DE LA MONNAIE FIDUCIAIRE AUX CRYPTO-ACTIFS ET STATUT DE L'EURO

Christian BIALÈS
Conférence à « Initiatives Plurielles »
du 3 avril 2026

Introduction

Les usages numériques ont été fortement accélérés à la suite de la pandémie de Covid-19 et son cortège de mesures barrières. Par exemple, le recours massif au télétravail a fait exploser le nombre d'appareils connectés aux réseaux d'entreprises. Les nouvelles technologies ont également été une soupape de décompression et un terrain de réinvention des loisirs (*streaming, gaming*, etc.), ce qui a radicalement modifié les habitudes de consommation des produits et des services. Selon la Banque Mondiale (2022), deux tiers des adultes à travers le monde ont désormais recours à des transactions électroniques ou numériques pour effectuer ou recevoir un paiement. En France, dans le domaine de la FinTech, les mots « NFT » (NFT signifie non-fungible token (jeton non fongible). « Non fongible » signifie essentiellement qu'il s'agit d'une chose unique et irremplaçable*. À l'instar de certaines cartes à collectionner et œuvres d'art, les NFT ont une identité unique et ne peuvent être reproduits) et *« Bitcoin* » ont été parmi les plus cités par la presse en 2021.

*Fongibilité : qualité des choses qui peuvent se remplacer mutuellement sans en altérer l'usage et/ou qui se consomment par l'usage et peuvent être remplacés par des biens analogues. La monnaie légale est fongible par définition (les billets et pièces de monnaie sont totalement substituables) ; les matières premières sont d'autres exemples. Fongible vient du latin fungi qui veut dire « s'acquitter, consommer ».

Retour préalable et schématique sur les fondements de la monnaie :

Les 3 caractéristiques de la monnaie

- **Universalité** : la monnaie est acceptée par tout le monde et pour toute opération d'échange, dans un espace déterminé qui constitue la communauté de paiement.
- **Fongibilité** : étymologiquement, cela signifie que la monnaie permet de s'acquitter de toute dette. Cela signifie aussi que les moyens de paiement sont interchangeables.
- **Liquidité** : la monnaie se confond avec la liquidité absolue ; la liquidité étant l'aptitude d'un bien à se transformer plus ou moins rapidement en moyen de paiement.

Liquidité décroissante

liquidité primaire	→ monnaie	} actifs monétaires
liquidité secondaire	→ quasi-monnaie (épargne liquide)	} actifs financiers non risqués et à c.t.
liquidité tertiaire	→ valeurs mobilières	} actifs financiers risqués et à m. l. t.
	→ actifs réels	

Les 3 pouvoirs de la monnaie

- Pouvoir libératoire
- Pouvoir d'achat
- Pouvoir de choix
  - dans l'espace ⇒ la monnaie est un instrument de gestion patrimoniale
  - dans le temps ⇒ la monnaie est un instrument d'arbitrage intertemporel

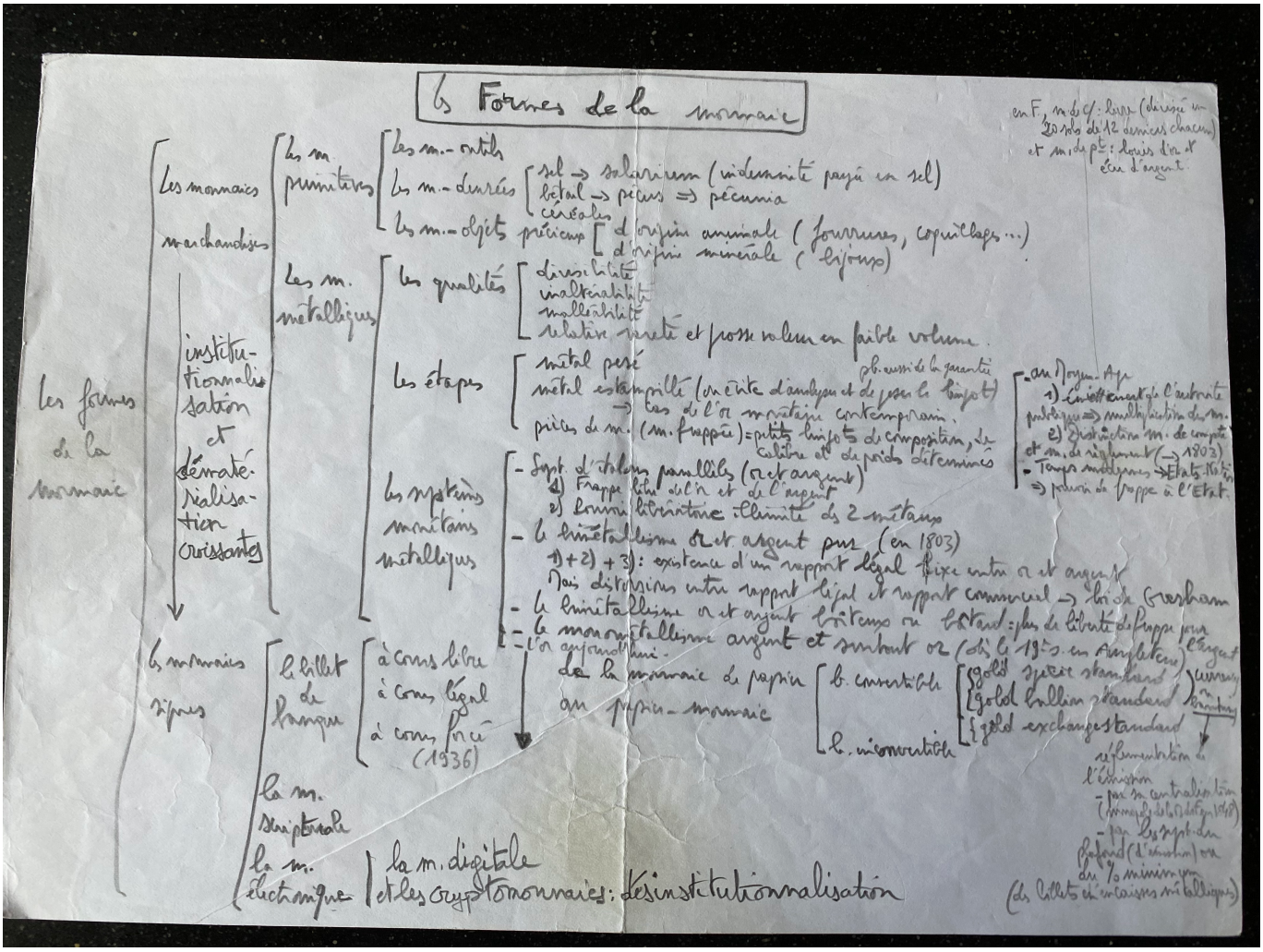
Actif

- rendement monétaire : revenu courant / gain (ou perte) en capital.
- rendement d'usage

Actif liquide

- rendement monétaire peu important car actif non risqué
  - revenu croissant mais en faible → "coût de la liquidité"
  - pas de fait risque de perte en capital
- rendement d'usage → Sécurité car cible les risques de retournement de l'incertitude du futur
  - risque d'insolvabilité (défaillance du débiteur)
  - risque d'illiquidité avec ses 3 coûts
    - de non paiement
    - de liquidation
    - de transaction
    - coûts explicites
    - coûts implicites

Pouvoir de choix et d'achat dans le temps (avec coûts de liquid. et de transact. faibles voire nuls).



La double analyse de la nature de la monnaie :

Deux remarques importantes préalables

• La nature de la monnaie est d'être ambivalente puisqu'elle est à la fois un bien *public* car elle réalise l'unité des règles qui structurent le système des paiements de la communauté de paiements considérée, et l'objet de tous les désirs *privés* d'appropriation.

La monnaie met fin aux rivalités généralisées entre agents économiques et, en tant que telle, elle fait l'objet d'un désir unanime de richesse, surtout que c'est en même temps la référence commune à laquelle tous les autres objets de désir se mesurent ; l'essence profonde de la monnaie est de se confondre avec la liquidité absolue (la liquidité d'un actif étant son aptitude à être transformé en moyen de paiement c'est-à-dire précisément en monnaie, plus ou moins rapidement, plus ou moins facilement et plus ou moins coûteusement), liquidité absolue, unanimement acceptée et donc commune à tous ; le désir de richesse dont la monnaie est l'objet est, autrement dit, un désir de liquidité. Ce référent commun est donc une institutionnalisation collective.

• Toute monnaie est une dette qu'une banque émet sur elle-même pour la prêter à un agent non financier (de façon à ce qu'il puisse mener à bonne *fin* son projet) et cette dette bancaire prend le statut de monnaie dès lors que les agents non financiers la reconnaissent comme moyen de paiement entre eux et la font donc circuler dans la communauté de paiement qu'ils constituent (voir sur ce sujet « Par ici la monnaie »).

La monnaie légale qu'émet le Banque centrale est le pivot d'un système de dettes dont elle est la dette supérieure et la confiance dans la monnaie implique que la hiérarchie des dettes soit respectée. C'est précisément quand cette hiérarchie n'est pas respectée ou, autrement dit, quand le système de dettes n'est pas convenablement hiérarchisé que des symptômes de crise se manifestent.

Il en est ainsi dans deux cas typiques.

Le premier, c'est quand les débiteurs sont soumis à des contraintes excessives de remboursement ou de coût des crédits qui leur ont été octroyés qui menacent leur solvabilité pour des raisons globales et indépendantes de leurs propres choix de projets à financer. Alors, il y a concrètement un manque de monnaie, le règlement des dettes est paralysé, d'où multiplication des faillites et l'effondrement du prix de tous les actifs : on entre donc dans une crise déflationniste.
Dans le second cas, en quelque sorte symétrique du premier, le financement des débiteurs est facilité au maximum, au point que le renouvellement des dettes se trouve assuré par une création monétaire automatique ; au point de soustraire les débiteurs à la contrainte de règlement, et ce, quelle que soit la qualité de leurs dettes (et de leurs projets), ce qui frustre les créanciers de leurs droits sur le capital. Alors, comme l'évaluation de la qualité des dettes est brouillée et que la création excessive de monnaie ne préserve plus l'intégrité de la monnaie dans ses trois fonctions essentielles (voir ci-après), il y a effondrement de la confiance dans la monnaie, d'autant plus que la conservation et la transmission des patrimoines sont gravement altérées. C'est la crise inflationniste, voir hyperinflationniste.

L'analyse fonctionnelle :

Voir https://christian-biales.fr/wp-content/uploads/2017/11/Fonctions-monnaie.pdf

L'analyse institutionnelle de la monnaie :
Comme il a été dit, la monnaie est une institutionnalisation collective et c'est ce processus d'institutionnalisation qui valide la convention monétaire pour toute la communauté de paiement, convention rassemblant toutes les règles codifiées par la puissance publique.
Cette analyse institutionnelle est importante car elle autorise une *analyse hétérodoxe du statut de l'euro*, la monnaie unique de la zone euro, que fait Michel Aglietta en particulier dans son livre « La monnaie, entre dettes et souveraineté », dont la publication date tout juste de 10 ans.
Nous reprenons cette analyse pour notre compte :
La banque centrale européenne est une institution qui présente la grande particularité de ne pas être placée sous l'autorité d'une source de souveraineté. En effet, la souveraineté est toujours conférée par un ordre constitutionnel qui formalise les fondements du vivre ensemble dans une société. Or, dans la zone euro, un tel ordre constitutionnel n'existe pas. L'Euro n'est donc pas une monnaie de plein exercice qui unit les citoyens sous l'égide d'un parlement souverain conférant à la Banque centrale la légitimité de la loi dans ses rapports organiques avec l'État. En ce sens, l'euro est fondamentalement une monnaie internationale. La non-existence du lien organique entre la monnaie unique et le souverain politique a d'importantes et graves conséquences. Nous vivons dans un espace monétaire commun sans espace public, donc sans institutions qui pourraient animer une vie démocratique, source de coordination et de choix collectifs. La BCE ne peut pas en principe être le prêteur en dernier ressort de la dette publique d'un quelconque État membre. Cela rabaisse les dettes publiques des pays membres au rang de dettes privées vis-à-vis de la contrainte de règlement. Puisque tout État membre peut faire défaut sur sa dette, comme on l'a vu pour la Grèce depuis 2010, tout se passe, comme si l'euro était une monnaie étrangère pour les États membres. Il en découle une fragmentation de l'espace monétaire : un euro déposé dans une banque grecque n'a pas alors la même valeur qu'un euro déposé dans une banque allemande ou française.
Par contre, zone euro est davantage qu'une union monétaire telle qu'on en rencontre dans l'histoire, comme l'union latine fondée en décembre 1865 et l'union scandinave créé en mai 1873. Car dans la zone euro les monnaies nationales ont disparu. Il s'ensuit que le système de paiement est complètement unifié. La finalité des paiements est réalisée dans toute la zone par un étage supérieur de compensation-règlement entre les banques centrales nationales sur les livres de la BCE, via le système TARGET2.
Il n'empêche que l'incomplétude de l'euro au niveau politique affecte gravement la macro-économie de la zone euro. L'Euro n'étant pas placé sous une souveraineté politique dans son espace de circulation, les politiques économiques des États membres ne font pas une unité, empêchant la zone comme un tout d'avoir une macro-économie cohérente. Les limitations du traité de Maastricht empêchent les instances de médiation européenne, que sont la commission européenne, l'Eurogroupe et le parlement européen, d'exercer la gouvernance adéquate sur les politiques économiques au niveau agrégé. Non souveraine, la zone euro n'a pas de politique budgétaire et n'a pas de politique monétaire extérieure. Il s'ensuit un triple

NON contradictoire qui affecte la crédibilité du Conseil des gouverneurs de la zone euro : *pas* de budget fédéral sous l'autorité du Parlement, *pas* de transferts budgétaires entre États membres et *pas* de défaut d'un État. Ces trois impératifs ne sont pas tenables en situation de crise financière sévère. De là, résulte la menace politique des divisions à l'intérieur des États membres avec la montée des forces dites « souverainistes ».
En définitive, tant qu'il en sera ainsi, la zone euro ne sera qu'un système monétaire international défini par un traité intergouvernemental. Encore faut-il qu'il puisse évoluer d'une gouvernance intergouvernementale qui se contente de surveiller un carcan de règles produisant des ajustements asymétriques vers une coopération institutionnalisée produisant des ajustements symétriques. Le compromis initial qui a fondé l'euro a laissé soigneusement de côté les transformations politiques impliquées par une monnaie unique. C'est là que les héritages politiques opposés de l'Allemagne et de la France ont entraîné un dialogue de sourds.

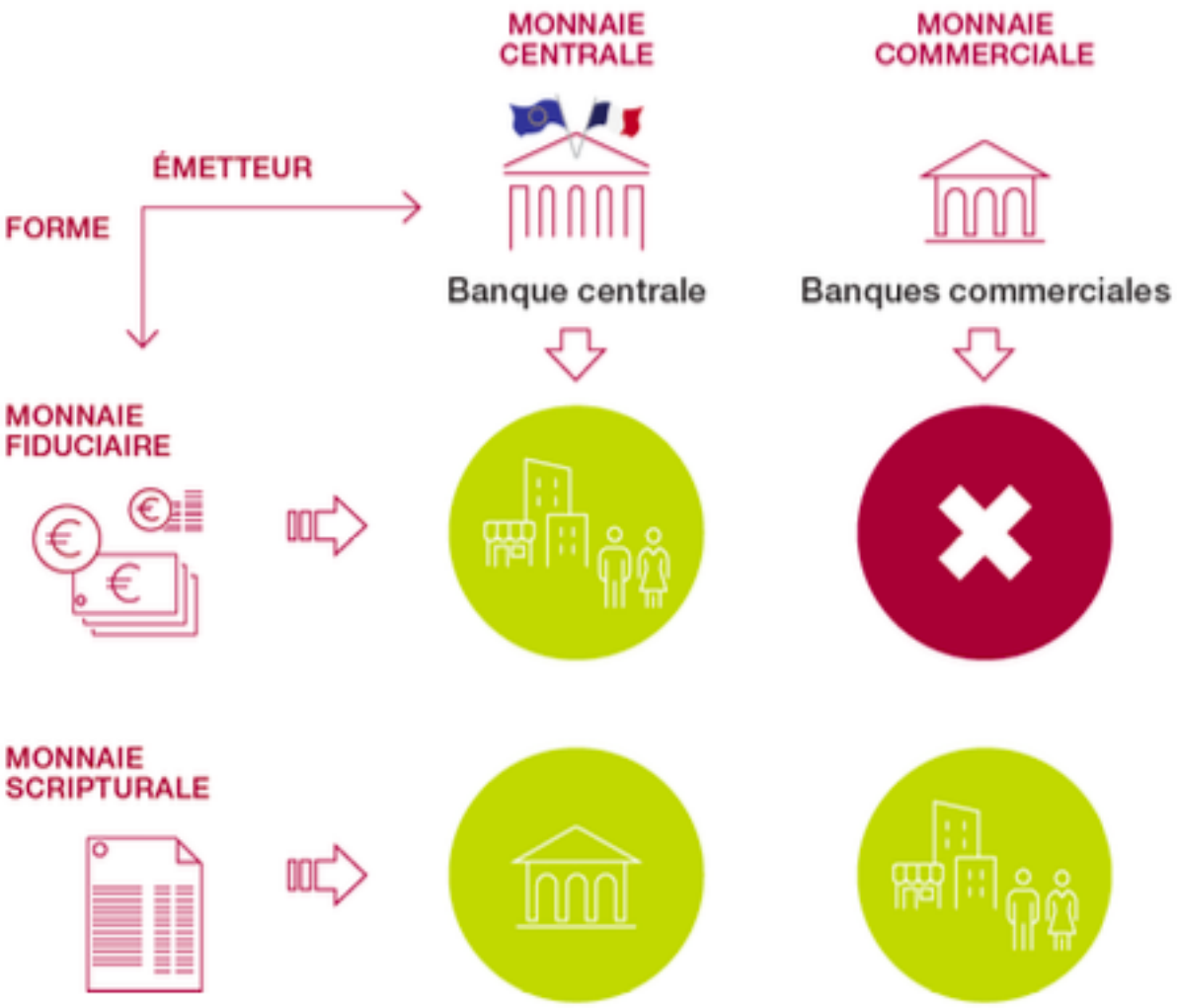
I- Les différentes formes de la monnaie

On peut les classer selon la nature de leur émetteur :

1- La monnaie de la Banque centrale, dont une version digitale est possible, avec les billets pour les agents non financiers (**monnaie « fiduciaire »)** et la monnaie centrale (monnaie scripturale pour les banques commerciales)
La monnaie fiduciaire se compose non seulement des billets mais aussi des pièces. En général, les billets sont émis par la banque centrale, tandis que les pièces sont émises par letrésor (elles sont ensuite physiquement mises en circulation par la banque centrale).
La monnaie fiduciaire bénéficie en outre souvent (et c'est le cas en France) d'un cours légal.
La notion juridique de cours légal désigne le fait que, sur le territoire où celui-ci s'applique, personne ne peut refuser de recevoir en règlement d'une dette libellée dans une unité monétaire donnée, un moyen de paiement bénéficiant du cours légal. Elle permet aux autorités publiques d'imposer le pouvoir libératoire de ces moyens de paiement (Il s'agit du pouvoir donné à un moyen de paiement qui permet à tout débiteur de s'acquitter d'une dette en utilisant ce moyen de paiement. Le débiteur est libéré de son obligation de paiement envers le créancier dès lors que la somme de monnaie convenue a été transférée à ce dernier).
La notion de cours légal est ainsi différente de celle de cours forcé (inconvertibilité dans l'actif sous-jacent lorsque la monnaie était définie par un poids de métal), mais on peut considérer qu'elle en constitue un corollaire, le cours légal visant, une fois l'inconvertibilité d'un instrument prononcée, à protéger ses porteurs de sorte qu'ils ne puissent se le voir refuser en paiement (condition fondamentale de son acceptabilité).
La notion de cours légal n'est toutefois pas appréhendée de la même manière dans toutes les juridictions et dans tous les contextes. Dans l'eurosystème, les textes (article 3.4 du TFUE et transposé dans l'article L 111-1 du Code monétaire et financier) indiquent que « l'Union établit une union économique et monétaire dont la monnaie est l'euro », et que « les billets de banque émis par la BCE et les banques centrales nationales sont les seuls à avoir cours légal dans la Communauté ». Pour préciser cette notion, la Commission européenne a adopté le 22 mars 2010 une recommandation sur l'étendue et les effets du cours légal des billets et des pièces en euros. Les différents États membres ne donnent toutefois pas tous la même force juridique à la notion de cours légal.
En droit français, l'article 1343-3 nouveau du Code civil dispose que « le paiement en France d'une obligation de somme d'argent s'effectue en euros » et l'article r. 642-3 du Code pénal français sanctionne le refus d'accepter en paiement les billets et les pièces ayant cours légal : le cours légal s'applique bien alors au support de l'unité de compte. Par ailleurs, l'article 442-4 du Code pénal rend passible de cinq ans de prison et 75 000 euros d'amende « la mise en circulation de tout signe monétaire non autorisé ayant pour objet de remplacer les pièces de monnaie ou les billets de banque ayant cours légal en France ». on notera aussi que, en France, la force du cours légal est atténuée par des dispositions obligeant un créancier à effectuer, au-delà d'un certain

montant, ses paiements par voie scripturale. Par ailleurs, l'obligation faite au créancier d'accepter de recevoir en paiement une forme monétaire ayant cours légal ne lui interdit pas d'exiger du débiteur de faire l'appoint.
Note : une façon simple de savoir si une monnaie a « cours légal » est de savoir si oui ou non l'État accepte la monnaie considérée pour payer les impôts.

2- Les monnaies des banques commerciales : ce sont des **monnaies « scripturales** » enregistrées dans les comptes bancaires (à chaque banque sa monnaie), qui sont des créances sur la monnaie fiduciaire et qui peuvent être mouvementées grâce à plusieurs instruments de paiement : chèque, carte de crédit et carte de paiement (cas spécial des cartes de paiement délivrées par certains magasins)
Les banques d'affaires utilisent aussi une autre forme de monnaie scripturale, fondée sur la technique de la blockchain, nécessairement non seulement publique mais « permissionnée » (voir plus loin).
Notons qu'il y a plusieurs sortes comptes bancaires. Seuls les « comptes de dépôt à vue transférables » sont monétaires ; et les découverts ne sont pas en principe autorisés. Les comptes d'épargne sont certes « à vue » aussi mais ne sont pas monétaires puisqu'ils ne sont pas transférables ; mais ils sont « quasi-monétaires » puisque leurs avoirs sont facilement et à bref délai transformables en liquidités. Il y a aussi les comptes courants et les comptes à terme.
Quand l'établissement financier n'est pas une banque, on peut avoir un compte de paiement (exemple le compte Nickel), qui permet de faire des paiements électroniques, mais pas de possibilité de chéquiers ni de découvert.

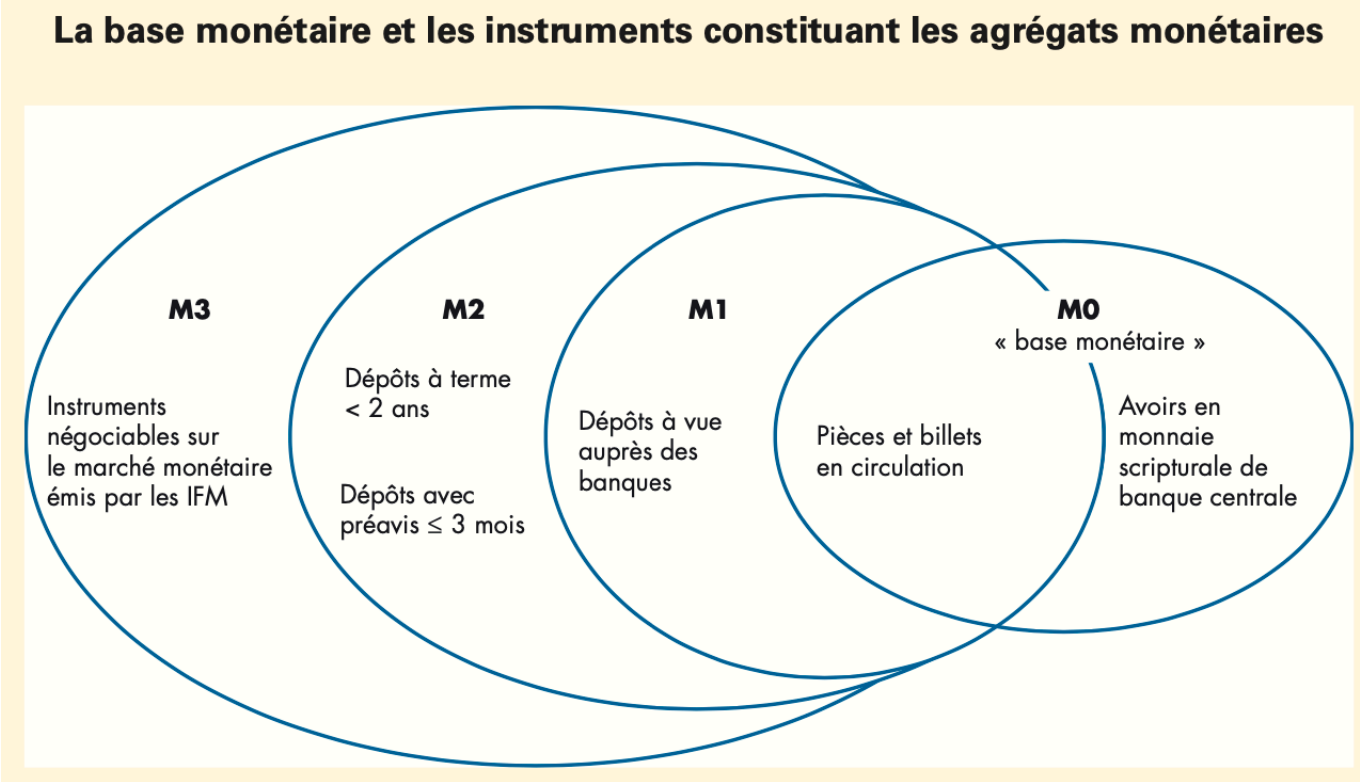


9,5% Part de la monnaie fiduciaire dans le total de la monnaie en circulation en zone euro

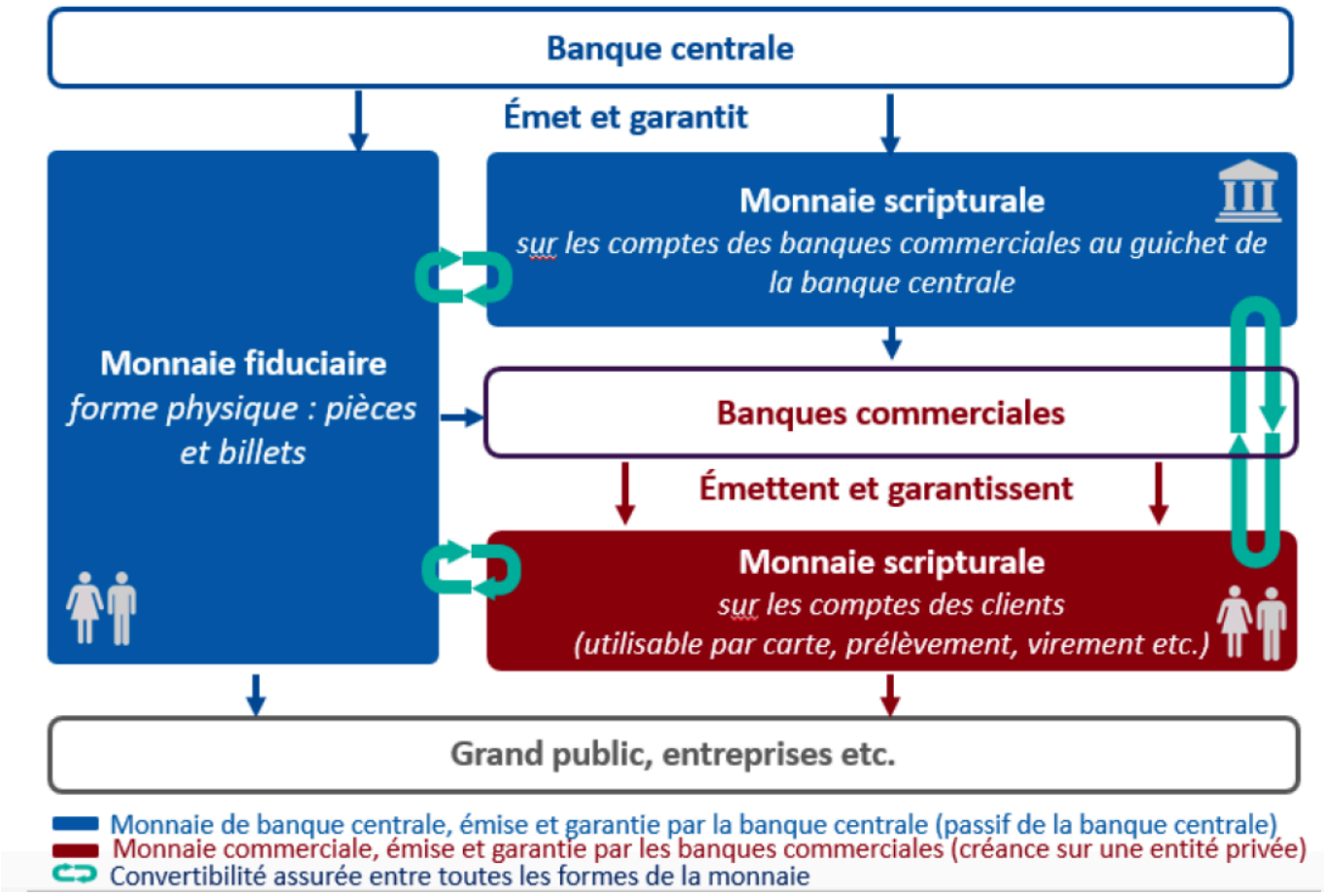
90,5% Part de la monnaie scripturale commerciale dans le total de la monnaie en circulation en zone euro

Monnaie utilisée par les agents économiques

Monnaie utilisée par les banques commerciales



Autre schéma sur l'articulation entre la monnaie de Banque centrale et les monnaies commerciales :



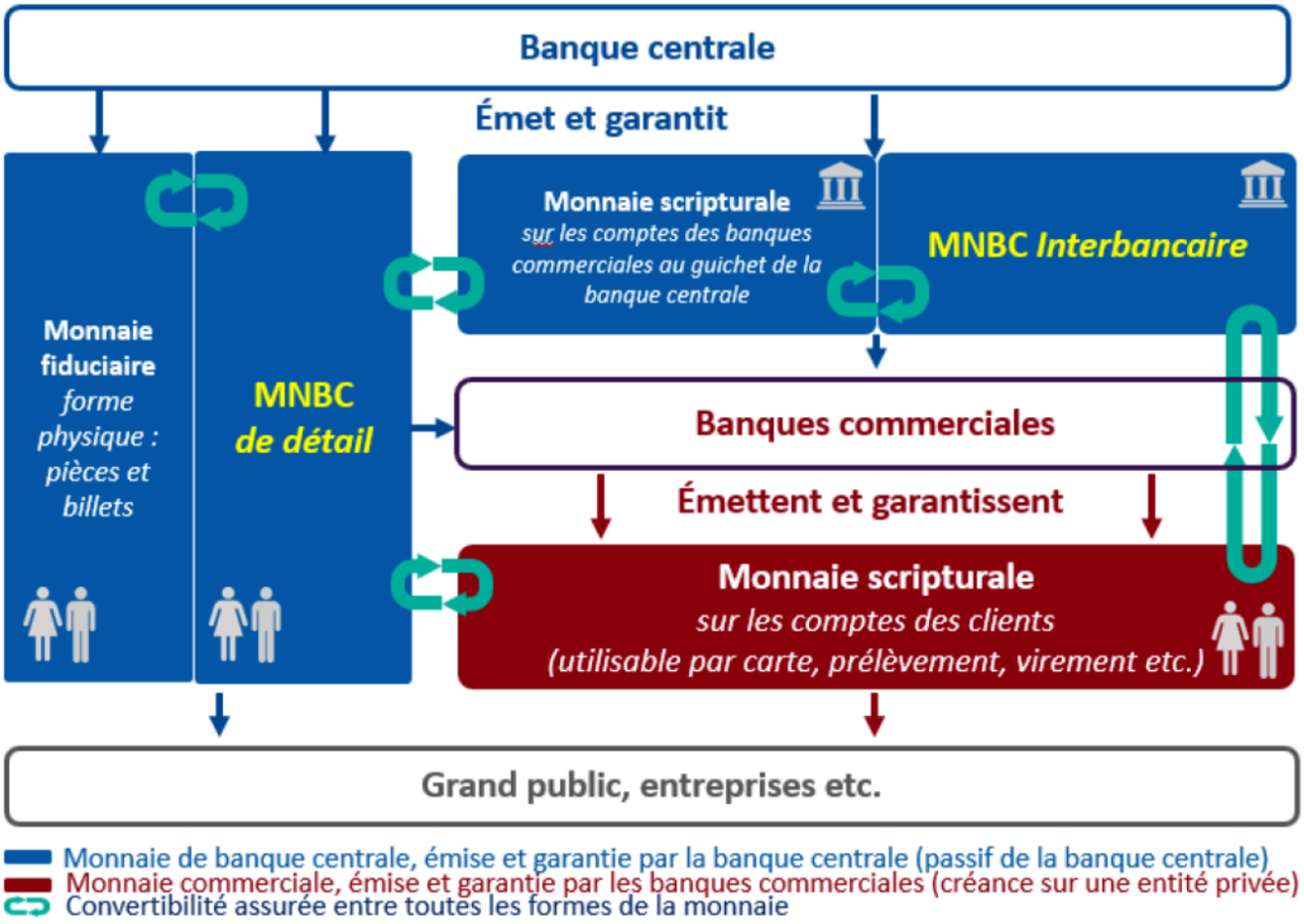
(Banque de France)

Notes :

• Actuellement, il y a deux formes de « monnaie de Banque centrale », la monnaie « fiduciaire » avec les billets - et les pièces - pour les agents non financiers - ménages et entreprises –, et la monnaie centrale pour les établissements financiers, au premier rang desquels se trouvent les banques commerciales (celles-ci ont besoin de monnaie centrale pour satisfaire le système des réserves obligatoires et pour satisfaire leur besoin de refinancement).

Mais ce schéma est amené à évoluer parce qu'il y aura deux formes supplémentaires de Monnaie de Banque centrale : une monnaie numérique de Banque centrale dite « de détail », comme le sera *l'euro numérique* dans la zone euro, équivalent numérique du billet, et une monnaie numérique de Banque centrale dite « interbancaire », équivalent numérique de la monnaie centrale ; cette monnaie numérique interbancaire servirait à régler les transactions sur des actifs « tokenisés par le biais de la technologie de la blockchain.

Le schéma précédent deviendrait alors celui-ci :



• Note sur l'euro numérique : « Dans un monde où les paiements numériques deviennent rapidement la norme, l'utilisation des espèces diminue et la transition vers les achats en ligne s'accélère. L'euro numérique serait une forme d'espèces qui permettrait aux consommateurs d'utiliser de la monnaie de banque centrale sous un format numérique, en complément des billets et des pièces.

Il leur faciliterait la vie en proposant une solution qui n'existe pas actuellement : un moyen de paiement numérique universellement accepté dans l'ensemble de la zone euro, pour les paiements dans les magasins, en ligne ou entre particuliers. Comme les espèces, l'euro numérique serait accessible, permettrait d'effectuer et de recevoir des paiements gratuitement et aurait cours légal.

Il préserverait en outre l'autonomie stratégique et la souveraineté monétaire de la zone euro en améliorant l'efficacité de l'écosystème européen des paiements dans son ensemble, en favorisant l'innovation et en renforçant sa capacité de résistance aux cyberattaques et aux perturbations techniques. (…)

Les prestataires de services de paiement supervisés, tels que les banques, joueraient un rôle essentiel dans la distribution de l'euro numérique. Ils serviraient de point de contact principal pour les particuliers, les

commerçants et les entreprises s'agissant de toutes les questions liées à l'euro numérique, et assureraient tous les services destinés aux utilisateurs finaux.
L'euro numérique pourrait également ouvrir de nouveaux créneaux commerciaux aux prestataires de services de paiement, en leur permettant d'avoir un rayonnement immédiat dans l'ensemble de la zone euro. (…) ». (BCE)
Signalons qu'en janvier 2026, près de 70 économistes européens ont publié une lettre ouverte pour inciter les eurodéputés à finaliser le projet d'euro numérique face au risque de perte de contrôle monétaire et d'une dépendance accrue aux États-Unis. Rappelons aussi que le 30 octobre 2025 les gouverneurs des Banques centrales nationales de la zone euro ont donné leur feu vert à la phase opérationnelle du projet d'euro numérique et que le calendrier prévoit les premiers tests en 2027 et le lancement définitif en 2029.
Autrement dit, la mise en place d'un euro numérique renforcerait la souveraineté monétaire de la zone euro. Et il est vrai que la domination internationale du dollar et les privilèges que cela procure aux États-Unis incitent légitimement les responsables européens et tout spécialement les dirigeant de la BCE à défendre notre souveraineté monétaire. Surtout que « le gouvernement américain promeut activement les cryptomonnaies, surtout les stablecoins, actifs numériques adossés à une monnaie de référence. Cette stratégie dépasse le cadre financier national : elle vise à consolider la domination mondiale du dollar et à remodeler l'ordre monétaire international. En favorisant les stablecoins adossés au dollar, les États-Unis souhaitent renforcer l'influence de leurs géants technologiques dans les paiements ainsi que la demande d'actifs en dollars, notamment leur dette publique. La loi Genius fournit le socle juridique de cette orientation, contrastant avec le règlement européen MiCAR qui favorise, quant à lui, la protection des consommateurs face au risque financier des stablecoins. La politique américaine pourrait affaiblir les efforts de la BCE pour accroître le rôle international de l'euro et menace la souveraineté monétaire de nombreux pays. Pour éviter qu'il en soit ainsi l'UE gagnerait, avec ses partenaires, à défendre un système de paiement multilatéral fondé sur la coopération » (CEPII, Éric Monnet, sept 2025).
Remarque importante : l'euro numérique n'est en rien une « cryptomonnaie » puisque son système reste très centralisé et contrôlé.

3- Parmi les établissements non bancaires, il y en a qui sont spécialisés dans les instruments de paiement électroniques, comme Treezor, entreprise de technologie financière française fondée en 2014, qui fournit des services de paiement en France et dans l'UE, en particulier en ouvrant des « comptes de monnaie électronique », mouvementée par cartes de paiement. On parle dans ce cas de « **monnaies électroniques** » (ou « monnaies virtuelles » ou encore « monnaies digitales »), qui sont aussi des créances sur la monnaie fiduciaire.
   Comme ces monnaies sont émises par des institutions qui ne sont ni réglementées ni supervisées, cela entraîne des risques pour les détenteurs, risque de conversion en monnaie fiduciaire selon le degré de liquidité des actifs détenus par les émetteurs ; risque de défaut des fournisseurs du service de paiement, risques de marché et risque de change.
4- Il y a enfin les « **crypto-monnaies** » : ce sont des monnaies numériques, donc virtuelles aussi mais qui utilisent des techniques cryptographiques (d'où leur nom) pour sécuriser les transactions. Plus précisément, elles utilisent la technologie de la blockchain, ce qui explique qu'elles n'existent que sous forme électronique et aussi et surtout indépendamment de toute autorité centrale puisqu'elles fonctionnent sur des réseaux décentralisés qui ne sont en rien hiérarchisés comme c'est le cas avec le système bancaire classique (Banque centrale, dite de 1er rang, et banques commerciales, dites de second rang).
   Autrement dit, une cryptomonnaie est un système de paiement numérique qui ne s'appuie pas sur les banques ou sur tout autre intermédiaire financier pour vérifier les transactions. Il s'agit d'un système de partage P2P (peer-to-peer) permettant à tout le monde d'envoyer et de recevoir des paiements n'importe où. Il ne s'agit pas d'argent physique transporté ni échangé dans le monde réel : les paiements en cryptomonnaies sont des saisies purement virtuelles réalisées dans une base de données en ligne et correspondant à certaines transactions particulières. Lorsque vous transférez des fonds en cryptomonnaies, les transactions sont enregistrées dans un registre public. Les cryptomonnaies sont stockées dans des portefeuilles numériques.

Ces cryptomonnaies ont été désignées ainsi parce qu'elles utilisent le chiffrement pour vérifier les transactions. Autrement dit, elles intègrent un codage complexe pour stocker et transférer des données de cryptomonnaie à partir de portefeuilles vers des registres publics. Le chiffrement vise à assurer la sécurité.
La première cryptomonnaie a été Bitcoin, qui a été fondée en 2009 et reste la plus connue aujourd'hui. L'intérêt pour les cryptomonnaies réside en grande partie dans la recherche de profits, les spéculateurs faisant pa!ois grimper les prix en flèche. C'est d'ailleurs pourquoi, on est en droit de se demander si le Bitcoin n'est pas en réalité un « cryptoactif », au demeurant spéculatif, plutôt qu'une cryptomonnaie.

Remarque importante sur la distinction cryptomonnaie / cryptoactif :
Distinction commune :
Un cryptoactif (ou crypto-asset en anglais) est un actif numérique créé et géré grâce à des technologies de cryptographie et de registres distribués (comme la blockchain). Il s'agit d'une représentation électronique d'une valeur ou d'un droit, qui peut être transférée, stockée et échangée de manière décentralisée, sans intermédiaire central (banque ou institution).
Une cryptomonnaie (ou cryptocurrency) désigne traditionnellement un cryptoactif conçu pour fonctionner comme une monnaie numérique mais n'a pas de cours légal et peut avoir une très forte volatilité et être victime d'arnaques. Le terme est très répandu dans le langage courant (Bitcoin est souvent appelé « cryptomonnaie »).
Distinction institu-juridique :
Les autorités (Banque de France, AMF en France, G20, Banque centrale européenne, etc.) préfèrent le terme cryptoactif et déconseillent ou nuancent fortement l'usage de « cryptomonnaie ».
Pourquoi ? Parce que, pour être considérée comme une monnaie au sens juridique et économique, un actif doit généralement remplir trois fonctions : unité de compte, moyen d'échange et réserve de valeur (voir plus haut). Or, Les cryptoactifs (même Bitcoin) ne remplissent pas pleinement ces trois critères de manière fiable : ils sont très volatils → pas une bonne réserve de valeur, ils n'ont pas de cours légal (aucun État ne les impose comme moyen de paiement obligatoire) et ils ne dépendent d'aucune banque centrale ni institution émettrice. C'est pourquoi on parle plutôt de cryptoactifs : ce sont des actifs financiers ou spéculatifs, pas des monnaies au sens strict. Le terme « cryptomonnaie » est souvent considéré comme abusif ou trompeur par les régulateurs.
Conséquence : les cryptoactifs est le terme qui convient (selon le règlement européen MiCA – Markets in Crypto Assets – entré en application progressive depuis 2024-2025 utilise exclusivement le terme « cryptoactif », le définissant de la manière suivante : « une représentation numérique d'une valeur ou d'un droit pouvant être transférée et stockée de manière électronique, au moyen de la technologie des registres distribués ou d'une technologie similaire »), mais il faut savoir qu'il concerne un ensemble large d'actifs avec tout à la fois les cryptomonnaies (sous-ensemble), les tokens (créés sur une blockchain existante, comme les ERC-20 sur Ethereum), les stablecoins (adossés à une devise fiat) et les utility tokens, security tokens, NFT, etc.
Autrement dit, toutes les cryptomonnaies sont des cryptoactifs mais tous les cryptoactifs sont loin d'être tous des cryptomonnaies !

II- La technologie de la blockchain

1- Caractéristiques principales de la blockchain

La *blockchain* est une structure de base de données distribuée, décrite pour la première fois par le mathématicien et informaticien américain David Chaum dans sa thèse de Doctorat en 1982. L'idée de Mr Chaum était de créer une monnaie qui pouvait être envoyée de manière intraçable et qui fonctionnerait sans entité centralisée. Il s'agissait donc de faire en sorte que les transactions soient anonymes tout en restant accessibles au public. Du point de vue de la théorie économique, l'on reconnaît aisément dans

cette idée de monnaie échappant à la tutelle de l'État, la posture libérale du *free banking* (Hayek, 1976) que l'on oppose généralement à celle du *central banking* (Aglietta, 1992).

On parle d'une technologie **décentralisée** car l'architecture de la blockchain est construite sans serveur central et parce que la gouvernance de la blockchain repose sur la répartition du pouvoir entre tous les utilisateurs de cette dernière ; d'où le principal avantage de cette solution, qui est d'éviter les coûts d'intermédiation, puisque, en particulier, point n'est besoin d'un tiers de confiance.
Remarque : la cryptomonnaie a, comme l'Internet, lui aussi décentralisé, hors de tout contrôle direct des gouvernements et avec une totale liberté d'accès, a à voir avec la philosophie libertarienne, sans confondre libertarien et libertaire (la philosophie libertarienne repose sur le refus absolu de la coercition étatique. Mais une cryptomonnaie telle que le Bitcoin n'est pas une monnaie pour Internet, c'est l'Internet de la monnaie.
La blockchain se matérialise par une base de données distribuée au sein d'une communauté d'utilisateurs. Cette base, appelée registre, contient l'historique de toutes les transactions effectuées entre les utilisateurs depuis la création de la blockchain ; en effet, ce registre est distribué dans les ordinateurs de tous les participants au réseau (qui leur appartient), que l'on appelle les « nœuds » du réseau ; il est donc à la fois décentralisé et automatisé. Les transactions – anonymes - sont regroupées au sein d'une succession de blocs reliés les uns aux autres par un procédé cryptographique. La cryptographie (du grec « crypto » signifiant caché et « graphie » signifiant écrire) prend appui sur une fonction mathématique de « hachage » qui transforme une donnée entrante en un identifiant numérique unique, le « hash », garantissant l'intégrité de la donnée.
La base de données qui, au sein de toute banque, rassemble les informations concernant les opérations faites par leurs clients, constitue un fichier informatique centralisé est ici complètement décentralisée en ce sens qu'elle est distribuée entre tous les agents qui sont les nœuds du réseau « peer-to-peer », appelés aussi les « mineurs » : ce sont eux qui sont les membres de la communauté et chacun d'eux possède en quelque sorte une copie de la totalité de la base de données. Cela nécessite bien sûr que chacun ait un matériel informatique suffisant et cela ne rend plus nécessaire une autorité centrale pour gérer une telle base de données.
Quand une transaction a lieu au sein du réseau entre deux de ses nœuds, elle est enregistrée partout, c'est-à-dire par tous les nœuds : on sait d'ailleurs non seulement entre quels nœuds a lieu la transaction mais aussi de quelle transaction antérieure provient la somme que doit verser l'acheteur au vendeur (pas besoin de vérifier la « provision » du compte et « double dépense » impossible).
Pour assurer la fiabilité de l'enregistrement des transactions dans le réseau, on utilise deux procédés :
• Le procédé de la cryptographie asymétrique (algorithme RSA) en ce sens que chaque nœud possède une clé électronique pour chiffrer ses messages, qui est connue de toute le monde, qui est donc publique, et une autre clé pour déchiffrer les messages qu'il reçoit, qui est au contraire rigoureusement privée ; c'est parce que ce procédé cryptographique, qui remplace la confiance par la preuve cryptographique, et que celle-ci joue un rôle fondamental dans le dispositif général, que ces monnaies sont appelées cryptomonnaies ;
Note : l'avantage principal du chiffrement asymétrique est qu'il élimine la nécessité d'un échange sécurisé de clés, ce qui est souvent considéré comme la principale vulnérabilité du chiffrement symétrique. Cependant, le chiffrement asymétrique est plus lent et consomme davantage de ressources que le chiffrement symétrique. C'est pourquoi les organisations et les applications de messagerie adoptent de plus en plus une méthode de chiffrement hybride qui utilise le chiffrement asymétrique pour la distribution sécurisée des clés, puis le chiffrement symétrique pour les échanges de données ultérieurs.
• Le procédé de la signature électronique est un procédé inverse au précédent : chaque nœud possède une clé privée pour enregistrer la transaction dans la base de données décentralisée et partagée par tous les nœuds, lesquels la décodent grâce à la clé publique du nœud qui est à l'origine de la transaction. Celle-ci est ainsi authentifiée : elle ne peut pas être falsifiée, de même d'ailleurs qu'elle ne peut pas être annulée.
Par conséquent, quand on adhère à une blockchain, on crée un compte pour vous et on vous attribue deux clés, l'une qui est privée et l'autre qui est publique.
Comme tous les nœuds du réseau doivent disposer de la même copie de la totalité de la base de données, il faut qu'ils se synchronisent quand une nouvelle transaction a lieu. Lorsqu'une nouvelle transaction a

lieu, chaque nœud l'enregistre dans une liste d'attente et à chaque instant les nœuds ont des listes d'attente qui peuvent varier quelque peu : il faut déterminer périodiquement le nœud dont la liste va être prise pour la synchronisation (jusqu'à la fin de 2017, la durée moyenne était de 10 minutes ; elle est passé depuis à 3-4 heures). La liste qui sera choisie est appelée « bloc ».
Le travail que doit faire chaque nœud pour être choisi est de trouver un identifiant pour caractériser sa propose liste de transactions. Pour ce faire, est utilisée la technique de hashage, qui transforme toute chaîne de caractères en nombre variable en une chaîne de caractères en nombre fixe et déterminée, et qui fait en sorte que le moindre changement de composition dans la 1ère chaîne entraîne un important changement dans la 2ème. Cette technique assure qu'un fichier, même lourd, a été correctement transmis. La 2ème chaîne de caractères que fournit la technique de hashage est en quelque sorte l'empreinte digitale du fichier, son identifiant.
Avec la technique de hashage, chaque nœud est en mesure de trouver un identifiant pour sa liste, sachant qu'entre aussi dans l'algorithme l'identifiant du bloc précédent : c'est cela qui fait que les blocs sont liés entre eux comme les maillons d'une chaîne, d'où le nom de blockchain, c'est-à-dire une chaîne de blocs, un enchaînement de blocs. La conséquence est que si on voulait modifier le contenu d'une transaction, cela aurait fatalement pour conséquence de modifier l'identifiant, ce qui imposerait de refaire tous les calculs des blocs précédents… !
Pour renforcer la fiabilité du système, on ajoute dans le processus de hashage de la liste de transactions non seulement l'identifiant du bloc précédent mais aussi un nombre aléatoire, appelé « nonce ». Le problème est alors de trouver le nonce qui satisfait à un certain nombre de conditions. En général, une dizaine de minutes suffisent pour trouver un hash de la forme voulue. Quand un nœud du réseau trouve une solution qui est conforme, sa liste devient le bloc de la dizaine de minutes qui se termine. Quand le bloc est trouvé, les autres « mineurs » vérifient que le « hash » trouvé est bon, ils le valident donc et se synchronisent dessus. Et ainsi de suite. L'activité de calcul des blocs s'appelle le « minage », d'où le nom de mineur. Et tous les mineurs sont intéressés à la recherche des blocs parce que celui qui, pour une tranche de dix minutes, a la liste qui devient le bloc, il reçoit une rémunération (un nombre de bitcoins dans le cas de cette blockchain-là).
Pour rester dans la blockchain, il faut y contribuer en « minant » et la confiance que l'on a dans la blockchain vient du fait qu'aucun « mineur » ne peut avoir une puissance de calcul suffisante pour compromettre le bon fonctionnement de la blockchain.
Quand le nombre de nœuds augmente, autrement dit quand le nombre de participants augmente, la puissance de calcul globale s'élève et il faut compliquer les conditions requises pour que l'on reste sur une période de base d'une dizaine de minutes.
Pour terminer ce paragraphe, faisons deux remarques :

1) On peut opposer la « philosophie » de la blockchain à celle de l'intelligence artificielle au travers de deux expressions – caricaturales pour frapper les esprits – de deux hommes d'affaires et investisseurs de capital-risque. D'un côté, Peter Thiel, cofondateur de PayPal, selon lequel « crypto, c'est libertarien. L'intelligence artificielle, c'est communiste », et de l'autre, Reid Hoffman, cofondateur du réseau LinkedIn, selon lequel, « crypto, c'est l'anarchie. L'intelligence artificielle, c'est l'État de droit ».
2) La naissance des cryptomonnaies utilisant la technologie de la blockchain pose en définitive une question fondamentale : avec ces « monnaies », a-t-on toujours affaire à une économie monétaire ? Ne revient-on pas en quelque sorte à une économie de troc ? En effet, à partir du moment où l'échange se fait entre un bien, quel qu'il soit, et une certaine quantité de « cryptomonnaie », n'est-ce pas comme s'il y avait simplement échange entre deux biens, surtout si cette cryptomonnaie joue en priorité un rôle d'actif financier. Car, comme l'économiste italien Augusto Graziani le démontre magistralement, « tout paiement monétaire doit relever d'une transaction triangulaire, impliquant au moins trois agents : le payeur, le payé et la banque ». Or, les cryptomonnaies fonctionnent en P2P, donc à partir de relations seulement bilatérales.
   Autrement dit, les cryptomonnaies nous replongent dans l'univers néo-classique qui est celui d'une économie de troc alors que Graziani décrit l'économie capitaliste monétaire, restant de ce point de vue, avec d'autres théoriciens européens, essentiellement français

d'ailleurs, l'un des grands représentants de « l'école du circuit » ; que l'on peut considérer comme authentiquement post-keynésienne.

Schéma d'une chaine de blocs

La blockchain est utilisée pour deux fonctions :

Première fonction « enregistrement et stockage » : la blockchain permet d'enregistrer et de stocker des valeurs et des transactions tout comme un notaire. Toute valeur ou information qui entre dans la blockchain par le biais d'une transaction est incluse dans un bloc relié cryptographiquement aux blocs précédents. Les blocs ne pouvant être modifiés (infalsifiabilité des données), la blockchain constitue une base de données immuable contenant l'historique de tous les échanges effectués sur la blockchain depuis sa création.
Seconde fonction « émission et transmission » : en s'appuyant sur cette capacité d'enregistrement et de stockage de données, la blockchain permet d'émettre et de transmettre des actifs numériques natifs, tels que des Bitcoins, mais aussi des actifs existants enrichis par un procédé appelé « tokenisation ». La tokenisation d'un actif réel consiste à convertir les droits qui lui sont attachés en un enregistrement numérique. C'est une manière de représenter dans le monde digital un bien immobilier par exemple, ou une obligation, une propriété intellectuelle, demain une monnaie, et de pouvoir échanger cet actif en bénéficiant des mécanismes de la blockchain. Une fois enregistré sur la blockchain, le token peut donc être échangé au sein de la communauté et tout l'historique lié à la détention de cet actif est tracé dans les blocs.
Note : le FMI vient de publier en ce début avril 2026 un article de Tobias Adrian sur la tokenisation en finance : https://www.elibrary.imf.org/view/journals/068/2026/001/068.2026.issue-001-en.xml

Schéma de tokenisation

Grâce à ces deux fonctions « enregistrement/stockage » d'une part et « émission/transmission » d'autre part, la technologie de la blockchain permet à des personnes connectées en réseau, qui ne se connaissent pas ou qui ne se feraient pas nécessairement confiance de :

- s'affranchir des intermédiaires tels que les banques, chambres de compensation, dépositaires, notaires, cadastres...
- s'assurer de la fiabilité et de la sécurité de leurs opérations.

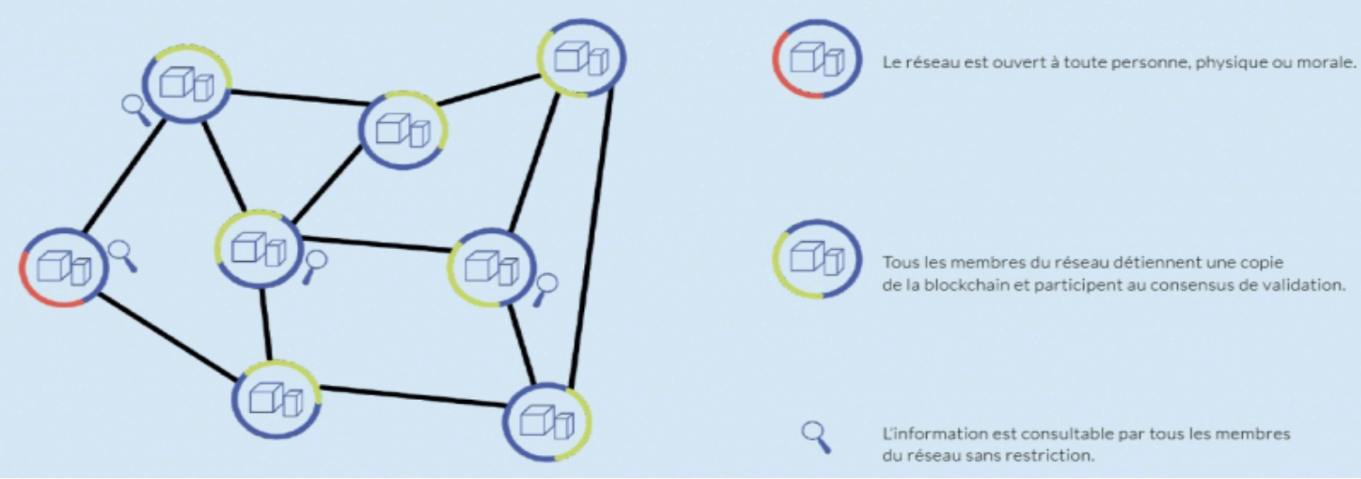
2- Les différents types de blockchain

Comme le montre le tableau suivant, il y a deux principaux types de blockchain :

- des blockchains *publiques* : l'accès et l'utilisation sont ouverts à tous depuis internet. Des exemples de ce type de blockchain sont Bitcoin ou Ethereum ;
- des blockchains *privées*, également appelées « permissionnées » : l'accès et l'utilisation sont réservés à un nombre restreint d'utilisateurs. Une unité centrale en contrôle les accès. Une blockchain privée est de fait moins décentralisée qu'une blockchain publique.

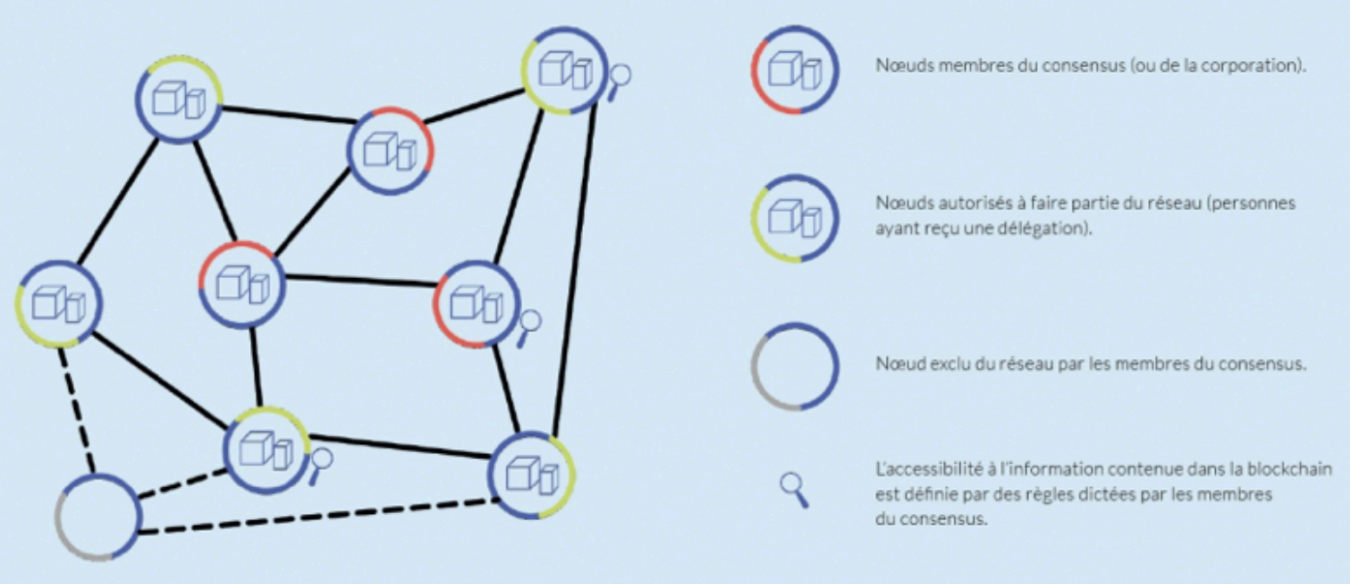
			Lecture	Écriture	*Commit*[1]	Exemple
Type de blockchain	Publique	Publique sans permissions	Ouvert à tous	N'importe qui	N'importe qui	Bitcoin, Ethereum[2]
		Publique avec permissions	Ouvert à tous	Autorisé aux participants	Tous les participants autorisés ou un sous-ensemble	Sovrin[3]
	Privée	Consortium	Limité à un ensemble de participants autorisés	Autorisé aux participants	Tous les participants autorisés ou un sous-ensemble	Plusieurs banques exploitant un grand livre partagé
		Privée avec autorisation (l'entreprise)	Entièrement privé ou limité à un ensemble de nœuds autorisés	Opérateur du réseau uniquement	Opérateur du réseau uniquement	Un grand livre bancaire interne partagé entre la société mère et les filiales

Fonctionnement d'une blockchain publique :



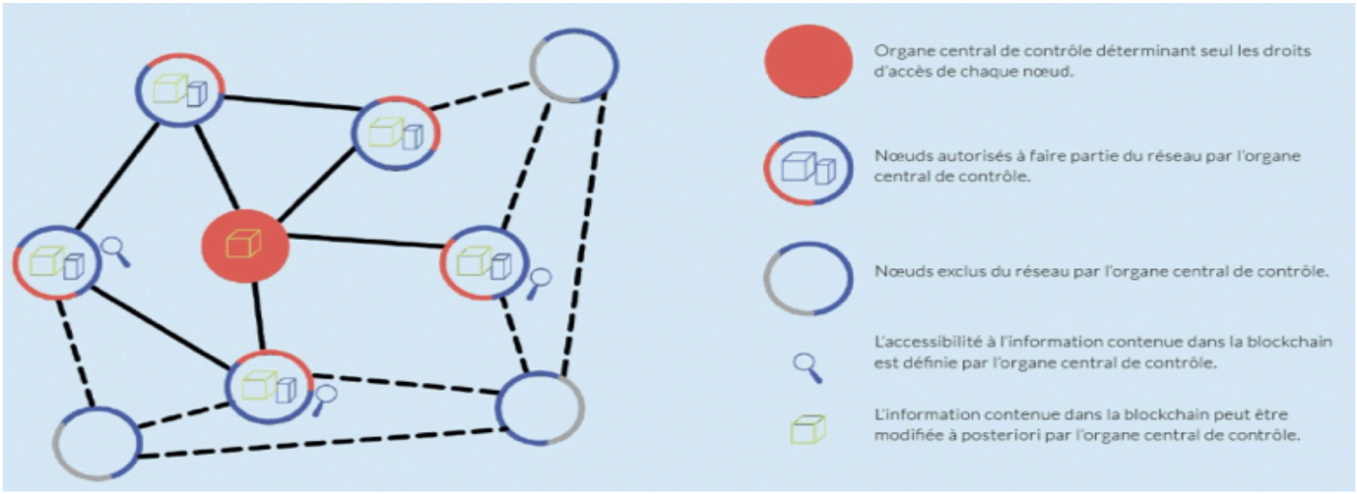
(d'après M. Della Chiesa)

Fonctionnement d'une blockchain permissionnée :



(idem)

Fonctionnement d'une blockchain privée



(idem)

3- <u>Un élargissement des applications de la blockchain</u>

La technologie blockchain a ouvert la voie à de nouvelles applications dans le partage, la sécurité et le commerce des données. Grâce à sa décentralisation, sa sécurité et sa traçabilité, elle a attiré d'importants investissements industriels. À l'heure actuelle, de nombreuses applications de la blockchain sont mises en œuvre dans un large éventail de secteurs, notamment la santé, l'Internet des objets (IoT), la protection des données, la chaîne d'approvisionnement, la traçabilité des marchandises, la gestion de l'énergie et la lutte contre la contrefaçon. Parmi ces applications, la FinTech s'est imposée comme un domaine prometteur et en plein essor.
Le système financier mondial fournit quotidiennement des services à des milliards de personnes et gère des milliers de milliards de dollars en espèces. Dans ce vaste environnement de marché, les infrastructures financières traditionnelles s'appuient sur des entités tierces établies pour instaurer et maintenir la confiance. Ce modèle dominant présente des défis inhérents, notamment les coûts liés à la multiplicité des parties prenantes, les retards persistants, la lourdeur des formalités administratives et la

menace constante de violations de données. L'impact cumulatif de ces défis se traduit par des coûts élevés, une faible efficacité et des problèmes de sécurité fréquents.
Cependant, le paysage des comportements financiers, notamment dans les secteurs bancaire et du trading, a été transformé depuis l'émergence de la blockchain. La technologie blockchain a le potentiel de résoudre les problèmes susmentionnés dans le domaine financier. Ce potentiel découle des caractéristiques distinctives de la blockchain, à savoir la décentralisation, la comptabilité multipartite et l'immuabilité. La robustesse et l'efficacité des systèmes financiers peuvent être améliorées grâce à la stratégie de gestion décentralisée de la blockchain, en particulier dans le contexte du marché des valeurs mobilières. L'utilisation de la technologie blockchain sur le marché des valeurs mobilières permet d'atténuer les coûts élevés supportés par les intermédiaires tels que les organismes de réglementation, les courtiers et les bourses. Par conséquent, la décentralisation du marché des valeurs mobilières représente une avancée majeure. Au cœur de ce changement se trouve la confiance distribuée intrinsèquement intégrée à la technologie blockchain, qui catalyse la révolution financière sous trois aspects : (1) l'élimination de la dépendance à l'égard de tiers de confiance, (2) la diminution du coût des transactions et (3) la réduction du délai.

III- L'utilisation concrète des cryptomonnaies

1- *Les 3 étapes pour acheter des cryptomonnaies :*

Étape 1 : Choix d'une plateforme
La première étape consiste à décider de la plateforme à utiliser. En général, vous avez le choix entre un courtier traditionnel et une plateforme d'échange de cryptomonnaies spécialisée :
Courtiers traditionnels. Il s'agit de courtiers en ligne qui proposent des moyens d'acheter et de vendre des cryptomonnaies, ainsi que d'autres actifs financiers tels que des actions, des obligations et des ETF (Exchange-Traded Fund : fonds de placement qui regroupe un ensemble de valeurs mobilières dans un but essentiellement spéculatif ; la traduction française est FNB, fonds négocié en Bourse). Ces plateformes ont tendance à offrir des coûts de négociation moins élevés, mais moins de fonctionnalités liées aux cryptomonnaies.
Plateformes d'échange de cryptomonnaies. Il existe de nombreuses plateformes d'échange de cryptomonnaies parmi lesquelles il est possible de faire son choix, chacune offrant différentes cryptomonnaies, différents stockages de portefeuille, différentes options de comptes générant des intérêts, et plus encore. De nombreuses plateformes d'échange appliquent des frais en fonction des actifs.
Lorsque vous comparez les différentes plateformes, prenez en compte les cryptomonnaies proposées, les frais qu'elles facturent, leurs fonctionnalités de sécurité, les options de stockage et de retrait, ainsi que les ressources éducatives.
Étape 2 : Alimentation de votre compte
Une fois que vous avez choisi votre plateforme, l'étape suivante consiste à alimenter votre compte afin de pouvoir commencer à échanger des monnaies. La plupart des plateformes d'échange de cryptomonnaies permettent aux utilisateurs d'acheter des cryptomonnaies en utilisant des monnaies fiduciaires (c'est-à-dire émises par le gouvernement), comme le dollar américain, la livre sterling ou l'euro en utilisant leurs cartes de débit ou de crédit (bien que cela varie selon la plateforme).
Les achats de cryptomonnaies par carte de crédit sont considérés comme risqués, et certaines plateformes d'échange ne les prennent pas en charge. Certaines entreprises de cartes de crédit n'autorisent pas non plus les transactions relatives aux cryptomonnaies. En effet, les cryptomonnaies sont très volatiles et il n'est pas conseillé de risquer de s'endetter (ni de payer potentiellement des frais de transaction élevés par carte de crédit) pour certains actifs.
Certaines plateformes acceptent également les transferts ACH (un paiement ACH est un paiement électronique de banque à banque effectué par l'intermédiaire du réseau ACH - Automated Clearing House -, plutôt que par un réseau de cartes. Les paiements ACH sont également souvent appelés "transferts" ou "transactions" ACH) ainsi que les virements bancaires. Les modes de paiement acceptés et les délais de dépôt ou de retrait diffèrent selon les plateformes. De même, le temps nécessaire à la validation des dépôts varie selon le mode de paiement.

Les frais sont un facteur important à prendre en compte. Il s'agit notamment des éventuels frais de transaction de dépôt et de retrait ainsi que des frais de transaction. Les frais varient en fonction du mode de paiement et de la plateforme, ce qu'il convient de vériffer dès le départ.

Étape 3 : Passage d'un ordre

On peut passer un ordre via la plateforme Web ou mobile de votre courtier ou de votre plateforme d'échange. Si on envisage d'acheter des cryptomonnaies, on peut le faire en sélectionnant « acheter », en choisissant le type d'ordre, en saisissant le montant des cryptomonnaies que l'on souhaite acheter et en conffirmant l'ordre. Le même processus s'applique aux ordres de « vente ».

Il existe également d'autres moyens d'investir dans les cryptomonnaies. Il s'agit notamment de services de paiement, comme PayPal, Cash App et Venmo, qui permettent aux utilisateurs d'acheter, de vendre ou de détenir des cryptomonnaies. Les instruments d'investissement suivants sont également disponibles :

•Fonds en Bitcoin : vous pouvez acheter des actions de fiducies en Bitcoin avec un compte de courtage ordinaire. Ces instruments permettent aux investisseurs particuliers d'avoir une exposition aux cryptomonnaies par le biais du marché boursier.

•Fonds communs de placement en Bitcoin : il existe des ETF en Bitcoin et des fonds communs de placement en Bitcoin parmi lesquels on peut faire son choix.

•Actions ou ETF de blockchain : on peut également investir indirectement dans la cryptomonnaie par le biais d'entreprises de blockchain spécialisées dans la technologie qui sous-tend la cryptomonnaie et les transactions en cryptomonnaie. Il est également possible d'acheter des actions ou des ETF d'entreprises qui utilisent la technologie blockchain.

La meilleure option des objectifs d'investissement et du goût du risque.

2- *Les principales cryptomonnaies*

D'après IG.com :

	Bitcoin (BTC)[1]	Bitcoin cash (BCH)[1]	Ether (ETH)[1]	Litecoin (LTC)[1]	EOS (EOS)[2]	Stellar (XLM)[3]	Chainlink (LINK)[4]	Polkadot (DOT)[5]	Dc (I
Lancement	2009	2017	2015	2011	2018	2014	2019	2017	
Quantité en circulation	>17 millions	>17 millions	>102 millions	>58 millions	>906 millions	>18 milliards	>400 millions	>980 millions	n
Quantité maximale	21 millions	21 millions	Pas de limite maximum	84 millions	Pas de limite maximum	Pas de limite maximum	1 milliard	Pas de limite maximum	ma
Ratio minage/création	12,5 par bloc	12,5 par bloc	3 par bloc	25 par bloc	Jusqu'à 5 % d'inflation par an	Jusqu'à 1 % d'inflation par an	Jusqu'à 13 % d'inflation par an	Jusqu'à 10 % d'inflation par an	d'i
Transactions par seconde (maximum)	7	60	20	56	2800	1000	50000	1000	
Réseau	n/a	n/a	Ethereum	n/a	EOS.IO	Stellar	Ethereum	Libp2p	Et

[1] Coin Market Cap, 2018 ; Medium, 2018 ; How Much, 2018 ; BitInfoCharts, 2018

[2] Coin Market Cap, 2018 ; Medium, 2018 ; Cryptocurrency News, 2018

[3] Coin Market Cap, 2018 ; Stellar, 2018 ; Lumenauts, 2018

[4] Coin Market Cap, 2022 ; CoinDesk, 2022 ; Gemini, 2022

[5] Coin Market Cap, 2022 ; CoinDesk, 2022 ; Lexology, 2022

[6] Coin Market Cap, 2022 ; CoinDesk, 2022 ; AI Multiple, 2021

[7] Coin Market Cap, 2022 ; CoinDesk, 2022 ; Uniswap, 2022

[8] Coin Market Cap, 2022 ; AAX Academy, 2021 ; Nasdaq.com, 2022

« Les cryptomonnaies sont des devises virtuelles qui opèrent indépendamment des banques et des gouvernements. Elles peuvent cependant toujours être échangées, ou tradées, comme toute autre devise physique. Lancé en 2009, le bitcoin est la première cryptomonnaie décentralisée. Depuis, des milliers de cryptomonnaies, connues sous le nom de altcoins, ont été lancées.
Le bitcoin est actuellement le leader sur le marché, mais la demande croissante vers d'autres cryptomonnaies comme le bitcoin cash, le bitcoin gold, l'ether, le litecoin, l'EOS, le stellar (XLM), le NEO et le ripple, ainsi que des applications plus étendues et les avancées technologiques pourraient changer la donne.
Les *Altcoins* désignent des monnaies cryptographiques de seconde, voire de troisième génération. Afin de concurrencer le BTC, ils proposent des innovations technologiques plus ou moins mineures par rapport à ce dernier. Les *Stablecoins,* quant à eux, se présentent comme une réponse à la volatilité des cryptomonnaies « classiques » (*Bitcoin* et *Altcoins*). Leur cours est arrimé soit à une autre cryptomonnaie, soit à un actif financier (métaux précieux ou matières premières), soit à des monnaies classiques telles que le Dollar ou l'Euro. Ils tentent donc d'allier les avantages des monnaies numériques (décentralisation et indépendance vis-à-vis des autorités monétaires) d'une part, et la stabilité-prix des monnaies traditionnelles d'autre part. Ces cryptomonnaies « stables » ont connu une croissance fulgurante au cours de ces dernières années.

3- *Le stockage des cryptomonnaies*

Une fois que vous avez acheté des cryptomonnaies, vous devez les stocker en toute sécurité pour les protéger des piratages ou des vols. Habituellement, les cryptomonnaies sont stockées dans des portefeuilles de cryptomonnaies, qui sont des appareils physiques ou des logiciels en ligne utilisés pour stocker les clés privées de vos cryptomonnaies en toute sécurité. Certaines plateformes d'échange fournissent des services de portefeuille, ce qui vous facilite la tâche pour effectuer des achats directement sur la plateforme. Cependant, ce ne sont pas toutes les plateformes d'échange ni tous les courtiers qui fournissent automatiquement des services de portefeuille.

4- *Que peut-on acheter avec les cryptomonnaies ?*

Lorsqu'il a été lancé, Bitcoin était censé être un moyen de transaction quotidien, permettant d'acheter tout, allant d'une tasse de café à un ordinateur, voire des biens de grande valeur, comme des biens immobiliers. Cela ne s'est pas encore concrétisé et, bien que le nombre d'institutions acceptant les cryptomonnaies soit en augmentation, les transactions importantes les impliquant sont rares. Malgré cela, il est possible d'acheter une grande variété de produits sur des sites Web de commerce en ligne en utilisant des cryptomonnaies.

5- *Les risques attachés aux cryptomonnaies*. Le premier risque est celui de la valeur des cryptomonnaies, a fortiori des crypto-actifs, puisque cette valeur dépend directement de la loi de l'offre et de la demande. Les autres risques sont principalement liés à la fraude et même à la criminalité financière

en passant par des escroqueries diverses et variées : il peut y avoir de faux sites Web, des systèmes de pyramides virtuelles de Ponzi, le soi-disant soutien de « célébrités », soi-disant prétexte de rencontres romantiques en ligne, etc. Ajoutons aussi, évidemment, le risque de piratage informatique et la possibilité de transactions illicites puisqu'elles sont anonymes.
Enfin, il faut souligner les deux limites considérables que peut connaître la technologie de la blockchain : d'abord le fait que si elle prend beaucoup d'ampleur, le changement de son échelle de fonctionnement peut entraîner un ralentissement important dans le processus qui aboutit au paiement et ensuite le risque environnemental que fait courir la technologie de la blockchain puisqu'elle entraîne une consommation électrique considérable ; et c'est peut-être sa limite essentielle.

6- *L'utilisation des crypto-actifs par l'Iran*, d'après le mémoire de Roxana Khabazzadeh Moghadam, étudiante en Master 2 à l'EHESS, publié par la Banque de France début novembre 2025 :

« Presque entièrement isolé de la finance mondiale, l'Iran s'est tourné vers les crypto-actifs pour contourner les sanctions, créant un système de paiement parallèle hors du système bancaire traditionnel, de l'application des droits de douane et des contrôles de capitaux garantis par sa banque centrale. (…)
Contrairement à l'autorisation prudente et strictement réglementée des crypto-actifs par la plupart des autorités de marché et aux initiatives des banques centrales largement limitées à des expérimentations contrôlées, l'adaptation des cryptos par l'Iran est institutionnelle, délibérée et de plus en plus intégrée au système financier et commercial du pays. L'approche iranienne s'articule autour de trois axes : convertir l'électricité bon marché et fortement subventionnée en crypto-actifs via un minage réglementé par l'État, utiliser les réserves de crypto-actif pour payer les importations et explorer la possibilité d'établir des réseaux de monnaie numérique avec ses alliés.
La stratégie de l'Iran en matière de crypto-actifs
Premièrement, l'Iran a organisé le minage de bitcoins. Les mineurs agréés, dont l'activité a été légalisée en 2019, sont tenus de vendre leurs crypto-actifs à la Banque centrale d'Iran. Grâce à une électricité fortement subventionnée produite à partir du pétrole, l'Iran transforme ce qu'il ne peut pas exporter facilement en bitcoins. C'est un fondement de la stratégie d'évasion de l'Iran : transformer le pétrole sanctionné en crypto-actifs, et l'utiliser pour payer ses importations, en contournant ainsi les sanctions. Il est estimé qu'en 2021 seulement, 4,5 % du total des bitcoins minés dans le monde l'ont été en Iran, permettant au régime d'accéder à des centaines de millions de dollars par cette méthode. Cela a toutefois un coût important pour sa population. Le minage impulsé par l'État iranien affaiblit les contrôles de liquidité et de taux de change de la Banque centrale d'Iran, provoque des pannes d'électricité généralisées et prolongées liées au fonctionnement des fermes non autorisées, et est considéré par les régulateurs américains et européens comme une violation indirecte des sanctions, car il s'inscrit dans une zone grise du Groupe d'action financière (GAFI). (…)
Toutefois, le minage n'est qu'un des piliers de la stratégie de l'Iran en matière de crypto-actifs ; son usage dans les paiements transfrontières est encore plus perturbateur. L'Iran est devenu le premier pays à reconnaître formellement l'usage de crypto-actifs pour le commerce international. Il contourne ouvertement le système financier traditionnel fondé sur le dollar et l'infrastructure bancaire mondiale, perturbant potentiellement le système monétaire. Compte tenu de la nature intrinsèquement anonyme des crypto- actifs, qui contribue à permettre au régime de dissimuler ses activités financières, le gouvernement les utilise pour contourner les sanctions. (…)
Les conséquences de ce système menacent les fonctions essentielles de la politique monétaire. Lorsque le commerce se tourne vers les crypto-actifs, les banques centrales perdent le contrôle des flux de capitaux et des changes. Les entreprises iraniennes abandonnant le rial iranien au profit des crypto- actifs, la demande de monnaie nationale chute, accélérant sa dépréciation. Mais si l'Iran échappe aux sanctions américaines par l'usage de crypto-actifs, cela renforce la prédominance du dollar dans le système monétaire international puisque la plupart des stablecoins sont adossés au dollar. Le commerce « décentralisé » de l'Iran se fait toujours en dollars. Ce paradoxe illustre un dilemme plus profond et soulève des interrogations structurelles pour les banques centrales au niveau mondial, en montrant que l'usage des crypto-actifs, compromet leur autorité en leur retirant le contrôle des taux de change.

Les ambitions de l'Iran vont plus loin, et le pays tente de résoudre cette double réalité. La Banque centrale d'Iran étudie également l'idée d'une cryptomonnaie nationale. Bien qu'elle soit encore au stade préliminaire et théorique, l'objectif est de créer une monnaie numérique indépendante pour les règlements internationaux, en particulier avec des pays comme la Russie ou la Chine. De telles réflexions traduisent l'intention de l'Iran de bâtir un système parallèle de transfert de valeur, indépendant de la Society for Worldwide Interbank Financial Telecommunications (SWIFT, le système mondial de messagerie interbancaire pour les paiements transfrontaliers), des banques correspondantes ou du système du dollar. (…) ».