

L'enquête préliminaire dans l'univers de la blockchain en droit pénal béninois

The Preliminary Investigation in the Blockchain Environment under Beninese Criminal Law

Moktar ADAMOU,

Professeur agrégé de droit privé et sciences criminelles

Doyen de la Faculté de droit et science politique,

Université de Parakou – République du Bénin

Vice-président du Comité International des Pénalistes Francophones (CIPF)

Sêvi Rodolphe ADJAÏGBE,

Docteur en droit privé et sciences criminelles

Enseignant chercheur

Chargé des Partenariats, de Cyberdiplomatie et des Affaires juridiques au Centre national
d'investigations numériques (CNIN)

Membre du bureau du Comité de la Convention sur la Cybercriminalité (T-CY)

Bio Edouard GABA Y. SEKE,

Doctorant en droit privé et sciences criminelles

Faculté de droit et science politique

Université de Parakou – République du Bénin

Ecole doctorale de sciences juridiques, politiques et administratives

Date de soumission : 14/07/2026

Date d'acceptation : 04/09/2026

Digital Object Identifier (DOI) : www.doi.org/10.5281/zenodo.22645230

Résumé

L'essor de la technologie blockchain bouleverse les paradigmes traditionnels de la procédure pénale, notamment l'enquête préliminaire, pierre angulaire de la recherche de la vérité judiciaire. L'anonymat, la décentralisation et la traçabilité des transactions numériques complexifient l'identification des auteurs d'infractions et la collecte des preuves électroniques. Cet article examine les enjeux juridiques et techniques de l'enquête préliminaire dans un environnement blockchain, en insistant sur les défis liés à la compétence territoriale, à la coopération internationale et à la formation des acteurs judiciaires. À travers une approche analytique et comparative, il met en lumière la nécessité d'adapter les instruments juridiques béninois et internationaux aux exigences de la criminalité numérique fondée sur la blockchain.

Mots clés :

Enquête préliminaire - Blockchain - Droit pénal – Cybercriminalité – Cryptoactifs

Abstract

The rise of blockchain technology disrupts traditional criminal procedure paradigms, particularly the preliminary investigation, which remains essential to uncovering judicial truth. Anonymity, decentralization, and the traceability of digital transactions complicate both the identification of offenders and the collection of electronic evidence. This paper explores the legal and technical challenges of conducting preliminary investigations within blockchain environments, emphasizing issues of territorial jurisdiction, international cooperation, and the training of judicial officers. Using an analytical and comparative approach, it highlights the need to adapt Beninese and international legal frameworks to the realities of blockchain-based cybercrime.

Keywords:

Preliminary investigation - Blockchain - Criminal law - Cybercrime – Cryptoassets.

Introduction

« L'enquête est soumise à la dictature du facteur temps. Car presque tout se joue au cours des vingt-quatre (24) premières heures suivant la perpétration d'un crime. Et si pendant cette courte période, l'enquête piétine, il sera plus tard difficile, sinon impossible, de réunir les faits nécessaires à la preuve. ». Cette pensée traduit la nécessité de célérité que requiert l'enquête pénale. Mais cette réalité n'est pas toujours observée. Elle s'est davantage complexifiée avec l'utilisation de plus en plus fréquente de la technologie dans la préparation et la commission des infractions à la loi pénale. Chacune des technologies émergentes a ses spécificités et vise à apporter une solution propre à l'humanité ; mais malheureusement il arrive bien souvent qu'elle soit utilisée pour des travers à l'ordre social. Dans le cadre de cette réflexion, il s'agira pour nous d'analyser l'impact de la technologie blockchain sur le droit pénal de la procédure en l'occurrence sur le déroulement de l'enquête préliminaire.

Selon la doctrine, « l'enquête est la partie du procès pénal qui se déroule avant le déclenchement des poursuites¹ ». C'est une phase confiée à la police judiciaire « sous la direction effective du procureur de la République »² qui prépare au procès pénal en permettant la constitution du dossier de poursuite et qui se déroule hors des juridictions. La police judiciaire est une « activité consistant à constater les infractions à la loi pénale, à en rassembler les preuves et à en rechercher les auteurs tant qu'une information n'est pas ouverte, ainsi qu'à exécuter les délégations des juridictions d'instructions et à déférer à leurs réquisitions³ ». Ainsi, la police judiciaire est dotée de pouvoirs propres et de pouvoirs délégués. A l'occasion de l'exercice de ces pouvoirs, l'enquête prend généralement deux grandes formes, celle qui vise l'identification de l'identité d'une personne et celle conduite aux fins d'élucidation des faits. Dans l'une ou l'autre de ces deux formes, il faut rappeler que le code de procédure pénale a consacré l'enquête de flagrance⁴ et l'enquête préliminaire⁵.

L'enquête préliminaire est définie comme l'« enquête diligentée d'office ou à la demande du parquet par la police ou la gendarmerie avant l'ouverture de toute information et permettant au ministère public d'être éclairé sur le bien-fondé d'une poursuite ». Dans le même ordre, le Professeur Jean Pradel définit l'enquête préliminaire comme « une procédure diligentée par la police judiciaire agissant d'office ou sur les instructions du parquet et destinée à obtenir sur une

¹ Cf. PRADEL J., *Procédure pénale*, 13^{ème} édition CUJAS, Paris, 2006, p 481.

² Cf. art. 14 du Code de procédure pénale béninois.

³ Cf. ADAMOU M., *L'essentiel de la procédure pénale*, éditions du CREDIJ, Cotonou, 2022, p 129.

⁴ Cf. art. 48 du Code de procédure pénale béninois.

⁵ Cf. art. 76 du Code de procédure pénale béninois.

infraction les premiers renseignements afin de permettre au procureur de la République de prendre une décision sur l'opportunité des poursuites ». Il précise que cette « procédure n'est plus utilisable quand une information a été ouverte, la police judiciaire ne pouvant alors opérer que sur la base d'une commission rogatoire délivrée par le juge d'instruction ». L'enquête préliminaire est donc une enquête de « police judiciaire destinée à rapporter la preuve nécessaire à la manifestation de la vérité ». « Elle est née des nécessités de la pratique parce qu'elle présente l'évidente utilité d'éclairer le procureur de la République sur la suite à donner à un dossier ». Eu égard à cet intérêt de portée pratique de l'enquête préliminaire, cette réflexion est axée sur son déroulement dans l'environnement de la technologie blockchain.

La blockchain qui signifie en français, technologie des chaînes de blocs ou encore dispositif d'enregistrement partagé a provoqué un enthousiasme dans le secteur de la technologie comme une évolution majeure mais aussi et surtout dans le secteur de la finance et ne manque pas d'être appréhendée dans le secteur juridique. Bien que disposant d'un code du numérique, la technologie blockchain ne fait pas l'objet d'une définition légale car le législateur béninois a fait le choix de la neutralité technologique. Selon le dictionnaire, la blockchain est un « mode de stockage et de transmission de données sous forme de blocs liés les uns aux autres et protégés contre toute modification »⁶ ce qui fait d'elle, une « base de données contenant l'historique des échanges par blockchain »⁷. En France, la CNIL⁸ en donne une définition plus détaillée en ces termes : « la blockchain (chaîne de blocs) est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »⁹. La blockchain est en effet une technologie de stockage d'informations, où les différentes transactions sont inscrites dans des blocs liés c'est-à-dire, enchaînés les uns aux autres. Ces blocs ont pour particularité d'être en principe lisibles par tous ; la blockchain est donc transparente, ce qui permet de remonter la chaîne et les informations qu'elle contient¹⁰. Elle constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création, sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Il

⁶ <https://dictionnaire.lerobert.com/google-dictionnaire-fr?param=blockchain>, consulté le 28 octobre 2025.

⁷ <https://dictionnaire.lerobert.com/google-dictionnaire-fr?param=blockchain>, consulté le 28 octobre 2025.

⁸ CNIL signifie Commission National de l'Informatique et des Libertés.

⁹ CAPRIOLI E., *La blockchain ou la confiance dans une technologie*, La Semaine Juridique, édition générale, n°23, 6 juin 2016, p.672.

¹⁰ BARON R., *Aspects techniques de la technologie blockchain*, in *Blockchain et droit*, Paris, Dalloz, 2018, p. 9.

existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs.

Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable¹¹. Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et donc indestructible. »¹² Il est clair que la technologie blockchain a un caractère disruptif, souvent mis en avant compte tenu du fait qu'elle crée une véritable rupture au sein d'un secteur d'activité en renouvelant radicalement son fonctionnement à travers la suppression des intermédiaires. Elle présente trois caractéristiques principales.

D'abord, elle est *décentralisée* et distribuée ce qui signifie que contrairement à une base de données centralisée, la blockchain n'a pas de serveur central. Chaque utilisateur du réseau possède une copie identique du registre¹³, le rendant plus résilient et éliminant un point de vulnérabilité unique. De façon concrète, la décentralisation s'opère ensuite au niveau de la validation des transactions effectuées. Il s'agit, ici, de l'idée véritablement révolutionnaire, « disruptive », de la blockchain¹⁴. Ce sont les pairs qui certifient les transactions, généralement par la technique dite du « minage »¹⁵. Ceci permet de se passer d'un organe central de contrôle, d'un « tiers de confiance ». Dans le cadre de la blockchain en effet, ce n'est plus à la banque ou au notaire de certifier une opération, mais à la communauté des utilisateurs qui s'assure elle-

¹¹ Cf. LABBE Th., *Le droit face aux technologies disruptives : le cas de la blockchain*, thèse de doctorat en Droit privé, Université de Strasbourg, 2021, p 15. Sur le caractère infalsifiable, il y a lieu de retenir que du fait du caractère de technologie de consensus de la *blockchain*, il faudrait pouvoir réunir une puissance de calcul supérieure à la moitié de la puissance de la majorité des serveurs participant à la *blockchain* pour pouvoir en prendre le contrôle et ainsi la modifier. De plus, chaque transaction étant horodatée et implantée dans un bloc, la modification d'un bloc peut mettre en péril la totalité de la chaîne de blocs. Dès lors, toute modification a posteriori d'une *blockchain* aura pour conséquence, d'une part, de laisser une trace partagée sur l'ensemble des serveurs connectés, et d'autre part, potentiellement provoquer une défaillance de l'ensemble de la *blockchain*.

¹² <https://www.cnil.fr/fr/definition/blockchain>, consulté le 28 octobre 2025.

¹³ CORNU G., *Vocabulaire juridique*, PUF, collection Quadrige, 8^e édition, 2007 ; Registre : livre constituant un instrument de preuve ou de publicité, parfois doté d'une valeur constitutive, sur lequel on note des informations d'un type qui le caractérise et sert généralement à le dénommer et dont la tenue incombe parfois à un service officiel, parfois au principal intéressé.

¹⁴ Comme nous le verrons dans la section suivante, la technologie blockchain ne mobilise pas de techniques informatiques nouvelles, puisqu'elle se fonde principalement sur la cryptographie (plus précisément, la cryptographie « asymétrique »), mais l'ingéniosité repose sur la décentralisation de la validation des transactions.

¹⁵ Le cryptomining, ou **minage de cryptomonnaies**, est un processus informatique décentralisé permettant de **valider une transaction** et de **créer de nouvelles unités de cryptomonnaie**. On pourrait comparer le minage numérique à l'extraction de minerais précieux. Cf. www.nexa.fr/post/cryptomining-définition.

même de l'exactitude des informations. Comme l'exprimait le journal *The Economist* dans un article remarqué, la blockchain joue le rôle d'une « machine créatrice de confiance »¹⁶.

Ensuite, elle est *sécurisée*, c'est-à-dire que la cryptographie¹⁷ est utilisée pour lier chaque bloc de manière sécurisée. Ainsi, chaque transaction est chiffrée et groupée dans des blocs. Une fois qu'un bloc est ajouté à la chaîne, il devient pratiquement impossible à modifier ou à supprimer. Enfin, elle est *transparente* car le registre est partagé entre tous les participants, qui peuvent consulter l'historique des transactions. Si une information erronée est enregistrée, l'historique permet de la corriger en ajoutant un nouveau bloc qui la corrige, tout en conservant l'information initiale. Relativement à son fonctionnement, il y a lieu de relever quatre aspects.

D'abord, sur les transactions il faut constater que lorsqu'elles ont lieu, elles sont regroupées dans un bloc.

Ensuite, il y a l'étape de la validation du bloc par les participants du réseau (appelés "nœuds" ou "mineurs" sur les blockchains publiques) à travers la résolution d'énigmes cryptographiques complexes.

S'en suit la phase d'ajout à travers laquelle une fois validé, le bloc est ajouté à la chaîne de manière permanente et chronologique.

Enfin, il y a la dernière étape qui est celle de la réplique par laquelle le nouveau bloc est répliqué sur l'ensemble des copies du registre détenues par tous les utilisateurs du réseau, rendant le tout infalsifiable.

Il s'agit manifestement là d'une technologie véritablement révolutionnaire dont l'avènement a bouleversé le paysage numérique mondial, par ricochet, celui béninois et redéfini la conception classique de la preuve, de la traçabilité et de la responsabilité pénale. Cette technologie à l'origine conçue pour assurer la transparence et la sécurité des transactions dans le cadre des cryptomonnaies, la blockchain s'est étendue à de nombreux domaines : finance, santé, propriété intellectuelle, et aujourd'hui le droit pénal.

¹⁶ « *Simply put, it is a machine for creating trust* » (*The Economist*, « The trust machine. The technology behind bitcoin could transform how the economy works », 31 octobre 2015). En somme, des utilisateurs « qui ne se font pas mutuellement confiance peuvent entrer en relation sans avoir recours à un intermédiaire de confiance » (M. LOGNOUL, « La blockchain comme outil de protection et de gestion des actifs de propriété intellectuelle », in *Les blockchains et les smart contracts à l'épreuve du droit*, op. cit., p. 288). La confiance est donc placée « dans la technologie, plutôt que dans un intermédiaire » (Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *J.T.*, 2018, p. 803).

¹⁷ Sur la cryptographie l'écriture est secrète. Voir à ce sujet, ADAMOU M. et ADJAÏGBE S. R., « *Le droit criminel béninois à l'épreuve de la cryptologie* », In *REVUE AFRICAINE DE SCIENCES POLITIQUES ET SOCIALES* N°57 OCTOBRE 2025, pp 43-74.

Selon un auteur, dans son ouvrage intitulé « l'essentiel du droit pénal général », le droit pénal est « le droit qui étudie les faits infractionnels, tels que déterminés par l'État et la réaction sociale que les faits engendrent ».

Toutefois, le fonctionnement décentralisé de la blockchain, son anonymat relatif et son architecture cryptographique posent de nouveaux défis pour les autorités judiciaires et policières, notamment lors de la phase cruciale de l'enquête préliminaire dans le but d'établir des faits infractionnels.

Dans le contexte béninois, marqué par une digitalisation progressive des services et des échanges, l'adoption et la promulgation du code du numérique en 2018, la blockchain représente à la fois une opportunité et un défi pour le système judiciaire. Si elle offre des potentialités en matière de traçabilité et de sécurisation des preuves, mais elle complique aussi la tâche des enquêteurs face à la dématérialisation et la transnationalité des infractions. La question se pose de savoir: **comment concilier les exigences de l'enquête préliminaire en droit pénal béninois avec les spécificités techniques et juridiques de la technologie blockchain?**

Cette réflexion s'articule autour de deux axes : d'une part, les défis imposés par la technologie blockchain à l'enquête préliminaire (1) et, d'autre part, les perspectives d'adaptation du droit pénal béninois face à ces nouveaux enjeux (2).

1. Les défis imposés par la technologie blockchain à l'enquête préliminaire

Dans le cadre de l'enquête préliminaire, la technologie blockchain soumet l'enquêteur à de vrais défis liés d'une part, à l'anonymat et la traçabilité relative des transactions sur la blockchain (1.1.) et, d'autre part, aux limites juridiques et techniques de l'enquête préliminaire face à la décentralisation (1.2.).

1.1. L'anonymat et la traçabilité relative des transactions sur la blockchain

L'un des objectifs de l'enquêteur est l'identification de l'auteur ou des auteurs présumés d'infraction à la loi pénale et la collecte des éléments de preuves. Mais lorsque l'on considère la blockchain publique, elle fonctionne suivant un principe de pseudonymat de ses utilisateurs. Ce qui n'est pas sans conséquence sur le déroulement de l'enquête. Il faut donc analyser d'une part, le pseudonymat des utilisateurs et ses conséquences sur l'identification des auteurs

recherchés (1.1.1.) et, d'autre part, d'examiner, en s'appuyant sur la traçabilité des transactions, si cette fonctionnalité de la blockchain constitue un atout ou une illusion pour l'enquêteur (1.1.2.).

1.1.1. Le pseudonymat des utilisateurs et ses conséquences sur l'identification des auteurs recherchés

S'agissant du pseudonymat des utilisateurs et ses conséquences sur l'identification des auteurs, dans un cas de blockchain publique, les utilisateurs interagissent à travers des clés publiques ou adresses numériques, mais leur identité réelle est souvent masquée derrière ces pseudonymes. En l'absence de lien clair entre une clé publique et une personne physique, l'identification de l'auteur potentiel d'un acte illicite (escroquerie, blanchiment, financement terroriste, etc.) devient extrêmement difficile. Cette opacité complique dès lors l'enquête préliminaire et subséquemment, la mise en œuvre d'acte de poursuite, comme l'établissement d'un commencement de preuve, ou la confrontation d'éléments à charge.

A titre illustratif, dans les blockchains publiques, même si toutes les transactions sont visibles, les adresses ne révèlent pas automatiquement qui les contrôle. Le rapport du Conseil de l'Europe sur les blockchains note que « seule leur adresse publique est visible et il est, en principe, impossible de savoir qui se cache derrière une adresse publique ». Or, sans l'identification, ni réquisition d'informations auprès d'intermédiaires, ni perquisition ciblée n'est possible et il est en conséquence difficile de lier une transaction à une personne donnée. Le pseudonymat, défini comme l'usage d'un nom d'emprunt ou d'une signature différente du nom à l'état civil de l'auteur, peut apparaître comme un instrument de protection de la vie privée ou de liberté d'expression ; mais il engendre en même temps des effets significatifs sur la paternité de l'œuvre, la responsabilité juridique et la traçabilité de l'auteur. En droit béninois, la législation relative à la propriété littéraire et artistique reconnaît que l'auteur peut « rester anonyme ou utiliser un pseudonyme » mais pas dans d'autres cas.

Ce pseudonymat pose aussi des risques pour la fiabilité de la preuve. En droit pénal béninois, comme dans beaucoup de systèmes juridiques, la preuve doit permettre d'identifier l'auteur de l'infraction avec un degré de certitude suffisamment fort pour garantir le droit à la défense. Sans des preuves complémentaires (témoignages, expertise technique, traçage hors chaîne, fournisseurs de services numériques ou plateformes de change), le dossier de poursuite en constitution dans un cas pareil risque d'être fragile.

1.1.2. La traçabilité des transactions : atout ou illusion pour l'enquêteur ?

La blockchain offre, en pluralité, une traçabilité aux transactions : les opérations sont inscrites dans des blocs horodatés, publiquement consultables dans les chaînes distribuées. Ceci semble à première vue un atout majeur pour l'enquêteur : il est possible de reconstituer un chemin de transfert de fonds, de repérer des adresses impliquées dans des flux suspects, etc.

Dans un contexte marqué par la dématérialisation croissante des échanges, elle se présente, à première vue, comme un instrument privilégié d'investigation permettant de remonter la chaîne des flux financiers et d'identifier les acteurs impliqués dans des activités illicites. En effet, chaque transaction électronique laisse des traces numériques comme : l'adresse IP, les identifiants bancaires, les registres de transactions susceptibles d'être exploités par les enquêteurs .

Cependant, cette traçabilité reste relative. Plusieurs facteurs en limitent l'utilité pratique :

- l'usage de mixers ou de services de mélange de crypto-actifs, qui brouillent les flux ;
- l'emploi de blockchains avec mécanismes de confidentialité avancés (zk-SNARKs, signatures en anneau, transactions confidentielles) qui rendent illisibles certaines parties de la transaction ou cachent les montants ou adresses ;
- le fait que certaines transactions ne reflètent pas directement un usage illicite : la traçabilité des flux ne garantit pas l'interprétation juridique ou morale des mouvements d'argent.

Cette apparente transparence dissimule de nombreuses limites qui relativisent son efficacité réelle.

D'une part, la multiplication des intermédiaires financiers et des plateformes numériques, souvent situés dans des juridictions différentes, complexifie le suivi des flux et retarde les investigations .

D'autre part, l'essor des cryptomonnaies et des systèmes de paiement anonymes brouille les pistes en offrant aux délinquants une certaine opacité technologique, rendant la traçabilité parfois illusoire.

En outre, la traçabilité impose des moyens techniques et humains : les enquêteurs doivent disposer de compétences en blockchain forensic, en analyse de flux, en cryptographie, etc. En l'absence de ces compétences ou de ces outils, la traçabilité reste théorique. Sur le plan

juridique, même si la blockchain peut documenter des flux, le droit béninois doit reconnaître dans ses textes l'admissibilité de ces éléments d'information, leur fiabilité, et garantir les droits de la défense quant à la vérification des preuves techniques.

En définitive, elle oscille entre promesse d'efficacité et illusion d'omnipotence, selon la nature des transactions et les dispositifs de contrôle mis en place .

1.2. Les limites juridiques et techniques de l'enquête préliminaire face à la décentralisation

La décentralisation présente des limites à la fois juridiques et techniques dans les situations d'enquête préliminaire. Cela est perceptible à deux niveaux. D'une part, l'absence d'intermédiaire central est un véritable obstacle à la perquisition et à la réquisition (1.2.1) et, d'autre part, la compétence territoriale et les difficultés liées à l'extraterritorialité des données (1.2.2).

1.2.1. L'absence d'intermédiaire central : obstacle à la perquisition et à la réquisition

Dans les systèmes traditionnels, les enquêteurs peuvent viser des intermédiaires (banques, fournisseurs d'accès, opérateurs de plateformes numériques, etc.) pour obtenir des informations, saisir des documents, etc. Or, dans la blockchain, particulièrement les chaînes décentralisées et sans autorité centrale de contrôle, il n'existe pas toujours un tiers identifiable ou juridiquement responsable sur le territoire national à qui adresser des réquisitions ou des injonctions.

L'un des fondements des technologies décentralisées, telles que la blockchain, réside dans l'absence d'un intermédiaire central de contrôle ou de validation des transactions. Si cette caractéristique garantit l'autonomie et la transparence du réseau pour les utilisateurs, elle soulève en revanche de profondes difficultés pour les autorités judiciaires, notamment dans la mise en œuvre des mesures coercitives classiques telles que la perquisition et la réquisition de données numériques.

Par exemple, une plateforme d'échange de cryptomonnaies peut être basée à l'étranger, ou ne conserver qu'une partie minimale des informations d'identification de ses utilisateurs. Si l'enquête préliminaire béninoise ne dispose pas de traités ou accords de coopération internationale, il est difficile de forcer la collaboration ou d'obtenir l'accès aux données hors du territoire national.

En effet, dans les systèmes traditionnels, les enquêteurs peuvent solliciter les établissements bancaires, les fournisseurs d'accès ou les opérateurs de plateformes numériques, en vertu des dispositions du code de procédure pénale, afin d'obtenir des informations pertinentes sur une opération suspecte ou sur l'identité d'un utilisateur. Ces entités jouent ainsi un rôle d'intermédiaire technique et juridique, garantissant un point d'accès à l'information .

Or, dans un réseau décentralisé fondé sur un registre distribué, aucune autorité ou institution unique ne détient la maîtrise des données. Les informations sont partagées entre plusieurs nœuds indépendants, souvent dispersés à travers différentes juridictions. Dès lors, aucune instance identifiable ne peut être contrainte de remettre ou de conserver les données recherchées, ce qui rend la perquisition numérique particulièrement complexe . De même, la procédure de réquisition judiciaire, traditionnellement adressée à un prestataire de service ou à un opérateur, se heurte à une absence de destinataire légalement responsable, limitant considérablement la portée de l'action de l'enquêteur .

D'un point de vue technique, l'absence d'un serveur ou d'un centre de données unique rend également la perquisition « physique » difficile. Pour saisir des données numériques pertinentes, il faut identifier l'emplacement des données (serveurs, nœuds), ce qui peut être réparti dans plusieurs juridictions, sous différentes législations. La nature distribuée de la blockchain complique l'obtention de preuves matérielles ou de copies vérifiables d'un état donné de la chaîne sans risque d'altération (ou du moins d'accusation d'altération).

1.2.2. La compétence territoriale et les difficultés liées à l'extraterritorialité des données

L'un des défis majeurs que pose l'investigation numérique réside dans la détermination de la compétence territoriale lorsque les données utiles à la manifestation de la vérité sont hébergées en dehors du territoire national. En effet, la dématérialisation des informations et leur stockage sur des serveurs situés dans plusieurs États rendent incertaine la délimitation de compétence des autorités judiciaires.

La décentralisation implique souvent que certaines données ou certains nœuds de la blockchain soient situés en dehors des frontières du Bénin. Dès lors, la compétence territoriale pour enquêter, saisir des données, obtenir la communication de preuves se heurte à des obstacles juridiques substantiels :

- nécessité de coopération internationale judiciaire ou policière : demandes d'entraide, d'entraide mutuelle, de réciprocité ;
- divergences législatives entre pays (ce qui est licite dans un pays peut ne pas l'être dans un autre, ou le degré de protection des données à caractère personnel peut varier) ;
- difficultés pratiques : délai, coût, absence de convention bilatérale ou multilatérale adaptée, refus d'un État de coopérer pour des raisons de souveraineté, protection des données, etc.

Traditionnellement, le principe de territorialité de la loi pénale confère compétence aux juridictions d'un État pour connaître des infractions commises sur le sol ou produisant leurs effets sur celui-ci. Or, dans le cyberspace, la localisation des données devient problématique : un acte délictueux commis depuis le Bénin peut impliquer des serveurs situés en Europe, en Asie ou aux États-Unis, relevant de législations étrangères aux conceptions parfois divergentes en matière de protection des données et d'accès à l'information.

Cette situation crée une tension entre souveraineté nationale et coopération internationale. D'une part, les autorités béninoises peuvent se retrouver juridiquement impuissantes face à des prestataires étrangers refusant de communiquer des données au motif qu'ils sont soumis à d'autres législations. D'autre part, les procédures de coopération judiciaire internationale, notamment les commissions rogatoires internationales, apparaissent souvent lentes et inadaptées à la rapidité des investigations numériques.

L'extraterritorialité des données interroge ainsi les fondements classiques de la compétence territoriale en droit pénal. Plusieurs auteurs suggèrent une approche fonctionnelle de la compétence, fondée non plus sur le lieu de stockage des données, mais sur le lieu où le préjudice est subi où l'acte produit ses effets. Une telle approche, bien que novatrice, requiert une harmonisation normative internationale, condition essentielle pour éviter les conflits de juridiction et garantir une efficacité réelle de la coopération en matière de cybercriminalité.

La loi portant code du numérique en République du Bénin aborde dans son deuxième livre des sujets essentiels concernant la preuve électronique, la signature électronique, l'intégrité des écrits numériques, mais ne semble pas contenir de disposition spécifique traitant des défis de l'extraterritorialité des données blockchain. L'absence de cadre législatif spécial (ou de jurisprudence claire) crée un vide qui peut être exploité par les défenseurs pour contester la

recevabilité ou la légalité de la preuve. Il y a lieu alors d'envisager les perspectives d'adaptation de l'enquête préliminaire aux exigences de la technologie blockchain.

2. Les perspectives d'adaptation de l'enquête préliminaire à l'univers de la blockchain au Bénin

Pour une enquête préliminaire efficace dans le domaine de la blockchain, il y a lieu d'œuvrer au développement d'un cadre juridique et procédural adapté aux technologies basées sur la blockchain (2.1.) et au renforcement des capacités des acteurs de la chaîne pénale (2.2.).

2.1. Le développement d'un cadre juridique et procédural adapté aux technologies basées sur la blockchain

Pour un droit pénal efficace, il est nécessaire qu'une législation spécifique ou révisée encadrant les cryptoactifs et la blockchain au Bénin (2.1.1.) et il faut aussi assurer l'encadrement juridique des moyens d'investigations numériques (perquisitions, saisies de wallets, etc.) (2.1.2).

2.1.1. La nécessité d'une législation spécifique ou révisée encadrant les cryptoactifs et la blockchain

L'émergence des cryptoactifs et de la technologie blockchain bouleverse profondément les paradigmes juridiques traditionnels fondés sur la centralisation, la traçabilité et la responsabilité des acteurs économiques. Ces innovations, reposant sur des registres distribués et des transactions décentralisées, échappent largement aux cadres normatifs classiques élaborés pour les systèmes financiers centralisés. Or, cette absence d'encadrement juridique clair crée un vide normatif propice aux risques de fraude, de blanchiment de capitaux, de financement du terrorisme et d'insécurité juridique pour les utilisateurs.

Au Bénin, comme dans de nombreux États africains, le droit positif demeure muet ou fragmentaire sur le statut juridique des cryptoactifs. Le cadre législatif actuel, notamment la loi n° 2017-20 du 20 avril 2018 portant Code du numérique en république du Bénin, bien qu'elle aborde certaines questions relatives à la cybersécurité et aux transactions électroniques, ne prévoit aucune disposition spécifique applicable à la blockchain ou aux actifs numérique. Cette lacune rend difficile la qualification juridique des cryptoactifs, sont-ils des monnaies, des biens meubles incorporels, des valeurs mobilières ou simples données ? et par conséquent, complique leur intégration dans le système juridique national.

Pour que l'enquête préliminaire au Bénin soit efficace dans les affaires impliquant la blockchain, il est indispensable que le cadre juridique national intègre explicitement les cryptoactifs et les particularités techniques de la blockchain. Cela suppose :

- d'adopter une loi spécifique ou un ensemble de textes (loi, décrets, règlements) qui définissent ce qu'est un cryptoactif, qui régissent les prestataires de services de cryptoactifs (échanges, garde de wallets, plateformes d'ICO, etc.), et qui fixent les obligations de transparence, de conservation des données, de vérification d'identité (en anglais : KYC qui signifie know your customer) pour ces acteurs ;
- de prévoir des dispositions législatives pour encadrer la preuve électronique blockchain : reconnaissance de la signature électronique, règles sur l'horodatage, l'immutabilité des données, leur intégrité, leur admissibilité devant les juridictions pénales, etc. ;
- de combler les vides et clarifier les zones grises. Par exemple : que faire en cas de transactions dans des blockchains anonymisées, ou de recours à des services de mélange ("mixers") ? Le droit devrait prévoir des sanctions, des obligations de collaboration des plateformes, etc. ;
- le Bénin dispose déjà d'un Code du numérique (loi n° 2017-20 du 20 avril 2018). Au terme de son article 2, ce code vise à « régir les activités qui relèvent (...) de la cybercriminalité et la cybersécurité ». Cependant, ce texte ne semble pas avoir encore intégré de manière explicite toutes les spécificités des cryptoactifs ou des blockchains décentralisées, ni des mécanismes précis de perquisition numérique de wallets ou d'accès aux clés privées ;
- enfin, l'adoption de textes d'application, décrets ou arrêtés, pour compléter et préciser des dispositions du Code du numérique est toujours en cours. A titre illustratif, il peut être citer le compte rendu du Conseil des ministres tenu le 02 juillet 2025, le gouvernement béninois a adopté huit nouveaux textes d'application du Code du numérique afin de renforcer le cadre réglementaire¹⁸ des acteurs du secteur numérique¹⁹.

¹⁸ Cf. le décret n° 2025-366 du 02 juillet 2025 portant modalités de déclaration, d'autorisation et d'agrément des moyens et services de cryptologie ainsi que les modalités des règlements transactionnels et le décret n° 2025-368 du 02 juillet 2025 portant règles d'interception et d'accès aux données, définissant les autorités habilitées et fixant les modalités de mise en œuvre des opérations et les dispositions particulières en matière de cryptologie.

¹⁹ Cf. <https://sgg.gouv.bj>.

Ces instruments peuvent servir de base pour adapter la législation aux réalités de la blockchain.

2.1.2. L'encadrement juridique des moyens d'investigations numériques (perquisitions, saisies de wallets, etc.)

Au-delà de la législation relative aux cryptoactifs, il est fondamental de prévoir un cadre procédural adapté pour les moyens d'investigations numérique. A cet effet, il faut :

- définir légalement la perquisition numérique et la saisie des données blockchain (wallets²⁰, clés privées, historiques de transactions). Cela inclut la précision de l'autorité compétente qui peut autoriser une perquisition (procureur, juge), sous quelles conditions, sous quel contrôle, avec des garanties pour la vie privée, le respect du secret professionnel, etc. ;
- mettre en place des procédures claires pour la saisie de portefeuilles numériques ("wallets") et la récupération des clés privées ou phrases mnémotechniques, selon les cas. Il faudra veiller à ce que cela ne contrevienne pas au droit à ne pas s'auto-incriminer ;

²⁰ Le wallet, dont la traduction de l'anglais en français est « portefeuille », désigne un portefeuille électronique dans lequel il est possible de stocker diverses cartes et autres supports numériques. C'est un espace sécurisé sur votre appareil mobile qui centralise vos [moyens de paiement](#), cartes de fidélité, billets de voyage, coupons de réduction et bien plus encore. Cette plateforme vous permet de gérer efficacement vos actifs numériques et vos documents importants, tout en réduisant le besoin de transporter des documents papier. Il existe deux principaux types de wallets mobiles, chacun offrant des fonctionnalités adaptées aux besoins des utilisateurs : **Les wallets natifs** sont pré-installés sur les smartphones. Sur iPhone, l'application Apple Wallet (anciennement « Cartes ») est impossible à supprimer. Pour les utilisateurs Android, Google Wallet et Samsung Wallet sont de plus en plus souvent pré-installés sur les nouveaux appareils. Ces wallets sont généralement compatibles avec la plupart des cartes de crédit et cartes de paiement des réseaux standard.

Ces wallets natifs offrent une intégration parfaite avec le système d'exploitation du téléphone, garantissant une expérience utilisateur fluide et sécurisée. Ils permettent d'effectuer un paiement rapidement et en toute sécurité, que ce soit pour des paiements en ligne ou des paiements sans contact en magasin.

Les wallets tiers et wallets crypto : contrairement aux wallets natifs, les wallets tiers nécessitent un téléchargement de la part de l'utilisateur. Des applications comme PayPal, Lydia, Stocard ou Fidme entrent dans cette catégorie. Bien que principalement connues pour la gestion des paiements, ces applications élargissent de plus en plus leurs fonctionnalités pour inclure la dématérialisation d'autres types de cartes et supports marketing. Certains wallets sont spécialement conçus pour les crypto-monnaies, on les appelle wallets crypto ou portefeuilles crypto. Ces wallets crypto permettent aux utilisateurs d'accéder à leur compte sur une plateforme privée, de stocker leurs clés privées et clés publiques, d'effectuer des transactions sur la blockchain, et de gérer divers types d'actifs numériques, y compris les NFT, pour sécuriser leur argent. Des solutions comme Coinbase (un hot wallet) ou Trezor (un hardware wallet pour le stockage à froid ou cold wallet) sont populaires dans ce domaine. In <https://www.captainwallet.com/blog/wallet-concept-definition-et-fonctionnement/>, consulté, le 31 octobre 2025.

- assurer la conservation de la chaîne de garde (“chain of custody”) pour les preuves issues de la blockchain : garantir que les données recueillies, analysées, transférées n’ont pas été altérées, que leur intégrité peut être vérifiée, etc. ;
- intégrer dans les droits de la défense un accès aux preuves techniques, aux méthodes de forensic, aux rapports d’experts qui auront analysé les données blockchain afin que l’accusé puisse les contester, ou demander des contre-expertises s’il le faut, etc. ;
- prévoir des dispositions légales concernant la coopération technique avec les plateformes d’échanges ou autres prestataires de services numériques, y compris à l’étranger, afin d’obtenir les informations utiles pour la preuve (identification des utilisateurs, logs, accès aux serveurs le cas échéant).

Sur le plan juridique, l’encadrement de ces techniques d’investigation requiert un équilibre délicat entre l’impératif d’efficacité de la justice pénale et l’exigence de protection des libertés individuelles. En Europe, par exemple, la directive 2016/680 du 27 avril 2016 encadre le traitement des données à caractère personnel par les autorités répressives, imposant des garanties strictes lors des opérations de perquisition et de saisie numériques²¹. De même, la jurisprudence de la cour européenne des droits de l’Homme (CEDH) rappelle que toute ingérence dans la vie privée doit être prévue par la loi, poursuivre un but légitime et demeurer proportionnée²².

Dans le système juridique africain, et particulièrement en droit béninois, l’encadrement des moyens d’investigations numériques reste encore lacunaire. Si la loi n° 2017-20 du 20 avril 2018 portant Code du numérique en république du Bénin reconnaît la validité juridique des preuves électroniques et prévoit certaines mesures d’enquêtes, elle ne précise pas toujours les conditions procédurales strictes applicables à la saisie ou à la perquisition des supports numériques²³.

L’encadrement juridique des moyens d’investigations numériques appelle donc une réforme approfondie, visant à harmoniser les pratiques nationales avec les standards internationaux en matière de protection des droits numériques. Il s’agit, en définitive, de

²¹ Directive de l’UE 2016/680 du parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnelles par les autorités compétentes à des fins de prévention, de détection, d’enquête ou de poursuite d’infractions pénales.

²² CEDH, affaire Klass et autre C. Allemagne, arrêt du 6 septembre 1978, série A n° 28.

²³ Art. 570 du Code du Numérique béninois.

concilier l'efficacité de la lutte contre la cybercriminalité avec les garanties procédurales inhérentes à un État de droit.

2.2. Le renforcement des capacités des acteurs de la chaîne pénale

Le renforcement des capacités des acteurs de la chaîne pénale passe par la formation technique des officiers de police judiciaire et des magistrats (2.2.1.) et la promotion de la coopération nationale et internationale en matière de lutte contre la criminalité liée à la technologie blockchain (2.2.2.).

2.2.1. La formation technique des officiers de police judiciaire et des magistrats

Une législation bien conçue ne suffit pas si les acteurs (agents de police, magistrat, experts) ne disposent pas des compétences techniques nécessaires. C'est pour cette raison qu'il est important, outre, l'adaptation de cadre juridique d'assurer :

- une formation spécifique en matière de blockchain qui permettra aux bénéficiaires de comprendre les fondements techniques (cryptographie, wallets, smart contracts, consensus, etc.), les types de blockchains (publics, privés, permissionnés, anonymisés), et les outils d'investigation (blockchain forensic, analyse de flux, traçage, etc.) ;
- une formation judiciaire (juges et procureurs) sur la preuve numérique, le rôle de l'expert, l'interprétation des données blockchain, leur valeur probante, les garanties procédurales. Il faut rappeler en exemple qu'au Bénin, le projet GLACY+ a organisé une **formation des formateurs sur la cybercriminalité et les preuves électroniques** pour juges et procureurs, afin de les rendre capables de former à leur tour au niveau national²⁴. De même, un atelier consultatif (12-13 juin 2023) a visé l'intégration de la cybercriminalité et des preuves électroniques dans les formations judiciaires nationales²⁵ ;
- une formation des officiers de police judiciaire spécifiques à la blockchain (wallets, clés privées, opérations de saisie numérique, forensic). Ceci pourrait inclure aussi des formations continues, modules spécialisés, partenariats avec des universités ou des écoles techniques numériques.

²⁴ https://www.coe.int/fr/web/cybercrime/-/glacy-training-of-trainers-on-cybercrime-and-electronic-evidence-delivered-in-ben-1?utm_source=chatgpt.com, Consulté, le 31 octobre 2025.

²⁵ https://www.coe.int/fr/web/cybercrime/-/glacy-advisory-workshop-on-mainstreaming-cybercrime-and-electronic-evidence-for-judicial-and-prosecutors-training-institutions?utm_source=chatgpt.com, consulté le 31 octobre 2025.

Ainsi, la formation technique apparaît comme un levier stratégique pour garantir une application effective des normes relatives à la cybersécurité et la lutte contre la cybercriminalité. Comme le souligne Béranger DOSSOU « l'absence de maîtrise des outils numériques par les acteurs juridiques compromet la crédibilité des enquêtes et fragilise la preuve électronique devant les juridictions ».

Au Bénin, la loi n° 2017-20 du 20 avril 2018 portant Code du numérique confère à la police judiciaire et au parquet des prérogatives étendues en matière de cybercriminalité²⁶. Toutefois, l'application de ces dispositions demeure souvent limitée par l'insuffisance de la formation technique des acteurs. Si certaines initiatives nationales, telles les programmes de renforcement des capacités organisés par l'Agence nationale de la Sécurité des Systèmes d'information (ANSSI-BENIN), ont contribué à sensibiliser les professionnels de la justice, elles restent ponctuelles et insuffisamment institutionnalisées²⁷. La coopération est aussi un axe très important en matière d'enquête dans l'univers de la blockchain.

2.2.2. La coopération nationale et internationale en matière d'enquête préliminaire liée à la blockchain

La nature transfrontalière des blockchains et des services associés impose une coopération efficace. C'est pourquoi il est recommandé d'envisager :

- le renforcement de la coopération internationale judiciaire et policière : traités d'entraide, conventions spécifiques, participation à des conventions internationales comme la Convention de Budapest sur la cybercriminalité, la Convention des nations unies contre la Cybercriminalité ou d'autres instruments régionaux (la directive portant lutte contre la cybercriminalité dans l'espace CEDEAO, la Convention d'extradition A/P1/8/94 du 6 août 1994 signée par les États membres de la CEDEAO, la Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel) ;
- la coopération technique avec des fournisseurs de services numériques, des prestataires étrangers, plateformes d'échange, services hébergés dans d'autres juridictions, pour obtenir des logs, des données d'identification, etc. ;
- des partenariats avec les organisations régionales ou internationales : Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO), Union

²⁶ Loi n° 2017-20 du 20 avril 2018 portant Code du numérique en république du Bénin.

²⁷ Rapport annuel, ANSSI-BENIN, Cotonou, 2021.

Économique et Monétaire Ouest Africaine (UEMOA), Conseil de l'Europe, projet OCWAR-C (Lutter contre la criminalité organisée en Afrique de l'Ouest), GLACY+, etc. Au Bénin, on voit déjà des initiatives : la formation de la chaîne pénale lutte contre le blanchiment de capitaux / financement du terrorisme (LBC/FT) grâce à la Cellule Nationale de Traitement des Informations Financières (CENTIF), où parmi les piliers figure la coopération internationale. Et le projet Enabel qui facilite le partage d'outils entre professionnels de la cybercriminalité au Bénin ;

- l'établissement de mécanismes de mutualisation technique régionale : laboratoires forensiques, plateformes de données, observatoires de la blockchain, etc., qui peuvent servir plusieurs pays.

A l'échelle internationale, la coopération constitue un impératif, car les infractions impliquant des transactions sur la blockchain dépassent fréquemment les frontières étatiques. Les mécanismes classiques d'entraide judiciaire, tels que les commissions rogatoires internationales, se révèlent souvent inadapté face à la rapidité et à la volatilité des échanges numériques²⁸.

Conclusion

L'avènement de la blockchain constitue à la fois une opportunité et un défi pour les systèmes judiciaires contemporains. Si cette technologie garantit la transparence, l'intégrité et la traçabilité des transactions, elle complexifie en revanche le travail des enquêteurs et des magistrats, en raison de son architecture décentralisée, de l'anonymat qu'elle procure et de la nature immuable des données qu'elle héberge. Dans ce contexte, l'enquête préliminaire, phase essentielle du processus pénal, se trouve confrontée à une mutation profonde de ses méthodes et de ses outils.

Au Bénin comme ailleurs, les textes existants, notamment le Code du numérique et le Code de procédure pénale, bien qu'ils offrent un socle juridique de base, demeurent insuffisants pour appréhender les spécificités techniques de la blockchain et des cryptoactifs. Les autorités judiciaires doivent désormais conjuguer le respect des garanties procédurales avec l'exigence d'efficacité dans la recherche et la conservation de la preuve électronique. Cette conciliation passe nécessairement par la formation technique des officiers de police judiciaire et des

²⁸ OUEDRAOGO S., « *Les défis de la coopération judiciaire internationale face à la cybercriminalité en Afrique de l'Ouest* », Revue africaine de droit et de gouvernance, 2020, p. 92.

magistrats, ainsi que par la coopération tant nationale qu'internationale entre d'une part, services d'enquêtes et juridictions et, d'autre part, prestataires et fournisseurs de services numériques car la nature transnationale des données échappe souvent aux frontières étatiques. Dès lors, il apparaît indispensable d'engager une réflexion normative et institutionnelle plus approfondie afin d'adapter le droit positif aux nouvelles réalités numériques fondées sur la blockchain. Le renforcement du centre national d'investigations numériques (CNIN) dont la mission est de lutter contre la criminalité liée aux technologies de l'information et de la communication et de contribuer, en relation avec les organismes compétents, à la cybersécurité du Bénin, ainsi que le renforcement des capacités des acteurs judiciaires et la promotion d'accords de coopération bilatérale ou régionale en matière de lutte contre la cybercriminalité et de recueil des preuves électroniques, constituent, à cet égard, des pistes prioritaires. En somme, seule une approche globale, intégrant les dimensions juridique, technique et humaine, permettra à l'enquête préliminaire de demeurer un instrument efficace de manifestation de la vérité à l'ère de la blockchain.

BIBLIOGRAPHIE

I. OUVRAGES GÉNÉRAUX

1. ADAMOU Moktar :
 - « L'essentiel du droit pénal général », Cotonou, Éditions du CREDIJ, 2025, 580 p.
 - « L'essentiel de la procédure pénale », Cotonou, Éditions du CREDIJ, 2022, 423 p.
2. CUSSON Maurice et LOUIS Gaétan, « L'art de l'enquête criminelle : à la recherche de la vérité, de la sécurité et de la justice », Montréal, Presses de l'Université de Montréal, 2009.
3. LARGUIER Jacques, « La procédure pénale », 8^e éd., Paris, Presses Universitaires de France (PUF), 1994.
4. PRADEL Jean, « Procédure pénale », 13^e éd., Paris, CUJAS, 2006.
5. VLAMYNCK, Hubert, « Droit de la police », 6^e éd., Paris, Vuibert-Droit.

II. OUVRAGES SPÉCIFIQUES

- 1- BARON Romain, « Aspects techniques de la technologie blockchain », in Blockchain et droit, Paris, Dalloz, 2018.
- 2- BENSAMOUN Alexandra et VIVANT Michel, « Le droit à l'épreuve du numérique », Paris, Dalloz, 2021.
- 3- G'SELL Florence et MARTIN-BARITEAU Félix, « L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit », Rapport pour le Conseil de l'Europe, Strasbourg, 2022.
- 4- LABBÉ Thomas, « Le droit face aux technologies disruptives : le cas de la blockchain », Thèse de doctorat en droit privé, Université de Strasbourg, 14 décembre 2021.

III. LOIS, DECRETS, CONVENTION ET DIRECTIVE

- 1- République du Bénin, Loi n°2017-20 du 20 avril 2018 portant Code du numérique en République du Bénin.
- 2- République du Bénin, Loi n°2012-15 du 18 mars 2013 portant Code de procédure pénale en République du Bénin.
- 3- République du Bénin, Décrets d'application du Code du numérique, textes adoptés en juillet 2025.
- 4- Convention sur la cybercriminalité (Convention de Budapest).
- 5- Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des données à caractère personnel dans le cadre des activités policières et judiciaires.

IV. RAPPORTS ET DOCUMENTS INSTITUTIONNELS

- 1- ASIN/ GLACY+, Formation des formateurs sur la cybercriminalité et les preuves électroniques, Abomey-Calavi, 16–19 août 2022.
- 2- ASIN/ GLACY+, Atelier consultatif sur l'intégration de la cybercriminalité et des preuves électroniques pour les établissements de formation des juges et procureurs, Abomey-Calavi, 12–13 juin 2023.
- 3- CENTIF-Bénin, Formation de la chaîne pénale béninoise : Lutte contre le blanchiment des capitaux et le financement du terrorisme (LBC/FT), 2023.
- 4- Projet ENABEL, Appui à l'opérationnalisation de la Police républicaine (PAOP) dans le cadre de la lutte contre la cybercriminalité au Bénin.
- 5- OCWARC Organisations régionales de cybersécurité en Afrique de l'Ouest.

V. ARTICLES ET DOCTRINE

- 1- ADAMOU Moktar et ADJAÏGBE Sêvi Rodolphe, « Le droit criminel béninois à l'épreuve de la cryptologie », Revue africaine de sciences politiques et sociales, n°57, octobre 2025, pp. 43–74.
- 2- EL MEJRI Ahmed, « La pyramide de Ponzi », Revue de droit bancaire et financier, n°4, juillet 2020, étude n°11.
- 3- CAPRIOLI Eric, « La blockchain ou la confiance dans une technologie », La Semaine Juridique, Édition générale, n°23, 6 juin 2016.
- 4- LE MAIGAT Pierre, « Du bon usage de la cryptologie en droit pénal », ActuJuridique, en ligne : <https://www.actu-juridique.fr/droit-penal/du-bon-usage-de-la-cryptologie-en-droit-penal/>, consulté le 27 octobre 2025.
- 5- KOBOYAH Jean-Paul, « Afrique : droit à l'effacement face à la blockchain, un défi pour les législations ? », Village Justice, juillet 2025, en ligne : <https://www.village-justice.com/articles/afrique-droit-effacement-face-blockchain-defi-pour-les-legislations,53993.html>, consulté le 27 octobre 2025.

VI. DICTIONNAIRE JURIDIQUE

- 1- GUILLIEN Raymond, VINCENT Jean (dir.), GUINCHARD Serge et al., Lexique des termes juridiques, 17^e éd., Paris, Dalloz, 2010.

VII. REVUES

- 1- Revue africaine de sciences politiques et sociales, n°57, octobre 2025.
- 2- Revue de droit bancaire et financier, n°4, juillet 2020.
- 3- La Semaine Juridique (Édition générale), Dalloz.
- 4- ActuJuridique.fr
- 5- Village-Justice.com

VIII. SITOGRAPHIE

- 1- <https://www.village-justice.com>
- 2- <https://www.actu-juridique.fr>
- 3- <https://www.coe.int> (Conseil de l'Europe – rapports sur la blockchain)
- 4- <https://www.anssi.bj> (Agence Nationale de la Sécurité des Systèmes d'Information – Bénin)