

Pour une transposition fonctionnelle du droit de la construction aux architectures numériques distribuées

La fiabilité structurelle, principe directeur de la responsabilité du fait des systèmes

par

Olivier MESKENS KUFUANGA

Licencié en droit (UCL), Conseiller juridique

Résumé

La généralisation des architectures numériques distribuées (blockchain, smart contracts, registres infalsifiables, systèmes d'intelligence artificielle, infrastructures cloud critiques, plateformes algorithmiques opaques) transforme les fondements du droit de la responsabilité. Là où la sécurité des échanges reposait sur des tiers institutionnels, elle s'adosse désormais à la fiabilité technique du code et à la stabilité des architectures numériques, sous la responsabilité des acteurs qui les conçoivent et les exploitent. L'article propose de consacrer la *fiabilité structurelle* comme *concept sui generis* et *principe directeur* du droit des systèmes distribués, inspiré du droit belge de la construction et ancré, sur le plan textuel, sur l'article 5.71 du nouveau Code civil. Il démontre que la stabilité, la cohérence et la sécurité du code constituent les exigences opposables que ce principe directeur impose à l'ensemble des acteurs des architectures numériques distribuées concernées. En articulant cette approche avec les exigences issues du droit européen contemporain (MiCA, DORA, NIS 2, DAC 8, directive (UE) 2024/2853, Règlement (UE) 2024/1689), l'étude plaide pour une refondation de la confiance juridique dans l'économie numérique décentralisée.

Mots-clés

Blockchain – Smart contracts – Responsabilité numérique – Fiabilité structurelle – Concept sui generis – Principe directeur – Article 5.71 du nouveau Code civil – Garantie décennale – Directive (UE) 2024/2853 – Règlement (UE) 2024/1689 – Proposition AILD – Clauses exonératoires – Clauses abusives – Gouvernance technologique – Régulation européenne – MiCA – DORA – NIS 2 – DAC 8.

Introduction

Les technologies dites de « confiance distribuée », au premier rang desquelles figurent la blockchain et les smart contracts, traduisent un renversement paradigmatique du modèle juridique classique de sécurisation des opérations et des décisions automatisées¹. Là où la sécurité juridique reposait traditionnellement sur des institutions hiérarchisées (banques, notaires, autorités de régulation), elle prétend désormais s'appuyer sur la stabilité intrinsèque d'un code informatique et la cohérence logique d'un réseau décentralisé.

Cette substitution d'une confiance institutionnelle à une confiance technologique pose une question juridique fondamentale : qui est responsable lorsque la défaillance ne procède plus de l'action humaine

¹Sur la notion de « confiance distribuée », v. P. DE FILIPPI et A. WRIGHT, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.

identifiable, mais du dysfonctionnement d'un système autonome ? Les incidents récents (piratages massifs, pertes irréversibles d'actifs numériques, exécutions erronées de contrats automatisés) démontrent que le code n'est ni axiologiquement neutre, ni techniquement infaillible. L'architecture logicielle, aussi sophistiquée soit-elle, demeure l'œuvre d'une intelligence humaine et, partant, reste sujette aux aléas de la conception, de l'implémentation et de l'exploitation.

Face à cette incertitude structurelle, nous proposons de dégager une notion fédératrice susceptible de fonder un régime cohérent de responsabilité : **la fiabilité structurelle**². Empruntée au vocabulaire des sciences de l'ingénieur, cette notion exprime la capacité d'un système à préserver sa cohérence fonctionnelle et sa sécurité opérationnelle malgré les sollicitations et les aléas auxquels il est soumis. Transposée au champ juridique, elle devient un principe normatif imposant à tout acteur d'une architecture numérique distribuée une obligation de stabilité, de transparence et de continuité du système, applicable au premier chef à la blockchain et plus largement aux technologies dites « *boîte noire* »³, au rang desquelles figurent les systèmes d'intelligence artificielle.

Il importe à ce stade de préciser le statut juridique reconnu à cette notion. La fiabilité structurelle, telle qu'élaborée dans la présente étude, n'est ni un *régime de responsabilité autonome* qui se substituerait aux branches existantes du droit positif (le présent essai n'entend ni refonder le droit des obligations, ni supplanter le régime de la responsabilité civile), ni un simple *outil d'interprétation* réductible à l'application littérale d'une disposition existante. Elle est un **concept sui generis**, doté d'une logique normative propre, élaboré à partir d'une transposition fonctionnelle du raisonnement civiliste de la garantie décennale du droit belge de la construction. Sur le plan fonctionnel, elle opère comme **principe directeur** du droit des systèmes distribués ; sur le plan textuel, elle trouve dans l'article 5.71 du nouveau Code civil⁴, qui oblige le débiteur à toutes les suites que la loi, la bonne foi ou les usages donnent à l'obligation d'après sa nature et sa portée, un point d'ancrage positif décisif qui la rend opératoire à droit constant.

Le choix de l'article 5.71 comme siège textuel de l'obligation appelle une justification, dans la mesure où d'autres dispositions auraient pu être envisagées. L'article 5.83 du Code civil (sanctions de l'inexécution imputable) suppose préalablement identifié le contenu de l'obligation dont l'inexécution

²La notion de « fiabilité structurelle » (structural reliability) est principalement constituée en sciences de l'ingénieur dans le domaine du génie civil et mécanique. La présente étude la transpose au champ numérique en s'appuyant sur l'analogie fonctionnelle avec la notion informatique de « dependability », qui désigne la propriété générale d'un système à délivrer un service auquel on peut légitimement se fier et regroupe les attributs de fiabilité, disponibilité, sûreté, intégrité et maintenabilité (v. J.-C. LAPRIE (éd.), *Dependability: Basic Concepts and Terminology*, Springer-Verlag, Dependable Computing and Fault-Tolerant Systems, vol. 5, 1992 ; A. AVIZIENIS, J.-C. LAPRIE, B. RANDELL et C. LANDWEHR, « Basic Concepts and Taxonomy of Dependable and Secure Computing », *IEEE Transactions on Dependable and Secure Computing*, vol. 1, n° 1, 2004, p. 11-33). La constitution juridique du concept procède d'une transposition fonctionnelle du raisonnement civiliste de la garantie décennale, dont la présente étude propose la systématisation.

³L'expression « boîte noire » désigne tout système technique dont les entrées et les sorties sont observables, mais dont le fonctionnement interne est soit techniquement opaque, soit juridiquement inaccessible, soit intellectuellement inintelligible pour l'utilisateur ou le tiers concerné. Sur la notion appliquée au droit, v. F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015 ; J. BURRELL, « How the machine 'thinks': Understanding opacity in machine learning algorithms », *Big Data & Society*, vol. 3, n° 1, 2016. En doctrine francophone belge, sur l'opacité algorithmique et la « gouvernementalité algorithmique », v. A. ROUVROY et T. BERNIS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, vol. 177, n° 1, 2013, p. 163-196 ; Y. POULLET, *La vie privée à l'heure de la société du numérique*, Larcier, 2019.

⁴Art. 5.71 du Code civil (Livre 5, loi du 28 avril 2022, M.B., 1er juillet 2022, en vigueur depuis le 1er janvier 2023) : « Le contrat oblige non seulement à ce qui y est convenu, mais encore à toutes les suites que la loi, la bonne foi ou les usages lui donnent d'après sa nature et sa portée ». Cet article reprend, en substance, la solution de l'ancien article 1135.

est sanctionnée ; il est un point d'aval, non d'amont, du raisonnement. Les articles 6.5 et 6.6, qui codifient la faute aquilienne, gouvernent le terrain extracontractuel mais ne déterminent pas, à eux seuls, le contenu obligationnel imposé au prestataire dans la relation contractuelle qui l'unit à son client. Quant aux anciens articles 1792 et 2270, transposés par analogie, ils fournissent un modèle conceptuel mais n'ont pas vocation à régir directement les contrats portant sur des systèmes informatiques. L'article 5.71 occupe une position singulière : il prescrit que toute prestation contractuelle est augmentée des suites que la loi, la bonne foi ou les usages donnent à l'obligation d'après *sa nature et sa portée*. Or, lorsqu'un prestataire propose un service blockchain (conception d'un smart contract, développement d'un protocole, fourniture d'une infrastructure de validation, conservation de crypto-actifs), la fiabilité technique du système qu'il met sur le marché n'est pas un accessoire négociable : elle est de l'essence même de la prestation promise. Un système dépourvu de fiabilité structurelle n'est pas un système moins performant ; c'est un système qui ne remplit pas sa fonction. La fiabilité structurelle est donc, au sens de l'article 5.71, une suite naturelle de la nature de la prestation. Cet ancrage présente un double avantage doctrinal : il rend l'obligation opératoire à droit constant, sans intervention législative préalable ; et il en module le contenu en fonction de la prestation effectivement promise, ce qui préserve la flexibilité nécessaire à un domaine technologique en évolution rapide.

La présente étude entend démontrer que cette fiabilité structurelle peut constituer le socle d'un régime cohérent de responsabilité numérique, fonctionnellement analogue à l'exigence de solidité de l'ouvrage consacrée par les anciens articles 1792 et 2270 du Code civil belge. Elle propose ainsi une transposition méthodique des mécanismes éprouvés du droit belge de la construction au domaine émergent des systèmes distribués, en vue d'établir un cadre de responsabilité adapté aux spécificités de l'économie du code⁵.

Avant d'aborder les développements qui suivent, une précision méthodologique s'impose. Le concept de fiabilité structurelle, tel qu'élaboré dans la présente étude, est conçu comme un **principe transversal** applicable à l'ensemble des architectures numériques distribuées dont la fiabilité technique conditionne la sécurité des utilisateurs ou des tiers : systèmes blockchain au premier rang, mais également systèmes d'intelligence artificielle (singulièrement ceux à haut risque au sens du Règlement (UE) 2024/1689), infrastructures algorithmiques opaques, plateformes automatisées et, plus largement, technologies dites « *boîte noire* » caractérisées par l'asymétrie informationnelle entre le concepteur et le bénéficiaire. Si l'analyse qui suit se concentre principalement sur la blockchain, c'est à titre *illustratif et paradigmatique* : la blockchain présente, à un degré particulièrement aigu, l'ensemble des traits qui appellent la mobilisation du concept (irréversibilité des opérations validées, dimension collective et systémique du risque, dispersion des responsabilités entre acteurs techniques, économiques et institutionnels), et constitue de ce fait le terrain d'expérimentation privilégié de la doctrine ici proposée. Les développements méthodologiques, conceptuels et normatifs élaborés à son propos ont vocation à se déployer, *mutatis mutandis*, à toutes les architectures numériques distribuées partageant les mêmes traits structurels, ainsi que la Partie III du présent article s'attachera à le démontrer.

L'analyse procédera en trois temps. Il conviendra d'abord d'établir les fondements conceptuels de la fiabilité structurelle comme nouvelle exigence de confiance dans l'économie numérique décentralisée (I). Il s'agira ensuite de démontrer comment cette notion peut servir de fondement à un régime de responsabilité des acteurs des architectures distribuées, illustré par le cas de la blockchain (II). Enfin,

⁵Sur l'analogie entre code et architecture normative, v. L. LESSIG, *Code: Version 2.0*, Basic Books, 2006.

seront examinées les conditions d'effectivité de cette garantie de fiabilité structurelle dans le contexte normatif européen actuel, ainsi que la portée transversale du concept aux technologies « boîte noire » (III). Au sein de cette analyse seront également abordées l'articulation avec la directive (UE) 2024/2853 sur la responsabilité du fait des produits défectueux et avec le retrait de la proposition AILD, le contrôle des clauses exonératoires et abusives, ainsi que les questions d'identification des acteurs responsables dans les architectures distribuées.

I. La fiabilité structurelle : une nouvelle exigence de confiance dans l'économie numérique décentralisée

A. De la confiance institutionnelle à la stabilité technologique

Le modèle classique de sécurisation des opérations et des décisions juridiques repose sur l'intervention de tiers de confiance : institutions bancaires pour les paiements, notaires pour l'authenticité des actes, autorités publiques pour la certification. Ces intermédiaires tirent leur légitimité d'une délégation institutionnelle qui fonde leur pouvoir de certification et engage leur responsabilité⁶. La blockchain, qui constitue le terrain d'application paradigmatique de la présente étude, propose un modèle radicalement différent : elle déplace la confiance, naguère placée dans la responsabilité d'un tiers institutionnel identifié, vers un protocole technique réputé infalsifiable, conçu et opéré par des acteurs identifiables qui en répondent à un autre titre. Cette mutation, dont la blockchain a été le déclencheur historique, soulève toutefois une question de portée plus large, qui se retrouve, à des degrés divers, dans toutes les technologies dites « *boîte noire* » (systèmes d'intelligence artificielle, infrastructures algorithmiques, plateformes automatisées) : comment articuler la responsabilité juridique avec l'autonomie technique d'un système ?

Cette mutation ne saurait abolir la question de la responsabilité ; elle la déplace. L'autonomie technique du système, aussi avancée soit-elle, ne supprime pas le fait qu'il a été conçu, développé, déployé et exploité par des acteurs humains ou des organisations identifiables. La confiance ne disparaît pas ; elle change de nature et d'objet : elle ne porte plus sur la probité d'un intermédiaire institutionnel, mais sur la robustesse d'une architecture. Loin d'évincer la responsabilité humaine, cette translation la reformule : l'acteur humain ne répond plus comme tiers de confiance institutionnelle, il répond désormais comme garant de la fiabilité structurelle du système qu'il a conçu, déployé ou exploité.

B. De l'intégrité technique à la notion juridique de fiabilité

Le concept de fiabilité structurelle trouve son origine dans les sciences de l'ingénieur, où il désigne la capacité d'une structure à résister aux contraintes et sollicitations auxquelles elle est soumise tout en maintenant sa fonction essentielle dans des conditions de sécurité acceptables. Appliquée aux systèmes informatiques distribués, cette notion se décompose en trois dimensions interdépendantes : l'*intégrité technique* (conformité du code et immunité aux altérations), la *cohérence fonctionnelle* (alignement entre les effets produits par le système et les intentions juridiques qu'il est censé matérialiser), et la *résilience opérationnelle* (capacité de continuité du service en cas d'incident).

Transposée au domaine juridique, la fiabilité structurelle acquiert une dimension normative : elle fonde une véritable obligation pesant sur les concepteurs et exploitants d'architectures numériques distribuées (systèmes blockchain au premier rang, mais aussi systèmes d'intelligence artificielle et

⁶Sur la transformation de la confiance par la technologie, v. K. WERBACH, *The Blockchain and the New Architecture of Trust*, MIT Press, 2018.

autres technologies « boîte noire »). Cette obligation comporte plusieurs volets : une obligation de conception conforme aux standards de sécurité reconnus⁷, une obligation de documentation permettant l'auditabilité du système, et une obligation de gouvernance assurant la maîtrise des causes prévisibles de défaillance.

La fiabilité structurelle devient ainsi une qualité juridique implicite attachée à toute architecture numérique distribuée destinée à un usage transactionnel ou décisionnel, comparable à la solidité exigée d'un ouvrage en droit belge de la construction, analogie dont la pertinence sera développée en Partie II.

C. Un principe transversal de gouvernance et de conformité

La fiabilité structurelle ne concerne pas seulement les développeurs initiaux du code ; elle irrigue l'ensemble de la chaîne de valeur des architectures numériques distribuées. Dans l'écosystème blockchain, qui constitue le terrain d'application principal de la présente étude, elle s'impose aux prestataires de services sur crypto-actifs (PSCA au sens du règlement MiCA)⁸, aux auditeurs de sécurité, aux administrateurs de protocoles et aux opérateurs d'infrastructure, chacun à la mesure de son intervention dans le système. Mais cette logique se déploie tout aussi bien, *mutatis mutandis*, dans les écosystèmes de l'intelligence artificielle (fournisseurs, déployeurs, intégrateurs, distributeurs au sens du Règlement (UE) 2024/1689) et dans les infrastructures logicielles critiques.

Cette transversalité se traduit par une pluralité d'obligations corrélatives : audits réguliers, maintenance continue et veille sécuritaire au plan technique⁹ ; diligence dans la conception, transparence documentaire et loyauté informationnelle au plan juridique ; prudence dans le déploiement et réactivité dans la correction des failles au plan déontologique.

II. La fiabilité structurelle comme fondement d'un régime de responsabilité des acteurs de la blockchain

A. La transposition fonctionnelle du modèle du constructeur

Le droit belge de la construction a consacré, dans la continuité du Code civil de 1804, un régime de responsabilité des constructeurs dont les anciens articles 1792 et 2270 du Code civil constituent le fondement. Ce régime repose sur un postulat simple : celui qui édifie un ouvrage destiné à durer répond de sa solidité pendant une période de dix ans à compter de l'agrément des travaux, délai suffisant pour que les vices de conception ou d'exécution puissent se révéler. L'ancien article 1792 du Code civil dispose ainsi que « si l'édifice construit à prix fait périclite en tout ou en partie par le vice de la construction, même par le vice du sol, les architecte et entrepreneur en sont responsables pendant dix ans ». Ce régime, d'ordre public, exclut toute renonciation ou exonération contractuelle, caractéristique transposable à la fiabilité structurelle (v. infra, II.D). La loi du 31 mai 2017 (Peeters-Borsus) a imposé à tous les acteurs de la construction une obligation d'assurance couvrant leur responsabilité décennale, modèle dont la transposabilité au numérique sera examinée en Partie III.B.

⁷V. notamment les standards ISO/IEC 25010 (qualité des systèmes et logiciels), ISO/IEC 27001:2022 (sécurité de l'information) et ISO 22739:2024 (blockchain — vocabulaire, 2^e édition abrogeant ISO 22739:2020).

⁸Art. 59 et s. du règlement (UE) 2023/1114 (MiCA) ; en droit belge, loi du 11 décembre 2025 mettant en œuvre le règlement (UE) 2023/1114 (MiCA) et le règlement (UE) 2023/1113 (TFR), M.B., 24 décembre 2025, entrée en vigueur le 3 janvier 2026.

⁹OWASP, Smart Contract Top 10: 2026, OWASP Smart Contract Security (SCS) Project, 2026, disponible sur scs.owasp.org/sctop10/ ; voir également, sur les exigences de vérification associées, OWASP, Smart Contract Security Verification Standard (SCSVS), disponible sur owasp.org/www-project-smart-contract-security-verification-standard/.

La transposition de ce modèle au domaine de la blockchain présente une pertinence fonctionnelle évidente. Comme l'ouvrage immobilier, le système blockchain constitue une infrastructure collective dont la stabilité conditionne la sécurité de multiples utilisateurs. Comme le constructeur, le développeur de smart contracts et le prestataire d'infrastructure blockchain conçoivent et déploient des systèmes dont ils maîtrisent (ou sont censés maîtriser) les caractéristiques techniques et les conditions de fonctionnement.

La blockchain présente en outre une caractéristique qui renforce la pertinence de l'analogie : elle constitue un ouvrage collectif au sens où chaque acteur de l'écosystème contribue, par son intervention, à la sécurité ou à la vulnérabilité de l'ensemble. La fiabilité structurelle devient ainsi le pivot d'une responsabilité partagée mais ordonnée, où chaque intervenant répond de la stabilité de sa partie du système, dans la mesure de sa contribution à l'ouvrage commun.

B. Vers une garantie de stabilité et de sécurité du code

Sur le modèle de la responsabilité décennale, une garantie de fiabilité structurelle applicable aux systèmes blockchain pourrait s'articuler autour de *quatre obligations cardinales*, correspondant aux phases successives de la vie du système.

La première obligation concerne la *conception fiable* du système. Elle impose au développeur de fournir une documentation complète et intelligible du code, de soumettre celui-ci à des audits indépendants préalables au déploiement, et d'assurer sa conformité aux standards de sécurité reconnus (normes ISO applicables aux systèmes d'information, recommandations sectorielles de l'OWASP, exigences prudentielles du règlement MiCA¹⁰). Cette obligation de conception s'apprécie au regard de l'état de l'art au moment du développement, selon un standard de diligence professionnelle. La même exigence se retrouve, *mutatis mutandis*, dans les autres architectures numériques distribuées que la régulation européenne traite spécifiquement¹¹.

La deuxième obligation porte sur la *stabilité dans le temps* du système déployé. Elle comprend la maintenance corrective (résolution des bugs et failles de sécurité identifiés), la maintenance évolutive (adaptation aux évolutions de l'environnement technique), et la continuité des fonctions critiques (notamment la gestion des clés cryptographiques et des mécanismes de gouvernance dans les systèmes blockchain ; la gestion des modèles et des données d'entraînement dans les systèmes d'intelligence artificielle ; la disponibilité opérationnelle dans les infrastructures cloud critiques). Cette obligation de stabilité s'étend sur une durée déterminée, qui pourrait être calquée sur le modèle décennal ou adaptée aux cycles de vie propres à chaque technologie. Elle trouve un écho direct dans le système de gestion de la qualité couvrant l'ensemble du cycle de vie consacré à l'article 17 du Règlement (UE) 2024/1689 pour les systèmes d'IA à haut risque, ainsi que dans les exigences de continuité opérationnelle posées par le règlement DORA pour les entités financières.

La troisième obligation concerne la *gouvernance transparente* du système. Elle exige l'identification claire des responsables techniques et décisionnaires, la traçabilité des modifications apportées au code après déploiement, et la mise en place d'une supervision interne permettant de

¹⁰Règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs (MiCA), JOUE L 150, 9 juin 2023, art. 68 sur les exigences prudentielles.

¹¹Pour les systèmes d'intelligence artificielle à haut risque, art. 9 du Règlement (UE) 2024/1689 (système de gestion des risques continu sur l'ensemble du cycle de vie) et art. 15 (niveau approprié de précision, robustesse et cybersécurité). Pour les infrastructures cloud critiques, règlement DORA (tests de résilience et audit régulier de la sécurité opérationnelle).

détecter et de réagir aux incidents de sécurité. Cette obligation s'inscrit dans le cadre plus général des exigences de gouvernance posées par le règlement DORA pour les entités financières¹², et trouve sa traduction sectorielle dans les obligations de transparence (article 13) et de contrôle humain (article 14) imposées par le Règlement (UE) 2024/1689 aux fournisseurs de systèmes d'IA à haut risque. Sa portée concrète varie selon la technologie¹³.

La quatrième obligation, *la clôture responsable*, organise la fin de vie du système et préserve les intérêts des utilisateurs au-delà de son exploitation active. Elle comprend la planification documentée de la migration des actifs, la conservation des preuves et journaux d'exécution, et la prise en charge des opérations résiduelles (clôture des comptes, restitution des dépôts, archivage des contrats). Trop souvent négligée dans la pratique blockchain, cette obligation prend une importance particulière dans les protocoles à durée de vie incertaine ou dans les hypothèses d'abandon de projet, où la défaillance de la clôture peut générer des pertes irréversibles pour les utilisateurs.

L'acuité de cette obligation se manifeste dans trois configurations typiques : l'*abandon silencieux* du projet, le *rug pull* partiel ou total, et la *fin de support* d'une *layer 2* ou d'une infrastructure de validation¹⁴. Dans chacune, le manquement à l'obligation de clôture engage la responsabilité du prestataire défaillant au sens des articles 5.83 et suivants du Code civil.

C. Responsabilité en cas de défaillance technique ou d'erreur de smart contract

La question de l'imputation des dommages résultant d'une défaillance technique constitue le cœur du régime de responsabilité à construire. Traditionnellement, la responsabilité du fait des choses, désormais consacrée par l'article 6.16 du Code civil belge (qui a remplacé l'ancien article 1384, alinéa 1er, sans intervention législative préalable), a pu être proposée comme fondement de la responsabilité du fait des algorithmes. Toutefois, cette approche présente des limites dans le cas des systèmes blockchain, où la défaillance peut résulter de causes multiples et imbriquées — erreur de conception du code, faille dans un oracle externe, défaut de maintenance, ou encore manipulation malveillante — et où l'identification d'un gardien unique de la chose au sens de l'article 6.16 se heurte à la dispersion des interventions techniques.

La fiabilité structurelle offre un critère d'imputation plus adapté à cette complexité. Elle permet de déterminer, pour chaque type de défaillance, l'acteur dont le manquement à l'obligation de fiabilité a causé ou contribué au dommage. L'imputation s'apprécie alors selon le rôle de chaque intervenant dans le système et la nature de son obligation.

¹²Règlement (UE) 2022/2554 (DORA), art. 5 et s. sur la gouvernance et la gestion des risques ; règlement délégué (UE) 2025/532 de la Commission du 2 juillet 2025 complétant DORA sur les conditions de sous-traitance de fonctions critiques ou importantes par les entités financières.

¹³Dans les systèmes blockchain, la gouvernance transparente impose la traçabilité des modifications du smart contract et l'identification des détenteurs de clés administratives ; dans les systèmes d'IA, elle exige la documentation des choix de conception, l'explicabilité des décisions automatisées et la garantie d'un contrôle humain effectif ; dans les infrastructures cloud critiques, elle impose la traçabilité des changements de configuration et la documentation des chaînes de sous-traitance.

¹⁴L'abandon silencieux désigne la situation où les fondateurs cessent toute maintenance, les oracles tombent en désuétude et les interfaces deviennent inopérantes, alors même que le contrat intelligent reste formellement actif et que les actifs des utilisateurs y demeurent immobilisés ; la clôture responsable imposerait, dès la conception, l'inclusion d'une procédure documentée de migration ou de retrait d'urgence. Le *rug pull*, partiel ou total, désigne la liquidation organisée par les promoteurs à leur seul profit ; la clôture responsable y appelle une asymétrie protectrice : préavis raisonnable et faculté de retrait égale aux fondateurs. La fin de support d'une *layer 2* ou d'une infrastructure de validation appelle des dispositifs documentés de migration des actifs vers la *layer 1* et une période transitoire suffisante.

Sur le plan contractuel, le prestataire de services blockchain répond envers son client du défaut de fiabilité du système qu'il a fourni, selon les règles désormais codifiées aux articles 5.83 et suivants du Code civil belge (sanctions de l'inexécution imputable) et 5.86 et suivants (réparation du dommage), qui ont remplacé l'ancien article 1147. Cette responsabilité peut être aménagée par des clauses de niveau de service (SLA) définissant les performances attendues et les conditions d'engagement de la garantie. La qualification du contrat (prestation de services, vente de logiciel, licence d'utilisation) détermine le régime applicable et l'étendue des obligations de garantie, notamment au regard du vice caché¹⁵.

Sur le plan extracontractuel, le concepteur ou l'exploitant d'un système blockchain peut voir sa responsabilité engagée envers les tiers lésés par une défaillance technique, sur le fondement des articles 6.5 et 6.6 du Code civil belge (qui ont remplacé les anciens articles 1382 et 1383)¹⁶. La faute s'apprécie alors au regard du manquement à l'obligation de fiabilité structurelle : conception non conforme aux standards, défaut de maintenance, absence de réaction appropriée à une faille connue.

D. Le sort des clauses exonératoires et abusives

L'effectivité du régime suppose de tenir compte des clauses qui prétendraient en restreindre la portée. Dans toutes les architectures numériques distribuées, les conditions générales des prestataires multiplient les clauses exonératoires et limitatives, souvent rédigées sur le modèle anglo-saxon¹⁷. Ces clauses doivent désormais être confrontées à l'article 5.89 du Code civil¹⁸, qui codifie le régime de la clause exonératoire de responsabilité. Le principe demeure celui de la validité : les parties peuvent convenir d'une clause exonérant le débiteur, en tout ou en partie, de sa responsabilité contractuelle ou extracontractuelle, fût-ce pour faute lourde, à condition que cette exonération soit expresse et ne se présume pas. L'article 5.89, § 1er, énonce toutefois trois limites impératives qui circonscrivent étroitement la portée de telles clauses dans le contentieux des architectures distribuées.

Premièrement, sont réputées non écrites les clauses qui exonèrent le débiteur (ou une personne dont il répond) de sa *faute intentionnelle*. Cette règle, héritée de la jurisprudence belge constante, prohibe par exemple la clause par laquelle un développeur entendrait s'exonérer des conséquences d'une porte dérobée intentionnellement insérée dans le code, ou d'un mécanisme caché de captation de fonds activable par les fondateurs. *Deuxièmement*, sont également réputées non écrites les clauses qui exonèrent d'une faute *causant une atteinte à la vie ou à l'intégrité physique d'une personne*. Cette limitation, inédite dans son explicitation textuelle, prend une portée concrète à l'heure où les systèmes blockchain s'intègrent dans des dispositifs sensibles : registres de santé, traçabilité des dispositifs médicaux, identités numériques régaliennes, chaînes d'approvisionnement pharmaceutiques. Une faille de fiabilité ayant entraîné une atteinte à l'intégrité physique ne saurait être couverte par une clause

¹⁵Anciens art. 1641 et s. du Code civil belge (en vigueur dans l'attente du Livre 7).

¹⁶Articles 5.83 et s. (sanctions de l'inexécution) et 5.86 et s. (réparation du dommage) du Code civil (Livre 5, loi du 28 avril 2022, en vigueur depuis le 1er janvier 2023), qui ont remplacé l'ancien art. 1147. Pour la responsabilité extracontractuelle, art. 6.5 et 6.6 (Livre 6, loi du 7 février 2024, en vigueur depuis le 1er janvier 2025), qui ont remplacé les anciens art. 1382 et 1383. Sur l'articulation des deux régimes, art. 6.3, § 1er, qui rompt avec la jurisprudence dite « Stuwadoor » ou « L'Arrimeur » (Cass., 7 décembre 1973, Pas., 1974, I, p. 376, concl. Premier avocat général MAHAUX) consacrant la quasi-immunité des agents d'exécution.

¹⁷Les conditions générales empruntent souvent au modèle anglo-saxon des clauses « as is » ou « no warranty » et des limitations à un montant symbolique. On les rencontre dans les conditions d'utilisation des plateformes blockchain, dans les contrats de fourniture d'intelligence artificielle (limitations sur les erreurs de classification, biais algorithmiques ou réponses incorrectes des modèles génératifs), et dans les contrats cloud (limitations de disponibilité, exonérations en cas de défaillance technique majeure).

¹⁸Art. 5.89 du Code civil. Sont notamment réputées non écrites : (i) les clauses exonérant de la faute intentionnelle ; (ii) celles exonérant d'une faute causant une atteinte à la vie ou à l'intégrité physique ; (iii) toute clause vidant le contrat de sa substance.

d'exonération, fût-elle stipulée entre opérateurs professionnels avertis. *Troisièmement*, et c'est sans doute la limite la plus opératoire pour notre matière, est réputée non écrite « *la clause qui vide le contrat de sa substance* ». Cette consécration légale, qui codifie une jurisprudence ancienne de la Cour de cassation, joue un rôle décisif dans le contentieux blockchain : une clause d'exonération qui priverait l'obligation de fiabilité structurelle de toute portée (par exemple en exonérant le développeur de tout vice de conception du code, qui constitue pourtant l'objet même de sa prestation), serait frappée d'inopposabilité. La fiabilité, parce qu'elle est de l'essence de la prestation au sens de l'article 5.71, ne peut être contractuellement abolie sans que la clause concernée vide le contrat de sa substance.

E. Les trois régimes coexistants des clauses abusives

Au contrôle de l'article 5.89 s'ajoute, pour certains contrats, un contrôle des clauses abusives. Trois régimes coexistent en droit belge, dont les domaines d'application respectifs et les sanctions méritent d'être distingués¹⁹.

Le premier est le régime *B2C*, organisé par les articles VI.83 à VI.86 du Code de droit économique pour les contrats conclus entre une entreprise et un consommateur. Il combine une liste noire (vingt-trois clauses réputées abusives en toutes circonstances) et un standard général prohibant toute clause créant un déséquilibre manifeste entre les droits et obligations des parties au détriment du consommateur. Dans le contentieux blockchain, ce régime trouve à s'appliquer aux contrats des plateformes d'échange grand public, des prestataires de portefeuilles non hébergés (dans les rapports *B2C*) et des services délégués destinés aux particuliers. Une clause par laquelle le prestataire exclurait sa responsabilité pour défaut de sécurité du système (défaut qui constitue précisément l'attente légitime du consommateur) serait susceptible d'être qualifiée d'abusives et frappée de nullité, peu important sa rédaction soignée ou la qualité d'opérateur professionnel du prestataire.

Le deuxième régime est le régime *B2B*, introduit par la loi du 4 avril 2019 et codifié aux articles VI.91/3 à VI.91/6 du Code de droit économique. Conçu à l'origine comme un correctif aux déséquilibres entre grandes entreprises et PME, il s'est progressivement imposé comme un régime général applicable à tous les contrats entre entreprises, à l'exclusion des marchés publics et des matières financières spécifiques. Il combine, lui aussi, une liste noire et une liste grise, complétées par un standard général prohibant les clauses créant un déséquilibre manifeste. Ce régime trouve à s'appliquer aux contrats entre opérateurs professionnels de l'écosystème blockchain : conventions entre développeurs et plateformes d'échange, contrats d'audit de smart contracts, contrats de services d'infrastructure entre PSCA, conventions d'apport de liquidité entre teneurs de marché et protocoles. Sa portée est considérable, car il constitue le régime dans lequel s'inscrivent la grande majorité des relations contractuelles structurantes de l'écosystème.

Le troisième régime est le régime *résiduel* institué par l'article 5.52 du Code civil, qui interdit, à titre de droit commun, les clauses créant un déséquilibre manifeste entre les droits et obligations des

¹⁹ Articles VI.83 à VI.86 du Code de droit économique (clauses abusives *B2C*) ; articles VI.91/3 à VI.91/6 du Code de droit économique, introduits par la loi du 4 avril 2019 (clauses abusives *B2B*), M.B., 24 mai 2019 ; article 5.52 du Code civil (régime résiduel). La liste noire *B2B* (art. VI.91/4 CDE) prohibe irréfragablement : 1° l'engagement irrévocable de l'autre partie alors que l'exécution dépend de la seule volonté de l'entreprise ; 2° le droit unilatéral d'interpréter le contrat ; 3° la renonciation à tout recours en cas de conflit ; 4° la reconnaissance irréfragable de l'adhésion à des clauses non effectivement portées à la connaissance de la partie. La liste grise *B2B* (art. VI.91/5 CDE) présume abusives, sauf preuve contraire, huit catégories de clauses, notamment celles autorisant la modification unilatérale du prix ou des caractéristiques du contrat, la prorogation tacite sans préavis raisonnable, le déséquilibre dans la répartition du risque économique, et la libération de la responsabilité pour faute grave de l'entreprise.

parties dans les contrats qui ne relèvent ni du B2C ni du B2B au sens des dispositions précitées du Code de droit économique. Cet article appréhende notamment les contrats entre consommateurs (C2C) et certaines configurations atypiques de l'économie collaborative, fréquentes dans l'univers blockchain (échanges entre particuliers via interface décentralisée, prêts inter-utilisateurs, jeux en ligne tokenisés). Il joue ainsi un rôle de filet doctrinal, comblant les interstices laissés par les régimes spéciaux. L'articulation de ces trois contrôles, combinée à celui de l'article 5.89, conduit à un constat opératoire : les clauses qui prétendraient anéantir la portée de l'obligation de fiabilité structurelle disposent en droit belge d'un espace très étroit. Cela renforce considérablement l'effectivité du concept proposé, en garantissant que la fiabilité, parce qu'elle est de l'essence de la prestation, ne puisse être contractuellement abolie sans que la clause concernée soit frappée d'invalidité ou réputée non écrite.

F. Concours des responsabilités, protection des auxiliaires et solidarité

Le nouveau Livre 6 a, par ailleurs, profondément modifié le régime du concours de responsabilités. L'article 6.3, § 1er, du Code civil rend désormais applicables, sauf clause contraire, les règles de la responsabilité extracontractuelle entre cocontractants, rompant avec la jurisprudence de quasi-immunité issue de l'arrêt du 7 décembre 1973. Cette innovation a une portée considérable pour notre matière : elle ouvre aux victimes d'une défaillance blockchain la possibilité de cumuler, dans les limites posées, les fondements contractuel et extracontractuel ; elle autorise les actions directes contre les auxiliaires (développeurs sous-traitants, mandataires techniques, prestataires d'audit, organes décisionnaires d'une plateforme) ; et elle ouvre, dans le rapport principal, la voie à des actions extracontractuelles directes contre les développeurs initiaux du protocole, par-delà la chaîne contractuelle qui les sépare des utilisateurs finaux.

Cette ouverture est cependant tempérée par le mécanisme de protection des auxiliaires institué par l'article 5.89, § 2, du Code civil. Selon cette disposition, les auxiliaires bénéficient désormais d'une double protection : ils peuvent invoquer contre le créancier principal la clause d'exonération valablement convenue avec le débiteur principal, ce qui rétablit, dans une certaine mesure, l'écran que le nouvel article 6.3 avait fait sauter en autorisant les actions extracontractuelles directes. Cette articulation invite à une rédaction soignée des clauses contractuelles dans les chaînes de prestataires technologiques : la clause d'exonération stipulée entre la plateforme et son auditeur de smart contracts, valable au regard de l'article 5.89, sera opposable à l'utilisateur final qui agirait directement contre l'auditeur sur le fondement de l'article 6.3 du Code civil.

G. L'identification des responsables dans les architectures distribuées

Reste l'objection la plus exigeante adressée à toute construction de ce type : qui est le débiteur de l'obligation lorsque l'architecture est totalement décentralisée ? Si le concept de fiabilité structurelle suppose un débiteur identifié de l'obligation, comment l'appliquer à un protocole sans personnalité juridique, sans direction effective, sans propriétaire ? L'objection est sérieuse, mais elle ne ruine pas la construction proposée ; elle en circonscrit le domaine d'application et appelle un examen différencié des configurations possibles. Cette difficulté est, en effet, largement *graduelle* plutôt qu'absolue, ce qu'une typologie sommaire des architectures blockchain démontre.

Les blockchains *permissioned* reposent sur des consortiums identifiés et sur des opérateurs personnellement responsables ; l'imputation y suit les voies du droit commun et ne soulève aucune difficulté particulière. Les blockchains *permissionless* présentent une structure plus diffuse, mais

comportent toujours, à divers stades de la chaîne, des acteurs identifiables : développeurs des clients de référence, opérateurs de pools de minage ou de validation, plateformes d'échange centralisées, fournisseurs d'oracles, opérateurs de réseaux secondaires, interfaces utilisateurs qui donnent accès au protocole²⁰. Seul un sous-ensemble, celui des protocoles « véritablement décentralisés », pose une difficulté irréductible, et encore : cette catégorie est elle-même plus mince qu'on ne le prétend généralement, ainsi qu'on le verra.

Pour structurer l'imputation dans les configurations identifiables, l'article 8 de la directive (UE) 2024/2853 fournit une grille opérationnelle particulièrement éclairante, transposable *mutatis mutandis* en droit belge interne. Cette disposition désigne comme responsables, dans un ordre subsidiaire : en premier lieu, le fabricant ou le développeur du composant logiciel défectueux ; à défaut d'établissement dans l'Union, l'importateur ou le mandataire ; à défaut, le prestataire de services d'exécution des commandes ; à défaut enfin, le distributeur ou le fournisseur de plate-forme en ligne ayant joué un rôle actif dans la mise sur le marché²¹. Cette logique permet d'articuler ce que l'on peut nommer une *chaîne de responsabilité ordonnée, contributive et différenciée*. Elle est *ordonnée*, parce qu'elle suit un ordre subsidiaire d'imputation qui privilégie l'acteur le plus proche de la conception et descend la chaîne en cas d'inaccessibilité du précédent ; elle est *contributive*, parce que chaque maillon répond à hauteur de sa contribution effective à la fiabilité globale et non d'une responsabilité indifférenciée ; elle est *différenciée*, parce qu'elle s'apprécie en fonction du périmètre de diligence propre à chaque acteur (le développeur du protocole de base ne répond pas du même standard que l'opérateur d'un nœud de validation, ni que la plateforme d'interface utilisateur).

Cette grille fonctionnelle se déploie au-delà de la seule blockchain, et s'applique transversalement aux autres architectures numériques distribuées. Pour les *systèmes d'intelligence artificielle*, elle se traduit dans la chaîne de valeur organisée par l'article 25 du Règlement (UE) 2024/1689 : fournisseur initial du système (responsable principal), déployeur (responsable de l'usage conforme et de la supervision humaine), importateur, distributeur, intégrateur ; chacun répond à hauteur de son intervention dans la chaîne de fiabilité, selon une logique remarquablement parallèle à celle exposée pour la blockchain. Pour les *infrastructures cloud critiques*, la directive NIS 2 et le règlement DORA articulent une logique comparable : opérateur essentiel (responsable principal), prestataires tiers de services TIC (responsables contributifs sous le régime DORA), sous-traitants critiques. Pour les *plateformes algorithmiques opaques*, la chaîne se compose du développeur de l'algorithme, de l'opérateur de la plateforme, et des intermédiaires qui en distribuent les services. Dans tous ces cas, la chaîne de responsabilité ordonnée, contributive et différenciée fournit une grille unificatrice, qui transforme la diversité des écosystèmes en une logique imputative commune fondée sur le rôle effectif de chaque acteur dans la fiabilité globale du système.

L'illusion d'une décentralisation totale doit être maniée avec prudence. La Banque des règlements internationaux a relevé, dans ses travaux de 2021 et 2022, ce qu'elle qualifie d'« illusion of decentralization » : la quasi-totalité des protocoles présentés comme entièrement décentralisés

²⁰Pour les blockchains permissioned, v. par ex. Hyperledger, Quorum, Corda. Pour les blockchains permissionless, v. par ex. Bitcoin (fondation Bitcoin Core) et Ethereum (Ethereum Foundation). Les réseaux secondaires (layer 2) construits sur la chaîne sous-jacente (layer 1), et les interfaces utilisateurs (frontends) hébergées par des opérateurs identifiables, complètent la chaîne d'acteurs.

²¹Art. 8 de la directive (UE) 2024/2853 : sont responsables, dans un ordre subsidiaire, le fabricant ou développeur du composant logiciel défectueux ; à défaut, l'importateur établi dans l'Union ; à défaut, le mandataire ; à défaut, le prestataire de services d'exécution des commandes ; à défaut, le distributeur ou la plateforme en ligne ayant joué un rôle actif.

conservent, en pratique, des points de centralité opérationnelle qui constituent autant d'ancrages pour l'imputation. On peut en énumérer cinq : les détenteurs majoritaires de jetons de gouvernance (qui répondent de leurs décisions au sens de l'article 6.6 du Code civil) ; les équipes de développement actives, qui contrôlent les clés de mise à jour ; les multisignatures administratives, par lesquelles un nombre réduit d'opérateurs conservent la maîtrise effective de fonctions critiques (mise en pause d'urgence, gestion de la trésorerie, déploiement de mises à jour) ; les oracles centralisés, dont la défaillance entraîne des conséquences systémiques ; et les interfaces utilisateurs, qualifiables de PSCA au sens du règlement MiCA lorsqu'elles sont opérées par des acteurs identifiés. Ces cinq points d'ancrage se traduisent, sur le plan de l'action en responsabilité, en quatre voies subsidiaires — les équipes de développement actives et les multisignatures administratives étant respectivement absorbées par la voie fabricant (voie 4) et par la voie détenteurs majoritaires (voie 2) exposées ci-après.

Pour le résidu réellement décentralisé, c'est-à-dire l'hypothèse-limite des protocoles dont aucun des acteurs précédents ne peut être personnellement identifié (par exemple un protocole DeFi entièrement gouverné par une DAO, sans personne morale émettrice ni intermédiaire commercial), le règlement MiCA, conscient de cette difficulté, exclut expressément de son champ d'application les services « *entièrement décentralisés et sans intermédiaire* » (cons. 22 et art. 2, § 4). Cette exclusion ne signifie pas l'absence de tout recours pour les utilisateurs : quatre voies subsidiaires d'action conservent leur portée²². Première voie, la responsabilité des *interfaces utilisateurs* qui donnent accès au protocole décentralisé, généralement qualifiables de PSCA au sens du règlement MiCA. Deuxième voie, la responsabilité des *détenteurs majoritaires de jetons de gouvernance* en application de l'article 6.6 du Code civil. Troisième voie, la responsabilité des *oracles et auditeurs externes* pour manquement à leurs obligations professionnelles. Quatrième voie, la responsabilité des *fabricants de logiciels* au sens de la directive (UE) 2024/2853, qui institue une responsabilité objective indépendante de la preuve de la faute. Ces quatre voies, sans résoudre intégralement la difficulté du résidu véritablement décentralisé, en réduisent significativement la portée pratique.

Reste, pour les configurations exceptionnelles où aucune de ces voies ne permettrait l'imputation, le chantier de la *reconnaissance juridique des collectifs de gouvernance*, à l'image de l'évolution déjà engagée dans certains États américains²³. Cette évolution, qui exigerait une intervention du législateur belge ou européen, permettrait d'attribuer à un protocole décentralisé une personnalité juridique fonctionnelle débitrice de l'obligation de fiabilité structurelle, sans renoncer pour autant à la logique de gouvernance distribuée.

²²Première voie : les interfaces utilisateurs, opérées par un acteur identifié, sont soumises aux obligations prudentielles, de gouvernance et d'information attachées à leur qualification de PSCA ; voie particulièrement opératoire, la quasi-totalité des accès grand public aux protocoles DeFi passant par des interfaces hébergées. Deuxième voie : la responsabilité aquilienne des détenteurs majoritaires de jetons de gouvernance suppose la démonstration d'une décision fautive ayant causé le dommage, adoptée par un vote dans lequel ces détenteurs disposent d'une influence prépondérante. Troisième voie : les oracles, qui acheminent les données externes nécessaires à l'exécution du protocole, et les auditeurs de smart contracts répondent selon les règles du droit commun de la responsabilité du prestataire. Quatrième voie : la directive (UE) 2024/2853 doit être transposée au plus tard le 9 décembre 2026 ; combinée à la cascade de son article 8, elle ouvre aux victimes une voie d'action indépendante de la preuve de la faute.

²³Sur l'« illusion of decentralization » dans les protocoles DeFi, v. S. ARAMONTE, W. HUANG et A. SCHRIMPF, « DeFi risks and the decentralisation illusion », BIS Quarterly Review, décembre 2021, p. 21-36, qui forme l'origine littérale de l'expression ; v. également R. AUER, J. FROST et J. M. VIDAL PASTOR, « Miners as intermediaries: extractable value and market manipulation in crypto and DeFi », BIS Bulletin n° 58, 16 juin 2022. Pour la reconnaissance juridique des collectifs de gouvernance dans certaines législations américaines : Wyoming, Decentralized Autonomous Organization Supplement, signed into law on March 21, 2021 ; Vermont, Blockchain-Based Limited Liability Company, 30 V.S.A. § 4173. Le règlement MiCA exclut expressément de son champ les services « entièrement décentralisés et sans intermédiaire » (cons. 22 et art. 2, § 4).

Enfin, en cas de défaillance combinée (lorsque le dommage résulte de la conjonction d'une erreur humaine et d'un défaut structurel), le régime de la responsabilité solidaire (art. 6.31 et s. du Code civil) permet au demandeur d'agir contre l'ensemble des responsables, à charge pour ceux-ci de régler entre eux la contribution définitive à la dette de réparation. Cette mécanique, bien rodée en droit belge, constitue un instrument décisif dans le contexte d'une chaîne de prestations technologiques où l'imputation univoque est rarement possible. Combinée à l'ouverture du concours par l'article 6.3, elle renforce considérablement la portée pratique des actions exercées par les victimes d'une défaillance blockchain, en leur permettant d'agir contre l'acteur le plus solvable de la chaîne, charge à ce dernier de se retourner contre les autres responsables au stade de la contribution.

III. Les conditions d'effectivité de la garantie de fiabilité structurelle et sa portée transversale

A. Les critères techniques et contractuels de la fiabilité structurelle

La fiabilité structurelle appelle une définition précise de ses critères d'appréciation. Sur le plan technique, ces critères se mesurent à trois niveaux complémentaires : la robustesse du code, évaluée par des métriques de qualité logicielle et des tests de résistance et d'intrusion ; la résilience de l'infrastructure, appréciée au regard de sa capacité à maintenir ses fonctions essentielles en cas de sollicitation anormale ou d'attaque ; la traçabilité des opérations, permettant l'audit *a posteriori* des opérations effectuées et des modifications du système.

Sur le plan contractuel, la fiabilité structurelle se traduit par l'insertion de clauses spécifiques dans les contrats liant les acteurs de l'écosystème blockchain : clauses de fiabilité (performances attendues et seuils de tolérance), clauses d'auditabilité (accès du client ou d'un tiers certificateur au code source et à la documentation), clauses de notification d'incident (obligation d'information en cas de faille), clauses de réversibilité (conditions de reprise du système ou de migration). Ces outils remplissent une double fonction : ils organisent la preuve du manquement à l'obligation de fiabilité, et ils définissent les modalités de la réparation en cas de défaillance avérée.

B. Les mécanismes d'assurance et de gouvernance du risque technologique

Comme en droit de la construction, la garantie de fiabilité structurelle doit être relayée par des mécanismes d'assurance et de certification permettant d'en assurer la solvabilité et la crédibilité. L'exemple de la loi Peeters-Borsus, qui a généralisé l'obligation d'assurance décennale à l'ensemble des acteurs de la construction en Belgique, démontre la faisabilité d'un tel dispositif. Trois mécanismes complémentaires peuvent être envisagés pour l'écosystème blockchain. L'*assurance de code et d'exploitation* couvre les dommages résultant d'une défaillance technique du système, qu'elle procède d'un vice de conception ou d'une erreur d'exploitation ; son développement suppose une standardisation des critères d'évaluation du risque et une mutualisation suffisante. La *certification de fiabilité*, délivrée par des organismes certificateurs indépendants, permettrait aux utilisateurs d'identifier les systèmes conformes aux standards reconnus, sur le modèle des labels existants en sécurité de l'information (ISO 27001, SOC 2). La *supervision institutionnelle*, enfin, concerne les prestataires critiques dont la défaillance pourrait avoir des conséquences systémiques, et s'inscrit dans le cadre des compétences attribuées aux autorités nationales (en Belgique, la FSMA et la BNB) et européennes par les règlements MiCA et DORA.

C. Inscription dans le paysage normatif européen : MiCA, DORA, NIS 2, DAC 8 et la directive (UE) 2024/2853

La notion de fiabilité structurelle s'inscrit dans le mouvement de régulation européenne des technologies numériques, dont les règlements MiCA, DORA, la directive NIS 2 et la directive DAC 8 (étendant la coopération administrative fiscale aux crypto-actifs) constituent les jalons structurants²⁴. Ces textes, distincts dans leurs objets, convergent vers une exigence commune : la résilience opérationnelle des systèmes numériques²⁵. MiCA impose aux prestataires de services sur crypto-actifs des exigences prudentielles incluant gouvernance, gestion des risques et continuité d'activité ; DORA étend ces exigences à l'ensemble du secteur financier en matière de résilience numérique ; NIS 2 élargit le cercle des entités soumises à des obligations de cybersécurité et renforce les exigences de notification des incidents ; DAC 8 instaure pour les prestataires de services sur crypto-actifs des obligations de diligence, de collecte et de transmission d'informations à fin fiscale, dont la traçabilité présuppose la fiabilité structurelle des systèmes employés.

À ces instruments s'ajoutera, à compter du 9 décembre 2026, le régime rénové de la responsabilité du fait des produits défectueux issu de la directive (UE) 2024/2853, qui abroge la directive 85/374/CEE et opère une refonte substantielle adaptée aux technologies numériques contemporaines²⁶. Cette directive procède d'une logique radicalement distincte de celle de la fiabilité structurelle : là où nous proposons une exigence de *comportement* pesant sur le prestataire (obligation positive de diligence dans la conception, le déploiement et la maintenance du système, dont l'inexécution est sanctionnée par les régimes contractuel et extracontractuel ordinaires), la directive institue une responsabilité *objective* du producteur, indépendante de toute faute, fondée sur le seul fait de la défectuosité d'un produit mis en circulation. La nouveauté décisive du texte de 2024 est l'inclusion expresse, dans la notion de « *produit* », des logiciels et des systèmes d'intelligence artificielle, ainsi que des mises à jour et services connexes. Le même régime s'appliquera donc, à compter de la transposition, aux algorithmes d'IA et, sous réserve de certaines limites tenant à l'open source non commercial, aux logiciels distribués dans le cadre d'une activité commerciale, ce qui couvre une large part des composants logiciels mobilisés par les architectures distribuées.

Le contraste avec notre construction est éclairant et permet d'établir leur *complémentarité*, non leur concurrence. La directive 2024/2853 vise à indemniser des personnes physiques victimes pour des dommages corporels, matériels (biens à usage privé) ou, innovation du texte, psychologiques médicalement reconnus, ainsi que pour la destruction ou corruption de données non professionnelles. Elle relève d'une logique d'exposition au risque : le fabricant qui met une technologie sur le marché en assume les conséquences dommageables à l'égard des tiers victimes, indépendamment de toute faute. La fiabilité structurelle, telle que nous la concevons, gouverne au contraire un terrain que la directive ne couvre pas : celui des *rapports contractuels* entre prestataires et bénéficiaires professionnels (relations B2B structurantes de l'écosystème blockchain), ainsi que celui des actions en responsabilité extracontractuelle *inter partes* désormais ouvertes par l'article 6.3 du Code civil. La directive 2024/2853 et la fiabilité structurelle conjuguent ainsi deux logiques distinctes mais complémentaires : la première

²⁴Directive (UE) 2022/2555 du 14 décembre 2022 (NIS 2), JOUE L 333, 27 décembre 2022, transposée en droit belge par la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, M.B., 17 mai 2024, en vigueur le 18 octobre 2024 ; Directive (UE) 2023/2226 du 17 octobre 2023 (DAC 8), JOUE L, 24 octobre 2023, applicable depuis le 1er janvier 2026.

²⁵Cons. 1 du règlement DORA.

²⁶Directive (UE) 2024/2853 du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE, JOUE L, 18 novembre 2024 ; délai de transposition : 9 décembre 2026. La notion de « produit » englobe désormais les logiciels et systèmes d'IA (art. 4, point 1 ; cons. 13 et 18).

offre une protection objective aux victimes-tiers personnes physiques ; la seconde organise les obligations comportementales dans la chaîne contractuelle de l'écosystème.

D. Enseignements du retrait de la proposition AILD

Le retrait, en 2025, de la proposition de directive sur l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (proposition dite AILD)²⁷, n'est pas anodin pour notre propos. Cette proposition entendait spécifiquement adapter les règles de responsabilité civile aux systèmes d'IA, en allégeant la charge de la preuve par une présomption réfragable de causalité et par un mécanisme de divulgation forcée des éléments techniques. Son retrait, motivé par l'absence d'accord prévisible entre les institutions européennes et par le contexte de simplification réglementaire post-rapport Draghi, laisse subsister un vide doctrinal : la réparation des dommages causés par les systèmes d'IA repose désormais, en droit de l'Union, principalement sur la directive 2024/2853 (responsabilité objective du producteur, à l'égard des seules personnes physiques victimes) et, pour le surplus, sur les régimes nationaux de responsabilité contractuelle et extracontractuelle.

Ce vide donne à notre construction une portée renforcée. Faute d'instrument européen spécifique sur la responsabilité IA, les juridictions belges devront, pour les contentieux qui ne relèvent pas de la directive produits défectueux, mobiliser les ressources du droit civil interne. La grille d'interprétation par la fiabilité structurelle, adossée à l'article 5.71 du Code civil et déclinée selon les régimes contractuel (articles 5.83 et s.) et extracontractuel (articles 6.5 et 6.6), fournit alors un instrument doctrinal opérationnel. Elle permet d'articuler la responsabilité du prestataire d'IA avec les exigences techniques opposables résultant du Règlement (UE) 2024/1689, lesquelles deviennent autant de *règles de l'art* dont le manquement caractérise la faute au sens de l'article 6.6 du Code civil. Le retrait d'AILD, paradoxalement, donne ainsi à la doctrine nationale (et singulièrement à la doctrine belge) une opportunité doctrinale précieuse : celle de proposer un cadre civil interne capable de répondre aux défis de la responsabilité IA sans attendre une harmonisation européenne dont l'horizon s'éloigne.

Cette construction n'est, par ailleurs, pas circonscrite à la seule blockchain. Sa logique est *structurale* : dès lors que la prestation principale d'un contrat consiste à fournir une technologie dont la fiabilité conditionne la sécurité de l'utilisateur ou de tiers, l'article 5.71 du Code civil impose au prestataire une obligation implicite de robustesse, indépendamment du substrat technologique concret. Cette logique trouve à s'appliquer à toute technologie dont la complexité interne dépasse l'intelligibilité immédiate de l'utilisateur, technologies que la doctrine désigne couramment par l'expression de « *boîte noire* » : systèmes d'intelligence artificielle au premier chef, mais également objets connectés grand public, plateformes algorithmiques opaques, infrastructures cloud critiques. Toutes ces technologies partagent une même caractéristique fonctionnelle : l'opacité du système pour le bénéficiaire et la maîtrise technique exclusive du fournisseur. C'est cette asymétrie structurelle qui appelle une obligation correspondante de fiabilité pesant sur le prestataire.

Si la présente étude se concentre sur la blockchain, ce n'est pas que la fiabilité structurelle s'y limiterait, mais parce que cette technologie présente des traits aggravants qui justifient un traitement prioritaire : l'irréversibilité des opérations validées (la transaction ne peut être annulée par un tiers), la

²⁷ Proposition de directive sur l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (« AILD »), COM(2022) 496 final, 28 septembre 2022. Retrait inscrit au Programme de travail de la Commission pour 2025, COM(2025) 45 final, 11 février 2025, annexe IV.

dimension collective et systémique du risque (une faille affecte simultanément l'ensemble des utilisateurs du protocole, et peut produire des effets en chaîne sur des protocoles dépendants), la dispersion des responsabilités entre acteurs techniques, économiques et institutionnels souvent multi-juridictionnels. Sur ces trois points, la blockchain conjugue à un degré particulièrement aigu ces traits, ce qui justifie qu'elle constitue le terrain d'expérimentation privilégié de la doctrine ; l'extension aux systèmes d'IA — qui présentent des configurations de risque comparables, notamment pour ceux qualifiés à haut risque au sens du Règlement (UE) 2024/1689 — s'en trouve doctrinalement d'autant plus légitime. Mais l'extension du concept à ces derniers est non seulement possible, elle est doctrinalement souhaitable, et elle est même empiriquement préfigurée par le législateur européen lui-même.

Il importe toutefois de circonscrire avec rigueur le domaine d'efficacité de la fiabilité structurelle. On peut, à titre de première systématisation, distinguer trois présupposés fonctionnels dont la réunion paraît commander l'applicabilité du concept à une architecture numérique distribuée donnée. Premièrement, l'existence d'une asymétrie informationnelle structurelle entre le concepteur et le bénéficiaire, telle que ce dernier ne peut, par ses propres moyens, vérifier la fiabilité technique du système. C'est cette asymétrie qui justifie l'obligation pesant sur le concepteur. Deuxièmement, le caractère critique de la fiabilité technique pour la sécurité de l'utilisateur ou des tiers, qui élève l'exigence au rang d'obligation principale et non d'accessoire négociable. Troisièmement, la possibilité d'identifier au moins un acteur dans la chaîne de fiabilité, qui rend l'obligation imputable et confère au régime son effectivité. Lorsque ces trois présupposés se trouvent réunis, la fiabilité structurelle paraît se déployer sans difficulté, ainsi qu'il en va dans la grande majorité des architectures rencontrées en pratique : blockchains permissioned et permissionless, protocoles DeFi (par les voies subsidiaires d'action exposées plus haut), systèmes d'intelligence artificielle, infrastructures cloud critiques, plateformes algorithmiques. Pour le résidu marginal des architectures véritablement décentralisées dont aucun acteur identifiable ne peut être atteint (hypothèse rare en pratique, ainsi que l'a démontré l'analyse de l'illusion de décentralisation en II.G), les deux premiers présupposés demeurent satisfaits, mais le troisième fait défaut : le concept appellerait alors une intervention législative complémentaire (reconnaissance juridique des collectifs de gouvernance, sur le modèle des évolutions américaines précitées). Cette circonscription, dont le développement théorique systématique dépasse le cadre du présent article et relève d'une étude doctrinale plus ample, n'affaiblit pas la doctrine ; elle en garantit l'opérationnalité dans la quasi-totalité des configurations concrètes, tout en identifiant honnêtement le périmètre où une évolution du droit positif s'imposerait pour en achever le déploiement.

E. Vocation transversale aux technologies « boîte noire » et convergence avec le Règlement (UE) 2024/1689

Sans nommer le concept de fiabilité structurelle ni en revendiquer la filiation, le législateur européen, dans le Règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act), a imposé aux fournisseurs de systèmes d'IA à haut risque des obligations cardinales qui, sur le plan analytique, transposent au champ sectoriel de l'IA les quatre piliers articulés ci-dessus pour les architectures numériques distribuées. Cette concordance n'est ni accidentelle, ni purement rhétorique : elle révèle qu'un principe directeur, élaboré à partir du raisonnement civiliste de la garantie décennale, articule une logique normative que le législateur européen a, par voie sectorielle et sans en avoir formulé la doctrine d'ensemble, implicitement épousée pour les systèmes d'intelligence artificielle.

La correspondance s'établit point par point. La *conception fiable* trouve son écho dans les obligations de *gestion des risques* (article 9, qui impose un système de gestion continu sur l'ensemble du cycle de vie) et de *robustesse, exactitude et cybersécurité* (article 15). La *stabilité dans le temps* se reflète dans le *système de gestion de la qualité* couvrant l'ensemble du cycle de vie consacré à l'article 17, ainsi que dans les obligations de conservation des journaux et de surveillance post-commercialisation (articles 12 et 26). La *gouvernance transparente* se déploie dans les exigences de *transparence* et de *fourniture d'information* aux déployeurs (article 13) ainsi que dans l'obligation de *contrôle humain* (article 14). La *clôture responsable* se reconnaît dans les obligations générales des fournisseurs (article 16, incluant coopération avec les autorités, conservation de la documentation technique, mesures correctives) ainsi que dans la *chaîne de responsabilités tout au long de la chaîne de valeur* organisée par l'article 25, qui répartit les obligations entre fournisseurs, déployeurs, importateurs et distributeurs selon une logique remarquablement proche de la chaîne ordonnée, contributive et différenciée exposée plus haut.

La doctrine ici proposée, autonome dans sa filiation et plus large dans sa portée, n'est ni dérivée de l'AI Act ni anticipée par lui ; elle constitue une formulation systématique d'un principe que le législateur européen a, par une voie sectorielle autonome, implicitement épousé. La fiabilité structurelle apparaît ainsi comme un *dénominateur commun* entre des technologies hétérogènes (blockchain, intelligence artificielle, objets connectés, infrastructures cloud critiques), instrument méthodologique d'unification du raisonnement juridique sur les technologies « *boîte noire* », dont la blockchain ne constitue qu'un cas d'application particulièrement aigu parmi d'autres.

Conclusion

La fiabilité structurelle, concept sui generis et principe directeur élaboré par transposition fonctionnelle de la garantie décennale et ancré sur l'article 5.71 du nouveau Code civil, exprime la maturité juridique du numérique décentralisé : les infrastructures technologiques, aussi sophistiquées soient-elles, demeurent des créations humaines dont la défaillance engage la responsabilité de leurs concepteurs et exploitants. Ce principe n'entrave pas l'innovation ; il l'encadre et la rend juridiquement durable. Articulé avec les régimes contractuel et extracontractuel codifiés aux Livres 5 et 6 du Code civil, il offre aux utilisateurs des architectures distribuées une protection comparable à celle dont bénéficient les maîtres d'ouvrage, tout en préservant la flexibilité nécessaire à un domaine en évolution rapide.

La transposition fonctionnelle du droit belge de la construction aux technologies blockchain ne constitue pas un archaïsme : elle témoigne de la capacité du droit à adapter ses catégories éprouvées aux défis inédits de l'économie numérique. C'est à cette condition que la blockchain (et plus largement les technologies « *boîte noire* », en ce compris les systèmes d'intelligence artificielle) pourra devenir un espace de responsabilité aussi sûr que de liberté. La consécration de la fiabilité structurelle comme concept sui generis et standard normatif ici proposé, appelée à acquérir, par sa diffusion progressive, le statut de principe général du droit, appelle désormais un travail doctrinal et jurisprudentiel d'approfondissement. Il appartiendra à la pratique contractuelle, à la régulation sectorielle et, le cas échéant, au législateur national ou européen, de préciser les contours de ce régime et d'en assurer l'effectivité.