



Livre Blanc

AVRIL 2026

La Blockchain :

Un outil de confiance numérique

Enjeux et perspectives

ACN

Alliance pour la confiance numérique ■ ■

Edito



Philippe Latombe

Député de la 1^{ère} circonscription
de la Vendée

Blockchain : transformer la défiance en opportunité

En rédigeant ces quelques mots, je ne peux m'empêcher de penser à ce propos de Warren Buffett : « La plupart des gens ne comprennent pas vraiment ce qu'est la blockchain, mais ils en parlent quand même ». Plus que toute autre innovation technologique contemporaine, la blockchain appelle en effet une acculturation suffisante pour qui tente de l'aborder avec pertinence.

À cette difficulté s'ajoute un certain discrédit pour cette nouvelle technologie, une mauvaise réputation née de scandales, de dérives spéculatives, de limites techniques encore importantes ou de besoins énergétiques immenses, qui lui ont d'ailleurs valu les critiques de Bill Gates lui-même. Dès ses débuts, la blockchain a, pour son malheur, été associée à des activités illégales. L'utilisation de cryptomonnaies sur des plateformes comme Silk Road, par exemple, a elle aussi contribué à forger une image négative, liant cette technologie à des pratiques de blanchiment ou de trafic.

Par ailleurs, un développement rapide de son usage sans évaluation des risques a favorisé de nombreuses dérives spéculatives. La volatilité des cryptomonnaies et la multiplication des escroqueries ont renforcé la méfiance. L'effondrement de la plateforme FTX qui illustre ces excès, a profondément marqué l'opinion publique. Aussi la blockchain est-elle souvent vue comme un espace peu régulé, propice aux abus.

Toutefois, cette perception ne doit surtout pas occulter son réel potentiel. La blockchain apparaît ainsi comme une technologie prometteuse, quoi que, encore immature, dont l'avenir dépendra de sa capacité à dépasser les critiques et à s'inscrire dans des usages concrets et maîtrisés. C'est d'ailleurs pour toutes ces raisons qu'elle doit s'imposer au politique et au législateur comme un sujet majeur de réflexion et d'étude.

Les fondements techniques d'un système de confiance

Cette technologie repose sur un principe fondamental : celui d'un registre distribué, infalsifiable et transparent, partagé entre différents acteurs sans autorité centrale. Techniquement, elle s'appuie sur des mécanismes de consensus, tels que la preuve de travail (*Proof of Work*) ou la preuve d'enjeu (*Proof of Stake*), qui permettent de valider les transactions de manière sécurisée. Chaque bloc de données, lié cryptographiquement au précédent, constitue une chaîne immuable, garantissant l'intégrité des informations. Des réseaux comme Bitcoin ou Ethereum illustrent concrètement cette architecture.

Mais au-delà de ces fondements techniques, la blockchain pose des questions politiques majeures. Elle remet en cause le rôle traditionnel des tiers de confiance, banques, notaires, institutions publiques, en permettant des échanges directs, automatisés et vérifiables via des "smart contracts".

Les applications en sont nombreuses. Un travailleur expatrié peut aujourd'hui transférer des fonds à sa famille en quelques minutes, avec des frais réduits, sans passer par les circuits bancaires classiques. De même, dans le secteur de l'assurance, un contrat intelligent peut déclencher automatiquement une indemnisation en cas de retard d'un vol, sans intervention humaine. Cette désintermédiation, si elle ouvre des perspectives d'efficacité, soulève également des enjeux de responsabilité juridique, en cas de dysfonctionnement.

Le législateur se trouve ainsi face à un double impératif. D'une part, il doit accompagner l'innovation, en offrant un cadre juridique clair et attractif pour les entreprises et les porteurs de projets. D'autre part, il lui revient de prévenir les dérives : blanchiment, fraude, spéculation excessive ou encore atteintes à la vie privée. L'équilibre est délicat. Une régulation trop stricte risquerait d'étouffer un écosystème en pleine émergence ; une absence de règles créerait un vide propice aux abus.

Des usages concrets en pleine expansion

En attendant, les applications concrètes de la blockchain se multiplient et illustrent l'urgence de cette réflexion. Dans l'industrie agroalimentaire, par exemple, elle permet de tracer un produit de la ferme au consommateur, facilitant l'identification rapide de la source en cas de crise sanitaire. Dans le domaine des services publics, une identité numérique fondée sur cette technologie pourrait offrir aux citoyens un accès sécurisé et souverain à leurs données, réduisant les risques de piratage massif liés aux bases centralisées.

Dans la sphère financière, l'essor de la finance décentralisée (DeFi) permet déjà à des particuliers d'emprunter ou de prêter des actifs, sans passer par une institution bancaire, sur la base d'algorithmes transparents. Parallèlement, les jetons non fongibles (NFT) redéfinissent la propriété numérique : des artistes peuvent vendre des œuvres certifiées uniques, tout en percevant des revenus automatiques lors de chaque revente. Ces innovations interrogent donc directement nos cadres juridiques existants, qu'il s'agisse du droit de la consommation, du droit financier ou du droit d'auteur.

Blockchain et intelligence artificielle : une convergence stratégique

L'articulation entre blockchain et intelligence artificielle ouvre des perspectives particulièrement structurantes. L'un des défis majeurs de l'intelligence artificielle réside dans la traçabilité : comprendre l'origine des données utilisées pour entraîner les modèles, retracer les modifications apportées, et garantir l'intégrité des processus décisionnels. La blockchain peut apporter une réponse concrète à ces enjeux.

En enregistrant de manière immuable les différentes étapes du cycle de vie d'un modèle d'IA, collecte des données, entraînement, mises à jour, décisions produites la blockchain permet de constituer un véritable "journal de confiance". Une administration publique ou une entreprise peut ainsi auditer un algorithme, vérifier l'origine des données et s'assurer qu'aucune altération frauduleuse n'est intervenue. Cette capacité de traçabilité est essentielle pour répondre aux exigences croissantes de transparence, notamment dans des domaines sensibles comme la santé, la justice ou la finance.

Alors que l'intelligence artificielle soulève de nombreux enjeux autour des données et des modèles utilisés, une symbiose entre intelligence artificielle et blockchain peut renforcer la responsabilité des acteurs. En rendant chaque étape vérifiable, la blockchain facilite en effet l'attribution des responsabilités en cas de biais, d'erreur ou de dommage causé par un système automatisé. Elle constitue ainsi un levier puissant pour construire une intelligence artificielle de confiance, conforme à nos exigences démocratiques et juridiques.

Former pour maîtriser la révolution blockchain

Face à ce développement rapide et à cette ambivalence, une exigence s'impose avec force, celle de la formation. Il est impératif d'intégrer sans délai la blockchain et ses usages dans les formations professionnelles, initiales comme continues. Juristes, ingénieurs, fonctionnaires, acteurs financiers ou encore responsables publics doivent acquérir une compréhension opérationnelle de cette technologie. Il serait judicieux, par exemple, que son étude soit inscrite au programme de la nouvelle école des douanes qui va ouvrir à Lille.

Former, c'est aussi garantir que les citoyens, les entreprises et les administrations puissent s'approprier ces outils en toute confiance, en maîtrisant leurs opportunités comme leurs risques. Cela vaut pour les parlementaires : un législateur qui comprend les mécanismes techniques est mieux à même d'élaborer des normes adaptées, proportionnées et efficaces. Sans cet effort collectif, le risque est double : voir se creuser un fossé entre innovation et régulation, et dépendre (encore et encore) de compétences et de solutions développées hors de nos frontières.

Des enjeux de souveraineté et de choix de société

Car la blockchain interroge notre conception même de la souveraineté. À l'heure où les données deviennent une ressource stratégique, le développement de blockchains publiques, privées ou hybrides pose la question du contrôle des infrastructures numériques. Certains envisagent même son utilisation pour des systèmes de vote électronique, capables de garantir la transparence d'un scrutin, tout en soulevant des défis considérables en matière de secret du vote et de cybersécurité.

Ainsi, la blockchain n'est pas seulement une innovation parmi d'autres. Elle est un révélateur de nos choix de société. En tant que représentants de la Nation, nous autres, parlementaires avons la responsabilité de l'encadrer avec lucidité, ambition et pragmatisme mais aussi de préparer dès aujourd'hui les compétences qui permettront de la comprendre et de la maîtriser.

« *What is real ? How do you define real ?* », dit Morpheus dans The Matrix. Au fond, cette question reste étonnamment actuelle : qu'est-ce qui fait foi dans un monde saturé de systèmes invisibles ? La blockchain n'apporte pas une réponse philosophique, mais une réponse technique : la confiance ne dépend plus d'un centre, elle se construit collectivement, dans un réseau où chacun peut vérifier les règles du jeu. Entre illusion et transparence, elle dessine peut-être une nouvelle manière de définir ce qui est réel, non plus comme ce que l'on nous dit de croire, mais comme ce que nous pouvons tous constater.

Table des matières

Résumé :	7
Introduction	9
I. Panorama des marchés blockchain et opportunités de développement	19
I.1 Une architecture en couches au cœur de la création de valeur.....	20
I.2 Infrastructures blockchain : un marché stratégique encore en structuration	22
I.3 Finance numérique, tokenisation et nouveaux instruments de valeur	23
I.4 Blockchain et services de confiance numérique.....	26
I.5 Traçabilité, industrie et chaînes de valeur.....	27
I.6 Blockchain publique, privée.....	28
Conclusion I : Comprendre les marchés avant la souveraineté	32
II. La France et l'Europe faceauxenjeuxde souveraineté numérique de la blockchain ...	33
II.1 La blockchain comme enjeu de souveraineté numérique.....	34
II.2 Une dépendance croissante aux infrastructures extra-européennes.....	35
II.3 Blockchain et confiance numérique : un enjeu politique	36
II.4 Le rôle central de l'État dans la structuration de l'écosystème.....	38
II.5 Une approche européenne fondée sur la régulation et l'interopérabilité	44
Conclusion II : Un choix politique structurant	49
III. Cas d'usage de la blockchain : applications techniques et opérationnelles	50
III.1 Identité numérique et gestion des droits.....	51
III.2 Registres, certification et valeur probante.....	52
III.3 Traçabilité des chaînes de valeur et passeports numériques.....	52
III.4 Finance, paiements, enquêtes et automatisation des processus	54
III.5 Traçabilité de l'énergie, décarbonation, compensation carbone	55
III. 6 Partage de données et interopérabilité entre acteurs	62
Conclusion III : Des usages au service d'une stratégie cohérente	64
Conclusion :	65
Remerciements	68
A propos de l'ACN :	69

Lexique

Terme	Traduction	Définition
Bloc		Structure de données incluant des transactions, contenant un en-tête avec notamment une structure d'empreintes cryptographiques garantissant l'intégrité de son contenu, et une référence au bloc précédent.
Blockchain/ Chaîne de blocs	Blockchain	Suite de transactions organisées en blocs successifs reliés cryptographiquement depuis le bloc « genèse » au bloc le plus récent.
Blockchain privée	Private Blockchain	Une blockchain est privée lorsque son usage est réservé à des utilisateurs autorisés.
Blockchain publique	Public Blockchain	Une blockchain est publique lorsque tout le monde peut l'utiliser sans aucune autorisation préalable.
Blockchain permissionnée	Permissioned Blockchain	Une blockchain est permissionnée lorsque les participants au consensus sont des acteurs connus et autorisés selon le mode de gouvernance de la blockchain. Une blockchain permissionnée peut se limiter à un seul acteur disposant de plusieurs dispositifs participant au consensus.
Blockchain Non- permissionnée	Permissionless Blockchain	Une blockchain est non permissionnée lorsque tout le monde peut participer au consensus, sans aucune autorisation préalable.
Bloc génèse	Genesis Block	Bloc initial, ou racine, de la chaîne de blocs.
Informatique en nuage	Cloud computing	Désigne la fourniture de services informatiques (serveurs, stockage, bases de données, logiciels, etc.) depuis des serveurs distants.

Consensus		Protocole d'accord des différents pairs du réseau participant au consensus sur le choix et le contenu du nouveau bloc qui est ajouté à la chaîne.
Consortium		Ensemble d'acteurs indépendants maintenant ensemble une blockchain permissionnée.
Crypto-actif		Actif numérique généré avec une technique cryptographique, qui est la représentation numérique d'un bien, d'une valeur ou d'un droit, enregistré sur une blockchain.
Crypto-monnaie	Currency	Monnaie numérique décentralisée.
Couche	Layer	Niveau de communication ou de service composant un système.
Contrat intelligent	Smart contract	Code informatique dont l'exécution, déclenchée par la réception d'une transaction, se déroule automatiquement sur un réseau distribué de pairs participant au consensus.
Finance décentralisée	DeFi	Système financier alternatif qui utilise la technologie blockchain et les smart contracts pour effectuer des transactions financières.
Jetons	Tokens	Actifs numériques gérés par des smart contracts, une couche applicative superposée à la blockchain.
Registre	Ledger	Suite de blocs chaînés cryptographiquement, formant la blockchain, partagé et répliqué entre tous les pairs du réseau distribué.
Jeton non fongible	Non-Fungible Token, NFT	Jeton numérique unique et infalsifiable, enregistré sur une blockchain, qui certifie la propriété et l'authenticité d'un actif numérique (œuvre d'art, musique, vidéo, etc) ou physique.

Protection des données dès la conception	Privacy-by-design	Principe d'intégration de mesure de sécurité permettant de protéger les données à caractère personnel (RGPD) dès la conception d'un produit ou d'un système.
Preuve d'enjeu	Proof-of-Stake	Mécanisme basé sur la mise initiale d'une certaine quantité de crypto-monnaie dans la blockchain pour participer au consensus.
Preuve de travail	Proof-of-Work	Mécanisme basé sur l'exécution d'un calcul intensif pour participer au consensus.
Stablecoins		Cryptomonnaie conçue pour maintenir une valeur stable indexé sur une devise traditionnelle (comme le dollars).
Jeton fongible	Fungible Token	Jeton numérique dont toutes les unités sont de même valeur et interchangeables.
Web3		Technologie, basée sur l'usage de la blockchain, qui décentralise la propriété, le paiement ou le contrôle d'accès.
XRP Ledger		Blockchain privée de consortium entre plusieurs banques, servant à l'échange de devises et aux paiements transfrontaliers.

Résumé

Ce texte est une analyse des **enjeux stratégiques, économiques et opérationnels** liés à la technologie blockchain. Il s'articule autour de trois axes majeurs : **le panorama des marchés blockchain**, les **défis de souveraineté numérique** pour la France et l'Europe, et les **cas d'usage concrets** illustrant son potentiel transformateur.

Le document décrypte la structuration des marchés blockchain, organisée en couches, et met en lumière les opportunités dans des secteurs clés comme la finance numérique, les services de confiance (identité numérique, registres infalsifiables), et la traçabilité industrielle (passeports numériques, lutte contre la contrefaçon). Les chiffres sont éloquentes : un marché mondial estimé à 393 milliards de dollars d'ici 2032, avec des segments comme la tokenisation d'actifs projetée à 18 900 milliards de dollars d'ici 2033.

Ce livre blanc aborde la souveraineté numérique comme un enjeu critique. Face à une dépendance croissante aux infrastructures extra-européennes, l'Europe doit renforcer sa maîtrise technologique et réglementaire. L'État a un rôle central à jouer, non seulement en tant que régulateur, mais aussi comme facilitateur d'écosystèmes de confiance, notamment dans des domaines régaliens comme la traçabilité des données ou la lutte contre la fraude. Le document illustre des cas d'usage opérationnels qui démontrent la maturité de la technologie.

Que ce soit pour l'identité numérique souveraine, la traçabilité des chaînes de valeur, ou l'automatisation des processus financiers, la blockchain se positionne comme un accélérateur de transparence et d'efficacité. Cependant, son adoption massive suppose de relever des défis comme l'interopérabilité, la gouvernance partagée, et l'alignement avec les cadres juridiques (RGPD, eIDAS 2).

Ce livre blanc souligne que la blockchain n'est plus une technologie émergente, mais un pilier stratégique pour l'économie numérique. Son déploiement réussi dépendra de la capacité des acteurs publics et privés à **articuler, innovation, régulation et souveraineté**, tout en répondant à des besoins concrets et mesurables.

Pour la France et l'Europe, l'enjeu est clair : transformer la blockchain en levier de puissance numérique, tout en préservant leur autonomie et leurs valeurs.

Introduction

Depuis plusieurs années, la blockchain occupe une place centrale dans les débats médiatiques et technologiques. Pourtant, la définir avec précision et en cerner les contours reste un exercice complexe. Il est tout aussi difficile d'illustrer, par des exemples concrets et percutants, les raisons pour lesquelles cette technologie suscite autant d'engouement et de controverses. Ce document ne prétend pas apporter une réponse exhaustive à ces questions, mais il s'inscrit dans une démarche collective, portée par l'Alliance pour la Confiance Numérique (ACN), visant à offrir une vision objective et actualisée de la blockchain.

L'objectif est double : clarifier les avantages clés de cette technologie en constante évolution et démontrer leur pertinence pour les gouvernements, les administrations, les entreprises et les particuliers. Notre approche se concentre sur les usages alignés avec la vocation de l'ACN, c'est-à-dire ceux qui renforcent la sécurité des systèmes numériques, la confiance dans l'information et la souveraineté numérique. Nous mettons également en lumière les applications qui améliorent l'efficacité du partage d'information, la collaboration et l'industrie. Ainsi, bien que les crypto-monnaies et les NFT soient souvent les premiers exemples cités par le grand public, ils ne seront abordés ici que pour compléter l'analyse, notre focus restant sur les innovations structurelles et durables.

Mais par ailleurs, il est nécessaire de montrer à quel point la blockchain est en passe de devenir un élément clé dans de multiples secteurs. La blockchain, comme premier protocole de confiance auto-suffisant, élimine les risques de falsification des données, de censure, de fraude ou de monopole.

Pour illustration, en 2025, 90 % des échanges mondiaux reposent encore sur des intermédiaires ; banques, États, géants du numérique. Mais il apparaît un profond bouleversement avec la mise en œuvre de la

blockchain. Alors que les États-Unis agissent : cette technologie n'est plus une option, mais un impératif stratégique pour notre autonomie.

Sur le front de la confiance dans la donnée, nécessaire à tout process technique ou économique, la blockchain est également en passe de devenir un agent essentiel de la collaboration, de la confiance dans les données et les informations, données, textes ou images, hors des travers initiaux de cette technologie encore en évolution permanente. Le Web3, porté par cette technologie, permettra de faire face aux enjeux critiques autour de ces problématiques.

Ce livre blanc vise à en décrypter les mécanismes, les modes d'usage, les marchés, et les leviers d'action.

*« Le Web3 est une révolution pour l'Europe,
une chance de devenir leader. »*

Jean-Noël BARROT, Ministre délégué à la Transition numérique, 2023

Pourtant, éclipsé par l'intelligence artificielle dans l'actualité récente, le Web3 reste une réalité bien vivante et en pleine expansion. Il incarne la promesse d'un Internet décentralisé, où les utilisateurs reprennent le contrôle de leurs données et de leurs avoirs en ligne, sans dépendre des géants du numérique. Après le Web 1.0, simple vitrine d'informations statiques, et le Web 2.0, marqué par l'avènement des réseaux sociaux et des plateformes centralisées, le Web3 propose une alternative radicale : un Internet où les données ne sont plus captées par quelques entreprises, mais gérées directement par les utilisateurs grâce à la **blockchain**. Cette technologie permet de sécuriser les échanges, d'automatiser les contrats appelés *smart contracts* et de créer des applications décentralisées, tout en garantissant transparence et résistance à la censure. Le marché du Web3, estimé à

3,2 milliards de dollars en 2024, devrait exploser pour atteindre plus de 49 milliards en 2034, tiré par une demande croissante de respect de la vie privée, de propriété des données et d'architectures décentralisées. Les entreprises, notamment dans la finance, la santé ou les médias, adoptent progressivement ces solutions pour limiter les risques de monopole, de failles de sécurité et de points uniques de défaillance. Les portefeuilles numériques, les NFT et les réseaux sociaux décentralisés illustrent cette tendance, offrant aux utilisateurs de nouvelles façons de monétiser leur présence en ligne et de participer à des communautés autonomes. Cependant, le Web3 se heurte encore à des obstacles majeurs : un manque de standardisation entre les différentes blockchains, une complexité technique qui freine l'adoption massive, et des problèmes d'évolutivité, avec des réseaux parfois saturés et coûteux. En France, près de 12 % des Français détiennent des crypto-actifs en 2024, et le pays ambitionne de devenir un hub européen du secteur, soutenu par des régulations comme MiCA et une volonté politique forte.

La blockchain est un pilier de confiance d'Internet et de la valeur, les technologies décentralisées, et en particulier la blockchain, redéfinissent les paradigmes de la confiance, de la sécurité et de la circulation de la valeur en ligne. La blockchain est un registre partagé, transparent et immuable, sans autorité centrale, qui sert de socle au Web3. Elle se décline en deux grandes familles.

D'une part, les **blockchains utilitaires**, majoritairement en *Proof-of-Stake* (Preuve d'enjeu, basée sur un mécanisme proche des parts détenues par les associés d'une société) ou contrôlées par un consortium, soutiennent des usages variés : identité numérique, traçabilité, Internet des objets, tokenisation et collaboration de confiance avec la mise en place de *smart contracts* (programmes informatiques infalsifiables exécutés par une blockchain). Ces blockchains, portées par des consortiums d'acteurs

identifiés et une gouvernance rigoureuse, sont une réponse efficace et robuste pour la collaboration de confiance, une confiance absolument nécessaire à la santé de nos systèmes économiques. Une condition forte à l'instauration de cette confiance repose sur la transparence de leur gouvernance et des modèles économiques sous-jacents. Ce bon usage de la blockchain doit reposer sur une infrastructure (serveurs, moyens d'accès, outils d'interaction) dont les porteurs, la gouvernance, les règles de fonctionnement et les modes de financement sont parfaitement connus et vérifiables.

D'autre part, **la finance décentralisée**, ou DeFi, s'appuie sur la blockchain pour supprimer les intermédiaires traditionnels comme les banques ou les courtiers, permettant aux utilisateurs de gérer, échanger et contrôler leurs actifs directement. Par exemple, la blockchain Bitcoin, basée sur le consensus *Proof-of-Work* (preuve de travail), offre une solution totalement autonome et inviolable pour échanger des actifs numériques. La preuve de travail rémunère la force de calcul mise en œuvre et indirectement l'énergie qu'il a fallu mettre en œuvre pour fournir cette force de calcul. Au 9 décembre 2025, la capitalisation totale du marché crypto s'élève à environ 3,18 trillions de dollars, avec un encours de valeur totale verrouillée dans la finance décentralisée (DeFi) oscillant entre 120 et 170 milliards de dollars. Les *stablecoins*, crypto-monnaies dont la valeur est peu spéculative car liée à un actif fiduciaire ou réel (comme le dollar ou l'or), représentent un encours d'environ 309 milliards de dollars. La tokenisation d'actifs (comme dans l'immobilier) est également une composante de la DeFi, elle repose sur la possession d'actifs matériels (part d'immeubles, ...) ou immatériels (obligations, fonds, ...) à travers des actifs numériques décentralisés.

1 Compilation : Statista, Forbes, Fortune Business Insights, Mordor Intelligence. **Finance = plus grand marché de la blockchain**

Domaines d'applications blockchain	Marché (Revenus) par domaine 2024*	Marché (Revenus) par domaine 2030*
Identité numérique	0,85 Md \$	6,8 Mds \$
IoT	0,77 Md \$	4,5 Mds \$
Smart contracts	1,9 Md \$	9,2 Mds \$
Tokenisation d'actifs	2,3 Mds \$	10,9 Mds \$
Lutte contre les contrefaçons	0,89 Md \$	14,9 Mds \$
Finance / Transferts / Stablecoins	20,5 Mds \$	231 Mds \$

Figure 1 : Compilation des domaines d'applications blockchain (Source : Orange)

Aux États-Unis, la réglementation sur les *stablecoins* adoptée en 2025 impose des réserves en actifs liquides et des exigences de transparence, renforçant la domination du dollar numérique, qui représente 99 % de la valeur en circulation des *stablecoins*. La tokenisation progresse également, avec des initiatives comme BlackRock BUIDL, qui dépasse 2,5 milliards de dollars d'encours, et les « *tokenized Treasuries* », qui atteignent plus de 9 milliards de dollars. Citi prévoit une émission de *stablecoins* entre 1,9 et 4 trillions de dollars d'ici 2030, avec un potentiel de flux annuels de 100 à 200 trillions de dollars.

Capitalisation Stablecoins : +300 Mds \$ de (2025)
Prévision 2030 : jusqu'à 3,7 billions \$ (JP Morgan)
Aussi, une étude du BCG en 2025 prévoit un marché à 18 900 Mds \$ prévus d'ici 2033 pour la Tokenisation
Sur cardano : +24 000 smart contracts en janvier 2024

Figure 2 : Prévision 203 de la capitalisation des stablecoins, 2026 (Source : Orange).

En Europe, le cadre réglementaire MiCA vise à harmoniser les règles pour les émetteurs et prestataires crypto, incluant les *stablecoins* assimilés à de la monnaie électronique. Les banques européennes accélèrent leurs initiatives, comme SG- FORGE, qui émet des *stablecoins* EURCV et USDCV,

soutenus par des infrastructures de marché avancées telles que SDX, Eurex Clearing et Euroclear. SWIFT intègre également un registre blockchain partagé pour améliorer les paiements interbancaires transfrontaliers. Les *stablecoins* jouent un rôle de pont entre la finance traditionnelle et le Web3, avec un encours de 309 milliards de dollars et des flux ajustés à environ 9 trillions de dollars sur 12 mois. En Afrique subsaharienne, ils représentent 43 % des volumes crypto, avec un usage massif au Nigeria. La tokenisation des actifs, notamment des obligations et fonds, améliore la liquidité et l'accès aux marchés, tandis que les *smart contracts* automatisent les processus financiers, bien que nécessitant une gestion rigoureuse des risques. En France, des acteurs comme BPCE, qui intègrent l'achat et la vente de crypto-monnaies dans ses applications mobiles pour 12 millions de clients d'ici 2026, ou Revolut, qui utilise les *stablecoins* USDC et USDT pour les rémittances (ou transfert de fonds international) avec près de 690 millions de dollars traités via Polygon, illustrent cette dynamique. L'écosystème français, dynamique et innovant, compte des acteurs spécialisés dans la *custodie*, le *staking*, le développement de protocoles, l'identité numérique et la tokenisation, avec des projets phares comme Société Générale- FORGE.

En 2025–2026, plusieurs groupes du CAC 40 sont passés de pilotes à des mises en production dans la tokenisation, les *stablecoins* et la traçabilité sur la chaîne de bloc.

- BNP Paribas a poursuivi sa feuille de route RWA (Real World Asset) : après des parts de MMF tokenisées au Luxembourg, BNP Paribas Asset Management a testé en février 2026 l'émission de parts d'un fonds monétaire sur une blockchain publique via AssetFoundry, et le groupe a parallèlement rejoint fin 2025 un consortium bancaire européen visant un *stablecoin* adossé à l'euro (Qivalis).
- Société Générale, via SG-FORGE, a consolidé son rôle d'émetteur de *stablecoin* euro avec l'extension d'EUR *Coinvertible* (EURCV) au XRP Ledger en février 2026, après Ethereum, Solana et Stellar, tout en

élargissant sa distribution via des partenaires marchés en 2025 ; l'encours et la base d'utilisateurs progressent dans le cadre MiCA.

- Le groupe BPCE a activé l'accès *retail* aux crypto-actifs directement dans les apps Banque Populaire et Caisse d'Épargne via sa filiale Hexarq (PSCA/AMF), avec un pilote lancé fin 2025 avant extension nationale en 2026 ; l'initiative illustre l'entrée des réseaux bancaires grand public français dans une passerelle d'entrée/sortie régulée.

Côté gestion d'actifs, Amundi prépare le lancement de ses premiers produits listés sur le Bitcoin (ETN/ETP) pour début 2026, mouvement confirmé par plusieurs publications à la suite des révélations de *The Big Whale* ; ce positionnement met un acteur de référence européen sur la rampe d'accès aux expositions crypto sous cadre MiCA. Hors de la finance, des champions du CAC 40 industrialisent la traçabilité « internet de la valeur ».

- LVMH a étendu Aura Blockchain Consortium (avec Prada et Richemont) à plusieurs dizaines de marques et des dizaines de millions de produits enregistrés, un jalon aligné avec l'arrivée des Passeports Digital des Produits européens à partir de 2027.
- Carrefour continue d'exploiter IBM Food Trust pour la traçabilité de filières alimentaires à grande échelle, cité comme cas d'usage de référence pour 2026.
- ENGIE fait évoluer son offre de certificats d'origine et de traçabilité énergétique via la plateforme Attributes (ex-TEO), qui s'appuie sur des *smart contracts* et l'Energy Web Chain.

L'écosystème français foisonne aussi de jeunes pousses qui outillent cette transition. Lise (Kriptown) prépare une bourse DLT pour PME/ETI sous régime pilote européen, soutenue opérationnellement par CACEIS (Crédit Agricole) devenu actionnaire en 2025. Fipto, fintech de paiements en *stablecoins* entre entreprises, combine en France l'agrément

d'établissement de paiement (ACPR, mars 2025) et l'autorisation MiCA/CASP (janvier 2026) pour offrir une API unifiée fiat-crypto. Au total, les banques du CAC 40 accélèrent sur la tokenisation, les rails de paiement en *stablecoins* et la distribution d'expositions crypto sous MiCA, tandis que le luxe, la distribution et l'énergie font de la traçabilité blockchain un levier industriel et réglementaire de premier plan pour 2026 et au-delà.

L'adoption de la blockchain dans la finance ainsi que dans le secteur marchand et le e-commerce, notamment via l'IA agentique, s'accélère avec la révolution des *stablecoins*, devenus un véritable rail de paiement traitant plus de 12 000 milliards de dollars par an. Des géants tels que Visa, Mastercard, MoneyGram et Western Union industrialisent déjà ces solutions. Pour toutes les entreprises, cette transformation signifie qu'il faut adapter leurs systèmes et leurs processus internes afin de pouvoir traiter des paiements en continu, 24 heures sur 24 et 7 jours sur 7, avec des règlements effectués le jour même, tout en réduisant les coûts par rapport aux réseaux de paiement et de transfert traditionnels.

Le secteur marchand évolue parallèlement avec l'émergence d'une nouvelle génération de consommateurs. Aux États-Unis, 75 % des détaillants prévoient d'accepter les cryptomonnaies et les *stablecoins* d'ici 2028 selon Deloitte. En Europe, les projections indiquent que 20 à 25 % de la population détiendra des cryptomonnaies d'ici 2030. Des entreprises comme Walmart, Rakuten, ATCT et Emirates acceptent déjà des paiements Web3. Par ailleurs, le e-commerce porté par l'IA agentique devrait s'appuyer largement sur des paiements en *stablecoins*, comme l'indique le World Economic Forum. Il est donc stratégique de se préparer dès maintenant à capter ces nouveaux consommateurs, aussi bien entre entreprises qu'entre une entreprise et ses clients particuliers.

Les secteurs bancaires et financiers connaissent également une transformation structurelle majeure. Le marché de la tokenisation d'actifs

est estimé à 18 900 milliards de dollars à l'horizon 2033 selon Boston Consulting Group. La Banque centrale européenne a confirmé que l'euro numérique s'appuiera sur des blockchains publiques. Des acteurs tels que Société Générale via Forge, BPCE et JPMorgan Chase proposent déjà des produits tokenisés, tandis que Deutsche Bank et UBS développent des solutions de conservation de crypto-actifs. La finance décentralisée sur blockchain représente par ailleurs 11 milliards de dollars échangés chaque jour.

D'autres domaines d'application de la blockchain affichent également des perspectives de forte croissance. Le marché de l'identité numérique basée sur la blockchain est estimé à 9,1 milliards de dollars d'ici 2036, celui de la lutte contre la contrefaçon via blockchain à 11 milliards de dollars à la même échéance, le marché des infrastructures blockchain en tant que service (*blockchain-as-a-service*) devrait atteindre 24,94 milliards de dollars d'ici 2027, et les solutions blockchain destinées aux télécommunications devraient générer plus de 15,06 milliards de dollars supplémentaires d'ici 2030. Enfin, le marché mondial de la technologie blockchain B2B, évalué à 20,2 milliards de dollars en 2024, devrait atteindre 393 milliards de dollars d'ici 2032, soit un taux de croissance annuel composé estimé entre 43% et 44%, confirmant une dynamique d'expansion exceptionnelle sur l'ensemble de l'écosystème.

Ce document explore les dimensions clés de cette révolution technologique et ses implications pour les acteurs financiers, économiques et institutionnels. Il s'articule autour de trois axes majeurs. D'abord, il propose une définition de la blockchain, en décryptant ses mécanismes fondamentaux et ses modèles économiques. Il analyse également l'évolution des marchés actuels et présente les projections à l'horizon 2030, afin d'anticiper les tendances et les opportunités à venir.

Ensuite, le document examine la place stratégique de l'Europe et de la France

dans un paysage dominé par les États-Unis. Il interroge notamment le positionnement des acteurs locaux face à cette omniprésence, en s'appuyant sur des cadres réglementaires comme MiCA, tout en identifiant les atouts et les défis spécifiques à ces territoires.

Enfin, il illustre les cas d'usage concrets de la blockchain à travers des exemples techniques, notamment dans la finance, la banque de détail ou les paiements transfrontaliers, ou encore les passeports numériques, la collaboration et la confiance numérique. Il montre comment des acteurs intègrent déjà ces innovations dans leurs stratégies. À travers ces thèmes, ce livre blanc vise à éclairer les enjeux, les opportunités et les défis posés par la blockchain, tout en offrant une vision prospective des transformations à venir.

I. Panorama des marchés blockchain et opportunités de développement

La blockchain s'est imposée progressivement comme l'une des évolutions structurantes de l'économie numérique contemporaine. Longtemps cantonnée à une lecture réductrice, associée quasi exclusivement aux crypto-monnaies et à des usages spéculatifs, elle doit aujourd'hui être appréhendée comme une infrastructure numérique à part entière, comparable dans ses effets systémiques à l'émergence d'Internet, du *cloud computing* ou des systèmes de paiement électroniques. Cette transformation du regard est essentielle pour comprendre non seulement ce dont il est question, mais surtout où se situent les opportunités économiques, industrielles et institutionnelles qui en découlent.

La blockchain ne constitue pas un marché unique et homogène. Elle correspond à un ensemble d'infrastructures et de services imbriqués, qui supportent des usages variés allant de la finance à l'industrie, en passant par l'identité numérique, la traçabilité, la gestion des données et l'automatisation des processus. À ce titre, elle peut être décrite comme un socle technologique transversal, sur lequel viennent se greffer plusieurs marchés distincts, chacun avec ses acteurs, ses modèles économiques et ses dynamiques propres. Cette pluralité explique en grande partie la difficulté à en proposer une définition simple et univoque, mais elle constitue également la clé pour identifier les espaces de développement encore ouverts. Cette approche par les marchés permet de dépasser une lecture purement technologique pour se concentrer sur les chaînes de valeur. Elle invite à s'interroger non pas uniquement sur le fonctionnement interne de la blockchain, mais sur les rôles qu'elle redistribue, les intermédiaires qu'elle transforme et les positions stratégiques qu'elle rend accessibles. Dans ce contexte, l'enjeu pour les acteurs publics et privés européens n'est pas de « rattraper » un supposé retard de manière indifférenciée, mais de

comprendre précisément où la valeur se crée et comment elle peut être captée durablement. Cette première partie propose donc une lecture structurée des marchés de la blockchain, en identifiant les grandes briques de valeur, les dynamiques économiques en cours et les opportunités de développement qui se dessinent, avant d’aborder, dans un second temps, les implications en matière de souveraineté et de stratégie publique.

I. 1 Une architecture en couches au cœur de la création de valeur

Pour appréhender les marchés de la blockchain, il est nécessaire de revenir à son organisation fondamentale, souvent décrite sous la forme d’une architecture en couches. Cette représentation, permet de comprendre comment la valeur se distribue le long de la chaîne technologique et pourquoi certaines positions sont plus structurantes que d’autres.

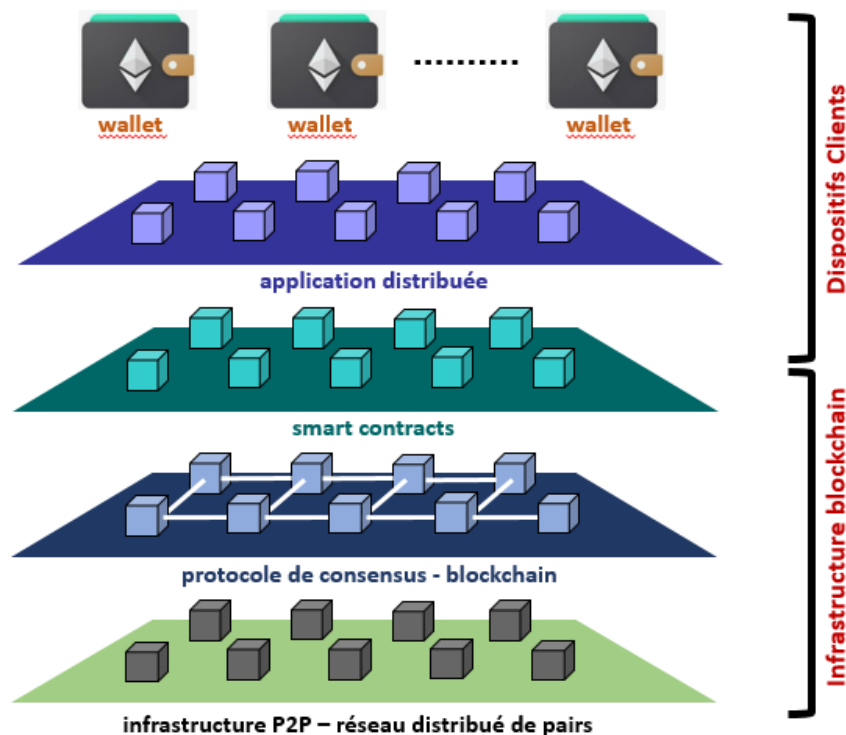


Figure 3: Représentation systémique d'une blockchain en couches

À la base de cette architecture se trouvent les infrastructures blockchain proprement dites, parfois qualifiées de “couches fondamentales”. Ces infrastructures assurent le maintien d’un registre distribué (la blockchain), partagé entre plusieurs acteurs, dans lequel sont enregistrées des transactions ou des événements de manière immuable, horodatée et vérifiable grâce aux mécanismes de consensus mis en œuvre. Elles constituent le socle de confiance sur lequel reposent l’ensemble des usages ultérieurs. À ce niveau, les enjeux sont principalement liés à la sécurité, à la résilience, à la performance et à la gouvernance du réseau.

Au-dessus de cette couche d’infrastructure se situe la couche des *smart contracts*. Ces programmes auto-exécutables, déployés sur la blockchain, permettent d’automatiser des règles de gestion, des échanges de valeur ou des processus métier sans intervention humaine directe. Ils jouent un rôle central dans la transformation des modèles économiques, en rendant possible une automatisation native de la confiance et des transactions. La valeur générée à ce niveau tient autant à la fiabilité du code qu’à sa capacité à s’intégrer dans des cadres juridiques et opérationnels existants.

Enfin, la couche applicative regroupe les applications décentralisées, qui constituent l’interface visible pour les utilisateurs finaux, qu’il s’agisse de citoyens, d’entreprises ou d’administrations. C’est à ce niveau que se matérialisent les usages concrets, mais aussi que se concentrent une grande partie des modèles économiques orientés vers le service.

Cette structuration en couches met en évidence un point fondamental : la valeur ne se situe pas uniquement dans les applications visibles, mais dans l’ensemble de la pile technologique, et en particulier dans les infrastructures et les standards qui la sous-tendent. Comprendre cette répartition est indispensable pour identifier les opportunités de développement les plus pertinentes pour l’Europe.

I.2 Infrastructures blockchain : un marché stratégique encore en structuration

« La blockchain bien employée est une technologie efficace et robuste pour la collaboration de confiance, une confiance absolument nécessaire à la santé de nos systèmes économiques. »

Philippe OGIER, Président du collectif Alliance Blockchain France

Ce bon usage de la blockchain doit reposer sur une infrastructure dont les porteurs, la gouvernance, les règles de fonctionnement et les modes de financement sont parfaitement connus et vérifiables.

Le marché des infrastructures blockchain constitue la couche la plus structurante de l'écosystème. À l'image des systèmes d'exploitation dans l'informatique ou des protocoles fondamentaux d'Internet, ces infrastructures conditionnent l'ensemble des usages qui peuvent émerger par la suite. Elles définissent les règles du consensus, les mécanismes de sécurité, les modèles économiques associés aux transactions et les possibilités d'évolution du réseau.

Aujourd'hui, les infrastructures blockchain les plus largement utilisées sont majoritairement issues d'écosystèmes non européens. Elles se sont développées dans un contexte d'innovation rapide, souvent en dehors de cadres réglementaires formalisés, ce qui leur a permis de gagner en adoption et en maturité technique. Toutefois, cette domination ne signifie pas que le marché est fermé. Au contraire, l'évolution des usages vers des applications industrielles, financières ou institutionnelles met en lumière de nouvelles exigences, notamment en matière de gouvernance, de conformité et d'interopérabilité avec les systèmes existants.

Ces exigences ouvrent des espaces de développement pour des

infrastructures blockchain conçues dès l'origine pour répondre à des contraintes réglementaires fortes, à des besoins de confidentialité ou à des modèles de gouvernance partagée. Dans ce contexte, la capacité à opérer des **blockchains permissionnées** (dont l'accès est contrôlé et restreint) ou de consortium, appelées aussi **permissionned**, intégrant des acteurs publics et privés, constitue un levier important. Elle permet de concilier les propriétés fondamentales de la blockchain avec les exigences propres aux secteurs régulés.

La question n'est donc pas tant de reproduire des infrastructures existantes que de développer des solutions adaptées à des usages spécifiques, en particulier dans les domaines où l'Europe dispose déjà d'atouts structurels, tels que la finance régulée, les services de confiance ou l'industrie. Cette approche pragmatique permet de repositionner la blockchain non comme une rupture isolée, mais comme une évolution cohérente des infrastructures numériques existantes.

La France, à travers la force de ses institutions, et des grands acteurs du numérique et de la finance, a une carte à jouer dans la mise en place et l'émergence d'un écosystème de collaboration de confiance, autour de la donnée et des échanges financiers.

I.3 Finance numérique, tokenisation et nouveaux instruments de valeur

Parmi les marchés les plus visibles de la blockchain figure celui de la finance numérique, qui regroupe les crypto-monnaies, les *stablecoins*, la finance décentralisée et la tokenisation d'actifs. Ces usages ont largement contribué à la notoriété de la technologie, mais ils ne sauraient être réduits à des phénomènes spéculatifs. Ils traduisent avant tout une transformation

profonde des mécanismes de circulation de la valeur.

La tokenisation permet de représenter des actifs, financiers ou réels, sous forme de jetons numériques inscrits sur une blockchain (on parle aussi de *ledger* ou de registre). Cette représentation ouvre la voie à une automatisation accrue des processus financiers, à une meilleure liquidité de certains actifs et à une réduction des coûts de transaction. Les *stablecoins*, quant à eux, jouent un rôle d'interface entre la finance traditionnelle et les infrastructures blockchain, en offrant des instruments de paiement et de règlement relativement stables, utilisables à l'échelle mondiale.

Ces évolutions s'inscrivent dans une dynamique plus large de modernisation des infrastructures financières, déjà engagée par les institutions bancaires et les banques centrales. La blockchain apparaît ici comme un outil complémentaire, capable de renforcer l'efficacité, la transparence et la programmabilité des systèmes existants. Dans ce contexte, les opportunités de développement résident moins dans la création de nouveaux actifs que dans l'intégration de ces technologies au cœur des chaînes de valeur établies.

Cette intégration progressive crée un espace particulièrement pertinent pour les acteurs européens, qui disposent d'un cadre réglementaire structuré et d'un secteur financier solide. Elle permet d'envisager le développement de solutions conformes aux exigences de stabilité financière, de protection des consommateurs et de lutte contre les abus, tout en bénéficiant des apports technologiques de la blockchain.

Derrière le terme "crypto", couramment employé, se dissimulent des mécanismes de création et d'échange de valeur très différents selon qu'il s'agisse de crypto-monnaies, de *coins* ou de *tokens*, chacun obéissant à des règles économiques et techniques propres.

La **crypto-monnaie**, ou *currency*, est générée *ex nihilo* au niveau de la couche blockchain. Dans les réseaux **non-permissionnés** (ouverts), appelés **permissionless**, comme Bitcoin ou Ethereum, une quantité

prédéfinie de *crypto-monnaie* est créée à chaque nouveau bloc ajouté, servant de récompense aux validateurs qui maintiennent le réseau. Ce processus, régi par le protocole de consensus, peut reposer sur une **preuve de travail** (*Proof-of-Work*), où les validateurs doivent résoudre un problème cryptographique complexe pour proposer un bloc valide, ou sur une **preuve d'enjeu** (*Proof-of-Stake*), où la participation est conditionnée par le dépôt d'une certaine quantité de crypto-monnaie dans un registre partagé et répliqué entre tous, appelé *ledger*. Cette émission monétaire joue un rôle clé : elle participe à la sécurité du réseau tout en renforçant sa résilience. Dans Bitcoin, la création monétaire est liée à l'ajout d'un bloc valide au registre. Un mineur qui proposerait un bloc non conforme aux règles du protocole verrait celui-ci rejeté par le réseau et ne recevrait aucune récompense. Ce mécanisme aligne les incitations économiques avec le respect des règles, contribuant fortement à la sécurité du système sans toutefois l'immuniser contre toute forme d'attaque.

Dans les blockchains permissionnées, où l'accès est restreint à des acteurs autorisés, on ne parle pas de crypto-monnaie mais de jetons lorsqu'il y en a. Contrairement aux crypto-monnaies, les jetons ne sont pas émis progressivement : leur quantité de base est fixée dès le déploiement de la blockchain, dans le *bloc genesis*, puis distribuée selon les règles établies par ses créateurs. Ces jetons ne servent pas à sécuriser le consensus, mais sont utilisés pour payer des frais de transaction, évitant ainsi les risques de saturation du réseau, ou comme moyen d'échange, que ce soit au sein de l'écosystème ou sur des plateformes externes, contre des monnaies fiduciaires ou d'autres actifs numériques. Leur valeur dépend alors de leur utilité et de leur rareté, mais ils peuvent aussi n'avoir qu'une fonction technique, comme un "carburant" nécessaire pour exécuter des opérations sur la blockchain. Dans ce dernier cas, on les qualifie parfois de *fuel*. Cependant, il n'est pas nécessaire d'utiliser des jetons sur une blockchain permissionnée, la majorité n'en ont pas.

Les **tokens**, quant à eux, sont des actifs numériques gérés par des *smart contracts*, une couche applicative superposée à la blockchain. Contrairement aux crypto-monnaies ou aux *coins*, ils ne sont pas natifs du protocole mais créés et contrôlés par des programmes informatiques. Leur émission, appelée *minting*, et leur destruction, appelée *burning*, sont déterminées par les règles du *smart contract*, qui définit également leurs fonctionnalités et leurs conditions d'échange. Les *tokens* se déclinent en plusieurs catégories : les *tokens fongibles*, où chaque unité est interchangeable avec une autre de même valeur ; les *tokens non fongibles* (NFT) qui certifient l'unicité d'un actif numérique ; ou encore les *tokens sécurisés* conçus pour encadrer des actifs financiers réglementés. Ces standards, offrent des modèles éprouvés pour déployer des *tokens* de manière sécurisée et interopérable, limitant les risques de vulnérabilités ou d'incompatibilités entre les différentes applications décentralisées.

I.4 Blockchain et services de confiance numérique

Au-delà de la finance, la blockchain s'impose comme une brique clé des services de confiance numérique. Identité, certification, registres, horodatage ou archivage sont autant de fonctions essentielles à la vie économique et institutionnelle, pour lesquelles la blockchain apporte des garanties nouvelles en matière d'intégrité et de traçabilité.

Les travaux autour d'eIDAS 2 et des registres électroniques qualifiés illustrent cette convergence entre cadre juridique et innovation technologique. La blockchain, représente une des solutions permettant de répondre aux exigences de fiabilité, d'ordonnancement chronologique et de détection des altérations. Elle permet de renforcer la valeur probante des enregistrements numériques tout en restant compatible avec une approche technologiquement neutre.

Dans ce domaine, la valeur ne réside pas uniquement dans la technologie,

mais dans la capacité à articuler des infrastructures blockchain avec des prestataires de services de confiance qualifiés, des normes européennes et des exigences élevées en matière de sécurité et de protection des données. Cette articulation constitue un avantage compétitif majeur pour l'Europe, qui peut s'appuyer sur un cadre harmonisé et reconnu à l'international.

En France, il convient de citer l'application « Blockchain des Fréquences » portée par l'ANFR, qui depuis 2019 organise et régule les fréquences radio utilisées par les journalistes lors des grands événements, sportifs en particulier. Une blockchain privée assure de disposer en temps réel d'un registre certifié, permettant l'échange de fréquence entre les journalistes, et de résister aux cyber-attaques qui peuvent être très dommageables dans ce domaine. Cette blockchain a couvert les JO de Paris ainsi que des centaines d'autres événements sportifs et encore cette année elle sera employée sur le Tour de France.

I.5 Traçabilité, industrie et chaînes de valeur

La blockchain joue également un rôle croissant dans la transformation des chaînes de valeur industrielles, en particulier à travers les usages liés à la traçabilité et aux passeports numériques des produits. Ces dispositifs répondent à des besoins croissants de transparence, de conformité réglementaire et de lutte contre la fraude, tout en facilitant la circulation de l'information entre acteurs.

Dans ces usages, la blockchain agit comme un registre partagé, capable de fédérer des acteurs multiples autour d'une source de vérité commune. La valeur créée tient autant à la fiabilité des données qu'à la capacité à organiser la gouvernance du partage d'information. **Les retours d'expérience montrent que la réussite de ces projets dépend moins de la sophistication technologique que de la qualité de la gouvernance et de l'alignement des incitations entre participants.**

Ces marchés restent largement en construction. Ils offrent des opportunités significatives pour structurer des écosystèmes européens autour de standards communs, en lien avec les politiques industrielles et environnementales de l'Union européenne.

I.6 Blockchain publique, privée

La distinction entre blockchain publique et blockchain privée est importante pour comprendre la diversité des usages et des marchés, elle réside dans leur accessibilité et leur gouvernance. Mais cette distinction pourrait être amenée à disparaître avec l'évolution des modes de fonctionnement.

- Sur une **blockchain publique**, c'est-à-dire dont le contenu du *ledger* est transparent et accessible à tous en lecture, la possibilité de manipulation du contenu du *ledger* est quasiment impossible. La confiance dans l'information contenue dans le *ledger* est quasi-absolue. Cependant, si la blockchain est gouvernée par un acteur unique ou même un consortium d'acteurs, **la confiance est à la hauteur de la confiance dans ce consortium et du mode de gouvernance, même si la blockchain est publique.**
- Les blockchains dont l'usage, l'écriture est soumise à autorisation sont dites **privées**. Elles sont nécessairement portées par un ou plusieurs acteurs qui en assurent le maintien, la gouvernance technique et la gouvernance économique.

Les modes de consensus, mécanismes d'approbation de l'apport de nouvelles données dans le *ledger*, varient selon les besoins de sécurité et de performance.

La taille des données pouvant être inscrites vont varier selon les besoins, les règles fixées et la quantité de serveurs contribuant à la blockchain.

Le contenu du *ledger* étant transparent et, a priori accessible par tous les acteurs, aucune donnée confidentielle ou à caractère personnel ne doit y être enregistrée, même chiffrée. En effet, rien ne présage à l’instant de l’enregistrement d’un futur

		Dispositifs Client	
		Usage sans autorisation préalable	Autorisation requise pour l’usage
Infrastructure Blockchain	Participation au consensus sans autorisation préalable	NON-PERMISSIONÉE PUBLIQUE	✗
	Autorisation requise pour participer au consensus	PERMISSIONÉE PUBLIQUE	PERMISSIONÉE PRIVÉE

où des vulnérabilités de l’algorithme de chiffrement seraient divulguées. Aussi, seuls des hachés cryptographiques et des informations publiques devraient figurer sur le *ledger*.

Figure 4 : Taxonomie des différents types de blockchains

- Les **blockchains permissionnées**, déployées entre plusieurs acteurs dont l’implication est définie contractuellement, voir par un acteur unique, s’appuient sur des modes de consensus simplifiés et un nombre réduit de pairs validateurs actifs.

Chaque solution blockchain répond à des besoins précis : certaines optimisent les transactions financières, d’autres ciblent des applications industrielles exigeant un contrôle rigoureux.

Parmi les blockchains publiques, Bitcoin reste la référence historique avec son mécanisme de **Proof-of-Work**, tandis qu’**Ethereum** domine les *smart contracts* et les applications décentralisées, malgré les défis d’évolutivité partiellement atténués par des solutions *Layer 2*. **Solana**, avec son protocole **Proof-of-History**, se distingue par sa rapidité et ses faibles coûts, attirant les projets *DeFi* et *NFT*.

Les blockchains permissionnées et privées, comme **XRP Ledger** dont les banques ont l’usage, occupent une niche spécifique en ciblant les besoins des institutions financières. Contrairement aux réseaux entièrement ouverts, cette blockchain utilise un

protocole de consensus optimisé pour les paiements transfrontaliers, offrant rapidité et faibles coûts tout en restant compatible avec les exigences réglementaires.

Les solutions telles que *Hyperledger Fabric* et *Corda*, sont conçues pour des environnements professionnels où la confidentialité et le contrôle sont prioritaires. *Hyperledger*, développé sous l'égide de la Linux Foundation, permet aux entreprises de créer des réseaux permissionnés adaptés à des cas d'usage spécifiques, comme la traçabilité des *supply chains* ou la gestion des identités. *Corda* se concentre sur les transactions financières sécurisées, en utilisant un modèle où seules les parties concernées valident et voient les données. Ces plateformes évitent les contraintes des blockchains publiques (comme la transparence totale) tout en offrant l'immutabilité et l'auditabilité nécessaires aux entreprises.

Pendant, toutes se heurtent au trilemme fondamental de la blockchain : concilier sécurité, évolutivité et décentralisation, un équilibre difficile qui oriente leurs choix technologiques.

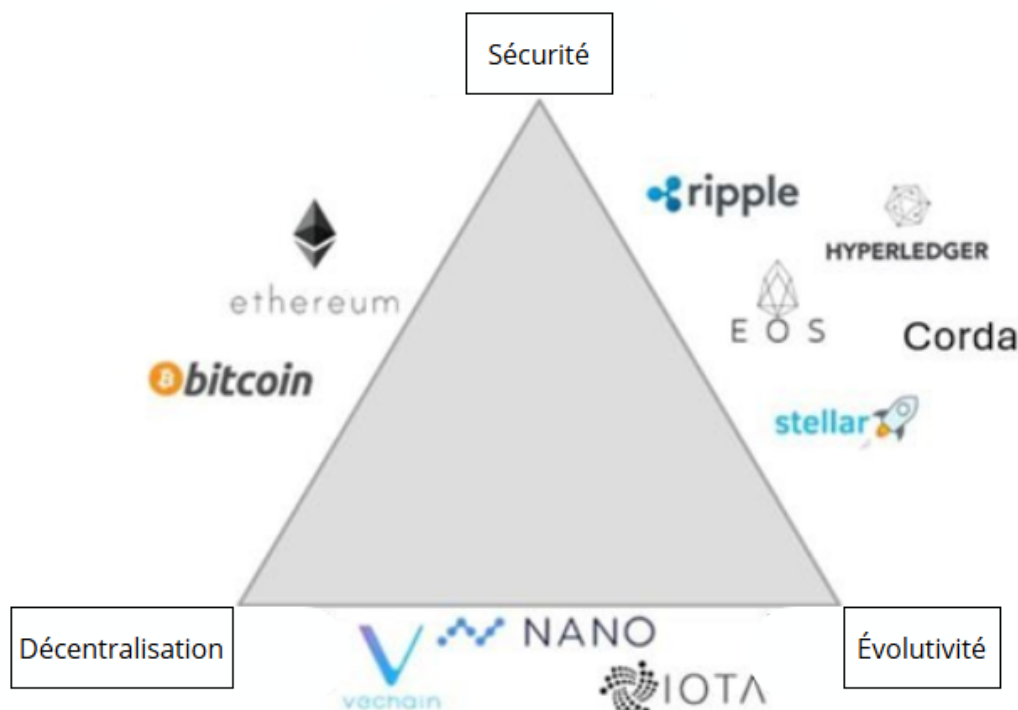


Figure 5: Trilemme fondamental de la blockchain : Sécurité, Décentralisation, Évolutivité

Parmi ces solutions, les blockchains publiques dominent en visibilité et en adoption, tandis que les solutions privées gagnent du terrain dans les secteurs réglementés.

L'innovation se tourne désormais vers des architectures évoluées :

- Layer 0 (protocoles d'interopérabilité comme Polkadot ou Cosmos) pour connecter les réseaux,
- Layer 1 : solutions de passage à l'échelle pour Ethereum et Bitcoin, permettant d'optimiser les performances,
- Blockchains modulaires et AppChains, On adopte des architectures blockchain plus spécialisées et personnalisables (modulaires ou dédiées à une application dit AppChains) afin d'obtenir plus de performance, de contrôle et d'évolutivité...

Cette évolution annonce une standardisation progressive de la blockchain comme infrastructure clé de l'économie numérique.

Dans la pratique, ces deux modèles ne s'opposent pas. De nombreuses architectures combinent des blockchains permissionnées pour les opérations internes et des blockchains non-permissionnées pour l'ancrage de preuves ou la vérification externe. Cette hybridation permet d'adapter la technologie aux exigences spécifiques de chaque cas d'usage, qu'il s'agisse de finance, d'industrie ou de services publics. **Ce choix architectural, loin d'être purement technique, reflète des arbitrages stratégiques en matière de gouvernance, de confiance et de conformité. Il constitue un levier essentiel pour le déploiement de la blockchain dans des environnements régulés.**

Conclusion I : Comprendre les marchés avant la souveraineté

Ainsi à l'issue de ce panorama, la blockchain apparaît comme un ensemble de marchés en pleine structuration, portés par des dynamiques économiques réelles et des usages de plus en plus intégrés aux systèmes existants. La valeur se concentre dans les infrastructures, les services de confiance, la finance numérique et la gouvernance des données, bien plus que dans les usages les plus visibles du grand public. La gouvernance, clé de voûte de la blockchain, est ce qui permet de transformer ces infrastructures en systèmes fiables et durables.

Cette cartographie des marchés est indispensable pour comprendre les enjeux qui dépassent la seule dimension économique. Elle permet de mesurer à quel point ces infrastructures deviennent critiques pour le fonctionnement des économies et des administrations. C'est à partir de cette compréhension que peut s'ouvrir l'analyse des enjeux de souveraineté, de dépendance et de stratégie publique.

II. La France et l'Europe face aux enjeux de souveraineté numérique de la blockchain

La blockchain n'est plus seulement une innovation technologique, mais un enjeu clé de souveraineté numérique pour la France et l'Europe. Alors qu'elle occupe une place croissante dans les systèmes de paiement, de certification et de gestion des données, le contrôle de son fonctionnement conditionne l'autonomie stratégique, la protection des informations sensibles et la résilience des infrastructures critiques. Pourtant, les principaux protocoles, plateformes et outils de gouvernance restent dominés par des acteurs extra-européens principalement américains, exposant l'Europe à une dépendance structurelle aux règles et technologies extérieures. Cette situation soulève une question centrale : comment préserver notre capacité à décider, innover et réguler dans un écosystème où les leviers de pouvoir nous échappent largement ?

Face à ce défi, l'Europe dispose d'atouts majeurs : un cadre réglementaire pionnier (comme le règlement MiCA), une expertise reconnue en matière de services de confiance, et une volonté politique croissante de réduire les dépendances stratégiques. Mais la souveraineté ne se limite pas à la régulation : elle exige aussi l'investissement dans des infrastructures contrôlées, la définition de standards inter communicables et l'implication active des États dans la gouvernance des réseaux. L'enjeu n'est pas de rejeter la blockchain, mais d'en faire un levier de puissance numérique en alignant innovation technologique, politique industrielle et intérêts stratégiques.

II.1 La blockchain comme enjeu de souveraineté numérique

La montée en puissance de la blockchain ne peut être analysée uniquement sous l'angle de l'innovation technologique ou du développement économique. À mesure que ces infrastructures s'intègrent dans les mécanismes de paiement, de gestion des données, de certification et d'identité, elles deviennent des composantes critiques de la souveraineté numérique des États. La capacité à maîtriser ces infrastructures conditionne directement l'autonomie de décision, la protection des données stratégiques et la confiance dans les systèmes numériques.

Là où les systèmes traditionnels reposaient sur des tiers centralisés, souvent nationaux ou européens, de nombreuses solutions blockchain s'appuient aujourd'hui sur des infrastructures globales, opérées et gouvernées en dehors du territoire européen. Cette évolution pose plusieurs questions : qui définit les règles ? Qui contrôle les évolutions technologiques ? Qui capte la valeur associée à ces nouveaux systèmes de confiance ?

Dans ce contexte, la blockchain doit être considérée comme une infrastructure stratégique, au même titre que les réseaux de télécommunication, les systèmes de paiement ou les services cloud. Ne pas s'y positionner revient à accepter une dépendance structurelle à des technologies et des acteurs extérieurs, avec des conséquences potentielles sur la capacité de l'État à garantir la sécurité, la résilience et la continuité de ses services numériques.

II.2 Une dépendance croissante aux infrastructures extra-européennes

L'analyse des marchés met en évidence une concentration importante des infrastructures blockchain dominantes entre les mains d'acteurs non européens, principalement états-uniens. Ces acteurs contrôlent non seulement les protocoles techniques les plus utilisés, mais aussi une grande partie des outils de développement, des plateformes d'échange et des services associés.

Cette dépendance n'est pas uniquement technologique. Elle est également économique et juridique. Les règles de gouvernance des principales blockchains publiques, les modalités d'évolution des protocoles et les décisions structurantes sont prises dans des cadres qui échappent largement aux institutions européennes. Par ailleurs, les entreprises et administrations qui s'appuient sur ces infrastructures s'exposent à l'application extraterritoriale des cadres juridiques étrangers, susceptibles d'entrer en tension avec les principes européens de protection des données, de neutralité technologique et de souveraineté réglementaire. Cette situation n'est pas le résultat d'un choix explicite, mais plutôt d'un enchaînement d'adoptions opportunistes, motivées par la maturité technique et la disponibilité immédiate de solutions étrangères. Toutefois, à mesure que les usages se généralisent, cette dépendance devient structurelle et difficilement réversible, ce qui renforce l'urgence d'une réflexion stratégique à l'échelle nationale et européenne.

II.3 Blockchain et confiance numérique : un enjeu politique

La blockchain se situe au cœur de la notion de confiance numérique, entendue comme la capacité à garantir l'intégrité, l'authenticité et la traçabilité des échanges et des données dans l'espace numérique. Or, la confiance constitue un fondement essentiel de l'action publique, du fonctionnement des institutions et de la cohésion économique et sociale.

Les cadres européens existants, notamment en matière de services de confiance et d'identité numérique, reposent sur une reconnaissance juridique forte des prestataires et des infrastructures qualifiées. L'introduction de la blockchain dans ces domaines soulève des questions fondamentales : comment garantir que les infrastructures utilisées respectent les exigences européennes ? Comment assurer la continuité des services en cas de crise ? Comment maintenir une capacité de contrôle et d'audit sur des systèmes distribués par nature ?

Une blockchain construit et maintient un *ledger*, un registre immuable et horodaté qui conserve un historique ordonné d'événements et de transactions, accessible publiquement. Ses cas d'usage exploitent cette propriété en y enregistrant des données courtes et non sensibles (le *ledger* n'étant pas une base de données), excluant toute information personnelle ou chiffrée (vulnérable aux futures attaques quantiques). Les données typiquement stockées sont des preuves cryptographiques sous forme d'empreintes numériques (hash SHA256), permettant de certifier :

- L'existence d'un bien numérique à une date précise.
- L'ordre chronologique d'événements (logs électroniques).
- L'intégrité ou la possession d'un actif.

Des services comme [ProofOfExistence.com](https://proofofexistence.com) enregistrent ainsi l'empreinte de documents dans la blockchain Bitcoin pour en prouver l'antériorité et l'intégrité, tandis que des démonstrateurs comme HistoTrust (CEA Leti) tracent les logs d'appareils connectés ou d'intelligences artificielles (IA) via leurs empreintes cryptographiques.

Parmi les applications à forte valeur ajoutée, le Passeport de Produit (DPP), exigence européenne du Pacte Vert, documente le cycle de vie d'un produit (origine, matériaux, recyclage) via des QR codes ou étiquettes RFID. Bien que les DPP standardisés (déploiement à partir de 2027 pour les batteries et textiles) restent centralisés chez les fabricants ou dans des bases nationales, leur évolution vers des Passeports Numériques Circulaires (CDP) nécessite une traçabilité fine et décentralisée. La blockchain, en tant que *ledger* partagé, devient alors idéale pour suivre individuellement les composants après démantèlement (ex. : graphite issu d'une batterie), assurant une traçabilité circulaire au sein de consortiums industriels via des blockchains permissionnées. Ces infrastructures permettent un partage sécurisé des données et des responsabilités entre acteurs, sans dépendre d'un unique détenteur.

La blockchain peut renforcer la confiance numérique, à condition d'être intégrée dans une gouvernance claire et conforme aux principes européens. À défaut, elle peut au contraire fragiliser cette confiance, en introduisant des dépendances opaques et des mécanismes de décision hors du champ démocratique. La souveraineté ne s'oppose donc pas à la blockchain ; elle conditionne au contraire son déploiement responsable dans les services publics et les secteurs régulés.

II.4 Le rôle central de l'État dans la structuration de l'écosystème

Face à ces enjeux, l'État ne peut se limiter à un rôle d'observateur ou de simple régulateur a posteriori. La nécessité d'une implication active des pouvoirs publics dans la structuration de l'écosystème blockchain, en particulier lorsque les usages concernent des fonctions régaliennes ou des infrastructures critiques.

Cette implication peut prendre plusieurs formes complémentaires. Elle passe d'abord par le soutien à des infrastructures blockchain compatibles avec les exigences de souveraineté, qu'elles soient publiques, privées ou hybrides. Elle implique également un accompagnement des acteurs économiques et institutionnels dans l'expérimentation et le déploiement de cas d'usage, en veillant à la cohérence avec les cadres juridiques existants.

Contrairement aux systèmes financiers traditionnels, souvent opaques, les transactions en crypto-actifs s'inscrivent dans un registre public et immuable : la blockchain. Chaque opération-code, montant, adresse de portefeuille y est enregistrée de manière indélébile, toutes ces données peuvent être auditées en temps réel par n'importe qui et n'importe où depuis un navigateur web. Cette transparence en fait un atout majeur pour les enquêteurs, leur permettant de retracer l'origine des fonds, détecter des schémas suspects et vérifier la conformité réglementaire. Grâce à des outils d'analyse spécialisés, les forces de l'ordre exploitent cette traçabilité pour démanteler des réseaux criminels, comme en témoignent des affaires emblématiques : l'investigation sur crypto-actifs vise par exemple à tracer et analyser les transactions suspectes en crypto-actifs impliquées dans des enquêtes criminelles.

Ainsi, cette caractéristique de transparence est une aubaine pour les enquêteurs qui sont en mesure, via des outils spécialisés, de détecter,

suivre, et analyser des activités illicites de crypto-actifs. Comme évoqué précédemment, la blockchain fonctionne comme un registre de données décentralisé où chaque transaction est enregistrée de manière sécurisée et transparente. Toutes les transactions sont visibles par tous les participants du réseau, ce qui permet une surveillance en temps réel de l'ensemble des activités. Une fois qu'une transaction est enregistrée, elle ne peut pas être modifiée ou supprimée, garantissant l'intégrité des données. Chaque transaction est liée à la précédente, créant une chaîne ininterrompue de données qui peut être suivie rétrospectivement.

La blockchain permet de vérifier plusieurs aspects cruciaux pour les enquêtes criminelles :

- **Origine des fonds** : les enquêteurs peuvent retracer les mouvements de fonds jusqu'à leur origine, identifiant ainsi les sources de financement illicite.
- **Conformité** : les transactions peuvent être vérifiées pour s'assurer qu'elles respectent les réglementations en vigueur.
- **Activités suspectes** : les schémas de transactions anormaux peuvent être détectés et analysés pour identifier des activités criminelles potentielles.

Ainsi, la blockchain est un allié précieux des enquêteurs sur des affaires criminelles car elle offre une traçabilité inégalée, une transparence totale et une sécurité accrue, réduisant ainsi les risques de falsification et de manipulation des données. Nous pouvons prendre plusieurs exemples :

L'affaire Silk Road

Créé en 2011, **Silk Road** était l'une des premières et plus grandes marketplaces du darknet utilisée principalement pour la vente de drogues, d'armes et de faux papiers. Afin de garantir l'anonymat, la plateforme combinait les outils d'anonymisation des données, le réseau Tor pour masquer les adresses IP et le Bitcoin comme monnaie numérique décentralisée.

L'analyse des transactions Bitcoin a permis d'identifier des portefeuilles appartenant à des collaborateurs de la marketplace, notamment le fondateur Ross Ulrich. Au total, le *Department of Justice* américain (DoJ) a saisi plus d'un milliard de dollars en Bitcoin liés à cette affaire.

L'attaque ransomware du Colonial Pipeline

Le 7 mai 2021, Colonial Pipeline, le plus grand réseau de pipelines de produits raffinés des Etats-Unis, a été victime d'une attaque de rançongiciel par le groupe *DarkSide*. Comme la plupart des rançons, celle-ci a été payée en Bitcoin pour un total de 75 BTC, soit un peu plus de 4 millions de dollars au moment des faits. Grâce à la traçabilité du Bitcoin, les enquêteurs ont pu tracer les transactions liées à la rançon et remonter à un portefeuille d'un affilié de *DarkSide* qui possédait environ 85% du montant de la rançon. En ayant récupéré sa clé privée, le FBI a ainsi pu saisir 63,7 BTC, soit 2,3 millions de dollars au moment des faits.

Welcome To Video, le plus grand marché d'exploitation sexuelle d'enfants

« *Welcome To Video* » était le plus grand site pédopornographique mondial, basé en Corée du Sud. Les utilisateurs payaient en Bitcoin pour télécharger du contenu. A l'aide d'un traçage sophistiqué des transactions en Bitcoins, les agents de l'IRS Criminal Investigation ont pu localiser le serveur du Darknet, identifier l'administrateur du site web et localiser le serveur en Corée du Sud. Chaque utilisateur recevait une adresse Bitcoin unique lors de la création de son compte. L'analyse du serveur a révélé que le site comptait plus d'un million d'adresses Bitcoin, soit un potentiel de plus d'un million d'utilisateurs. En coordination avec les forces de l'ordre du monde entier, le traçage des transactions des adresses Bitcoin ainsi que les informations du serveur ont permis l'arrestation de 338 personnes dans 38 pays différents. Au total, plus de 8 téraoctets de contenu et des milliers de Bitcoin ont été saisis.

L'ensemble de ces exemples d'investigations illustrent la transparence de la blockchain où les acteurs illicites s'exposent à la traçabilité de leurs

transactions dès lors qu'ils utilisent les crypto-actifs. Les blockchains représentent une nouvelle source de données transparentes et peuvent s'avérer être un formidable pivot sur certaines investigations. Même si les crypto-actifs restent utilisés par certains acteurs illicites, les transactions de ces acteurs décroissent progressivement et ne représentaient, en 2024, seulement 0,14% de l'ensemble des transactions de crypto-actifs contre 0,70% en 2020.

Les blockchains offrent de nouvelles perspectives d'enquêtes pour les investigateurs. En s'appuyant sur des outils spécialisés, ils sont en mesure de tracer et d'analyser en temps réel des transactions de crypto-actifs afin de détecter des mouvements suspects, de monitorer des acteurs illicites ou de valider transactionnellement des hypothèses criminelles.

Ces exemples illustrent comment la blockchain, bien qu'utilisée par des acteurs malveillants, peut se retourner contre eux : sa transparence et son immutabilité en font un levier puissant pour les investigations. Malgré une baisse des transactions illicites (0,14 % en 2024 contre 0,70 % en 2020), elle reste un pivot stratégique pour traquer les flux financiers opaques, valider des hypothèses criminelles et renforcer l'efficacité des enquêtes. L'État a un rôle clé à jouer dans la définition de standards, la participation aux instances de gouvernance et la promotion de solutions européennes à l'échelle internationale. En ce sens, la blockchain ne doit pas être envisagée uniquement comme une technologie à réguler, mais comme un levier de politique industrielle et numérique.

Alors que la blockchain se révèle un outil précieux pour les enquêtes criminelles et la souveraineté numérique, comme évoqué précédemment, son potentiel s'étend bien au-delà du secteur public. Les autorités françaises et européennes ont ainsi mis en place un cadre réglementaire ambitieux pour encadrer son développement, tout en favorisant l'innovation dans le secteur privé. La loi PACTE de 2019 a marqué une première étape en créant le statut de Prestataire de Services sur Actifs Numériques (PSAN), plaçant la France parmi les précurseurs en matière de régulation des crypto-actifs. Depuis 2023,

le règlement européen MiCA a harmonisé ces règles à l'échelle de l'UE, renforçant la supervision par l'AMF et l'ACPR. Depuis 2025, les acteurs du secteur doivent désormais obtenir une licence CASP (Crypto-Asset Service Provider), conforme à MiCA, ce qui garantit un niveau élevé de protection pour les utilisateurs tout en sécurisant l'écosystème.

Cependant, MiCA présente une limite majeure : il ne couvre pas les protocoles totalement décentralisés, où aucun intermédiaire identifiable ne peut être tenu responsable. L'AMF a souligné cette lacune et plaide pour une extension du principe « *même activité, même risque, même réglementation* », afin d'éviter les zones grises exploitables par des acteurs malintentionnés. Un décret de 2025 a par ailleurs renforcé les obligations des PSAN/CASP, notamment en matière de lutte contre le blanchiment (KYC/AML), de supervision renforcée et de stabilité financière. Parallèlement, une ordonnance de 2025 a autorisé l'usage des crypto-actifs comme collatéral pour des prêts (crédit lombard), franchissant une étape supplémentaire vers une intégration avec la finance traditionnelle et ouvrant la voie à des usages inspirés de la finance décentralisée (DeFi).

La DeFi est un levier stratégique pour les grands groupes et l'économie réelle. Pour les entreprises, et particulièrement les grands groupes, la finance décentralisée (DeFi) représente une opportunité majeure de modernisation et d'optimisation. Ses atouts sont multiples : réduction des coûts grâce à la suppression des intermédiaires, automatisation des processus via les *smart contracts*, et accès à de nouvelles formes de financement. Dans un marché en pleine mutation, la DeFi offre aux entreprises un avantage compétitif en leur permettant d'explorer la tokenisation d'actifs financiers (titres, créances, matières premières), d'améliorer leur souveraineté numérique et de s'affranchir partiellement des circuits financiers traditionnels. Concrètement, la DeFi permet aux entreprises d'optimiser leur trésorerie en tirant parti des rendements offerts par les protocoles de prêt/emprunt

(*lending/borrowing*), ou encore de fluidifier leurs paiements internationaux grâce à des transactions plus rapides, moins coûteuses et entièrement traçables.

Les *stablecoins* et les actifs tokenisés facilitent également l'accès à une liquidité immédiate, sans dépendre des banques. Par ailleurs, l'automatisation des processus via les *smart contracts* révolutionne le cash management, en permettant une gestion programmatique et sécurisée des flux financiers. La tokenisation, quant à elle, démocratise l'accès à des actifs autrefois illiquides (comme les créances commerciales) et réduit les risques opérationnels en supprimant les manipulations humaines. Au-delà de l'efficacité opérationnelle, la DeFi prépare les entreprises aux transformations futures de la finance, comme l'arrivée de l'euro numérique (*retail* et *wholesale*) ou le développement d'infrastructures financières basées sur les DLT (comme les systèmes *TARGET* sur blockchain). En s'engageant dès aujourd'hui dans ces technologies, les grands groupes anticipent les standards de demain, tout en renforçant leur résilience face aux évolutions réglementaires et technologiques. Enfin, la traçabilité native des blockchains publiques améliore la conformité, simplifie le *reporting* et renforce la lutte contre la fraude, faisant de la DeFi un outil aussi stratégique qu'opérationnel.

II.5 Une approche européenne fondée sur la régulation et l'interopérabilité

L'Union européenne dispose d'atouts spécifiques pour aborder la blockchain sous l'angle de la souveraineté. Contrairement à d'autres régions du monde, elle s'est dotée d'un cadre réglementaire structuré, visant à concilier innovation, protection des utilisateurs et stabilité des systèmes. Les initiatives européennes en matière de crypto-actifs, d'identité numérique et de services de confiance témoignent de cette approche. Or cette régulation ne doit pas être perçue comme un frein, mais comme un facteur de différenciation. En créant un environnement de confiance juridique et technique, l'Europe peut favoriser l'émergence de solutions blockchain adaptées aux usages institutionnels et industriels, là où les solutions existantes montrent leurs limites.

La blockchain face au droit européen se situe à mi-chemin entre une reconnaissance juridique et un encadrement strict. La blockchain s'impose progressivement comme un outil probant dans le système juridique européen, comme en témoigne une décision marquante du Tribunal judiciaire de Marseille en mars 2025. Dans cette affaire, la solution *BlockchainYourIP* a permis de prouver la date de création d'une œuvre contestée grâce à l'immutabilité et à l'horodatage inhérents à la technologie. Cette reconnaissance judiciaire confirme que les données inscrites sur une blockchain, une fois validées, constituent une preuve recevable, à condition que leur authenticité et leur intégrité soient démontrées. Cette position était déjà présente dans une réponse ministérielle de décembre 2019, qui rappelle que les preuves issues de la blockchain ne peuvent être écartées au seul motif de leur forme numérique. Ainsi, bien qu'elles ne bénéficient pas d'une présomption absolue de fiabilité, elles sont désormais admissibles en justice, sous réserve d'une appréciation au cas par cas par les magistrats.

Cette approche pragmatique s'étend aux signatures électroniques simples, où la blockchain peut jouer un rôle complémentaire. Comme le souligne la doctrine, le principe de non-discrimination interdit d'écarter une signature blockchain au motif qu'elle ne répondrait pas aux critères plus stricts de la signature électronique qualifiée. Toutefois, pour renforcer sa valeur probante, il est recommandé de l'associer à des preuves annexes, comme des fichiers d'audit ou des métadonnées supplémentaires, afin de confirmer son authenticité et son intégrité. Cette flexibilité juridique permet d'envisager des applications variées, tout en maintenant un équilibre entre innovation technologique et sécurité juridique.

Concernant la transparence et protection des données le RGPD et la blockchain forment un équilibre délicat. Le Comité européen de la protection des données (CEPD) a publié, en avril 2025, des lignes directrices ambitieuses pour concilier l'usage de la blockchain avec les exigences du RGPD. Ces recommandations, structurées en seize points clés, soulignent la nécessité d'une approche proportionnée et sécurisée pour éviter que la technologie ne devienne un vecteur de non-conformité. Parmi les principes fondamentaux, le CEPD insiste sur la documentation rigoureuse de l'architecture blockchain, notamment pour justifier son utilisation lorsque des données personnelles sont en jeu. Une attention particulière est portée sur la minimisation des données : seules les informations strictement nécessaires doivent être enregistrées sur la chaîne, tandis que les données sensibles sont stockées hors chaîne, avec des liens cryptographiques (hash) pour garantir leur intégrité sans exposer leur contenu.

La question du consentement et du droit à l'effacement (art. 17, RGPD) est particulièrement épineuse, car l'immutabilité de la blockchain semble a priori incompatible avec ces exigences. Le CEPD propose des solutions techniques, comme l'anonymisation des données hors chaîne ou l'utilisation de mécanismes de chiffrement avancés, pour permettre aux utilisateurs de retirer leur consentement sans remettre en cause l'intégrité du registre. Par

ailleurs, la gouvernance des protocoles doit être transparente et documentée, avec des procédures claires pour gérer les mises à jour et les incidents, notamment en cas de vulnérabilités logicielles ou de risques post-quantiques. Enfin, le CEPD encourage l'adoption de standards de confidentialité comme le *privacy-by-design* et les preuves à divulgation nulle de connaissance (ZKP), afin de limiter l'exposition des données personnelles tout en préservant les avantages de la blockchain.

Les *smart contracts* sont une force exécutoire des limites juridiques. La validité juridique des *smart contracts* est désormais reconnue en France, comme en attestent des textes tels que l'ordonnance 2016-520, qui autorise l'émission de mini- bons via des Dispositifs d'Enregistrement Électronique Partagé (DEEP). Ces dispositifs, bien que distincts des blockchains publiques, ont ouvert la voie à une reconnaissance progressive des contrats auto-exécutants. Un *smart contract* agit comme un exécuteur automatique de clauses, reflétant l'accord des parties sous forme de code informatique. Cependant, sa validité dépend du respect des conditions classiques du droit des contrats : consentement libre et éclairé, capacité juridique des parties, objet licite et cause déterminée.

L'exemple d'AXA avec son assurance Fizzy, qui indemnise automatiquement les voyageurs en cas de retard d'avion, illustre comment les *smart contracts* peuvent s'intégrer dans des cadres juridiques existants. Toutefois, leur déploiement nécessite des gardes fous techniques et juridiques, comme des mécanismes de révocation ou des oracles tiers, pour pallier les limites du code (bugs, imprévus, évolutions réglementaires). Le droit positif français s'adapte ainsi à ce nouveau paradigme, mais une approche hybride combinant contrats traditionnels et *smart contracts* reste souvent préférable pour garantir une sécurité juridique optimale.

Le règlement eIDAS 2 portant sur la création d'un portefeuille d'identités numériques européen pour chaque citoyen marque une avancée majeure

en introduisant le concept de Registres Électroniques Qualifiés (QELS), qui bénéficient d'une présomption légale d'intégrité et d'horodatage. Ce cadre juridique permet d'envisager la blockchain comme une infrastructure de confiance pour les services publics et privés, tout en restant technologiquement neutre. Les QELS, gérés par des Prestataires de Services de Confiance Qualifiés (QTSP), doivent respecter des exigences strictes : traçabilité des origines, ordonnancement chronologique exact, et détection des modifications. La blockchain, avec ses propriétés d'immutabilité et de transparence, se positionne naturellement comme une solution adaptée à ces critères, bien que le règlement n'impose aucune technologie spécifique.

Au-delà des QELS, eIDAS 2 ouvre la voie à une interopérabilité renforcée entre les États membres, en permettant l'utilisation de la blockchain pour d'autres services qualifiés, tels que l'horodatage, les signatures électroniques ou l'archivage probant. Des projets comme TRACE4EU (traçabilité logistique) ou VICTOR (diplômes) illustrent cette dynamique, tandis que des usages plus sensibles, comme le vote électronique transfrontalier, nécessitent des garanties supplémentaires (sécurité, gouvernance). Pour répondre à ces enjeux, des architectures hybrides sont recommandées, combinant réseaux permissionnés européens (comme EBSI) et ancrage multi-*blockchains* pour renforcer la résilience. Enfin, la conformité aux normes ETSI (EN 319 401, EN 319 421) et ISO/TC 307 assure la pérennité des preuves et l'interopérabilité transfrontalière, tout en anticipant les défis post-quantiques et environnementaux.

Cette approche réglementaire, fondée sur l'interopérabilité et la conformité, positionne l'Europe comme un acteur clé dans la structuration d'un écosystème *blockchain* souverain, sécurisé et durable, tout en préservant les principes fondamentaux de protection des données et de confiance numérique.

L'interopérabilité constitue un autre pilier de cette approche. Plutôt que de chercher à imposer une solution unique, l'enjeu est de permettre la coexistence et la communication entre différentes infrastructures, dans le respect de règles communes. Cette vision est particulièrement adaptée à la diversité des États membres et à la pluralité des usages identifiés.

La question de la souveraineté blockchain ne se limite pas à la maîtrise technique des infrastructures. Elle engage une réflexion plus large sur la capacité de la France et de l'Europe à orienter les usages, à protéger leurs intérêts stratégiques et à préserver leur autonomie de décision dans un environnement numérique globalisé.

Les choix effectués aujourd'hui en matière d'infrastructures numériques auront des effets de long terme. Une dépendance acceptée par défaut peut se transformer en contrainte stratégique durable. **À l'inverse, un investissement ciblé et coordonné dans des solutions compatibles avec les valeurs et les intérêts européens peut renforcer la position de l'Europe dans l'économie numérique mondiale.** Dans cette perspective, la blockchain apparaît moins comme une fin en soi que comme un révélateur des enjeux de souveraineté numérique contemporains. Elle met en lumière la nécessité d'articuler innovation technologique, régulation, politique industrielle et action publique de manière cohérente.

Conclusion II : Un choix politique structurant

La blockchain place la France et l'Europe face à un choix stratégique clair. Soit accepter une dépendance croissante à des infrastructures et des modèles de gouvernance extra-européens, soit s'engager activement dans la structuration d'un écosystème blockchain compatible avec les exigences de souveraineté, de confiance et de résilience. Ce choix ne se résume pas à une opposition entre innovation et régulation. Il s'agit au contraire de définir un cadre dans lequel l'innovation peut se déployer de manière maîtrisée, au service de l'intérêt général. La compréhension des marchés et des usages, présentée dans la première partie, permet d'éclairer ce choix et de poser les bases d'une stratégie publique cohérente. C'est sur cette base que peuvent être abordés, les cas d'usage concrets et les orientations opérationnelles permettant de traduire ces enjeux stratégiques en actions tangibles.

III. Cas d'usage de la blockchain : applications techniques et opérationnelles

La blockchain n'est pas une technologie théorique, mais un levier opérationnel déjà déployé dans des projets concrets, portés par des acteurs publics et privés. Après avoir analysé ses marchés et ses enjeux stratégiques, cette partie explore comment elle se traduit en applications tangibles, répondant à des besoins précis : sécurisation des données, optimisation des processus, traçabilité des flux ou automatisation des échanges.

Loin des promesses abstraites, les cas d'usage les plus pertinents s'inscrivent dans une logique pragmatique, celle d'une intégration progressive, compatible avec les contraintes juridiques, organisationnelles et budgétaires des institutions et des entreprises. De l'identité numérique souveraine aux registres infalsifiables, en passant par la traçabilité des chaînes de valeur, l'automatisation des paiements ou encore l'exploitation de nouveaux leviers énergétiques, la blockchain agit comme un accélérateur de confiance et d'efficacité.

Mais son succès ne dépend pas seulement de la technologie : il repose sur une gouvernance claire, une interopérabilité maîtrisée et une adéquation précise avec les besoins métiers. Cette partie décrypte ces applications techniques, leurs conditions de déploiement et leur potentiel à transformer durablement l'action publique et économique, non pas en bouleversant les systèmes existants, mais en les renforçant par la transparence, la sécurité et l'automatisation.

Il est nécessaire d'examiner les cas d'usage concrets permettant de traduire ces enjeux en applications opérationnelles. La blockchain ne constitue pas

une rupture isolée, mais une brique technologique mobilisable au service de problématiques existantes.

Les cas d'usage les plus pertinents répondent à des besoins clairement identifiés : sécurisation des données, fluidification des échanges entre acteurs, réduction des asymétries d'information, amélioration de la traçabilité ou automatisation de processus complexes. Dans ces contextes, la blockchain agit comme un levier d'optimisation et de confiance, complémentaire aux systèmes existants.

Cette approche pragmatique conditionne l'adoption. Elle permet de dépasser le stade des expérimentations isolées pour inscrire la blockchain dans des stratégies de déploiement progressif, compatibles avec les cadres juridiques, organisationnels et budgétaires des acteurs publics et privés.

III.1 Identité numérique et gestion des droits

L'un des cas d'usage les plus structurants concerne l'identité numérique et la gestion des droits associés. Dans un contexte de numérisation croissante des services publics et privés, la capacité à identifier de manière fiable les personnes physiques et morales constitue un enjeu central de souveraineté et de sécurité.

La blockchain permet de renforcer les dispositifs d'identité numérique en proposant des mécanismes de vérification décentralisés, traçables et auditables. Elle ouvre des perspectives vers des modèles d'identité dite auto-souveraine, dans lesquels les utilisateurs conservent la maîtrise de leurs attributs, tout en permettant aux autorités compétentes d'en garantir l'authenticité. Cette approche s'inscrit pleinement dans les travaux européens autour de l'identité numérique et des portefeuilles électroniques.

Au-delà de l'identité, la blockchain facilite la gestion des droits, habilitations

et autorisations. Les *smart contracts* permettent d'automatiser l'attribution, la révocation et la vérification des droits d'accès à des services, des données ou des infrastructures, renforçant ainsi la sécurité et la traçabilité des processus.

III.2 Registres, certification et valeur probante

La gestion des registres constitue un domaine d'application majeur de la blockchain. Qu'il s'agisse de registres administratifs, industriels, contractuels ou sectoriels, ces dispositifs reposent sur la capacité à garantir l'intégrité, l'antériorité et l'authenticité des informations enregistrées.

La blockchain offre des propriétés particulièrement adaptées à ces usages, notamment l'immutabilité des enregistrements et l'horodatage distribué. Elle renforce la valeur probante des données numériques en facilitant les mécanismes de vérification, d'audit et de contrôle, tout en restant compatible avec les cadres juridiques existants, notamment en matière de services de confiance.

L'intégration de la blockchain dans ces dispositifs ne vise pas à se substituer aux autorités compétentes, mais à **renforcer leur rôle**, en sécurisant les processus, en réduisant les risques de fraude et en améliorant la transparence des registres.

III.3 Traçabilité des chaînes de valeur et passeports numériques

La traçabilité des produits et des flux constitue un enjeu croissant pour les acteurs économiques et les pouvoirs publics, notamment dans les secteurs industriels, agroalimentaires, environnementaux et énergétiques. Les exigences européennes en matière de transparence, de durabilité et de conformité renforcent la nécessité de disposer d'outils fiables pour suivre

les chaînes de valeur.

La *blockchain* permet de créer des registres partagés entre les différents acteurs d'une chaîne d'approvisionnement, facilitant la circulation de l'information et la vérification des données. Elle constitue un socle pertinent pour le déploiement de passeports numériques des produits, intégrant des informations sur l'origine, la composition, les transformations successives et la fin de vie des biens.

Ces dispositifs reposent sur une gouvernance collective, souvent organisée sous forme de consortiums sectoriels. La valeur créée dépend alors moins de la technologie que de la capacité à définir des règles communes, à assurer l'interopérabilité des systèmes et à aligner les intérêts des parties prenantes.

En France, on peut citer l'exemple de *Circlechain.green* qui propose des passeports numériques pour le suivi des déchets, des matériaux et des produits de réemploi. Cet outil permet de partager de la donnée entre les acteurs de la chaîne de traitement et pour tracer le véritable devenir de ces produits. C'est également un moyen efficace pour permettre de qualifier les produits issus du recyclage ou du réemploi lorsqu'ils retournent sur le marché.

La *blockchain* apporte la confiance et la garantie d'inviolabilité permettant une collaboration effective entre les acteurs avec un gain de temps considérable sur l'échange de données nécessaire entre les différents acteurs.

Plusieurs approches *blockchain* sont possibles ; la plus pertinentes semble être de confier aux filières techniques le rôle de définir et contrôler le mode de fonctionnement et d'usage de *blockchains* dédiées (équipements électriques, terres excavées, meubles, etc).

III.4 Finance, paiements, enquêtes et automatisation des processus

La blockchain trouve également des applications concrètes dans le domaine financier, au-delà des crypto-actifs eux-mêmes. Elle permet d'automatiser des processus de paiement, de règlement et de compensation, en réduisant les délais, les coûts et les risques liés aux intermédiaires traditionnels.

Les *smart contracts* peuvent déclencher des paiements conditionnels, gérer des garanties ou automatiser des flux financiers complexes. Ces mécanismes intéressent aussi bien les acteurs privés que les administrations, notamment dans la gestion des subventions, des aides publiques ou des marchés conditionnés à des critères précis.

Par ailleurs, la transparence native des blockchains publiques en fait un outil de plus en plus central pour les investigations financières et criminelles. Contrairement aux systèmes financiers traditionnels souvent opaques, les transactions enregistrées sur une blockchain sont consultables, traçables et auditables. Les autorités disposent désormais d'outils spécialisés leur permettant d'analyser les flux, de détecter des schémas suspects et de reconstituer des chaînes transactionnelles complexes. Des investigations menées sur des attaques par rançongiciel ou des réseaux criminels internationaux, ont démontré que la blockchain constitue une nouvelle source de renseignement financier, renforçant l'efficacité des enquêtes et la coopération internationale.

III.5 Traçabilité de l'énergie, décarbonation, compensation carbone

Le domaine de l'énergie concerne ici les activités de distribution, stockage, et d'échanges d'électricité, de chaleur, de fluides et de gaz. L'énergie est historiquement une « commodité », un bien utile, mais sans attribut individuel spécifique : un kWh est habituellement complètement interchangeable avec un autre kWh. Cependant, depuis les années 2010, deux tendances contribuent à faire de l'énergie un bien qu'il est intéressant d'identifier et tracer : la décentralisation des moyens de production, avec l'idée de valoriser de ressources locales ou localisées ; et la décarbonation du système énergétique, qui requiert de tracer la production, le transport, le stockage de l'énergie, et de développer de moyens incitatifs : financiers, RSE, éthiques, etc... Ainsi, ces activités peuvent être vues comme des chaînes logistiques particulières, avec pour enjeu de suivre l'énergie depuis sa production jusqu'à sa consommation finale, en particulier dans l'objectif de décarboner le système énergétique.

De premières idées fondées sur le Bitcoin avaient émergé dès 2011 : paiement de l'électricité par des compteurs numériques (Bankymoon avec Eskom en Afrique du Sud), création de monnaies numériques dédiées à un mode de production d'énergie pour en favoriser le développement, selon une démarche inspirée du financement participatif (Solarcoin). Mais l'utilisation du Bitcoin est limitée à cause du coût en énergie du protocole Preuve de Travail et des fonctionnalités limitées du code.

L'émergence de blockchains capables d'exécuter du code riche en fonctionnalités (en particulier Hyperledger et Ethereum) a élargi les possibilités. Ethereum qui combine en particulier réseau public, tokenisation et mise en œuvre de contrats auto-exécutables a soutenu les premières expérimentations début 2016, alors qu'elle n'a six mois d'existence. Il s'agit en particulier d'échanges d'énergie solaire entre

quelques habitations voisines à Brooklyn aux USA (Brooklyn Microgrid, LO3 Energy) et de paiement de charges de véhicules électriques en Allemagne (RWE et Slock.it).

Energie Décentralisée

De nombreuses autres démonstrations ont été menées pour tracer les échanges et l'origine de l'énergie entre particuliers à l'échelle d'un quartier. Pour impacter de façon significative le système énergétique, des progrès étaient nécessaires en nombre de transactions par seconde, de passage à l'échelle, des modèles économiques robustes et des preuves de disponibilité et de cybersécurité. De 2016 à 2025, le passage à l'échelle a été atteint (par exemple de 4 maisons à 50, 500, 10 000 maisons ou objets..., de 1 heure à 1 minute, voire 10 secondes ...), la disponibilité et la sécurité ont été démontrées.

Cependant la gestion de la complexité d'un système par des acteurs se régulant de façon horizontale grâce à une recherche d'optimums locaux n'est pas encore opérante, dans l'état actuel des algorithmes et des réseaux de distribution. La gestion d'un système électrique requiert encore des acteurs centralisés (réseau Haute tension, réseau Basse et Moyenne Tension), à cause de sa complexité physique (planification et temps de réaction requis pour gérer les écarts production/consommation, avec des capacités de stockage limité). Le projet européen HORIZON U2DEMO, lancé en 2024, se concentre sur ce sujet et va tenter d'apporter des solutions, en particulier par de nouveaux algorithmes et une plateforme intégrant la Blockchain de l'Energy Web Foundation.

Traçabilité du CO2

L'autre grand domaine d'application en 2026 porte sur la traçabilité du CO2. L'idée est de tokeniser chaque kWh produit (renouvelable ou fossile) pour générer un certificat numérique horodaté, incluant l'origine, le type d'énergie et l'empreinte carbone calculée. La donnée provient de compteurs numériques, de capteurs sur sites de production ou transformation, des bases de données d'opérateurs de réseau. Les *smart contracts* automatisent l'adéquation entre un consommateur et une source de production décarbonée. La blockchain évite le double comptage en validant l'échange et annulant le certificat une fois consommé, et favorise l'interopérabilité entre Garanties d'Origine (GO/REGO) européennes, reporting CSRD et marchés carbone (EU ETS).

Par exemple, Attributes (exTEO), filiale d'Engie, utilise une blockchain pour tracer l'énergie verte. EDF a fourni un service de traçabilité de l'énergie aux JO de Paris en 2024 (service Trackelec développé par Exaion sur Energy Web Foundation). Des services d'effacement de consommation peuvent être tracés selon une démarche comparable.

Si on s'appuie sur un réseau public comme Ethereum, le fournisseur de services doit utiliser un registre public comme tiers de confiance distribué et de faire traiter toutes les transactions de l'application dans le réseau. Cela pose des questions de confidentialité. En France, la courbe de consommation d'électricité, aussi appelée « courbe de charge », constitue désormais, selon la CNIL une donnée à caractère personnel (DCP) et le coût d'exploitation peut être difficile à estimer car la valorisation des tokens requis pour employer le réseau n'est pas stable. Pour gérer le sujet des données, EDF a été l'entité responsable de traitement de l'expérimentation Mobilichain, ce qui suppose une centralisation partielle. Ce projet mené en région nantaise en 2021 a démontré deux usages « comptables » de la blockchain : la gestion des frais professionnels lorsqu'un salarié recharge son véhicule professionnel chez lui,

et la gestion du coût de la charge d'un véhicule personnel sur une borne mise à disposition par l'employeur.

Un autre sujet est l'effacement des données (droit à l'oubli). Ainsi la blockchain s'avère mal adaptée pour des factures dont la durée de validité est souvent de moins de trois mois, pour des certificats de consommation d'énergie ayant une durée de vie de 15 minutes. Une solution technique a été proposée via l'emploi des chaînes parallèles, chacune dédiée à des types de données. Par exemple, la chaîne principale stocke les données pérennes et les chaînes parallèles, régulièrement effacées, traitent les données dont l'utilité est temporaire.

Pour ces raisons de confidentialité et de sobriété énergétique, la solution des blockchains de consortium a prévalu. La question est alors le choix du consortium. Une première idée est d'employer une blockchain dédiée à l'énergie, ou différentes applications pourraient tourner entre acteurs authentifiés. On peut citer l'initiative Energy Web Foundation qui rassemble une vingtaine de validateurs fournisseurs d'énergie.

Il est aussi envisageable de construire de la confiance par la diversité des intérêts, en fédérant des acteurs qui couvrent différents aspects domaines, différents aspects de la chaîne de valeur, en incluant des utilisateurs finaux ou leurs représentants. C'est par exemple le choix du consortium Hedera Hashgraph.

Une autre option est de passer par des blockchains dédiées à des services publics et des communs. Par exemple, EUROPEUM est un consortium européen, créé le 21 mai 2024 par décision de la Commission européenne, à partir de EBSI. Il vise à industrialiser une infrastructure européenne de services de chaînes de blocs pour fournir des services publics transfrontaliers dans l'UE (identité numérique, vérification de documents, certificats et diplômes...). Neuf États membres (Belgique, Italie, Grèce,

Portugal...) sont fondateurs, avec possibilité d'extension aux pays de l'UE. EUROPEUM est un des consortiums européens pour une infrastructure numérique (EDIC), piliers de la stratégie « Décennie numérique 2030 » pour la souveraineté numérique européenne. Ainsi plusieurs blockchains vont coexister et se connecter ponctuellement par des systèmes de chaînes parallèles et de places d'échange.

L'intégration croissante des sources d'énergie renouvelables intermittentes (solaire, éolien) dans le système électrique européen pose un défi majeur de stabilité pour les gestionnaires de réseau. Le minage de Bitcoin qui repose sur le protocole de Preuve de Travail (PoW) énergivore est parfois proposé comme une solution innovante au service de la flexibilité du réseau. Comparé aux installations industrielles, le minage offre des caractéristiques uniques et potentiellement précieuses.

Pour le contrôle dynamique, les mineurs peuvent arrêter instantanément leurs machines sans interrompre de processus critiques. La consommation d'énergie peut être ajustée au niveau de chaque machine au kilowatt près pour une réponse très précise aux besoins du réseau (haute granularité).

Les installations de minage peuvent être déployées directement sur les sites de production d'énergie (ex : parcs éoliens isolés, torchères de gaz orphelines, centrales hydroélectriques au fil de l'eau), là où la demande est faible et l'énergie parfois excédentaire ce qui permet leur décentralisation.

Le minage peut ainsi contribuer à la flexibilité de manière simple et directe lors des pics de demande : les gestionnaires de réseau demandent aux mineurs de cesser temporairement leurs activités sans avoir à activer de centrales de secours (ex : barrages ou centrales à gaz). Ce transfert de consommation peut être plus économique que le recours à un stockage massif par batteries centralisées, car le capital investi dans les serveurs est une source permanente de revenus.

Enfin, des petites unités de minage peuvent être déployées au sein de communautés énergétiques locales avec des services de flexibilité locaux. Une communauté dotée de panneaux solaires peut utiliser une petite unité de minage pour absorber l'énergie solaire excédentaire. Les Bitcoins générés servent alors de rendement financier, réinvesti dans la communauté. Un serveur de minage domestique pourrait aussi gérer le surplus derrière le compteur, fournissant à la fois de la chaleur thermique et de la valeur économique.

Malgré l'attrait de ce concept de « batterie virtuelle », plusieurs défis pourraient empêcher le minage de devenir un outil fiable, évolutif et largement adopté pour la flexibilité du réseau en Europe. Notamment des incertitudes économiques, le minage de Bitcoin est une industrie à forte intensité capitalistique. Le matériel spécialisé devient obsolète en 3 à 5 ans en raison de la baisse tendancielle des récompenses de minage inscrite dans l'algorithme de Bitcoin. Ainsi, pour maximiser le retour sur investissement, les mineurs visent un taux d'utilisation de 95 à 99 %. Par conséquent, les revenus issus de la flexibilité (ex : compensation pour l'effacement) pourraient ne pas compenser la perte de revenus de minage lors des arrêts. En particulier, lorsque le prix du Bitcoin monte, le coût d'opportunité d'un arrêt devient prohibitif. De plus, la volatilité et l'incertitude à court et long terme sur la valeur du Bitcoin rendent difficile la modélisation économique du minage en tant que service de flexibilité.

Il existe deux sujets majeurs de défis réglementaires. Tout d'abord l'absence de garantie, les gestionnaires de réseau (ex : RTE en France) exigent une flexibilité garantie. Contrairement aux stations de pompage (STEP) ou aux batteries industrielles, les mineurs n'ont aujourd'hui aucune obligation légale ou contractuelle de répondre aux signaux du réseau. Ensuite, l'incompatibilité avec la Taxonomie Verte de l'UE, les gestionnaires de réseau ne considèrent la charge industrielle des crypto-mineurs comme

acceptable et utile que si elle est pilotable, visible et intégrée aux marchés de flexibilité et aux règles de raccordement. Cela implique que les réglementations soient définies au niveau européen, les réseaux et marchés de l'énergie étant interconnectés. Or, selon le cadre de classification durable de l'UE, le minage n'est pas considéré actuellement comme une activité durable. Cela limite la capacité des gestionnaires de réseaux publics à soutenir ou financer de telles initiatives. Cette situation est aggravée par les controverses publiques régulières sur le sujet du minage. Enfin, même en levant les défis économiques et réglementaires, il existe des risques stratégiques. Cependant, il existe de nombreuses alternatives techniques. Le stockage par batterie (petite ou grande échelle), la production d'hydrogène vert, les STEP (réserves hydrauliques par pompage), les interconnexions transfrontalières, ou encore le *Vehicle-to-Grid* (V2G). Ces technologies stockent ou déplacent l'énergie, alors que le minage PoW transfère de l'énergie contre un cryptoactif, ce qui est plus complexe à gérer. Avec l'électrification massive de l'économie pour bannir les énergies fossiles, le risque de pénurie durable d'énergie est plus probable qu'un excédent structurel. De plus, face à une énergie limitée, la construction de centres de calcul pour l'IA, des jumeaux numériques, du calcul scientifique, sera probablement priorisée par rapport au minage. D'autant plus que des centres de calcul intensif peuvent offrir les mêmes services de flexibilité sans les risques économiques ou les controverses liés au Bitcoin. La récupération de la chaleur fatale des centres de données va se généraliser. Or, couper un centre de minage (qui est un type particulier de centre de données) pour aider le réseau électrique contredit l'exigence de continuité de service nécessaire pour le chauffage urbain ou industriel.

III. 6 Partage de données et interopérabilité entre acteurs

Le partage de données entre acteurs publics et privés constitue un autre champ d'application structurant. Dans de nombreux secteurs, la valeur repose sur la capacité à échanger des données de manière sécurisée, tout en maîtrisant les droits d'accès, les responsabilités et la conformité réglementaire.

La blockchain peut servir de couche de coordination pour organiser ce partage, en assurant la traçabilité des accès, la gestion des consentements et l'exécution automatique de règles de gouvernance. Elle permet de créer des environnements de confiance dans lesquels les données restent hébergées chez leurs détenteurs, tout en étant référencées via un registre commun. Cette approche est particulièrement pertinente dans les projets multi-acteurs impliquant administrations, collectivités, opérateurs industriels et partenaires privés.

Mais elle nécessite une implication des acteurs et une implication infrastructurelle comme le montre le cas de TradeLens. TradeLens (transport

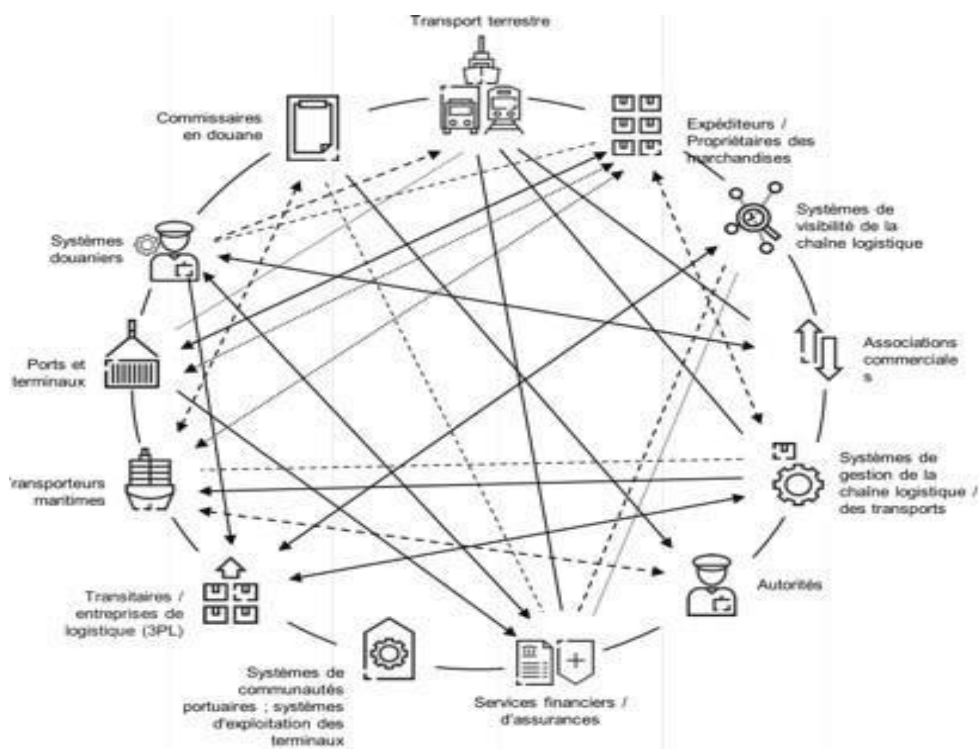


Figure 6 : Les échanges documentaires dans le domaine du transport maritime

maritime) était une plateforme blockchain de traçabilité du transport maritime, développée par IBM et Maersk entre 2016 et 2022. Elle visait à fluidifier les échanges documentaires entre ports, armateurs, transporteurs et douanes, dans un secteur encore très peu numérisé. Malgré une adoption institutionnelle large, l'usage réel est resté limité, faute d'incitations économiques, de gouvernance décentralisée et de modèle de financement durable, conduisant à l'arrêt du projet.

Dans la même direction, we.trade était une plateforme blockchain destinée à simplifier le commerce international des PME, portée par un consortium de grandes banques européennes et IBM. Conçue sur Hyperledger Fabric, elle reposait sur une gouvernance lourde et centralisée, exigeant un fort engagement opérationnel de chaque membre. L'absence de fondation indépendante et la complexité du modèle ont freiné l'adoption, aboutissant à l'arrêt du projet en 2022.

B3i réunissait de grands assureurs autour d'une plateforme blockchain visant à automatiser les processus de réassurance. Développée sur Corda, la solution a souffert d'un consortium trop large, d'une forte complexité réglementaire et d'objectifs trop ambitieux dès le départ. Après plusieurs années de développement et un lancement tardif, le projet a été abandonné en 2022 faute de ressources suffisantes.

Ces initiatives illustrent les limites des consortiums blockchain fermés, centrés sur des acteurs dominants et des modèles économiques proches des plateformes centralisées. L'absence de tokenisation, de gouvernance communautaire et de masse critique d'usage réel a freiné leur viabilité. À l'inverse, les projets émergents privilégient désormais l'interopérabilité, des périmètres fonctionnels ciblés et l'intégration à des blockchains publiques ou hybrides.

Conclusion III : Des usages au service d'une stratégie cohérente

Les cas d'usage présentés illustrent la diversité et la maturité croissante des applications de la blockchain dans les domaines publics, économiques, financiers et industriels. Ils montrent que la technologie peut répondre à des besoins concrets, à condition d'être intégrée de manière ciblée, gouvernée et interopérable.

Articulés avec les analyses de marché et les enjeux de souveraineté développés dans les parties précédentes, ces usages positionnent la blockchain comme un levier structurant de l'action publique et de la stratégie numérique européenne. La compréhension fine des cas d'usage constitue ainsi une étape indispensable pour passer d'une réflexion stratégique à une mise en œuvre opérationnelle maîtrisée.

Conclusion :

L'analyse menée tout au long de ce livre blanc permet de porter un nouveau regard sur la blockchain : la blockchain n'est plus une technologie émergente cantonnée à des usages marginaux, mais un **ensemble d'infrastructures et de marchés en cours de structuration**, appelés à jouer un rôle croissant dans le fonctionnement des économies, des administrations et des chaînes de valeur industrielles.

La première partie a montré que la valeur associée à la blockchain se concentre moins dans les usages grand public que dans les **infrastructures critiques**, les services de confiance, la finance numérique, la gouvernance des données et les mécanismes de coordination entre acteurs. Cette cartographie des marchés constitue un préalable indispensable pour appréhender les enjeux qui dépassent la seule dimension économique. **Elle révèle à quel point ces technologies deviennent structurantes, et donc stratégiques, pour la souveraineté numérique et la résilience des États et des entreprises.**

Dans ce contexte, la France et l'Europe se trouvent face à un **choix stratégique déterminant**. Accepter une dépendance croissante à des infrastructures, des protocoles et des modèles de gouvernance majoritairement extra-européens reviendrait à déléguer des fonctions critiques de confiance, de certification et de coordination. **À l'inverse, s'engager dans la structuration d'un écosystème blockchain européen implique de concilier innovation technologique, exigences de souveraineté, sécurité juridique et intérêt général. Ce choix ne saurait être réduit à une opposition entre innovation et régulation : il appelle la définition d'un cadre clair, stable et cohérent, permettant à l'innovation de se déployer de manière maîtrisée.**

La troisième partie montre que cette stratégie ne peut être uniquement théorique. Les cas d'usage concrets qu'il s'agisse de registres infalsifiables, de traçabilité des chaînes de valeur, d'automatisation des processus, d'enquêtes financières ou encore de valorisation énergétique – démontrent que la *blockchain* peut répondre à des besoins opérationnels réels. Toutefois, ces usages mettent également en lumière les **freins à l'adoption**, en particulier pour les acteurs industriels non spécialisés dans le numérique. La complexité technologique, la fracture culturelle avec l'univers des crypto-actifs, la question de la stabilité des crypto-monnaies ou encore les limites des blockchains permissionnées centralisées constituent autant de défis à relever.

À cet égard, la question de la **gouvernance des infrastructures blockchain** apparaît centrale. Les modèles entièrement centralisés peinent à instaurer une confiance durable, tandis que les blockchains publiques soulèvent des enjeux d'intégration économique et réglementaire. Le développement de blockchains de consortium, reposant sur des acteurs indépendants, des dispositifs validateurs diversifiés et une gouvernance partagée, constitue une voie exigeante mais structurante pour concilier confiance, résilience et souveraineté.

En définitive, la blockchain ne doit pas être appréhendée comme une solution universelle ou une fin en soi, mais comme un **outil stratégique**, à inscrire dans une démarche globale de transformation numérique. **Sa valeur dépendra de la capacité des acteurs publics et privés à articuler compréhension des marchés, maîtrise des usages, choix technologiques éclairés et gouvernance adaptée. C'est à cette condition que la blockchain pourra devenir un levier durable de confiance numérique, d'efficacité et de souveraineté au service de l'action publique et du développement économique européen.**

La blockchain se comprend donc comme un outil supplémentaire au service de la confiance numérique. Afin de permettre son déploiement, il est essentiel que les acteurs de cet écosystème naissant se fédèrent pour partager leurs expériences, leurs expertises, éclairer les décisions publiques et devenir acteurs de leur avenir. C'est précisément la démarche que propose l'ACN : structurer cet écosystème et promouvoir cet instrument de la confiance numérique, mais aussi de souveraineté.

Remerciements

L'ACN- Alliance pour la Confiance Numérique tient à adresser ses plus vifs remerciements à toutes les personnes et organisations qui ont contribué à l'élaboration de ce Livre Blanc.

Leur expertise et leur engagement ont été déterminants pour façonner ce document. Grâce à ces apports, ce projet mené dans le cadre du groupe de travail Blockchain de l'ACN incarne une vision collective et ambitieuse, essentielle pour répondre aux enjeux actuels et futurs de la blockchain.

Plus particulièrement, nos remerciements vont à :

- ABLIKOVA Elena, Noticio
- BERNIER Laurent, Cybalgoris
- COUSINEAU Andy, Sahar
- DURAND Marc, Kaplt
- EICH GOZZI Alexandre, Sopra Steria
- FAHER Mourad, Thales
- GROSJEAN Sophie, Alliance Blockchain France
- GEBEL Hélène, Sopra Steria
- HENNEBERT Christine, CEA
- HOTTEKIET BEAUCOURT Quentin, OBS/OCD
- MAISONNEUVE Antoine, OBS/DD
- MOREAU Sebastien, Noticio
- OGIER Philippe, Droon
- PORQUET Nicolas, CNRS
- SENOT Olivier, Docaposte
- SIMON Maryem, Orange
- THOMAS Benjamin, Orange
- THEVENET Thierry, Talao

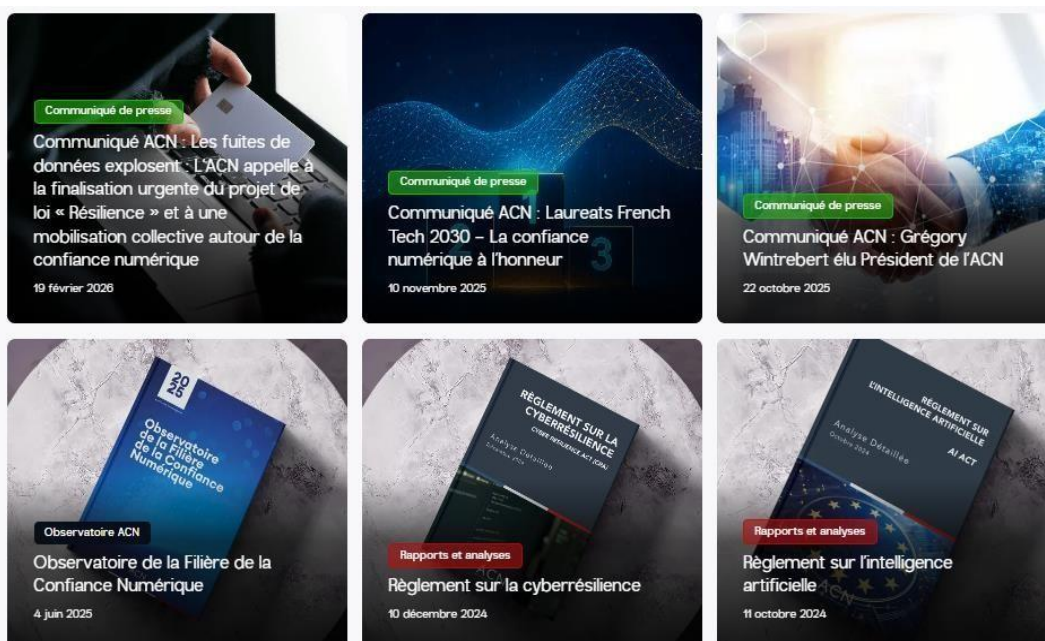
A propos de l'ACN :

L'Alliance pour la Confiance Numérique (ACN) est le syndicat professionnel qui représente les entreprises (leaders mondiaux, PME/TPE, et ETI) du secteur de la confiance numérique et notamment celles de l'identité numérique, de la cybersécurité, l'IA de confiance et de la blockchain.

La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre 2 178 entreprises réalisant en France 19 milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (8% de croissance annuelle moyenne depuis 2016). Les 120 membres de l'Alliance pour la Confiance Numérique (ACN), dont 87% de PME/ TPE-ETI, représentent 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité. Par ailleurs, l'ACN est également membre fondateur de l'association représentant l'écosystème européen de la cybersécurité : ECSO (European CyberSecurity Organisation).

Retrouvez nos publications (www.confiance-numerique.fr)



ACN

Alliance pour la confiance numérique



confiance-numerique.fr



SCAN ME

ACN - Alliance pour la confiance numérique