Cryptomonnaies : Promesses, Révolutions et Désillusions

Depuis l'émergence du Bitcoin en 2009, les cryptomonnaies se sont progressivement imposées comme une force de transformation potentielle du paysage financier mondial. Leur ambition : offrir une alternative aux systèmes bancaires traditionnels, redonner aux individus la maîtrise de leurs actifs, et ouvrir la voie à une économie plus transparente, décentralisée et inclusive.

Mais cette promesse, séduisante en théorie, s'accompagne de risques concrets, d'illusions persistantes et d'un brouillard idéologique qu'il est nécessaire de dissiper pour juger sereinement de la pertinence réelle de ces technologies.

Les vertus revendiquées : décentralisation, souveraineté, transparence

Les cryptomonnaies reposent sur un socle technologique précis : la blockchain, ou chaîne de blocs, qui constitue un registre distribué, c'est-à-dire une base de données répliquée sur un réseau de nœuds indépendants (ordinateurs interconnectés), sans autorité centrale de contrôle. Chaque transaction y est enregistrée sous forme cryptographiquement signée, horodatée et liée à la précédente, formant une séquence immuable, sauf consensus explicite du réseau pour la modifier, ce qui est en pratique quasi-impossible dans les blockchains publiques majeures comme Bitcoin ou Ethereum.

Cette décentralisation n'est pas qu'un principe abstrait : elle repose sur des mécanismes concrets tels que le Proof of Work (preuve de travail) ou le Proof of Stake (preuve d'enjeu), qui permettent à des participants, appelés mineurs ou validateurs, de sécuriser le réseau et de valider les blocs selon des règles protocolaires codées dans le logiciel. L'objectif est d'éliminer le besoin de tiers de confiance traditionnels : banques, institutions centrales, chambres de compensation. Une fois la transaction incluse dans un bloc confirmé, elle devient inaltérable et vérifiable publiquement.

D'un point de vue économique, cela se traduit par une souveraineté transactionnelle inédite : aucun acteur central ne peut bloquer un virement, geler un compte ou imposer une censure. Pour les défenseurs de cette architecture, cela garantit une forme de liberté monétaire, voire d'« auto-bancarisation », dans un monde où la monnaie n'est plus émise, ni garantie par une autorité souveraine, mais définie par un code et protégée par la cryptographie.

Parallèlement, les blockchains publiques offrent une transparence radicale. Chaque transaction est visible, traçable, et stockée de manière permanente. Des explorateurs de blocs *(comme Etherscan ou Blockchain.com)* permettent à n'importe quel internaute d'auditer les mouvements de fonds, de consulter l'activité des portefeuilles, ou d'analyser l'état du réseau. Cela constitue un environnement propice à l'auditabilité automatisée, à la comptabilité en temps réel, et à la programmabilité financière via des *smart contracts* (contrats intelligents), qui permettent l'exécution de clauses sans intervention humaine, dès lors que les conditions sont réunies.

Enfin, un argument souvent avancé est celui de l'inclusion financière. Dans les régions du monde où l'accès aux services bancaires traditionnels est limité en raison de l'absence d'infrastructure, de confiance ou de stabilité institutionnelle, par exemple, il suffit d'un smartphone et d'une connexion Internet pour détenir, envoyer ou recevoir des actifs numériques. Cela contourne les barrières d'entrée imposées par les systèmes classiques : contrôle d'identité, exigence de revenus, dépendance à une monnaie nationale instable.

Mais cette promesse repose sur des prérequis techniques (compétence numérique, accès à Internet, sécurisation des clés privées) qui limitent encore fortement son application concrète. L'inclusion théorique ne suffit pas à garantir une inclusion réelle sans efforts éducatifs, interfaces intuitives, et mécanismes de protection contre les pertes accidentelles ou les abus.

Les risques réels : instabilité, opacité sociale, dérive spéculative

Si les cryptomonnaies incarnent une innovation radicale dans le champ des technologies financières, elles n'en présentent pas moins des vulnérabilités majeures, trop souvent sous-estimées dans les discours enthousiastes. Ces vulnérabilités ne sont pas marginales ou temporaires puisqu'elles relèvent de caractéristiques systémiques qui remettent en question leur capacité à assumer, à court et moyen termes, les fonctions essentielles d'une monnaie ou d'un actif de confiance.

➔ *1. Instabilité monétaire et volatilité systémique*

La première limite tient à l'extrême volatilité des cours. Contrairement aux monnaies fiduciaires, qui sont stabilisées par des politiques monétaires actives (taux d'intérêt, interventions de banques centrales, mécanismes de change), les cryptomonnaies sont, pour la plupart, non adossées à des actifs réels et ne disposent d'aucune institution de lissage macroéconomique.

La valeur d'un token comme le Bitcoin ou l'Ether est purement déterminée par la loi de l'offre et de la demande sur des marchés fragmentés, peu régulés, et exposés à une forte spéculation. Les fluctuations de prix peuvent dépasser 20 à 30 % en une journée, en réponse à des événements exogènes (tweets de personnalités, annonces réglementaires, attaques informatiques) ou à des mouvements de liquidité.

Cette instabilité intrinsèque rend les cryptomonnaies inadaptées à un usage transactionnel quotidien : aucun commerçant ou salarié ne peut raisonnablement accepter un paiement dans une monnaie dont la valeur peut s'effondrer quelques heures plus tard. De même, leur rôle de réserve de valeur souvent revendiqué par analogie avec l'or, reste contestable : une réserve de valeur se caractérise par sa constance, sa liquidité et sa capacité à traverser les cycles économiques, ce qui est loin d'être démontré à ce stade.

Même les stablecoins, censés remédier à ce problème en s'indexant sur une devise (USD, EUR, etc.), sont vulnérables : certains sont sous-collatéralisés (ex. TerraUSD, effondré en 2022), d'autres centralisés et dépendants de réserves bancaires dont la transparence est discutable (ex. Tether/USDT). L'illusion de stabilité est donc souvent fragile.

➔ *2. Opacité socio-technique et usages dévoyés*

Si les blockchains publiques offrent une transparence structurelle au niveau des données, l'usage qui en est fait est loin d'être aussi limpide. Les adresses cryptographiques (longues chaînes alphanumériques) ne sont pas directement associées à des identités humaines. Cela confère aux utilisateurs un pseudo-anonymat, qui rend très difficile l'attribution formelle d'une transaction à une personne physique, sauf en présence d'une coopération judiciaire ou d'une erreur d'opsec de l'utilisateur.

Ce flou identitaire ouvre la voie à des usages détournés : les cryptomonnaies sont massivement utilisées dans des contextes illégaux (ransomwares, trafics, fraude fiscale, contournement des sanctions internationales, financement d'activités illicites…) précisément parce qu'elles permettent de déplacer des fonds à l'échelle mondiale sans l'intermédiation d'un système bancaire régulé.

Même les plateformes dites "KYC-compliant" (qui vérifient l'identité de leurs utilisateurs) ne garantissent pas un assainissement total de l'écosystème, d'autant que de nombreuses passerelles "off-ramp" ou portefeuilles auto-hébergés permettent d'échapper à toute supervision. Les outils d'obfuscation (mélangeurs de fonds, coins privés comme Monero ou Zcash, protocoles de confidentialité comme Tornado Cash) renforcent encore cette opacité.

Paradoxalement, cette transparence structurelle est donc souvent inopérante sur le plan social et judiciaire. Et le caractère irréversible des transactions sur blockchain interdit toute annulation en cas de fraude, d'erreur ou d'usurpation — contrairement à ce que permettent les circuits bancaires classiques via les mécanismes de litige ou de remboursement.

➔ 3. Concentrations de pouvoir dans un système prétendument décentralisé

Le mythe d'une décentralisation absolue se heurte à plusieurs réalités techniques et économiques. Sur le plan du minage (notamment dans les blockchains en Proof of Work), on observe une concentration géographique et technologique : les ressources informatiques nécessaires pour participer à la validation des blocs sont telles que seules de grandes entités industrielles, disposant d'un accès privilégié à de l'énergie bon marché et de matériel spécialisé (ASICs), peuvent opérer efficacement. Résultat : une poignée de pools de minage contrôlent une part significative du hashrate mondial, ce qui crée un risque de "cartelisation", voire de collusion.

Dans les protocoles de type Proof of Stake, la situation n'est pas fondamentalement différente : la probabilité de valider un bloc est proportionnelle à la quantité de tokens détenus. Cela favorise mécaniquement les acteurs déjà riches, accentue les inégalités initiales de distribution, et conduit à une ploutocratie technologique où le pouvoir décisionnel est corrélé à la richesse en jetons.

Par ailleurs, la gouvernance des projets est souvent centralisée autour d'une fondation, d'une équipe de développeurs, ou d'un consortium restreint de contributeurs. Les mises à jour des protocoles (hard forks, modifications de règles de consensus, évolutions fonctionnelles) ne sont pas toujours soumises à un processus démocratique ou formel, ce

qui pose la question de la légitimité des décisions techniques ayant des impacts économiques majeurs.

Enfin, les plateformes d'échange centralisées (CEX) comme Binance, Coinbase ou Kraken jouent un rôle structurant dans l'accès aux cryptomonnaies, leur liquidité et leur prix. Elles constituent des points de centralisation fonctionnels, souvent soumis à des logiques commerciales opaques, et vulnérables à la régulation, aux attaques ou à la faillite (cf. l'affaire FTX, 2022).

Ainsi, les cryptomonnaies ne sauraient être évaluées uniquement à l'aune de leur architecture technique. Leurs usages réels, leur gouvernance, leur intégration dans l'économie, et les externalités qu'elles génèrent doivent être pris en compte. Les risques identifiés ne sont pas anecdotiques car ils mettent en tension les fondements mêmes de la promesse originelle, liberté, transparence, décentralisation, en révélant une série de contradictions internes, qu'aucune ingénierie purement technologique ne peut résoudre seule.

Une technologie, pas une utopie

Il convient d'adopter une posture de discernement face au phénomène des cryptomonnaies, en résistant simultanément à deux dérives intellectuelles symétriques : le rejet condescendant qui les réduit à un simple engouement spéculatif voué à disparaître, et l'adhésion dogmatique à une vision utopique d'un monde désintermédié, affranchi des États, des institutions et de toute forme de régulation centralisée.

Dans les deux cas, l'erreur consiste à essentialiser la technologie, c'est-à-dire à lui prêter une finalité propre, intrinsèquement bonne ou mauvaise. Or les cryptomonnaies, au même titre que l'imprimerie, l'électricité ou l'intelligence artificielle, ne sont pas des idéologies incarnées, mais des infrastructures techniques. Elles ne font qu'offrir un cadre opérationnel nouveau pour concevoir, transférer et stocker de la valeur, à travers des systèmes distribués fondés sur la cryptographie.

En tant que telles, elles doivent être appréhendées comme des outils socio-techniques, dont la pertinence dépend intégralement :

- ➔ des usages qu'on en fait (paiements transfrontaliers, finance décentralisée, certification de données, spéculation, évasion fiscale, etc.) ;
- ➔ du contexte dans lequel elles s'insèrent (niveau de développement économique, cadre juridique, stabilité institutionnelle, taux de bancarisation) ;
- ➔ et de la gouvernance mise en place autour de leurs protocoles (architecture de validation, mécanismes d'évolution du code, modèles de participation communautaire ou de gouvernance d'entreprise).

L'erreur serait de projeter sur ces technologies un idéal politique totalisant. L'histoire a montré que toute infrastructure technique aussi prometteuse soit-elle, peut être détournée, captée ou corrompue par les dynamiques économiques et les rapports de force. Les cryptomonnaies n'échappent pas à cette règle : elles peuvent aussi bien renforcer la

souveraineté des individus que concentrer le pouvoir entre les mains d'oligopoles numériques ; favoriser l'inclusion financière que creuser les inégalités d'accès à la connaissance ; offrir un levier d'émancipation que devenir un vecteur d'instabilité ou de prédation.

Le caractère programmable et ouvert des blockchains n'est pas, en soi, garant de progrès social. L'automatisation n'abolit pas les conflits d'intérêts ; la transparence ne supprime pas l'opacité interprétative ; et la décentralisation technique ne garantit nullement une décentralisation politique ou économique effective.

Les cryptomonnaies doivent être jugées sur pièces, à partir de cas d'usage concrets, d'analyses empiriques rigoureuses, et non de projections théoriques. Ni gadget transitoire, ni révolution salvatrice, elles constituent un levier d'expérimentation institutionnelle, dont les conséquences dépendent moins du code que de la façon dont les sociétés s'en saisissent, les encadrent, les réorientent ou les laissent dériver.

Vers une régulation systémique : encadrer sans étouffer

À mesure que les cryptomonnaies s'inscrivent durablement dans l'architecture des échanges numériques, leur encadrement juridique devient un enjeu central, à la croisée de plusieurs champs : droit financier, souveraineté monétaire, sécurité informatique, protection des consommateurs et stabilité macroéconomique. Il ne s'agit plus, aujourd'hui, de décider s'il faut ou non « réguler » les crypto-actifs : la question est désormais de savoir comment construire un cadre normatif pertinent, c'est-à-dire à la fois proportionné, opératoire et technologiquement intelligible.

- ➔ 1. Un défi de qualification juridique

La première difficulté réside dans l'absence de consensus global sur la nature juridique des cryptomonnaies. Sont-elles des monnaies privées, des titres financiers, des actifs numériques, des instruments de paiement, des biens incorporels ? Cette indétermination compromet l'harmonisation des législations et ouvre la voie à des arbitrages réglementaires opportunistes de la part des acteurs économiques (exil fiscal, choix de juridiction, exploitation des zones grises).

L'Union européenne, avec le règlement MiCA (Markets in Crypto-Assets), a tenté de proposer un cadre unifié, en distinguant trois catégories :

- ➔ les utility tokens (jetons d'usage) ;
- ➔ les asset-referenced tokens (adossés à un panier d'actifs) ;
- ➔ et les e-money tokens (indexés sur une monnaie unique, comme certains stablecoins).

Cette catégorisation reste toutefois fragile face à l'hybridité des usages, à la rapidité de l'innovation technique et à l'apparition constante de nouveaux modèles économiques (DeFi, DAO, NFT, etc.).

➔ 2. Stabilité financière et risque systémique

À l'échelle macroéconomique, l'essor des cryptomonnaies en particulier des stablecoins à grande échelle, pose la question de leur interaction avec le système monétaire traditionnel. Si un stablecoin adossé au dollar venait à concentrer une part significative des transactions quotidiennes dans une zone monétaire, il pourrait bypasser les canaux classiques de transmission de la politique monétaire, voire menacer la souveraineté des banques centrales.

Ce risque a été explicitement reconnu par plusieurs institutions (Banque des Règlements Internationaux, BCE, Réserve fédérale). En réponse, des initiatives publiques ont émergé, telles que les monnaies numériques de banque centrale (MNBC ou *CBDC*), visant à offrir une alternative institutionnelle et régulée à l'innovation crypto-native. L'objectif est double : préserver la maîtrise étatique des infrastructures monétaires tout en intégrant certaines fonctionnalités techniques inspirées de la blockchain (programmabilité, traçabilité, paiement pair-à-pair).

Toutefois, les MNBC ne sont pas équivalentes aux cryptomonnaies : elles sont centralisées, émis par des institutions souveraines, et conçues dans un cadre réglementaire strict. Leur coexistence avec les crypto-actifs soulève des interrogations : faut-il interdire certains usages privés ? Imposer des limites de conversion ? Obliger les stablecoins à être entièrement collatéralisés par des actifs liquides ?

3. Protection des consommateurs et lutte contre les abus

Sur le plan microéconomique, l'environnement crypto reste largement dominé par une asymétrie d'information massive entre les développeurs, les investisseurs institutionnels et les usagers lambda. L'absence de garanties, de mécanismes de recours, ou de régulation des pratiques commerciales (publicité agressive, promesses de rendement irréalistes, pump and dump) expose les utilisateurs à des pertes considérables.

Les autorités cherchent donc à étendre aux acteurs crypto les obligations applicables aux services financiers traditionnels :

- obligations de transparence (white papers, audits de smart contracts) ;
- exigences de solvabilité pour les plateformes d'échange ;
- règles de prévention contre les conflits d'intérêts et la manipulation de marché ;
- normes de cybersécurité et gestion des risques opérationnels.

Par ailleurs, la lutte contre le blanchiment de capitaux (AML) et le financement du terrorisme (CFT) impose aux prestataires de services crypto (PSAN en France) de respecter des procédures KYC (Know Your Customer), ce qui entre parfois en tension avec les principes d'anonymat défendus par certaines communautés.

La question est ici de savoir jusqu'où pousser l'encadrement sans tuer l'innovation. Une régulation trop rigide risque de favoriser les acteurs déjà dominants, capables d'absorber les

coûts de conformité, et d'exclure les projets décentralisés ou communautaires qui ne disposent pas de structure juridique classique.

➔ 4. Gouvernance algorithmique et droit des protocoles

Un autre défi fondamental réside dans la gouvernance des protocoles eux-mêmes. À qui appartient le code ? Qui peut le modifier ? Qui est responsable en cas de faille ? Le droit positif peine à répondre à ces questions, car les smart contracts, les DAO (organisations autonomes décentralisées), ou les forks de blockchain ne rentrent pas dans les catégories classiques du droit des sociétés, du contrat ou de la propriété intellectuelle.

Il s'agit là d'un champ émergent du droit numérique : comment articuler la normativité algorithmique (le code fait loi) avec la normativité juridique (la loi encadre le code) ? Faut-il imposer une supervision humaine ? Introduire une responsabilité pénale ou civile des développeurs ? Reconnaître la personnalité juridique des protocoles ?

Des pistes commencent à émerger, mais elles restent encore exploratoires. L'approche par la soft law (chartes éthiques, codes de conduite, certifications de sécurité) coexiste avec des tentatives plus coercitives (interdiction de certains protocoles de confidentialité, sanctions contre des développeurs open source, etc.).

La régulation des cryptomonnaies ne peut pas se réduire à une simple transposition des normes existantes. Il s'agit d'un changement d'architecture dans la manière de concevoir la monnaie, la finance et la gouvernance économique. En ce sens, la question n'est pas tant celle de la conformité des cryptomonnaies à l'ordre juridique actuel, que celle de l'adaptabilité du droit à une nouvelle génération d'infrastructures décentralisées, transnationales et automatisables.

La régulation ne doit donc ni sanctuariser un statu quo bancaire dépassé, ni céder au solutionnisme technologique. Elle doit se concevoir comme un équilibre dynamique entre innovation, protection des citoyens, et sauvegarde des prérogatives publiques fondamentales. Cela suppose une montée en compétence des régulateurs, une coopération internationale renforcée, et une capacité à penser le droit non comme un frein à la technique, mais comme un dispositif d'orientation et de responsabilisation des innovations.

Annexe explicative : le fonctionnement technique des cryptomonnaies

Comprendre le fonctionnement des cryptomonnaies implique de décortiquer un ensemble de mécanismes technologiques imbriqués, allant de la théorie des registres distribués à la cryptographie asymétrique, en passant par les protocoles de consensus, les mécanismes d'émission monétaire et la validation des transactions. Ce système forme un écosystème computationnel autonome, dans lequel la confiance n'est plus déléguée à une autorité centrale, mais émerge de la robustesse mathématique et de la transparence structurelle du protocole.

➔ 1. La blockchain : un registre distribué, append-only

Le cœur d'une cryptomonnaie est la blockchain, ou « chaîne de blocs » : un registre décentralisé, distribué et infalsifiable, conçu pour enregistrer de manière chronologique et publique l'ensemble des transactions validées sur le réseau.

Chaque bloc contient :

- un ensemble de transactions validées ;
- un pointeur vers le bloc précédent (via un hash cryptographique) ;
- un horodatage ;
- des métadonnées (version du protocole, nonce, etc.).

L'ensemble forme une chaîne linéaire où chaque nouveau bloc renforce l'intégrité des blocs précédents. Toute tentative de falsification nécessite de recalculer tous les blocs suivants, ce qui devient rapidement computationnellement prohibitif.

➔ 2. Cryptographie asymétrique : propriété et signature des transactions

Chaque utilisateur du réseau possède une paire de clés cryptographiques asymétriques : une clé privée (secrète), utilisée pour signer les transactions, et une clé publique, servant d'identifiant pseudonyme (adresse) sur le réseau.

Une transaction valide consiste en un message (ex. : « A transfère 0,5 BTC à B ») signé par la clé privée de l'émetteur. Le réseau peut ensuite vérifier l'authenticité de cette signature sans jamais accéder à la clé privée, grâce aux propriétés mathématiques de la cryptographie à clé publique (algorithme ECDSA dans Bitcoin).

Ainsi, la possession de la clé privée équivaut à la possession des fonds associés. Cela rend le système résilient à la fraude, mais impitoyable en cas de perte de la clé : il n'existe aucun moyen centralisé de récupération.

➔ 3.Le modèle de validation : consensus sans confiance

Dans un système distribué sans autorité centrale, se pose un problème fondamental : comment s'assurer que tous les participants du réseau s'accordent sur un seul état de vérité ? C'est le rôle des protocoles de consensus, qui permettent à un réseau pair-à-pair d'ajouter de nouveaux blocs à la chaîne de manière coordonnée, sécurisée et sans recours à une entité centrale.

a. Preuve de travail (Proof of Work – PoW)

Le protocole originel de Bitcoin repose sur la preuve de travail : pour proposer un nouveau bloc, les nœuds (mineurs) doivent résoudre un problème mathématique complexe le *hash puzzle*, consistant à trouver un nonce tel que le hash du bloc commence par un certain nombre de zéros.

Ce mécanisme :

- assure la rareté (le bloc est coûteux à produire) ;
- rend les attaques économiquement dissuasives (coût en énergie) ;
- favorise l'émergence d'un consensus probabiliste (la chaîne la plus longue est considérée comme la plus fiable).

La récompense pour le mineur (nouveaux bitcoins + frais de transaction) constitue le mécanisme d'incitation économique à maintenir le réseau.

b. Autres consensus : Proof of Stake, etc.

D'autres cryptomonnaies (Ethereum depuis 2022, Cardano, etc.) utilisent des variantes comme la preuve d'enjeu (Proof of Stake – PoS), où la création des blocs est confiée à des validateurs sélectionnés proportionnellement à leur mise en jeu (staking). Cela réduit la consommation énergétique mais introduit de nouvelles problématiques (centralisation du capital, risques d'oligopole, etc.).

➔ 4. Émission monétaire et politiques économiques embarquées

La quantité totale d'unités monétaires peut être fixe (Bitcoin est limité à 21 millions de BTC), inflationniste (Dogecoin), ou algorithmique (stablecoins comme DAI). Les règles d'émission sont inscrites dans le code source du protocole et exécutées automatiquement par le réseau.

Dans le cas de Bitcoin :

- la création de nouveaux bitcoins est divisée par deux tous les 210 000 blocs (~ tous les 4 ans) : c'est le mécanisme de halving ;
- la récompense initiale (50 BTC par bloc) est aujourd'hui de 3,125 BTC (en 2025) ;
- ce modèle encode une déflation programmée, sans recours à une banque centrale.

➔ 5. Les nœuds : infrastructure décentralisée

Le réseau est composé de nœuds interconnectés : les nœuds complets (full nodes) conservent une copie intégrale de la blockchain et valident chaque transaction indépendamment et les nœuds légers (SPV clients) se fient à des nœuds complets pour obtenir des preuves cryptographiques minimales.
La résilience du réseau tient à la multiplicité des nœuds et à l'absence de point de défaillance unique. Même si certains nœuds sont déconnectés ou censurés, le reste du réseau continue de fonctionner.

➔ 6. Smart contracts : automatisation des règles transactionnelles

Sur certaines blockchains programmables (Ethereum, Solana, etc.), il est possible d'écrire des smart contracts : des programmes autonomes, exécutés de manière déterministe sur le réseau, qui conditionnent des transferts de valeur à des règles explicites (par exemple : « si A envoie X tokens à B, alors C reçoit Y en retour »).

Ces contrats sont :

- immuables une fois déployés (sauf architecture prévue) ;
- publics et auditables, mais souvent complexes à interpréter ;
- automatiquement exécutés, ce qui supprime le recours à un arbitre ex post.

C'est l'infrastructure de base de la finance décentralisée (DeFi), qui permet des prêts, échanges, assurances ou produits dérivés sans intermédiaire institutionnel.

Le fonctionnement d’une cryptomonnaie ne repose pas sur une entité, mais sur l’interopérabilité de briques technologiques (cryptographie, théorie des jeux, informatique distribuée, économie incitative) rigoureusement agencées pour faire émerger un ordre transactionnel sans confiance centralisée.

Ce système repose sur des hypothèses précises : intégrité des participants majoritaires, rationalité économique, stabilité logicielle. Il ouvre des perspectives inédites d’innovation monétaire, mais reste sensible aux dynamiques sociotechniques : concentration du pouvoir, bugs dans les smart contracts, conflits autour des forks, etc.

Donc comprendre la technologie n’est pas suffisant : encore faut-il l’inscrire dans une lecture systémique, mêlant code, institutions, acteurs, et usages. C’est à cette seule condition qu’on peut évaluer lucidement ce que la cryptomonnaie promet, et ce qu’elle produit réellement.

Les sources :

Halving de Bitcoin : périodicité (210 000 blocs ≈ tous les 4 ans), réduction des récompenses, approvisionnement total limité à 21 millions BTC
https://www.bitstore.net/en/blog/what-is-bitcoin-halving/
https://www.blockpit.io/en-us/blog/bitcoin-halving
https://proton.me/blog/how-does-bitcoin-work

Volatilité, limites des stablecoins, instabilité : discussions dans les publications économiques, même si non directement citées, base le paragraphe sur consensus académique et rapports régulateurs (e.g., BCE)
https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html

Usage criminel, blanchiment, ransomware : données historiques, volumes, usage des stablecoins illicitly ; Chainalysis, FBI
https://www.reuters.com/sustainability/boards-policy-regulation/global-financial-crime-watchdog-calls-action-crypto-risks-2025-06-26/
https://www.ft.com/content/84a4d927-3597-4c51-b8c9-86215f682eda

Cas concrets d'enquêtes internationales (Operation Destabilise, réseau de blanchiment via cryptos)
https://www.wired.com/story/operation-destabilise-money-laundering/

Législation européenne MiCA – structure, catégories de tokens, entrée en vigueur en 2023, objectifs (transparence, protection, stabilité)
https://www.innreg.com/blog/mica-regulation-guide
https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

Surveillance internationale et alertes des organismes (FATF, AMLA/FISMA) – conformité, volumes de reçus par adresses illicit crypto en 2024 (~51 milliards $), seulement 40 pays conformes en avril 2025
https://www.reuters.com/sustainability/boards-policy-regulation/global-financial-crime-watchdog-calls-action-crypto-risks-2025-06-26/

Recommandations du Conseil de Stabilité Financière (FSB) pour une approche proportionnée et coordonnée (principe « same activity, same risk, same regulation »)
https://www.fsb.org/uploads/P111022-3.pdf

Études académiques comparant les approches réglementaires mondiales, défis de classification juridique des tokens, gouvernance algorithmique
https://arxiv.org/abs/2404.15895
https://arxiv.org/abs/2109.01047

Influence de MiCA dans la structuration de la régulation européenne et ses implications en termes de conformité opérationnelle
https://www.jonesday.com/en/insights/2025/07/crypto-assets-casps-and-amlcft-compliance-the-new-european-regulatory-landscape-under-mica-and-amlr
https://link.springer.com/article/10.1007/s10657-024-09797-w