة القانونية للسجل الموثق بتقنية البلوكشين في إطار نظرية المحرر المنصوص عليها في الفصل 417 من قانون الالتزامات والعقود، وذلك بمنحه صراحة قوة ثبوتية معينة متى استوفى شروطا تقنية ومؤسسية محددة ككون الشبكة مرخصة وتخضع لإشراف سلطة قضائية معتمدة، وذلك لتجنب الفراغ الذي يترك للتفسير القضائي غير المستقر.
- دعوة المشرع إلى تحديد صريح للجهة المسؤولة عن أي خلل تقني يحدث في نظام توثيق سلسلة الحيازة، مع تفضيل نموذج مسؤولية السلطة القضائية المشغلة كمبدأ عام، دون استبعاد إمكانية اللجوء إلى الجهة التقنية المطورة في حال ثبوت خطأ برمجي صرف.
- اعتماد نموذج البلوكشين المرخص، مرافقة بآليات التوقيع المتعدد لإدارة مفاتيح الوصول، وذلك للحد من مخاطر نقطة الضعف البشرية التي حددتها الدراسة.
- دعوة الجهات المعنية للاستثمار في تكوين الأطر القضائية والأمنية على الأبعاد التقنية لهذه التكنولوجيا.

المراجع

باللغة العربية

النصوص القانونية

- الظهير الشريف رقم 1.03.197 الصادر في 16 رمضان 1424 (11 نونبر 2003) بتنفيذ القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 (22 ديسمبر 2003)، ص 4284.
- الظهير الشريف رقم 1.07.129 الصادر في 19 من ذي القعدة 1428 (30 نونبر 2007) بتنفيذ القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية عدد 5584 بتاريخ 6 ديسمبر 2007.
- القانون رقم 03.23 المغير والمتمم لقانون المسطرة الجنائية، وبالخصوص المواد 59 (الفقرات 8-14)، 101، و105 المتعلقة بالتفتيش الرقمي وحجز المعطيات المعلوماتية.
- مشروع القانون رقم 42.25 المتعلق بالأصول المشفرة، الصادر عن وزارة الاقتصاد والمالية بتنسيق مع بنك المغرب والهيئة المغربية لسوق الرساميل (AMMC)، قيد المصادقة البرلمانية.

الكتب والمؤلفات

- جميل عبد الباقي الصغير، "أدلة الإثبات الجنائي والتكنولوجيا الحديثة"، دراسة مقارنة، دار النهضة العربية، القاهرة، 2021.
- محمد شاهين، "الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي"، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ط1، 2018.

المقالات

- جليل الساعدي وعامر علي شاه، "حجية عقود البلوك تشين في الاثبات"، مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، العراق، مج4، ع 20، 2023.
- جهاد محمود عبد المبدي، "مدى حجية تقنية البلوك تشين في الإثبات المدني: دراسة تحليلية"، المجلة الدولية للفقه والقضاء والتشريع، مصر، بنك المعرفة المصري، مج4، ع 1، 2023.
- حنان كامل، "تأثير تطبيقات تقنية بلوكشين في تطوير الخدمات الحكومية الرقمية وآفاق المستقبل"، المجلة العلمية للمكتبات والوثائق والمعلومات، جامعة القاهرة - كلية الآداب، مج7، ع21، 2025.
- حسام رعون، "الإطار القانوني لدولة الإمارات: دليل شامل لتنفيذ تقنية البلوكشين"، 10 شتنبر 2024.
- سامي الصالحات، "الوقف وتقنية البلوكشن، قراءة شرعية في الاستثمار والتمويل"، مجلة كلية الشريعة والدراسات الإسلامية، جامعة قطر، مج41، ع1، 2023.

- علي محمود أحمد، "الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية، دراسة فقهية مقارنة"، جملة كلية الشريعة والقانون، جامعة الأزهر، مصر، مج2، ع32، 2020.
- هدى الرحيلي، وهناء الضحوي، "تطوير قطاع الإجيار العقاري بما يتماشى مع التحول الرقمي للمملكة العربية السعودية: دراسة مقترحة لتطبيق تقنية البلوك تشين"، جامعة الملك عبد العزيز، السعودية، جملة دراسات وتكنولوجيا المعلومات، مج1، ع1، 2020.
- هيثم السيد علي، "إبرام العقود الذكية عرب تقنية البلوكشين"، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة السادات، مج7، ع2، ديسمبر2021.
- وليد حفاف، سمري بوعافية، "دور تقنية سلاسل الكتل (البلوك تشين) في إدارة سلاسل الأحداث: تجارب دول عربية"، جملة دراسات في الاقتصاد وإدارة الأعمال، مج7، ع1، 2024.

المؤتمرات

- شرف شمس الدين، "مخاطر العملات الافتراضية في نظر السياسة الجنائية"، المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة، بعنوان "العملات الافتراضية في الميزان"، الامارات، 2019.
- مبروك نصر الدين، "محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي"، دار الهدى، المغرب، ط2، 2010.
- علي طوالبة، "حقوق منتجي ومستخدمي الإنترنت في مواجهة الإجراءات الجنائية"، جامعة اربد الاهلية، الاردن، 2014.
- عمر بن يونس، "الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي"، دار النهضة العربية للطبع والنشر والتوزيع، مصر، 2005، ط1، ص4.

الدراسات

- د. فاطمة السبيعي، "اتجاهات تطبيق تقنية البلوكشين في دول الخليج العربي"، مركز البحرين للدراسات الاستراتيجية والدولية والطاقة، يونيو 2019.

المصادر الإلكترونية

- " حسام رعون، "الإطار القانوني لدولة الإمارات: دليل شامل لتنفيذ تقنية البلوكشين"، 10 شتنبر 2024.
https://www.raalc.ae/ar/news/uaes-legal-landscape-a-comprehensive-guide-to-blockchain-implementation
- دور الكتابة والمحررات الإلكترونية في الإثبات وفق التشريع المغربي"، مجلة مغرب القانون، 9 فبراير 2019.
https://maroclaw.com/دور-الكتابة-و-المحررات-الإلكترونية-في /

المراجع الأجنبية

النصوص القانونية

- *12 V.S.A § 1913, "Blockchain enabling", Vermont statutes annotated, Justia.*
https://law.justia.com/codes/vermont/2016/title-12/chapter-81/section-1913

المقالات

- *"Blockchain Security: Cryptography, Decentralization, and Consensus", Rapid Innovation, 19 Sep 2024.*
- *Don Daugherty, "Using Blockchain in the admission of evidence M Chinese court leads the Way", Godfrey & Khan, 2019.*
https://www.gklaw.com/Insights/Using-Blockchain-in-the-Admission-of-Evidence-Chinese-Court-Leads-the-Way.htm
- *Dong, S., Abbas, K., Li, M., Kamruzzaman, J., "Blockchain technology and application: an overview", PeerJ Computer Science, 29 novembre 2023.*
- *G. S. RAMACHANDRAN et al., « Blockchain in Supply Chain: Opportunities and Design Considerations », in Duc A. TRAN, My T. THAI et Bhaskar KRISHNAMACHARI (dir.), Handbook on Blockchain, Springer, 2022.*
- *Harris, M., "Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges", Legal Studies in Digital Age, Vol. 2, No. 3, 2023.*
- *Library of Congress, "China: Supreme Court issues rules on internet courts, allowing for Blockchain evidence", Global Legal Monitor, 21 September 2018.*
https://www.loc.gov/item/global-legal-monitor/2018-09-21/china-supreme-court-issues-rules-on-internet-courts-allowing-for-blockchain-evidence/

- N. RANA, G. SANSANWAL, K. KHATTER et S. SINGH, *"Taxonomy of Digital Forensics: Investigation Tools and Challenges", arXiv preprint,* 2017.
https://arxiv.org/pdf/1709.06529
- *P. de Hert, C. Parlar & J. Thumfart, Legal Arguments Used in Courts Regarding Territoriality and Cross-border Production Orders: From Yahoo Belgium to Microsoft Ireland, 9 New J. Eur. Crim. L. 326, (2018).*
- *Ruan, K. (citant Vacca, J., 2005), in "Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics", arXiv preprint.*
https://arxiv.org/pdf/1410.2123
- *S. KIM, S. YUN et J. JANG, "Secure User-friendly Blockchain Modular Wallet Design Using Android & OP-TEE", arXiv, 22 juin 2025.*
https://arxiv.org/pdf/2506.17988
- *Tarun Kota, "Design and Evaluation of Multi-Agent AI Oracle Systems for Prediction Market Resolution", arXiv preprint.*
https://arxiv.org/pdf/2605.30802
- *Tripathi, G., Ahad, M. A., & Casalino, G. (2023). "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges". Decision Analytics Journal, 9, 100344, 2023.*
- *Vivien Chan & Co., "Blockchain evidence in internet courts in China:The fast track for evidence collection for online disputes", Lexology, 2020.*
https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb
- *Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E., "Blockchain for finance: A survey. IET Blockchain", 4(2), 2024.*

المؤتمرات

- *Keb Summers & Co.,"Digital Evidence Chain of Custody: Navigating New Realities", Arizona State University (SEFCOM), 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications.*
https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf

الدراسات

- *Blockchain Identity Management Systems", NIST Cybersecurity White Paper (CSWP 9), National Institute of Standards and Technology (NIST), Gaithersburg (MD), 14 janvier 2020.*

المصادر الإلكترونية

- *American Arbitration Association, "Smart Contracts: Legal Risks and Enforceability", ADR.org, 21 Mai 2026.*
https://www.adr.org/news-and-insights/smart-contracts-legal-risks/
- *Beige Media, "Blockchain Provenance and record in Chine an US".*
https://www.beigemedia.org/article/blockchain-evidence-admissibility-china-us-factom-provenance
- *"Chain of Custody in Digital Forensics Explained", KnowledgeHut, 14 mai 2026.*
https://www.knowledgehut.com/blog/security/chain-of-custody-in-cyber-security
- *Cheng Li, Liang-Jie Zhang, "A Block chain Based New Secure Multi-Layer Network Model for Internet of Things," IEEEInternational Congress on Internet of Things (ICIOT), 2017, p 34, DOI: 10.1109/IEEE.ICIOT.2017.*
https://www.rapidinnovation.io/post/what-is-blockchain-security
- *"Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems", arXiv preprint.*
https://arxiv.org/pdf/1302.6312
- CPI OpenFox , *"How Blockchain secures chain of custody in an era of AI deepfakes", CPI OpenFox, 22 Janvier 2026.*
https://www.openfox.com/news/how-blockchain-secures-chain-of-custody-in-an-era-of-ai-deepfakes/
- *"Cross-Border Evidence Gathering in Criminal Crypto Investigations: A Case Study of the Netherlands", Tilburg Law Review, 28 novembre 2025.*
https://tilburglawreview.com/articles/10.5334/tilr.423
- *David B. HOPPE, "Can Cryptographic Certainty Still Fail the Evidentiary Test?",* Gamma Law, *2026.*
https://gammalaw.com/can-cryptographic-certainty-still-fail-the-evidentiary-test/
- *"Digital Chain of Custody: ISO 27037 and Best Practices", TrueScreen, 15 mai 2026.*

https://truescreen.io/articles/digital-chain-of-custody-guide/

- *"Digital Forensic Investigation of the ChatGPT Windows Application", arXiv preprint.*
https://arxiv.org/pdf/2505.23938
- *Florian,"Preuve par Blockchain et force probante légale", Portail du droit, 17 Décembre 2018,*
https://www.droit.fr/actualite/1424-preuve-par-blockchain-et-force-probante-legale/
- *Guodong DU et Meng YU, "A Close Look at Hangzhou Internet Court: Inside China's Internet Courts Series -06", China Justice Observer, 3 November 2019.*
https://www.chinajusticeobserver.com/a/a-close-look-at-hangzhou-internet-court
- *Jason TASHEA, "Some states are allowing people and companies to use Blockchain to authenticate documents", ABA Journal, 01 September 2019.*
https://www.abajournal.com/magazine/article/best-evidence
- *Kaulartz, M., Gross, J., Lichti, C., Sandner, P., "Legal Aspects of Blockchain Technology — Liability", Frankfurt School Blockchain Center, 16 décembre 2021.*
https://jonasgross.medium.com/legal-aspects-of-blockchain-technology-liability-8f5b433030f
- *"Law enforcement real time digital information chain of custody assurance system and method", U.S. Patent Documentation, USPTO.*
https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/10231006
- *"Miami startup launches Blockchain platform that makes criminal evidence legally unchallengeable", Morningstar/AccessWire, 5 Mai 2026.*
https://www.morningstar.com/news/accesswire/1163836msn/miami-startup-launches-blockchain-platform-that-makes-criminal-evidence-legally-unchallengeable
- *Murielle Cahen, "La Blockchain comme preuve : une révolution pour le droit d'auteur", Cabinet Murielle Cahen, 26 Juin 2026.*
https://www.murielle-cahen.com/a/la-blockchain-comme-preuve-une-revolution-pour-le-droit-dauteur/
- *Safeheron Team, "What Are the Main Custody Risks in Crypto Investing", Safeheron, 24 Juillet 2025.*
https://safeheron.com/blog/main-custody-risk-crypto-investing-key-risks-protection/
- *Suyash RAIZADA, "Legal and Compliance Considerations for Smart Contracts: Enforceability, Liability, and On-Chain Governance", Blockchain Council, 30 mai 2026.*
https://www.blockchain-council.org/blockchain/legal-compliance-considerations-smart-contracts-enforceability-liability-on-chain-governance/
- *Tribunal judiciaire de Marseille, jugement du 20 Mars 2025, cité in:Santarelli, "Valeur probatoire Blockchain : 1ère décision du tribunal de Marseille", 24 Novembre 2026.*
https://www.santarelli.com/blockchain-evidential-value/