Cryptomonnaies : Genèse, Typologie, Débats et Tendances

Fabien Clive Ntonga Efoua

CAHIERS DU CEDIMES

Enjeux Sociaux et Stratégies Économiques

Hors-série :

Colloque du 50ème anniversaire de l'Institut CEDIMES

Recueil des communications (tome 2 – panels 5 à 7)

19e année – 2024/HS2

Revue trimestrielle

Mondialisation – Territoires – Entreprises

en partenariat avec l'Université Valahia de Târgoviște, Roumanie

ISSN : 2110-6045

LES CAHIERS DU CEDIMES

19è année- Numéro 2024/HS2 (septembre 2024)

Hors-série :
Colloque du 50ème anniversaire de l'Institut CEDIMES :
Recueil des communications (tome 2 – panels 5 à 7)

« Les Cahiers du CEDIMES » sont publiés par

L'Institut CEDIMES
Campus de la Mondialisation et du Développement Durable
FACO – Faculté de Droit, d'Economie et de Gestion, 115 rue Notre Dame des Champs, 75006, PARIS, France
www.cedimes.com

en partenariat avec l'Université Valahia de Târgoviște
Bd. Regele Carol I, nr. 2, 130024
Târgoviște, Roumanie,
www.valahia.ro

***Directeur de publication** : Valentin RADU, Université Valahia, Târgoviste, Roumanie*

***Rédacteur en chef** : Marc RICHEVAUX*

***Rédacteurs en chef adjoints** : Denis DHYVERT, Mihai MIEILA*

Vol 19 n° 2024/HS2, ISSN : 2110-6045

ISSN : 2110-6045

ISSN 2110-6045

Comité Scientifique de ce numéro

(Les noms des membres permanents du conseil scientifique sont précédés d'une *)

* ALBAGLI Claude, Université Paris Gustave Eiffel, Institut CEDIMES, France

ABDERRAMANE Djoher, Université d'Oran 2, Algérie

*BAYONGWA Désiré, Université de Développement Durable en Afrique Centrale Bagira/Bukavu (R.D.C.)

* BEN ABDENNEBI Hafedh, IHEC, Carthage, Tunisie

* BITYE MENDOMO Mireille, Université de Yaoundé II, Cameroun

BIZIMANA Léonard, ISD, Burundi

BUIRETTE Olivier, Université Sorbonne Nouvelle, Paris 3 – France

CHERABI Abdelaziz, Université de Constantine, Algérie

* CHRISOSTOME Elie, Université de Plattsburgh, Etats-Unis

* FIEVRE Narcisse, Université de Port-au-Prince, Haïti

GHAZOUANI Kamel, IHEC, Carthage, Tunisie

* GRUMO Rosalina, Université Aldo Moro, Bari, Italie

* GUEHAIRIA Amel, ENSSEA Alger, Algérie

* GULSOY Tanses, Université d'Istanbul, Turquie

MARCU Laura, Université Valahia Targoviste, Roumanie

MBALLA Nerry, Université de Bangui Centrafrique

MEYER Vincent, Université de Côte d'azur, Nice, France

MUKHAMETKALIEVA Gulnar, Université Al Farabi, Almaty, Kazakhstan

NEGREPONTI-DELIVANIS Maria, Université de Thessalonique, Grèce

* OLSZEWSKI Léon, Université Wroclaw, Pologne

* RICHARD Blanche Nirina, Université de Antananarivo, Madagascar

* RICHEVAUX Marc, Université du Littoral Côte d'Opale, France

* SCALERA Francesco, Université Aldo Moro, Bari, Italie

* SU Zhan, Université Laval, Québec, Canada

TCHIKO Faouzi, Université Mustapha Stambouli de Mascara, Algérie

TRID Sabah, Université de Fès, Maroc

TUGEN Kamil, Université d'Izmir, Turquie

YOUCEFI Rachid, Université Abdelhamid Ibn Badis, Mostaganem, Algérie

Comité d'Organisation du colloque

Président :

ALBAGLI Claude

Membres :

BEN ABDENNEBI Hafedh (Tunisie)

DHYVERT Denis (France)

GUEHAIRIA Amel (Algérie)

GIQUELLO Guy (France)

RICHEVAUX Marc (France)

SCALERA Francesco (Italie)

MHAMDI Mohamed (Maroc)

Les Cahiers du CEDIMES

2024, Volume 19, Hors-série n° 2024/HS2, 50ème anniversaire CEDIMES

ISSN 2110-6045

Cryptomonnaies : Genèse, Typologie, Débats et Tendances

Fabien Clive NTONGA EFOUA

FSEG/CEREG (Université de Yaoundé II, Cameroun), clivelandef@gmail.com

Résumé : Partant du constat d'un chaos généralisé dans la cryptosphère et de la nécessité d'une régulation de cet écosystème, cet article propose : (*i*) de revisiter la genèse et dresser un état de l'art relatif aux différentes formes de cryptomonnaies, (*ii*) d'en proposer une typologie et (*iii*) de conjecturer sur quelques tendances qui devraient marquer leur processus évolutif ; se situant de fait à un carrefour entre l'Economie, l'Informatique, le Droit et l'Histoire. La méthodologie s'appuie sur une approche dialectique. Cette dernière permet de distinguer deux principaux types de cryptomonnaies : celles dites « décentralisées » et celles dites « souveraines ». Cette catégorisation peut être affinée selon des critères plus spécifiques, notamment : la nature du flux digital, l'algorithme de consensus, l'émetteur et la technologie de base (avec ou sans *blockchain*). Nous parvenons ainsi à différencier sept sous-catégories de cryptomonnaies : les monnaies numériques « primitives », le *Bitcoin,* les *Altcoins*, les *Stablecoins*, et ce que nous appelons les *Iotcoins* d'une part ; puis les Monnaies Numériques de Banque Centrale (MNBC) et ce que nous appelons les Monnaies Numériques Nationales (MNN) d'autre part. Selon notre analyse, compte tenu de la volatilité des cryptomonnaies décentralisées, des risques de sécurité qu'elles posent et de leur propension à participer au financement de l'économie souterraine, la question de leur cohabitation avec les cryptomonnaies souveraines se posera inévitablement. Par ailleurs, en ce qui concerne les *Govcoins*, les MNBC semblent susciter davantage d'adhésion que les MNN, eu égard à la sempiternelle question de l'incohérence temporelle.

Mots-clefs : Monnaies numériques, Bitcoin, Altcoins, Stablecoins, Govcoins.

Abstract: Based on the observation that there is chaos in the crypto-world and the need to regulate this ecosystem, this paper proposes: (*i*) to revisit the genesis and draw up a state of the art concerning the different forms of cryptocurrencies, (*ii*) suggest a typology in order to (*iii*) review the directions that could be taken by their development. From an academic view, in addition to Economics, this could be of interest to many other disciplinary fields, particularly Computer science, Law and History. Methodologically, this paper is based on a historical and dialectical approach. That allows us to distinguish two main types of cryptocurrencies: those which are "decentralised" and those which are "sovereign". This common categorisation can be refined according to some specific criteria, in particular: the nature of the digital flow, the consensus algorithm, the issuer and the core technology. Thus, we can differentiate seven sub-categories of cryptocurrencies: the "primitive" digital currencies, the *Bitcoin*, the *Altcoins,* the *Stablecoins* and what we call the *Iotcoins*, on the one hand; then the *Central Bank Digital Currencies* (CBDC) and what we call the *National Digital Currencies* (NDC) on the other. From our view, given the volatility of the decentralised cryptocurrencies, the security aspects and their propensity to finance the shadow economy, their coexistence with the sovereign cryptocurrencies will undoubtedly arise. Concerning particularly the (future) *Govcoins*, the CBDC seem to have more support than the NDC, given the everlasting issue of temporal inconsistency.

Keywords : Digital currencies, Bitcoin, Altcoins, Stablecoins, Govcoins.

Classification JEL : E58, O33

1. 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. Dans les pays en développement, à l'exception de la Chine où les paiements digitaux sont déjà très répandus, environ 40 % des personnes qui ont effectué un paiement par voie électronique à partir d'un compte courant l'ont fait pour la toute première fois lors de la pandémie.

En France, dans le domaine de la FinTech, les mots « NFT » et *« Bitcoin* » ont été parmi les plus cités par la presse en 2021. En effet, le « Corona-krach » a affecté non seulement les marchés financiers qui ont enregistré leur pire performance depuis la crise de 2008, mais également celui des cryptomonnaies. Début Mars 2020, le cours du *Bitcoin* (BTC) est par exemple passé de moins de 8 000 USD (7 950 € environ) à moins de 4 000 USD (4 916 € environ), soit une baisse de 38,12 % qui représentait l'une des pires chutes de son histoire. Toutefois, contrairement aux valeurs des marchés boursiers, les cours de cryptomonnaies se sont redressés plus rapidement. Dès début Avril de la même année, le cours du BTC, porte-étendard des monnaies numériques dites « décentralisées », a ainsi retrouvé son niveau de Janvier 2020. Ce schéma de montagnes russes s'est reproduit fin 2022, lorsque la valeur du BTC est passée à moins de 17 000 USD, après avoir atteint un plafond historique de 67 000 USD en Octobre 2021. Ironie du sort, la cryptomonnaie *Omicron* a fait l'objet d'une activité frénétique, cotant jusqu'à 700 Dollars après la découverte d'un nouveau variant du Covid-19 portant le même nom, fin Novembre 2021.

Bien que cette « euphorie cryptographique » gagne du terrain à travers le monde (Adrian et Weeks-Brown, 2021), certains pays tels que l'Algérie, l'Argentine, la Chine, l'Inde ou encore la Thaïlande ont purement et simplement décidé d'interdire les transactions en « cryptos » sur leur territoire. D'autres pays, tels que la Suède, militent en faveur de l'interdiction du « minage » en Europe, estimant que cette activité compromet les engagements contre le réchauffement climatique. Cependant, il convient de préciser que parmi ces pays, quelques-uns – dont la Chine et la Suède notamment – ont déjà lancé leurs propres projets de monnaies numériques « centralisées », de type Monnaie Numérique de Banque Centrale (MNBC). Parallèlement, dans plusieurs des pays où l'usage des cryptomonnaies décentralisées est toléré, les Banques Centrales ont entamé une réflexion sur les projets cryptomonétaires de type MNBC. Selon un sondage de la Banque des Règlements Internationaux (BRI) réalisé auprès de 66 Banques Centrales des pays développés et émergents, 52 d'entre elles avaient engagé une réflexion sur ce sujet en 2020. En 2022, le nombre de Banques Centrales envisageant une forme numérique de leur monnaie à travers le monde était estimé à 112.

Partant de ces faits, cet article propose une catégorisation des cryptomonnaies et tente des conjectures sur leur évolution future, au vu des tendances actuelles. Son originalité repose sur trois aspects. D'un point de vue théorique tout d'abord, la réflexion s'appuie sur une démarche dialectique et historique qui permet de cerner les facteurs à l'origine de la création de la pléthore d'instruments monétaires cryptographiques actuellement observés et d'en dresser un état de l'art. En effet, s'il existe une littérature de plus en plus abondante sur le thème des cryptomonnaies d'une part – à propos de leurs origines –, à notre connaissance, la littérature ne propose qu'un aperçu du rôle des pionniers tels que David Chaum, Wei Dai, Nick Szabo et Hal Finney entre le début des décennies 1980 et 2000. D'autre part, les études qui s'intéressent aux origines de l'euphorie cryptographique (voir supra) s'appesantissent davantage sur l'impact qu'a eu la publication du Livret Blanc de Satoshi Nakamoto ; se concentrant de facto sur le *Bitcoin* ou sur certains

Stablecoins dont la création est relativement récente (voir infra). Or, ces derniers ne représentent que quelques-unes parmi la vingtaine de milliers de cryptomonnaies utilisées à travers le monde.

Ensuite, ce papier se démarque de la plupart des articles de référence qui abordent ce thème dans la mesure où il traite de l'ensemble des cryptomonnaies, tandis que les autres se concentrent plus ou moins exclusivement : soit sur la *blockchain* (Faure-Muntian et al., 2018), soit sur le *Bitcoin* (Lo et Wang (2014), Lakomski-Laguerre et Desmedt (2015), Dupré et al. (2015)), soit sur les monnaies numériques décentralisées de manière générale (Laurent et Monvoisin (2015), Chiu et Thorsten (2019), Fantacci et Gobbi (2021)), soit sur les MNBC (Bech et Garratt (2017), Carapella et Flemming (2020), Cunha et al. (2021), Infante et al. (2022), De Boissieu (2023)). La réflexion dans cet article porte également sur des concepts tels que les *tokens*, les NFT (*Non-Fungible Tokens*) et l'Internet des Objets. Partant de là, il nous sera alors possible de tenter des conjectures sur le devenir des moyens de paiement numériques et sur les débats qu'ils susciteront inéluctablement, de notre point de vue.

Enfin, d'un point de vue académique, cet article propose succinctement une revue de la littérature récente sur les enjeux des cryptomonnaies, ce qui permet à la fois d'expliquer les raisons de leur processus évolutif et d'en faire le point. Outre l'Economie, cet article pourrait de fait intéresser d'autres champs disciplinaires tels que l'Informatique, le Droit et l'Histoire. Une catégorisation des moyens de paiement numériques selon des critères bien spécifiques s'avère également capitale afin de rendre leur étude (opportunités et risques) et leur (future) régulation plus cohérente. En effet, ainsi que nous le verrons, le terme : « cryptomonnaie » fait référence à un assez large éventail d'instruments dont l'émission et l'échange peuvent se faire selon diverses modalités. Ces dernières vont largement au-delà de la dichotomie habituellement faite dans la littérature entre les « cryptos » décentralisées et les (futures) cryptomonnaies souveraines. C'est afin d'affiner cette catégorisation des cryptomonnaies que la démarche dialectique et historique sus évoquée nous semble particulièrement indiquée dans le cadre de cet article. En outre, cette catégorisation des cryptomonnaies permettra aux agents économiques de prendre des décisions plus rationnelles et, en même temps, d'éclairer les politiques économiques.

La suite du papier est structurée de la manière suivante : dans le paragraphe qui suit immédiatement l'introduction, nous définissons brièvement d'une part les notions de monnaies virtuelle, monnaie numérique et de cryptomonnaie et indiquons le positionnement de l'article par rapport à ces concepts d'autre part. Ensuite, nous revisitons les origines des supports monétaires cryptographiques en revenant sur l'impact majeur qu'a eu la création du *Bitcoin* (la cryptomonnaie décentralisée la plus populaire). Il sera ensuite question de l'essor des *Altcoins*, des *Stablecoins* et des cryptomonnaies sans *blockchain* (ce que nous appelons : les *Iotcoins*). Nous verrons enfin pourquoi et comment l'idée de monnaie numérique régulée a commencé à émerger et à quelle étape en sont quelques projets y relatifs au moment où cet article est rédigé. Cela débouchera naturellement sur un passage en revue des débats et des tendances qui, de notre pont de vue, devraient marquer l'évolution de ces moyens de paiement à terme.

2. Actifs numériques, monnaies virtuelles, monnaies numériques ou cryptomonnaies ?

Dans un rapport publié en 2012 et réactualisé en 2015, la Banque Centrale Européenne (BCE) définit les monnaies virtuelles – encore appelées monnaies digitales – comme des « monnaies numériques non régulées acceptées au sein d'une communauté virtuelle déterminée ». À quelques très rares exceptions près, elles n'ont pas de cours légal (cf. infra). Contrairement aux monnaies électroniques, elles ne sont pas émises par un établissement financier contre la remise de fonds et leur mise en circulation n'est pas régulée par une Banque Centrale[1]. Daniel (2019) les

[1] La BCE (2012 et 2015) rappelle que cette définition peut être sujette à changement si les caractéristiques fondamentales des monnaies virtuelles changent aussi.

classe en deux grands groupes : les monnaies virtuelles « fermées » d'une part, et les monnaies virtuelles « ouvertes » d'autre part.

Les monnaies virtuelles en système fermé sont par exemple utilisées dans les jeux vidéo ou les univers virtuels. Elles n'ont aucun lien avec l'économie réelle. Quant aux monnaies virtuelles en système ouvert, elles peuvent être classées en deux sous-groupes, selon qu'elles sont à flux unidirectionnel ou bidirectionnel. Les monnaies virtuelles avec un flux unidirectionnel, telles que les *Amazon Coins*, peuvent être achetées directement avec une devise légale à un taux de change défini, mais ne peuvent être reconverties en monnaie légale. Ces monnaies permettent d'acheter à la fois des biens/services virtuels et réels d'un montant limité (systèmes de micropaiements pour l'achat d'applications par exemple). Les monnaies virtuelles avec un flux bidirectionnel, quant à elles, peuvent être converties en monnaie légale. Elles ont à la fois un cours d'achat et un cours de vente. C'est le cas de certaines cryptomonnaies, dont les plus connues sont entre autres : *Bitcoin* (BTC), *Ethereum* (ETH), *Tether* (USDT), *Ripple* (XRP), *Binance Coin* (BNB) ou encore *Iota*.

Dans la suite de l'article, nous employons le terme « monnaie numérique » plutôt que le terme « monnaie virtuelle », afin d'éviter l'amalgame entre les monnaies bloquées dans le monde virtuel (monnaies fermées) d'une part, et les monnaies numériques issues du monde virtuel, à l'instar du *Bitcoin* et des *Altcoins* (cf. infra), qui sont utilisées dans l'économie réelle.

Pour des raisons pratiques, nous proposons également de généraliser l'emploi du terme « cryptomonnaie » à l'ensemble des actifs cryptographiques ou numériques. En effet, une cryptomonnaie fait intervenir deux mécanismes : la monnaie, c.-à-d. un moyen d'échange d'une part et le cryptage d'autre part (Daniel, 2019). Bien qu'ils répondent difficilement aux trois fonctions économiques traditionnelles de toute monnaie à savoir : unité de compte, intermédiaire pour les échanges et réserve de valeur (c.-à-d. des moyens de paiement ayant cours légal sur un territoire donné) et que l'appellation « monnaie » fasse encore débat dans la littérature à propos des cryptoactifs décentralisés (Jabotinsky (2020), Adrian et Weeks-Brown (2022), AEMF (2022)), notons que ces derniers sont des instruments quasi consensuellement acceptés en paiement de biens et de services ou en remboursement de dettes dans la majorité des pays du monde. À ce titre, ils peuvent donc prétendre au statut de monnaie, du moins au sens de Mishkin (2004). En outre, ainsi que le souligne Perrot (2018) à propos de ce qu'est une « vraie » monnaie, les coquillages et autres objets qui ont servi de monnaie à des périodes reculées de l'histoire étaient également des signes conventionnels sans intermédiaire bancaire. L'efficacité de ces signes était fondée, comme celle des cryptomonnaies, sur une confiance collective. Non pas d'abord la confiance dans une autorité publique, mais plutôt la confiance dans une « communauté de paiement ». Et de fait, en 2020, la Cour de cassation française a reconnu au *Bitcoin* le statut de monnaie (Perrot, 2021). Par ailleurs, il convient de noter que le *Bitcoin* et ses avatars (cf. infra) sont largement désignés sous le vocable de cryptomonnaies (*cryptocurrencies*) dans la littérature anglo-saxonne (Claeys et al. (2018), Chiu et Thorsten (2019), Sockin et Wei Xiong (2020), Cunha et al. (2021), Liu et al. (2022), Baer et al. (2023)). C'est également une telle lecture que suggère l'intitulé de l'article d'Aglietta et Lakomski-Laguerre (2022)[1] – qui fait référence à la réaction des autorités monétaires à l'annonce du lancement d'une monnaie numérique par l'entreprise Meta –, idem en ce qui concerne l'analyse de De Boissieu (2023).

3. Les monnaies cryptographiques « primitives »

Cette section revisite les origines des supports monétaires cryptographiques, ainsi que leurs fonctions traditionnelles. Ces éléments seront déterminants pour discuter du processus évolutif des cryptomonnaies, à la fois au fil des décennies passées et dans un avenir plus ou moins proche.

[1] « Les cryptomonnaies en plein essor : les banques centrales lèvent leurs boucliers ! ».

Contrairement à une opinion largement répandue, les concepts de *blockchain* (chaîne de blocs) et de cryptomonnaie existaient bien avant la création du *Bitcoin.* 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. Par la suite, il a publié un article sur le procédé de « signatures aveugles » permettant théoriquement d'envoyer de l'argent de manière anonyme[1]. Dans la cryptosphère, la *blockchain* sert de registre public de transactions cryptées, maintenues et mises à jour par des milliers de personnes dans le monde entier (voir Encadré 1). 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)[2] que l'on oppose généralement à celle du *central banking* (Aglietta, 1992).

En 1983, Chaum a conçu et tenté de commercialiser *eCash*, un système de paiement digitalisé et anonyme. Dans les grandes lignes, ce système prévoyait qu'une banque puisse « signer » des pièces de monnaie numériques qu'un utilisateur pourrait stocker sur son ordinateur et échanger par courrier électronique avec d'autres utilisateurs afin de réaliser un paiement. Basé sur le principe de « signature aveugle », ce système assurait l'anonymat : de même qu'un commerçant acceptant des pièces de monnaie en paiement n'a aucune information sur l'identité du payeur, de même un utilisateur payant en ligne avec *eCash* ne révélait rien de son identité (Ajdenbaum, 2021). Six années plus tard, M. Chaum a fondé l'entreprise DigiCash Incorporated, afin de mettre en œuvre le produit de ses propres recherches théoriques. Grâce à elles, il a créé *Digicash*, une monnaie virtuelle cryptographique et anonyme en 1990. Quelques banquiers acceptèrent de faire des tests avec *DigiCash*, mais la plupart d'entre eux pensait que les Banques Centrales auraient du mal à mesurer la masse monétaire en circulation avec un projet d'une telle ampleur, ce qui aurait inévitablement posé des inquiétudes du point de vue de la gestion des moyens de paiement. En effet, selon Antoine Champagne (premier journaliste français à avoir écrit sur les cryptomonnaies dès les années 1990), le *DigiCash* était nettement moins traçable que les cryptomonnaies actuelles[3].

DigiCash Inc. fut donc forcée de se déclarer en faillite en 1998, en raison du manque d'adhésion populaire. La même année, deux nouveaux protocoles d'échange monétaire et d'exécution des contrats ont été proposés : le *B-Money* et le *Bit Gold*. Conçu par l'informaticien d'origine chinoise Wei Dai, le premier était destiné à être un système de paiement (en même temps qu'une monnaie) électronique distribué(e) et anonyme ; afin de rendre possible une économie en ligne qui ne puisse être ni taxée, ni réglementée par la « menace de violence »[4]. Quant au second, il s'agissait du projet de création d'une monnaie numérique décentralisée, conçu par l'Américain Nick Szabo – qui avait travaillé en tant que consultant pour M. Chaum –. C'est sur cette lancée que plusieurs années plus tard, en 2005, Hal Finney (un célèbre crypto-anarchiste) soumettra à ses confrères un prototype de monnaie numérique intraçable, le *RPOW.*

Le *B-Money* fut un échec, tandis que le *Bit Gold* ne fut jamais implémenté, car vulnérable aux attaques. Quant au *RPOW*, il ressemblait davantage à une version améliorée du *Bit Gold* qui en plus, dépendait d'un serveur central. Néanmoins, à bien des égards, ces trois projets sont

[1] Voir par exemple Chaum (1985).

[2] Il existe néanmoins une différence majeure entre le projet de Chaum-Nakamoto (cf. infra) et celui de Hayek (op.cit.). Dans le scénario de la cryptosphère, il n'existe pas d'autorité de régulation qui puisse arrêter ou annuler les transactions. Chacun « est » sa propre banque, le transfert de fonds est indépendant et totalement gratuit ; tandis que, dans le scénario du second, les banques demeurent les émettrices du support monétaire.

[3] Voir https://www.bfmtv.com/crypto/bitcoin/on-a-retrouve-le-premier-journaliste-francais-a-avoir-ecrit-sur-l-ancetre-du-bitcoin-en-1995_AV-202207260296.html, visité les 10 Novembre 2023.

[4] La motivation de M. Dai était de « créer une communauté où la menace de violence est impuissante parce que la violence est impossible et où la violence est impossible parce que ses membres ne peuvent pas être reliés à leur vrai nom ou leur localisation géographique ».

unanimement reconnus comme étant les précurseurs directs du *Bitcoin* (Nakamoto (2009), Lakomski-Laguerre (2020)) – cf. Encadré 1.

4. Le *Bitcoin* : de la naissance à la notoriété

Il est difficile d'aborder le thème des cryptomonnaies sans accorder un intérêt particulier à la plus populaire d'entre elles : le *Bitcoin*. Ce vocable est issu de la fusion de deux mots anglais : *bit* (unité de mesure binaire) et *coin* (pièce de monnaie). Selon le site bitcoin.fr, ce terme serait apparu pour la première fois dans le Manga (bande dessinée japonaise) « *Ghost in the Shell 2 : Manmachine Interface* » publié entre 1991 et 1997. Cette cryptomonnaie a attiré l'attention du public en Octobre 2008, lorsqu'un individu (ou un mystérieux groupe de personnes) répondant au pseudonyme de Satoshi Nakamoto, a publié un Livret Blanc d'une dizaine de pages décrivant les fonctionnalités du réseau de *blockchain Bitcoin*[1]. Le document en question décrit le *Bitcoin* comme une ressource numérique théorique à source ouverte : personne n'en est propriétaire, tout le monde peut participer à son utilisation et à son développement. Son fonctionnement s'inspire largement de l'idéologie du mouvement activiste « *Cypherpunk* »[2] apparu à la fin au début des années 1990, qui s'inquiétait de la protection de la vie privée au moment de la démocratisation d'Internet ; face aux risques d'écoute et d'interférence des gouvernements (Ajdenbaum, 2021). On retrouve bien là, les idées contestataires qui étaient à l'origine de la création du *B-Money* ou encore du *DigiCash* plusieurs décennies plus tôt.

En effet, dans la lignée du mouvement crypto-anarchiste dont les principes de liberté individuelle et de confidentialité ont été diffusés par Timothy Christopher May, Phil Zimmermann et consorts vers la fin des années 1980, le développement du *Bitcoin* a été porté par la volonté de contourner le système financier traditionnel, jugé responsable du *krach* financier de 2007 et de la crise économique qui en a résulté (excès de dettes, financiarisation trop poussée, spéculation et instabilité). Ce discrédit s'est alors traduit par la volonté de concevoir un système alternatif d'échange de la valeur au moyen d'un instrument sur lequel les banques n'auraient aucun contrôle (Nakamoto, 2009). Toutefois, contrairement aux initiatives cryptomonétaires précédentes, celle de Nakamoto semble avoir fourni une solution au problème de la double dépense – c'est-à-dire au risque qu'une même somme soit dépensée deux fois de façon accidentelle ou malveillante – (Loignon, 2017). Effectivement, tout comme de la fausse monnaie, la double dépense mène à l'inflation dans la mesure où elle crée une nouvelle quantité de monnaie sans contrepartie (Encadré 1).

La suite est à peu près connue. Le 12 Janvier 2009, a lieu la toute première transaction en *Bitcoins* (BTC) : 10 *coins* sont alors envoyés par Nakamoto à Hal Finney (voir supra). Pendant plusieurs années, le (BTC) évolue hors des radars, n'intéressant que les *geeks* ou les blanchisseurs d'argent sale. S'échangeant contre 0,001 USD en 2009, le BTC atteint la parité avec le Dollar en 2011. En Novembre 2013, sa valeur dépasse celle de l'once d'or (près de 1.250 Dollars). Par la suite, le cours du BTC augmente régulièrement année après année, bien qu'il soit assez volatile. Ainsi, après une ascension en 2017 (*cf. supra*), sa valeur s'effondre de près de 80 % en fin 2018, à 3.700 Dollars. Le 09 Novembre 2021, le BTC franchit un nouveau cap : celui des 68.000 Dollars. L'idée de monnaie numérique décentralisée commence alors à attirer l'attention du public et des autorités monétaires (voir infra). En conséquence, au cours de ces dernières années, l'on a assisté au boom des alternatives au *Bitcoin* (les *Altcoins*), ainsi qu'à l'émergence des *Stablecoins* (Pavel (2017), Fantacci et Gobbi (2021)).

[1] Document disponible à l'adresse : http://www.bitcoin.org/bitcoin.pdf. Pour la traduction en français, voir Nakamoto (2009).

[2] *Cypherpunk* est composé de deux mots anglais : *cypher* (qui signifie chiffrement) et *punk* (qui désigne un esprit contestataire ou rebelle).

5. Les *Altcoins* et les *Stablecoins*

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. Dans la mesure où il existe actuellement plusieurs milliers d'*Altcoins*, nous n'en évoquerons que trois pour des raisons pratiques : *Ripple*, *Etherum* et *Praxxis*. Les deux premières figurent parmi les *Altcoins* les plus populaires, tandis que la dernière est le (futur) *Altcoin* développé par M. Chaum (considéré comme le « père des cryptomonnaies » – voir supra).

L'une des spécificités du protocole *Ripple* (XRP) lancé en 2012 est de servir comme « pont monétaire » (c.-à-d. servir de relais ou de plateforme d'échange) entre les différentes monnaies fiduciaires et les cryptomonnaies. En d'autres termes, ce système permet de payer n'importe quel utilisateur de *Bitcoin*s directement depuis un compte *Ripple*, sans qu'il ait à posséder cette monnaie numérique. Tout utilisateur de *Ripple* peut *de facto* agir comme un animateur de marché en offrant un service d'arbitrage (fourniture de liquidité au marché, conversion de devises ou de cryptomonnaies, etc.). Par ailleurs, les transactions en XRP sont vérifiées par consensus entre les membres du réseau, plutôt que par le processus de minage (utilisé par *Bitcoin*). Elles peuvent ainsi être validées en moins de quatre secondes, contre 10 minutes en moyenne pour le *Bitcoin* ; ce qui en fait une *blockchain* plus rapide. *Ethereum* (ETH) a, quant à lui, été lancé en 2015. Il est dérivé du code source de BTC et fait usage de contrats intelligents (*smart contracts*)[1] afin d'assurer une sécurité supérieure et réduire les coûts de transaction associés à la passation des contrats. En 2022, ETH a effectué sa transition de la preuve de travail (PoW) vers une preuve d'enjeu ou preuve de participation (PoS) – voir Encadré 1. Dans le même ordre d'idées, en 2019, M. Chaum (voir supra) a annoncé le développement de *Praxxis*, une cryptomonnaie « quantum-résistante ». Cette dernière innove sur les idées originales d'*eCash* ainsi que sur la technologie du BTC. *Praxxis* serait alors doté de mécanismes de sécurité informationnelle qui échappent au contrôle des pouvoirs publics d'une part, et utiliserait des « signatures » permettant de prévenir d'éventuelles cyberattaques d'autre part.

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. Début 2020, la valeur totale de tous les *Stablecoins* dépassait 5 milliards de Dollars. *Tether* (USDT) – apparu en 2014 – est le premier et le plus populaire d'entre eux. Sa valeur est théoriquement adossée au Dollar suivant la relation : 1 USDT = 1 Dollar. En conséquence, son cours ne devrait pas fluctuer. En réalité cependant, le maintien de cette parité n'est pas évident. En septembre 2020 par exemple, il y avait un peu plus de 14,4 milliards USDT en circulation. Les dirigeants de *Tether* affirmaient alors disposer de 14,6 milliards de Dollars en réserve ; ce qui n'était pas exact, selon la procureure de l'État de New York. Fin Février 2021, les premiers ont dû payer une amende de 18,5 millions de Dollars à l'État de New York afin de mettre fin aux poursuites judiciaires. De même, suite à un *flash-krach* vers la mi-2022, *Tether* a brièvement perdu sa parité avec le Dollar, passant de 1 USD à 0,95 USD. Cela a incité les investisseurs à retirer 10 milliards de Dollars dans les semaines suivantes et se ruer vers d'autres *Stablecoins* tels qu'*USD Coin* et *Binance USD*.

[1] Les *smart contracts* sont des programmes qui exécutent des tâches prédéfinies sur une *blockchain* de manière autonome. L'idée de leur conception remonte aux projets de Wei Dai et Nick Szabo (*cf. supra*).

Encadré 1. *Blockchain*, cryptomonnaies, minage, *coins*, *tokens* et NFTs

En général, lorsque l'on envoie un fichier numérique, une copie est conservée chez le destinataire. Avec la *blockchain*, cet aspect caractéristique des transferts numériques n'existe plus : il est possible de faire transiter un actif numérique vers un bénéficiaire tout en s'assurant que l'émetteur ne le possède plus. Cet échange est décentralisé, sécurisé, certifié et vérifiable. C'est pourquoi cette technologie constitue le socle de la mise en circulation des cryptomonnaies.

Les cryptomonnaies sont des instruments décentralisés basés sur un réseau de personne-à-personne, sans intermédiaire. Leur offre dépend des « mineurs », c.-à-d. des membres de la communauté (qui les accepte comme moyen de paiement) disposant d'ordinateurs dotés de la capacité de calcul nécessaire à la résolution d'algorithmes dont la complexité croît avec le nombre de *coins* créés. L'objectif du minage est de sécuriser (et valider) une chaîne de transactions en échange d'une certaine récompense. Dans le cas du *Bitcoin*, la récompense des mineurs est divisée par deux chaque année, de façon à limiter à 21 millions, le nombre total des *Bitcoins* en circulation. Fin Janvier 2022 par exemple, un mineur solitaire s'est vu récompenser de 6,25 BTC – soit l'équivalent de 220.000 Dollars –, à l'issue d'une série d'extractions de BTC. Quant à *Ethereum*, la récompense pour le minage d'un bloc est de 2 ETH (soit plus de 6.000 Dollars au cours actuel de mi-2023). Son réseau permet aux mineurs d'ajouter de nouveaux blocs après une moyenne d'environ 15 secondes.

La *blockchain* est donc un registre décentralisé et distribué permettant de créer la confiance entre des parties (utilisateurs) qui ne se connaissent théoriquement pas. Elle utilise des « algorithmes de consensus » afin de « choisir » le nœud qui ajoutera les nouvelles transactions de manière objective et irréfutable. Dans le cas du *Bitcoin*, le principe de consensus repose sur une preuve de travail (PoW – *Proof of Work*). Cette dernière consiste à proposer aux mineurs potentiels un problème cryptographique (retrouver une suite de caractères par exemple). Le premier mineur à résoudre ce problème obtient l'autorisation d'ajouter de nouveaux blocs.

Le problème de la PoW est qu'elle pousse les mineurs à engager de plus en plus la puissance de calcul de leurs ordinateurs pour résoudre les problèmes mathématiques et créer de nouveaux blocs, ce qui implique des dépenses croissantes en ressources énergétiques pour rester compétitif. Un seul mineur est en effet récompensé, même si les autres « perdants » pourraient également avoir fait des milliards d'essais pour résoudre le problème cryptographique. De même, si deux blocs sont trouvés presque en même temps, l'algorithme de consensus validera toujours la chaîne la plus longue. En outre, la PoW est un processus qui ralentit la validation des transactions à mesure que la *blockchain* grandit. C'est la raison pour laquelle la *blockchain* telle que conçue dans le système BTC est énergivore. En 2014, la consommation d'énergie du BTC était estimée à 240 kWh (soit 61 litres d'essence) par *coin*. Selon une étude d'impact menée par les autorités américaines en 2018, si le *Bitcoin* était un pays, sa consommation d'énergie serait classée au 31e rang mondial sur 230.

Compte tenu de ces inconvénients, l'on a assisté au développement d'algorithmes de consensus alternatifs à celui de Nakamoto ; même si ce dernier demeure actuellement le plus utilisé de la cryptosphère (voir section 5). L'une de ces alternatives les plus sérieuses est la preuve d'enjeu (ou preuve de participation) – PoS, *Proof of Stake* (Huynh-The et al., 2023). Elle détermine le choix du mineur en fonction d'un autre critère : son intérêt (ou son implication) qui peut être mesuré(e) par le volume des actifs détenus, la durée de détention des *coins* ou encore le nombre de transactions effectuées dans la *blockchain* par les participants. La PoS est conçue pour permettre à une *blockchain* d'être plus rapide en tenant compte de sa consommation en énergie et de son impact environnemental. En 2022, *Ethereum* a effectué sa transition de la PoW vers une PoS (*Ethereum 2.0*). Le principal inconvénient de la preuve d'enjeu est que, dans sa forme initiale, elle favorise les utilisateurs les plus « riches ». En revanche, elle a l'avantage de réduire considérablement les besoins en énergie.

Il existe également des cryptomonnaies telles que *Helium* (HNT) qui combinent à la fois la technologie *blockchain* et l'Internet des Objets (IdO) – voir section 5.

Les *coins* (« pièces » en français) sont souvent assimilé(e)s à tort aux *tokens* (« jetons » en français). Plusieurs médias affirment par exemple que *Bitcoin* est le premier *token* à avoir été créé vers la fin de la décennie 2000. En fait, *coins* et *tokens* ne renvoient pas à la même réalité stricto sensu. Techniquement, un *coin* est une unité de valeur qui existe sur sa propre *blockchain*, tandis qu'un *token* est l'unité de valeur d'un actif numérique qui repose (ou est hébergé) sur une *blockchain* préexistante. Ainsi, *Bitcoin* ou *Ethereum* (parfois abrégé *Ether*) sont des *coins* ; tandis que *Tether* (USDT) ou *Basic Attention Token* (BAT) sont des

tokens qui reposent tous sur la *blockchain Ethereum*. Les *tokens* présentent au moins un avantage par rapport aux *coins* : leurs développeurs n'ont pas à créer une *blockchain* qui leur est propre. Cela leur permet d'économiser des ressources. Il faut en effet du temps et beaucoup de mineurs pour créer une *blockchain* solide qui ne puisse être attaquée. Les *tokens* bénéficient donc de l'infrastructure de la *blockchain* sur laquelle ils se greffent. Certaines cryptomonnaies ont démarré en tant que *token*, puis ont évolué pour devenir des *coins*. Tel est le cas pour *Binance Coin* qui a d'abord été un *token* reposant sur la *blockchain Ethereum*.

Il est également possible de distinguer les jetons fongibles et les jetons non fongibles. Certaines entreprises lèvent des fonds en proposant de vendre des *tokens* fongibles. Ces jetons numériques sont ensuite achetés par des investisseurs *via* une cryptomonnaie. On parle ainsi d'ICO (*Initial Coin Offering*). Quant aux jetons non fongibles – c.-à-d. non interchangeables stockés sur une *blockchain* –, ils sont plus connus sous l'acronyme : NFTs (*Non-Fungible Tokens*).

En effet, les monnaies sont fongibles, de même que les cryptomonnaies. Il est par exemple possible d'échanger des Euros, des Dollars ou des *Bitcoins*. En revanche, les NFTs, associés à certains objets numériques (tels qu'une paire de chaussures, des fichiers audios, une peinture digitale, etc.) pouvant être utilisés dans un monde virtuel avec un casque de réalité virtuelle, sont non-fongibles. Un NFT permet donc à un artiste de vendre un fichier numérique comme il vendrait une œuvre physique. L'acheteur a alors la possibilité entre autres, de collectionner des œuvres d'art numériques et de spéculer sur ces œuvres. Certaines *blockchains* peuvent émettre des cryptomonnaies et des jetons fongibles ou non. Tel est le cas d'*Etherum*. La création des NFTs se fait moyennant des frais qui varient selon chaque *blockchain* utilisée.

Source : Construction de l'auteur.

6. Vers des cryptomonnaies sans *blockchain ?*

Les algorithmes de conse nsus sont des procédés par lesquels les nœuds d'un réseau pair-à-pair se mettent en accord sur un registre de transactions (voir supra). Bien que le consensus de Satoshi Nakamoto soit encore largement populaire dans l'univers des cryptomonnaies, de nouveaux algorithmes pour faire fonctionner une *blockchain* ont déjà vu le jour : la preuve d'enjeu, la preuve d'histoire, la preuve de service, etc. (Huynh-The et al., 2023). D'autres projets cryptomonétaires vont encore plus loin, dans la mesure où ils proposent purement et simplement de fonctionner sans *blockchain.* Tel est notamment le cas pour *Iota*[1] conçu en 2015, qui cotait 0,19 USD à la mi-Juillet 2023.

Iota est une cryptomonnaie dont le fonctionnement repose sur le protocole Tangle (technologie des graphes acycliques) et sur l'Internet des objets (*Internet of Things*, IoT en anglais). En effet, la *blockchain* n'est qu'une manière de structurer les données. Or, la limite de transactions sur le réseau BTC – pour ne citer que ce cas en raison de sa popularité – est régulièrement atteinte, ce qui entraîne sa congestion et des frais. Ces derniers dépendent alors de plusieurs facteurs parmi lesquels : la congestion du réseau, le temps de confirmation de la transaction et la taille de la *blockchain*. Sans vouloir rentrer dans les détails techniques, il faut préciser que ce sont là quelques freins à la généralisation de la *blockchain* (telle qu'elle est actuellement configurée) dans la sphère économique : une grande entreprise serait par exemple peu disposée à payer des frais supplémentaires ou à attendre que ses « blocs » soient validés pour effectuer ses transactions (processus qui prendrait 4 secondes à 10 minutes, dans l'état actuel de la technologie). C'est pourquoi le système *Iota* se passe des mineurs[2]. Il autorise des transactions instantanées et sans aucun coût supplémentaire des données électroniques via les appareils connectés. Ce système pourrait donc permettre à ses utilisateurs de monétiser leurs données contre des *Iotas* auprès d'entreprises tierces, sans qu'aucun organisme de contrôle puisse avoir accès aux détails de la transaction. Même si cette cryptomonnaie n'est encore qu'au stade d'essai, son potentiel de

[1] Dans un sens large, *Iota* désigne à la fois un grand livre décentralisé et une cryptomonnaie (tout comme *Bitcoin* désigne à la fois une technologie et la « crypto » correspondante). Cependant, la cryptomonnaie native du système Iota s'appelle précisément : *Miota*.

[2] Noter la différence avec *Helium,* qui utilise également l'IdO, mais dont le fonctionnement est basé sur une *blockchain* (voir Encadré 1).

développement est important, dans la mesure où elle ouvre de nouvelles perspectives vers une cryptographie plus légère. Fin 2017 de fait, *Iota* a amorcé une collaboration avec plusieurs grandes entreprises de divers secteurs, notamment : Fujitsu, Samsung, Microsoft et Deutsche Telekom ; afin de mettre en place un « marché de données » décentralisé et d'optimiser sa technologie, notamment sur le plan de la sécurité.

En effet, l'Internet des Objets (IdO) offre de nombreux avantages pour la cryptosphère. Entre autres, en raison de sa capacité à collecter d'importantes quantités de données/informations en temps réel, cette technologie entraîne une diminution des coûts de transaction. Ceci serait un avantage non négligeable s'il s'agit par exemple de trouver des produits ou de comparer des prix. De plus, en facilitant l'interopérabilité entre les *blockchains*, l'IdO élimine la dépendance à l'égard d'un point de vulnérabilité unique et garantit ainsi la disponibilité des données en temps réel (Wallcrypt, 2023)[1]. En revanche, le risque principal de cette interconnectivité (via Internet) est l'accès non autorisé au système embarqué : connecter un équipement quel qu'il soit à un réseau ouvert, c'est mettre une porte d'entrée sur son propre système ; d'où les risques de cyberattaques et/ou de manipulation des décisions et/ou de l'information par des entités privées ou gouvernementales.

Au-delà des multiples débats que suscite leur démocratisation, les moyens de paiement numériques recourant à la cryptographie avec ou sans *blockchain* interpellent sur la conception de la monnaie. Ces nouveaux moyens de paiement représentent également un défi, voire une menace pour les États. Ils empiètent à la fois sur le pouvoir monétaire et sur la régulation des paiements par les Banques Centrales (De Boissieu, 2023). En outre, les cryptomonnaies servent à contourner diverses réglementations relatives à la lutte contre le blanchiment de l'argent sale et contre le financement du terrorisme. En effet, l'un des avantages des cryptomonnaies décentralisées est aussi l'un des principaux écueils à leur usage, à savoir : l'absence de régulation (Ali et al. (2015), Böhme et al. (2015), Baer et al. (2023)). Leur émission n'est pas le fait d'un organisme central et leur circulation se fait dans des réseaux pair-à-pair au sein desquels n'existe théoriquement aucun tiers de confiance désigné. En conséquence, si un détenteur de *coins* et/ou de *tokens* perd soit l'une de ses clés, soit son ordinateur ou s'il est victime d'un piratage, il n'a aucun moyen de les récupérer.

Deux exemples récents permettent d'illustrer cette situation. Le premier est celui de Ruja Ignatova, surnommée : la « cryptoqueen ». Dès 2014, cette entrepreneuse allemande a pu collecter plus de 4 milliards de Dollars grâce à *OneCoin*, un projet cryptomonétaire. Depuis 2017, elle est portée disparue avec l'essentiel de ces fonds. Placée sur la liste des dix fugitifs les plus recherchés par le Federal Bureau of Investigation (FBI) en 2022, elle demeure introuvable au moment de la rédaction de ce papier. Le second exemple concerne Africrypt, une entreprise sud-africaine dont les fondateurs (Amir et Reez Cajee, deux frères âgés de 17 et 20 ans respectivement au moment des faits) se sont servis pour réaliser la plus grande arnaque aux *Bitcoins* de l'histoire ; en dérobant 69.000 *Bitcoins,* soit environ 3,6 milliards de Dollars à des investisseurs par un acte de piratage, en transférant leurs comptes et portefeuilles dans le darknet.

Par ailleurs, dans la mesure où les projets cryptomonétaires partent d'une initiative privée, l'intérêt croissant des investisseurs a pour effet de les rendre davantage chaotiques. En Juin 2019, le lancement de l'Association Diem (ex-Libra) chargée de piloter la construction d'un système de paiement mondial pour le compte de l'entreprise Facebook (métavers en construction) a eu l'effet d'une onde de choc. Comme le soulignent Ajdenbaum (2021), Aglietta et Lakomski-Laguerre (2022) puis Kotovskaia et Meier (2022), le fait qu'un géant de l'Internet (dont le pouvoir exorbitant effraie les gouvernements et les autorités de régulation du monde entier) décide d'étendre ses activités à un domaine jusque-là réservé aux États souverains : celui de battre monnaie, a

[1] Il faut rappeler que la *blockchain* permet de décentraliser des opérations en les attribuant à des milliers de nœuds indépendants. Elle permet également d' « anonymiser » ou du moins, « pseudonymiser » les transactions, ce qui permettrait de préserver la confidentialité des données récoltées par les objets connectés.

explicitement révélé la nécessité d'accélérer la réflexion sur la mise en circulation des monnaies numériques dites « centralisées » ou « régulées »[1].

7. Les monnaies numériques souveraines : les *Govcoins*

L'actualité relative à l'évolution des moyens de paiement numériques est riche en rebondissements. Suivant l'approche dialectique historique, nous tenterons néanmoins de repérer quelques événements qui en faciliteront la catégorisation présentée en fin d'article. Dans ce qui va suivre, nous proposons d'employer les termes : « cryptomonnaies » (tout court) pour désigner les monnaies numériques décentralisées (*Bitcoin, Altcoins, Stablecoins* et *Iotcoins*) ; tandis que les termes : « cryptodevise » et/ou « cryptonumeraire » seront employés pour désigner les monnaies numériques régulées par des autorités publiques (*Govcoins*). Or nous savons qu'en matière de politique économique, les « autorités » peuvent être de deux types : les administrations centrales d'une part, et les autorités monétaires d'autre part. Ceci permet alors d'envisager au moins deux types de cryptomonnaies souveraines selon l'émetteur (voir Encadré 2). Pour des raisons pratiques, les cryptodevises régulées par une administration centrale seront désignées par le terme : Monnaies Numériques Nationales (MNN), tandis que les monnaies numériques régulées par les autorités monétaires seront désignées par le terme : Monnaies Numériques de Banque Centrale (MNBC).

En 2016, la Banque Centrale de Suède (Riskbank) – historiquement pionnière dans l'émission des billets de banque vers la seconde moitié du 17è siècle – a été l'une des premières, avec celle du Canada (voir infra), à lancer un projet de création d'une monnaie numérique (*e-couronne*). Le projet s'est accéléré avec les annonces de Meta en 2019 (voir supra). C'est ainsi qu'en Février 2021, les autorités monétaires suédoises ont annoncé avoir achevé la phase 2 du lancement de ce projet pilote, dont l'objectif est d'enrichir les connaissances de la Riskbank quant à la conception et au fonctionnement d'une Monnaie Numérique de Banque Centrale (MNBC) permettant de se passer de l'argent liquide à terme. Dans le même ordre d'idées, la Banque du Canada a lancé un projet consistant à concevoir en 2017 un simulateur de système de paiement nommé *Jasper* basé sur la *blockchain*. Il s'agissait alors de la mise au point d'un dispositif (ou d'une plateforme) permettant aux participants d'échanger entre eux un actif (numérique) de règlement émis et contrôlé par la Banque Centrale[2] - voir Chapman et al. (2017).

Dans le même ordre d'idées, en 2021, la Banque Centrale Européenne (BCE) a lancé une phase d'étude qui devrait prendre fin en Octobre 2023, date à laquelle une décision sera prise sur la poursuite ou non du processus de lancement d'un *Euro numérique*. Selon la BCE – voir ECB (2020), cette cryptodevise serait complémentaire aux billets et aux pièces de monnaie. L'objectif d'une telle initiative, si elle venait à aboutir, renforcerait la numérisation des économies européennes, en même temps que la souveraineté monétaire de la Zone Euro. En outre, elle faciliterait les moyens de paiements. Il s'agirait alors d'un paradigme différent de celui présenté par les Banques de Suède et du Canada qui ont, d'entrée, opté pour le remplacement des espèces par leurs MNBC respectives (cf. supra).

Les autorités monétaires occidentales ne sont pas les seules à s'intéresser aux cryptodevises (voir Encadré 2). En fait, de tous les projets cryptomonétaires, l'*e-Yuan* chinois (e-CNY) est sans doute l'un des plus ambitieux et l'un des plus anciens. Lancé en 2014, il est presque abouti au

[1] Plusieurs auteurs insistent sur les avantages des cryptomonnaies : inclusion financière, diversification du portefeuille, réduction des coûts de transaction, gain de temps, etc. (voir par exemple IFC (2017)). D'autres en revanche soulignent leurs inconvénients à savoir : poussées spéculatives et volatilité (Sockin et Wei Xiong, 2020), consommation d'énergie et empreinte carbone élevées, financement des activités criminelles, risque de fraudes, arnaques et de cyberattaques, etc. (Daniel (2019), Valence (2019), Adrian et Weeks-Brown (2021)).

[2] Plusieurs acteurs prennent part à ce projet, notamment : la Banque du Canada, le laboratoire et centre de recherche de l'entreprise R3 spécialisée en innovation financière, la CIBC, la TD, la Banque Scotia, la Banque de Montréal, la Banque Royale du Canada, la Banque Nationale et la HSBC. Voir notamment Banque du Canada (2017), Bech et Garratt (2017).

moment de la rédaction de cet article. Les premières phases de tests ont débuté dans quelques villes chinoises en 2020. Après avoir expérimenté l'intégration du *crypto-Yuan* aux terminaux de paiements des commerçants et au paiement des salaires en 2021, la Banque Populaire de Chine (BPC) a déployé 3.000 ATM[1] à Beijing en 2021. C'est lors des Jeux Olympiques (JO) d'hiver de 2022 que les autorités de Pékin ont officiellement procédé à des tests grandeur nature. Ainsi, sur les différents sites où les épreuves des JO avaient lieu, les paiements ne pouvaient se faire qu'en liquide, par carte Visa, ou par *e-Yuan*. En Janvier 2022, plus de 261 millions de personnes se sont servies des différentes applications (dont AliPay, du géant Ant Group, et WeChatPay de la messagerie WeChat appartenant au groupe Tencent) pour payer avec des e-CNY émis par la BPC.

Plusieurs pays en voie de développement font également figure de pionniers dans le domaine des monnaies numériques. Début 2018 par exemple, le Venezuela a émis 38,4 millions de *Petros* (dont la valeur est adossée aux réserves de pétrole du pays) afin de contrebalancer les effets des sanctions économiques/financières américaines et avoir un meilleur contrôle des réserves de change. Lors de la mise en vente de cette cryptodevise sur la *blockchain Ethereum*, sa valeur était équivalente à celle d'un baril de pétrole, soit 60 USD à l'époque. Les mécanismes du *Petro* seraient donc proches de ceux d'un *Stablecoin* (cf. supra) ou d'un *token* ; ce qui rend cette cryptodevise assez différente des autres MNBC telles que le *crypto-Euro* ou le *crypto-Yuan* (cf. infra). Par ailleurs, selon le Livre Blanc du *Petro*, son émission est contrôlée directement par le Cabinet Economique de la Nation, ce qui laisse envisager l'interférence d'une autorité autre que celle de la Banque Centrale du Venezuela dans la gestion de cette cryptodevise (voir Encadré 2)[2]. Dans un même élan, les Bahamas ont également lancé un test pilote dénommé « Dollar des sables » pour le projet de numérisation de leur monnaie nationale en 2019. Une année après avoir lancé ces tests sur les îles d'Exuma et d'Abaco, la Banque Centrale des Bahamas a officiellement lancé sa cryptomonnaie nationale baptisée le *Sand Dollar*. Cette dernière est adossée au Dollar des Bahamas qui est lui-même rattaché au Dollar américain. Il s'agit donc de la toute première cryptomonnaie de Banque Centrale au monde à avoir été déployée à une échelle nationale.

En Afrique, le Nigéria – un des pays comptant le plus grand nombre d'utilisateurs de *Bitcoins* au monde avec près de 400 millions de Dollars échangés en 2020 – a également annoncé le lancement d'une version numérique de sa monnaie : l'*e-Naira*, en Octobre 2021. Dans un même élan, quelques mois après avoir légalisé le *Bitcoin* comme moyen de paiement sur son propre territoire, la Centrafrique a officiellement lancé son projet de monnaie numérique : le *Sango Coin* en 2022. Contrairement à l'*e-Naira*, ou au *Petro*, cette cryptomonnaie ne sera pas émise par une Banque Centrale, puisque la Centrafrique n'en dispose pas *de facto* et que la BEAC (Banque Centrale des États de l'Afrique Centrale, institut d'émission de la communauté à laquelle la Centrafrique appartient) ne prend pas part à ce processus, au moment où cet article est rédigé.

Il convient de noter que la plupart des initiatives sus évoquées (hormis celles des Bahamas, de la Centrafrique, du Nigéria et du Venezuela qui sont loin d'être des réussites pour le moment) sont encore plus ou moins en phase de test. Ainsi, au stade actuel, nous pouvons distinguer au moins deux types de *Govcoins* : (i) les Monnaies Numériques Nationales (MNN) régulées par un gouvernement ou une administration centrale – telles que le *Sango Coin* (Centrafrique) et le *Petro* d'une part et (ii) les Monnaies Numériques émises par les Banques Centrales (MNBC) – CBCC[3], *Central Bank Crypto Currencies* – telles que le *Sand Dollar* (aux Bahamas), le *DCash* (aux Caraïbes), l'*e-Naira* (Nigéria) ou encore l'*e-Yuan* (Chine). Les *Govcoins* ont donc en commun

[1] *Asynchronous Transfer Mode* (ATM) peut se traduire par « mode de transfert asynchrone ». Il s'agit d'une technologie réseau apparue au début des années 1990, gérant le transport de la voix, de la vidéo aussi bien que celle des données en garantissant une qualité de service. Par exemple, l'ATM transmet des données et des informations en nombre nettement supérieur à Ethernet.

[2] La naissance du *Petro* s'est accompagnée de la création d'une Direction des Monnaies Cryptographiques du Venezuela, un service intégré à la Vice-Présidence.

[3] Dans certains documents, l'acronyme CDCC (*Central Bank Digital Currencies*) est préféré à celui de CBDC Voir par exemple Malherbe et Montalban (2022).

d'être des cryptodevises émises par des autorités souveraines ; ce qui nécessitera comme l'on peut s'en douter, des vérifications d'identité – quoique l'anonymat soit théoriquement possible pour des transactions d'un montant relativement faible, selon la BCE (2019) –. Ils permettront donc de déplacer le pouvoir d'émettre des moyens de paiement, des individus vers les administrations centrales des États ou les Banques Centrales. Une telle initiative les éloigne de fait de l'idéologie des cryptomonnaies décentralisées. Néanmoins, leur sous-catégorisation selon l'émetteur (gouvernement ou Banque Centrale), ressuscite la sempiternelle question de l'indépendance de la Banque Centrale avec ses corollaires : planche à billets et politiques discrétionnaires, voire inflationnistes.

Encadré 2. Les premières cryptodevises

Officiellement, l'expression « *Govcoins* » (G*overnment digital currencies* ou Monnaies Numériques Gouvernementales) a fait sa première apparition en barrant la « Une » de l'hebdomadaire *The Economist* daté du 08 Mai 2021, indiquant que ces « nouvelles incarnations » de la monnaie numérique révolutionneraient la finance mondiale.

Notre choix de distinguer les cryptonumeraires (*Govcoins* ou cryptodevises) selon l'émetteur (gouvernement ou Banque Centrale) se fonde sur la définition du Fonds Monétaire International (FMI, 2000) selon laquelle « un numéraire désigne une monnaie nationale (ou étrangère) émise soit par une administration centrale, soit par une Banque Centrale ». En effet, si *The Economist* a employé les expressions « *Fedcoins* » et « *e-Euro* » pour désigner les (futures) monnaies numériques émises par des autorités monétaires (*resp.* américaines et européennes – ce qui en ferait des MNBC –), le lancement des projets *Petro* en 2018 (au Venezuela) et *Sango Coin* en 2022 (en République Centrafricaine) montre qu'il existe théoriquement des acteurs autres que les Banques Centrales, ayant le pouvoir de réguler la mise en circulation des cryptomonnaies souveraines. À notre connaissance, il s'agit là des premiers et des seuls *Govcoins* dans le monde, contrôlés par une administration autre que la Banque Centrale.

Le lancement du *Petro* en 2018 visait à ranimer à court terme les finances publiques, ainsi qu'à atténuer le manque de liquidités qui frappait le Venezuela. À long terme, cette initiative visait à se positionner face à un potentiel effondrement de la suprématie du Dollar américain dans le système monétaire international. Le Livre Blanc du *Petro* indiquait que le gouvernement vénézuélien ferait une émission de 100 millions de *Petros*, un *Petro* étant égal à un baril de pétrole (soit environ 60 Dollars à l'époque) et que cette MNN pourrait être utilisée pour payer les impôts et taxes à l'État, ainsi que pour régler des transactions entre les compagnies de l'État et les compagnies publiques ou privées, prestataires de services à l'État. Le *Petro* serait donc une monnaie contrôlée entièrement par le gouvernement vénézuélien, car celui-ci contrôlerait les mineurs, superviserait les opérations et fixerait le prix de chaque *token*.

De l'avis de plusieurs chercheurs, les objectifs et les procédures du *Petro* comportent quelques lacunes et ambiguïtés qui en obscurcissent la légalité et la transparence, tant au niveau national qu'international. En effet, les missions du pouvoir politique et celles de la Banque Centrale dans l'émission du *Petro* ne semblent pas clairement définies. De plus, en utilisant les réserves pétrolières comme garantie, le *Petro* fonctionnerait plutôt comme un contrat de vente de pétrole à terme, mais sans date d'échéance (CADTM, 2018). Ceci pourrait susciter l'intérêt des spéculateurs (dans un contexte d'embellie des prix internationaux du pétrole), et créer ainsi un marché secondaire qui aurait *de facto* une incidence sur le cours de cette cryptodevise. Et de fait, entre Août 2018 (au moment de sa mise en circulation) et début Décembre de la même année, la valeur du *Petro* est passée de 3.600 Bolivars à 9.000 Bolivars ; alors que dans le même temps, le baril du pétrole avait baissé de 62 Dollars à moins de 55 Dollars.

Si le *Petro* a été la première cryptomonnaie au monde contrôlée par un État, il n'est pas le premier moyen de paiement numérique dont la valeur est garantie par des réserves de pétrole. En 2017, R FinTech (une société londonienne) a créé le *Bilur* comme alternative au *Bitcoin*. Tout comme ce dernier, le *Bilur* est une cryptomonnaie fondée sur une *blockchain*. Cependant, elle ne dépend d'aucune autorité souveraine. Sa valeur est garantie par un bien physique (le pétrole en l'occurrence), tout comme les premiers billets de banque reposaient sur la quantité d'or détenue par les États émetteurs de la monnaie. Outre son aspect spéculatif, le *Bilur* est en quelque sorte un fonds indiciel coté – *Exchange Traded Fund* ou ETF, ces produits financiers au montage complexe qui ont été associés à la crise de 2008 –. Il est difficile de ne pas y voir une tentative de contester la suprématie de l'étalon or-dollar par un étalon-pétrole (Fantacci et Gobbi, 2021).

Malgré le peu d'enthousiasme qu'elle suscite, cette « tokenisation » des matières premières – comme l'appellent les mass-médias – semble faire des émules. Fin Juillet 2022 (trois mois jour pour jour après avoir légalisé l'usage du *Bitcoin* sur l'ensemble de son territoire et quelques semaines après avoir annoncé le projet de lancement de sa propre cryptomonnaie), la République Centrafricaine a lancé les premières ventes du *Sango Coin*, une MNN adossée sur les ressources minières du pays. En effet, selon le Ministère des Mines et de la Géologie centrafricain, environ 60% de la superficie totale du pays offre un socle précambrien riche en minerais (diamant, or, uranium, etc.). Au 28 Juillet 2022, 12 millions de *Sango Coins* avaient déjà trouvé preneurs (selon le Site cryptonaute.fr). Cependant, comme dans le cas du *Petro*, les ressources générées par le *Sango Coin* sont directement gérées par la Présidence de la République et échappent de fait à la comptabilité publique.

Source : Construction de l'auteur.

La problématique de l'inflation que l'on pensait dépassée trouve un écho dans le contexte actuel marqué par un renchérissement des prix. En effet, au cours des années 1970-80, la plupart des économies développées ont connu une forte inflation. L'une des principales théories avancées pour expliquer ce phénomène était relative à la mise en œuvre des politiques monétaires discrétionnaires par les Banques Centrales sous la pression des pouvoirs politiques – notamment en raison des considérations court-termistes motivées par les échéances électorales –. Du point de vue de la plupart des économistes, la solution à ce problème consistait alors à accroître l'indépendance (ou du moins l'autonomie) des Banques Centrales, afin de réduire l'ingérence du pouvoir politique dans leurs décisions de politique monétaire (Cukierman et al. (1992), Alesina et Summers (1993), Walsh (2010)) – voir section suivante. Cette indépendance des Banques Centrales a toutefois été remise en question au cours des quatre à cinq dernières années, entre autres par Donald Trump aux États-Unis et par Narendra Modī en Inde (Wachtel et Blejer, 2020).

Finalement, si la Banque des Règlements Internationaux, la Banque Centrale Européenne (BCE) et la Banque Populaire de Chine (BPC) n'envisagent l'émission des *Govcoins* que de type MNBC (BIS, 2021), les cas du Venezuela et de la Centrafrique (quoique marginaux par rapport aux autres projets de cryptodevises) montrent que cette question n'est pas encore complètement tranchée. Et de fait, fin Juillet 2023, le Cameroun a mené des réflexions (avec l'accompagnement du géant américain IBM) en vue de se doter de capacités techniques et opérationnelles pour l'exploitation d'une plateforme de cryptomonnaie. À terme, les objectifs de cette initiative seraient notamment (i) de mettre sur pied un système de paiement en cryptomonnaie destiné à « certaines dépenses de souveraineté » entre le Cameroun et certains de ses voisins tels que le Nigéria[1], (ii) d'améliorer significativement la balance de paiement des deux États (Cameroun et Nigéria) et (iii) réduire leur dépendance à l'Euro et au Dollar.

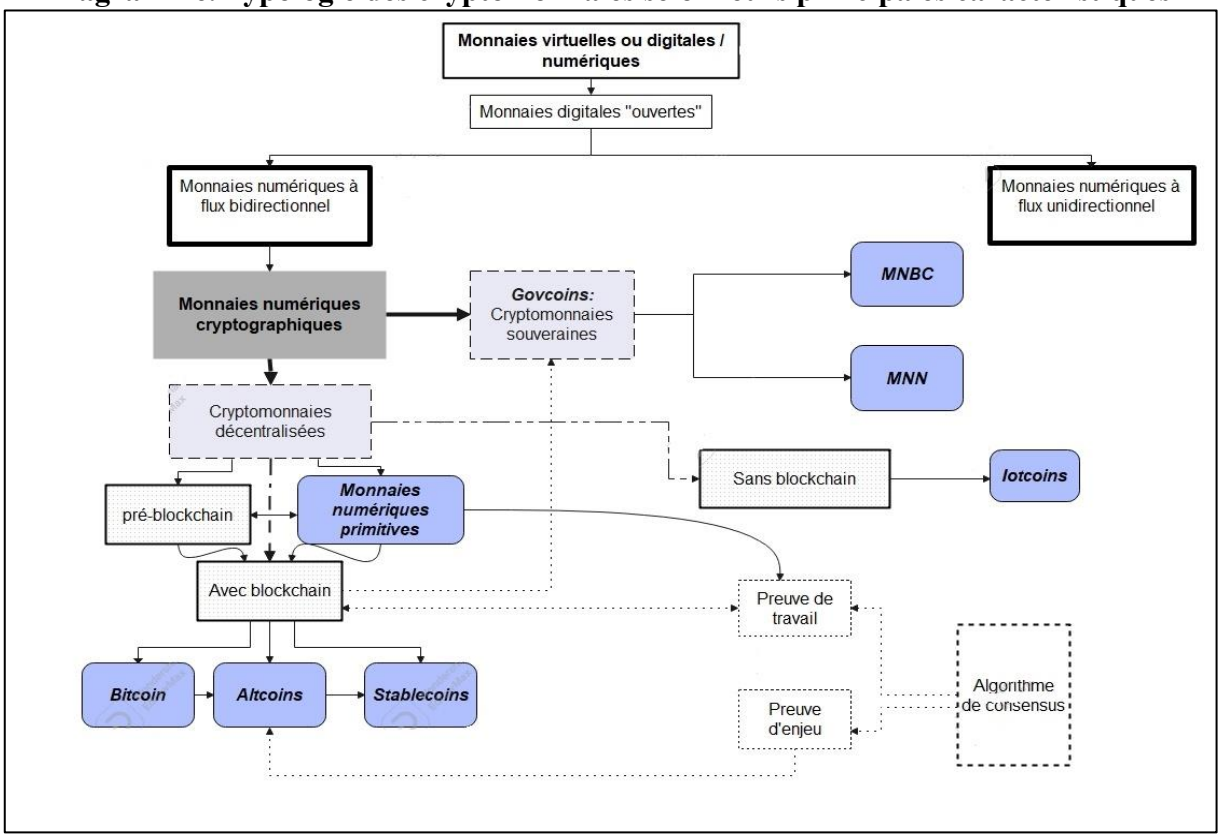
8. Tentative de catégorisation

Au regard de l'analyse faite dans les sections précédentes, il est possible de distinguer deux principales catégories de cryptomonnaies : les monnaies numériques décentralisées d'une part, et les monnaies numériques souveraines d'autre part. Au regard de la trajectoire suivie par le développement des cryptomonnaies depuis plus de quatre décennies, l'approche dialectique-historique permet d'affiner cette catégorisation usuelle selon des critères plus spécifiques, notamment : la nature du flux digital (unidirectionnel ou bidirectionnel), l'émetteur (privé ou autorité de politique économique), l'algorithme de consensus (preuve de travail ou preuve d'enjeu) et la technologie de base (avec ou sans *blockchain*) ; ce qui donne le diagramme ci-dessous où l'on voit apparaître d'un côté : les monnaies numériques « primitives », le *Bitcoin,* les *Altcoins,* les

[1] Le Nigéria est l'un des pays africains où l'usage des cryptomonnaies se démocratise le plus rapidement (voir supra) et par ailleurs l'un des principaux fournisseurs d'importations au Cameroun, derrière la Chine et la France, mais devant la Thaïlande et les Etats-Unis.

Stablecoins et ce que nous appelons les *Iotcoins* (ou *IdOcoins*) ; puis les MNN et les MNBC de l'autre.

Diagramme. Typologie des cryptomonnaies selon leurs principales caractéristiques



Source : Construction de l'auteur[1]

Rappelons que la notion de monnaie numérique en « système fermé » ou « ouvert » peut prêter à confusion selon le contexte. Dans cet article, elle renvoie à la possibilité d'une monnaie virtuelle à être utilisée dans l'économie réelle (cf. 2e section). Dans d'autres cas, le « système » en question peut désigner une *blockchain.* Cette dernière peut de facto être publique (ouverte) ou privée (fermée) – voir Perrot (2018). Ainsi, les systèmes *Bitcoin, Ethereum* ainsi que ceux de la majorité cryptomonnaies décentralisées sont « ouverts » dans la mesure où tout individu peut participer à la validation des transactions. A contrario, certaines *blockchains* telles que *Ripple* et très probablement celles des (futures) MNN et MNBC sont privées ou permissionnées, car tous les nœuds n'y disposent pas des mêmes droits en lecture[2]. Cela est fait afin de préserver la confidentialité de certaines informations et/ou données (surtout en écriture). Dans le diagramme ci-dessus, il ne nous a pas semblé judicieux de prendre en compte le caractère ouvert ou fermé des *blockchains* – et donc des cryptomonnaies qui y sont associées – afin de minimiser les risques de confusion.

[1] Notons que les (futurs) *Govcoins* pourraient également fonctionner soit sur des *blockchains*, soit sur l'IdO, soit sur une technologie intermédiaire entre les deux. Ils peuvent également fonctionner comme des *tokens*. Pour un panorama et une discussion sur les diverses modalités de mise en circulation des MNBC en particulier, voir par exemple Cunha et al. (2021).

[2] Théoriquement, une *blockchain* privée peut opérer un filtrage à l'entrée pour la consultation et l'utilisation des données internes d'une entreprise. Ce mode de fonctionnement semble donc davantage approprié pour le système bancaire. Selon la célèbre définition du mathématicien J-P. Delahaye, la *blockchain* (ouverte, puisqu'il s'agit du *Bitcoin*) est « un très grand livre de compte que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible ».

Il est difficile pour le moment de dire ce qu'il adviendra du marché des cryptomonnaies. En effet, bien que les moyens de paiement numériques existent depuis au moins quatre décennies, les stratégies des régulateurs, des banques commerciales et des États n'ont évolué de façon spectaculaire qu'au cours des six à sept dernières années – et plus particulièrement depuis la crise du Covid-19. Il ne semble donc pas exagéré d'affirmer qu'avec ou sans *blockchain,* la cryptographie devrait révolutionner le système bancaire et financier mondial (Aglietta et Valla, 2021). Cette assertion qui relevait de la pure spéculation intellectuelle dans un passé pas si lointain, semble se confirmer de plus en plus. En fait, les habitudes de paiement évoluent avec la technologie. Tout comme l'invention du papier a révolutionné les moyens de paiement en son temps, ces derniers seront inéluctablement impactés par les sauts technologiques.

Par exemple, dans les métavers – ces univers virtuels où les individus pourront interagir les uns avec les autres, vivre des expériences, créer des objets et des paysages, etc. –, les questions de gouvernance, de moyens de paiement et de propriété nécessiteront d'être interrogées. L'utilisation d'une technologie décentralisée (sans organe de contrôle central) et transparente sera donc primordiale. C'est pourquoi la plupart des métavers actuels (tels que Decentraland, Axie Infinity et The Sandbox) intègrent la *blockchain* dans leur technologie sous-jacente. Il devient alors aisé de faire le lien entre métavers, cryptomonnaies, NFTs et IA (Intelligence Artificielle) – voir par exemple Yang et al. (2022). Or, selon les résultats d'une enquête du cabinet de conseil McKinsey publiée en 2022, le métavers représente un marché potentiel de 5.000 milliards de dollars d'ici 2030 via les sessions de recrutement, les achats de terrains, les NFTs, etc. et 95 % des chefs d'entreprise à travers le monde s'attendent à ce qu'il ait un impact positif sur leur secteur d'activité d'ici une décennie. Les acteurs traditionnels de la finance (les institutions bancaires notamment) devront donc se réinventer et refondre leurs services, afin de s'adapter aux besoins de la clientèle. Ceci explique sans doute pourquoi State Bank of India (SBI), la plus grande banque indienne, a annoncé la création de BankChain, une plateforme pour la mise en œuvre d'une *blockchain* pour les banques en 2017[1].

9. Débats et perspectives

Parmi les nombreuses interrogations que suscitent ces nouveaux moyens de paiement, trois au moins retiennent l'attention. Quel sera le rôle des banques dans le monde du futur ? Qu'adviendra-t-il des formes de monnaie classiques une fois que l'adoption des cryptomonnaies aura été généralisée ? Au vu des tendances actuelles, les autorités de politique économique devront-elles laisser circuler des cryptomonnaies qui seront concurrentes directes de leurs propres cryptodevises ?

En guise de tentative de réponse à ces interrogations, les paragraphes précédents nous ont permis de constater que les *Govcoins* de type MNBC ont généralement plus d'assentiment que ceux de type MNN d'une part, et que les autorités monétaires ont des avis mitigés quant à la coexistence des MNBC et des autres formes de monnaie « classiques » (fiduciaire, scripturale et électronique) d'autre part. Toutefois, au regard du processus évolutif débuté depuis les années 1980, il semble de plus en plus évident que la révolution numérique se traduira par un recul de l'utilisation des espèces au profit des formes de monnaies dématérialisées. Parmi ces formes (électronique, virtuelle et/ou digitale), les monnaies numériques sont celles qui ont la plus forte probabilité de représenter le moyen de paiement du futur (Cunha et al., 2021). Cette assertion peut être considérée comme vraie, du moins si l'on considère l'engouement de la société pour les univers virtuels (migration des activités vers les métavers). Précisons néanmoins que, si la plupart des chercheurs s'accordent sur les avantages des cryptomonnaies – notamment en ce qui concerne la réduction des coûts de transaction et l'amélioration de l'inclusion financière (y compris dans les pays en développement) –

[1] Le réseau BankChain comprend non seulement des banques indiennes (State Bank of India, ICICI Bank, DCB Bank, Kotak Mahindra Bank, Federal Bank), mais également Deutsche Bank et UAE Exchange.

, il n'en demeure pas moins que certaines de leurs caractéristiques nécessitent quelques améliorations ; notamment sur les plans de la sécurité (risques de piratage), de l'impact environnemental, de la vitesse du processus de validation des transactions (voir supra) et des risques qu'elles font peser sur la stabilité monétaire et financière en raison de leur caractère spéculatif (Claeys et al. (2018), Sockin et Wei Xiong (2020)). En outre, il convient de rappeler que les cryptomonnaies servent très souvent à contourner les réglementations étatiques (blanchiment d'argent, évasion fiscale, financement de l'économie souterraine, etc – voir Baer et al., 2023) et impliquent une forte dépendance vis-à-vis des Bigtechs (Kotovskaia et Meier, 2022). Quand bien même des réponses appropriées seraient apportées aux préoccupations sus évoquées, il paraît évident qu'une légalisation généralisée des moyens de paiement numériques décentralisés créerait une économie parallèle ; avec des conséquences prévisibles sur le niveau général des prix, puisque les autorités monétaires n'auraient plus un contrôle absolu sur l'offre de monnaie (Benigno, 2021). Dès lors, il nous semble logique d'affirmer que la concrétisation des projets de *Govcoins* devrait sonner leur glas.

Nonobstant, force est de constater qu'à l'heure actuelle, l'adoption des monnaies numériques souveraines n'est pas une réussite dans les pays qui, voulant profiter du boom numérique, se sont empressés de les mettre en circulation ; qu'il s'agisse des MNN (Venezuela et Centrafrique), ou des MNBC déployées à une échelle nationale (Bahamas et Nigéria). L'on comprend pourquoi la plupart des Banques Centrales qui ont entamé une réflexion sur l'émission de leurs monnaies numériques (y compris la Chine) avancent sur ce sujet avec précaution et par étapes. En effet, à mesure que s'effritera l'hégémonie américaine, les projets cryptomonétaires se multiplieront ; ce qui ne fera qu'ajouter du chaos à la cryptosphère. C'est ce que semble confirmer l'annonce d'une levée de fonds pour la construction d'une crypto-ville nommée : Praxis (à ne pas confondre avec *Praxxis*, la cryptomonnaie quantum-résistante de M. Chaum) en Mars 2022, afin de fonder une « nouvelle » société exempte des règles économiques et politiques ; une sorte d'eldorado pour les investisseurs en cryptomonnaies.

Il n'existe pas de solution miracle pour mettre fin au désordre crypto-monétaire. Deux d'entre elles nous semblent néanmoins opportunes. La première consisterait à mieux réguler les cryptos décentralisées (Allen et al., (2022), Lalucq (2023)), voire à les taxer (Baer et al., 2023). La seconde consisterait à en interdire l'usage, en attendant la mise en circulation des *Govcoins*. La première solution s'avère difficile à mettre en œuvre en raison du quasi-anonymat qui constitue l'attrait des monnaies numériques décentralisées et surtout en raison de l'absence d'un consensus international. En effet, toute politique non coordonnée entre les Etats dans ce sens crée un « vide » juridique qui profite à certains pays, comme tel est le cas pour les paradis fiscaux. Soulignons qu'une législation pourrait toutefois être mise en place, au moins pour réduire les risques d'arnaque et de fraude (Jabotinsky (2020), Narain et Moretti (2022)) ; voire préserver la stabilité des systèmes financiers. Dans cette optique, en Décembre 2022, le Comité de Bâle a approuvé un ensemble de règles relatives à l'exposition des banques aux cryptomonnaies. Ces nouvelles règles prudentielles qui seront applicables à partir de 2025 stipulent notamment que les cryptomonnaies « stables » (*Stablecoins* et cryptomonnaies tokenisées) pourraient être incluses dans le bilan des banques à hauteur maximale de 2 %, tandis que toutes les autres catégories de cryptomonnaies ne pourront peser que 1 % de leurs bilans (BIS, 2022). De même, en troisième lecture d'un projet de loi sur les services et les marchés financiers, la Chambre Haute du Parlement du Royaume-Uni s'est prononcée en faveur d'une législation visant à soutenir et à réglementer l'adoption des cryptomonnaies en Juin 2023.

Quant à la décision d'interdire purement et simplement les transactions en cryptomonnaies, cette option ne semble ni réaliste, ni souhaitable d'un point de vue stratégique à long terme ; dans la mesure où l'observation du processus évolutif des cryptomonnaies décentralisées permet aux autorités de politique économique (en tant que « suiveurs ») de profiter de leur expérience, de s'ajuster, d'éviter de reproduire certaines erreurs et en même temps, de faire de la pédagogie, voire préparer l'opinion publique à l'avènement des monnaies numériques souveraines. Ainsi, en

Amérique par exemple, la question des cryptomonnaies laisse transparaître des divergences entre la Réserve Fédérale (FED) et le Trésor (De Boissieu, 2023). La Maison Blanche a exprimé son intérêt sur la question des MNBC, via la publication d'un rapport fin 2022[1] ; alors qu'à plusieurs reprises, le Président de la FED semblait jusque-là satisfait de l'existence de *Tether* (USDT) et de l'*USD Coin* (USDC), deux *Stablecoins* ancrés sur le Dollar et considérés à tort ou à raison comme d'assez bons « proxies » du (futur) *e-dollar* (ou *Fedcoin,* voir Gupta et al. (2017)).

Pour finir, notons qu'un consensus semble émerger, concernant le cas particulier des MNBC. Selon l'expression consacrée, dans l'éventualité où leur adoption serait généralisée, ces *Govcoins* pourraient être de deux natures : « de détail », ou « de gros ». Celles de détail seraient adressées aux particuliers (entreprises ou ménages). Celles de gros seraient réservées aux intermédiaires financiers ou serviraient dans les transactions transfrontalières (Chapman et al. (2017), Cunha et al. (2021), De Galhau (2022)). À ce sujet, selon un rapport corédigé par le cabinet Oliver Wyman et J.P. Morgan (2021), la mise en place d'un réseau international de MNBC permettrait aux entreprises d'économiser près de 100 milliards de Dollars par an en frais de transactions liés aux paiements transfrontaliers.

10. Conclusion

L'objet de cet article était de revisiter la genèse des cryptomonnaies puis d'en dresser un état de l'art, de tenter d'en faire une typologie, et de faire des conjectures sur les principaux débats tendances qui marqueront leur évolution future. Après avoir clarifié un certain nombre de concepts, notamment ceux de monnaie virtuelle en système fermé/ouvert (selon la nature du flux digital), l'approche dialectique et historique nous a permis de marquer cinq étapes principales dans l'évolution des cryptomonnaies. La première est celle des monnaies cryptographiques « primitives » du début des années 1980 avec *eCash* (puis *DigiCash*), *B-Money*, *Bit Gold* et *RPOW*, grâce aux travaux pionniers de David Chaum, Wei Dai, Nick Szabo et Hal Finney respectivement. Ces travaux ont permis à un certain Satoshi Nakamoto de créer le *Bitcoin* en 2008 (deuxième étape). Des tentatives d'amélioration de ce système (BTC) sont nés les *Altcoins* et les *Stablecoins* (troisième étape). En fait, plus que le *Bitcoin*, c'est la *blockchain* qui fait l'objet d'améliorations. Ceci explique sans doute pourquoi des algorithmes de consensus alternatifs à celui de Nakamoto ont vu le jour d'une part, et que parallèlement, l'on observe une mutation (certes marginale pour le moment) vers des cryptomonnaies sans *blockchain* ; ce que nous avons appelé : les *Iotcoins*, depuis le milieu des années 2010 (quatrième étape). Vers la fin de cette même décennie, des projets d'émission de *Govcoins* ont commencé à émerger (cinquième étape).

Cette analyse nous a logiquement permis de classer les différentes variétés de monnaies numériques en deux catégories principales : les cryptomonnaies décentralisées et les cryptomonnaies souveraines. Les premières comprennent les monnaies numériques « primitives », le *Bitcoin*, les *Altcoins*, les *Stablecoins* et les *Iotcoins* ; tandis que les secondes – *Govcoins* émis et régulés par des autorités souveraines – comprennent les Monnaies Numériques de Banque Centrale (MNBC) d'une part, et ce que nous avons appelé : les Monnaies Numériques Nationales (MNN) d'autre part.

Il n'est pas aisé de dire précisément quelle direction prendra le marché des cryptomonnaies décentralisées. Cependant, la réflexion dans ce domaine a beaucoup évolué depuis 2019. Outre les pays dont (*i*) les autorités en ont interdit l'émission, la détention et/ou les transactions par les résidents, (*ii*) ceux qui en ont juste interdit l'usage à certaines fins comme les paiements et (*iii*) ceux qui courtisent les entreprises pour développer ces marchés sur leur territoire, il existe certains pays qui mettent lentement en place un cadre juridique et une régulation ; quoiqu'évoluant en rangs dispersés. Le Japon et la Suisse ont par exemple modifié ou complété des législations couvrant les

[1] Voir The White House (2022).

cryptomonnaies et leurs prestataires de services, tandis que l'Union européenne, les Émirats Arabes Unis, le Royaume-Uni et les États-Unis en sont encore au stade de la rédaction. Au niveau international, l'une des principales préoccupations du Groupe d'Action Financière et du Conseil de Stabilité Financière concerne la préservation de l'intégrité financière.

Cette fragmentation du tissu réglementaire entre les initiatives nationales et internationales aura sans doute pour conséquence un rallongement des délais pour la mise en place d'un cadre législatif permettant d'assurer les conditions d'une concurrence équitable sur le marché des cryptomonnaies. Ce constat renforce la pertinence de cet article dans la mesure où non seulement ce dernier fait le point sur l'état de l'art en matière de développement des « cryptos », mais il met des outils pédagogiques à la disposition des autorités, ainsi que des informations qui faciliteront la prise de décisions rationnelles. En effet, savoir où en sont les cryptomonnaies permettra d'avoir suffisamment de recul pour éviter de reproduire certaines erreurs (sécurité, mode de fonctionnement, volatilité, écueils juridiques, etc.). Par ailleurs, au vu de toutes les inquiétudes que posent le *Bitcoin* et consorts, la question ne se pose de plus de savoir s'il est nécessaire de passer à des monnaies numériques centralisées ; mais plutôt de savoir quel sera le moment opportun pour ce faire et dans quelles conditions (notamment du point de vue réglementaire). Il est important que décisions relatives à ce processus soient prises avec beaucoup de prudence.

Bibliographie

1. Adrian, T., Weeks-Brown, R. (2021). Cryptoassets as national currency? a-step-too-far, https://www.imf.org/fr/News/Articles/2021/07/26/blog-cryptoassets-as-national-currency-a-step-too-far, World Bank.
2. AEMF – Autorité Européenne des Marchés Financiers (2022). Les régulateurs financiers de l'UE mettent en garde le public contre les risques, liés aux cryptoactifs, accessible à l'adresse : https://acpr.banque-france.fr/sites/default/files/medias/documents/20220317_es_joint_esas_warning_on_crypto_assets.pdf.
3. Aglietta, M., Lakomski-Laguerre O. (2022). Les cryptomonnaies en plein essor : les banques centrales lèvent leurs boucliers !, *L'économie mondiale*, pp. 103-117.
4. Aglietta, M., Valla N. (2021). *Le Futur de la monnaie*, Odile Jacob.
5. Aglietta, M. (1992). *Genèse des banques centrales et légitimité de la monnaie*, Annales.
6. Alesina, A., and Summers L.H. (1993). Central Bank Independence and Macroeconomic Performance: Some Comparative Evidence, *Journal of Money, Credit and Banking*, Vol. 25 (2), pp. 151-162.
7. Ali, S. T., Clarke D. and McCrory P. (2015). Bitcoin: Perils of an Unregulated Global P2P Currency, *Technical Report Series* (1470), Newcastle University.
8. Allen, F., Xian Gu and Jagtiani, J. (2022). Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China, *Journal of International Money and Finance*, https://doi.org/10.1016/j.jimonfin.2022.102625.
9. Banque du Canada (2017). *Projet Jasper : une expérience canadienne de technologie du grand livre distribué pour le règlement des paiements interbancaires au pays*, Septembre.
10. Baer K., De Mooji R.A., Hebous S., Keen M. (2023). Taxing Cryptocurrencies, *IMF Working Paper* No. 2023/144, International Monetary Fund, July 5.
11. Banque Mondiale (2022). La COVID-19 a dopé l'usage des services financiers numériques, https://www.banquemondiale.org/fr/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services?
12. CADTM – Comité pour l'Annulation de la Dette du Tiers Monde (2018). Le Petro et le labyrinthe économique vénézuélien, par Lenin Bandres, https://www.cadtm.org/spip.php?page=imprimer&id_article=15990, 22 Mars.
13. Bech, M., Garratt, R. (2017). Des cryptomonnaies émises par les banques centrales ?, *Rapport trimestriel BRI*, Septembre.
14. Benigno P. (2021). Monetary Policy in a World of Cryptocurrencies, https://benigno.ch/wp-content/uploads/2021/03/Bitcoin-060321-1.pdf.
15. BIS – Bank for International Settlements (2022). *Prudential treatment of cryptoasset exposures*, Basel Committee on Banking Supervision, https://www.bis.org/bcbs/publ/d545.pdf, Decembre.

16. BIS – Bank for International Settlements (2021). *CBDCs: an opporuntity for the monetary system*, BIS Annual Economic Report.
17. Böhme R., Christin N., Edelman B. et Moore T. (2015). Bitcoin: Economics, Technology and Governance, *Journal of Economic Perspectives*, vol. 29 (2), pp. 213-238.
18. Chaum, D. (1985). Security Without Identification: Transaction Systems to Make Big Brother Obsolete, https://dl.acm.org/doi/10.1145/4372.4373.
19. Chiu, J. and Thorsten, V.K. (2019). The Economics of Cryptocurrencies—Bitcoin and Beyond, *Bank of Canada Staff Working Paper* 2019-40, September.
20. Claeys, G., Demertzis, M., Efstathiou, K. (2018). Cryptocurrencies and monetary policy, *Policy Contribution Issue* n˚10, Committee on Economic and Monetary Affairs of the European Parliament, June.
21. Cukierman A., Webb S. B. and B. Neyapti (1992). Measuring the Independence of Central Banks and Its Effect on Policy Outcomes, *World Bank Economic Review* 6 (3): 353–98.
22. Cunha, P.R., Melo, P., Sebastião, H. (2021). From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution, *Future Internet*, 13, 165. https://doi.org/10.3390/fi13070165.
23. Daniel, J-M. (2019). Crypto-monnaies : leurs fonctions, leurs dangers : Crypto-monnaies ou cryptoactifs ?; Dans : Thierry de Montbrial éd., Ramses 2019 : *Les chocs du futur* (pp. 284-287), Paris : Institut Français des Relations Internationales. https://doi.org/10.3917/ifri.demon.2018.01.0284.
24. De Boissieu, C. (2023). Les monnaies numériques des banques centrales : où en est-on ? Où va-t-on ?, *Policy Brief*, www.policycenter.ma/sites/default/files/2023-04/PB_19_23_Boissieu.pdf, Avril.
25. Dupré, D., Ponsot, J.-F., Servet J-M (2015). Le bitcoin contre la révolution des communs, 5e congrès de l'AFEP, Lyon.
26. ECB – European Central Bank (2012). *Virtual Currency Schemes*, October.
27. ECB – European Central Bank (2015). *Virtual currency schemes – a further analysis*, February.
28. Fantacci, L. and Gobbi, L. (2021). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony: The Geopolitical Stake of Innovations in Money and Payments, Accounting, Economics, and Law: A Convivium, https://doi.org/10.1515/ael-2020-0053.
29. Faure-Muntian V., Ganay C. de, Le Gleut M.R. (2018). Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, *Rapport n° 584 au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques*, déposé le 20 Juin.
30. FMI – Fonds Monétaire International (2021). *Rapport sur la stabilité financière dans le monde*, https://www.imf.org/fr/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021.
31. FMI – Fonds Monétaire International (2000). *Manuel des Statistiques Monétaires et Financières*, https://www.imf.org/external/pubs/ft/mfs/manual/fra/pdf/mfsmch1f.pdf.
32. Gupta S., Lauppe P., Ravishankar S. and Feigenbaum J. (adviced by) (2017). Fedcoin: A Blockchain-Backed Central Bank Cryptocurrency, available at: https://law.yale.edu/sites/default/files/area/center/global/document/411_final_paper_-_fedcoin.pdf;
33. Hayek (Von), F. (1976). *Denationalization of Money- The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, London, The Institute of Economic Affairs, 3rd edition, 1990.
34. Huynh-The, T. and al. (2023). Blockchain for the metaverse: A Review, *Future Generation Computer Systems*, Volume 143, Pp. 401-419, June.
35. Jabotinsky, H.Y. (2020). The Regulation of Cryptocurrencies: Between a Currency and a Financial Product, *Fordham Intell. Prop. Media & Ent. Law Journal*.
36. Kotovskaia, A. and Meier, N. (2022). BigTech cryptocurrencies - European regulatory solutions in sight, *SAFE Policy Letters* 97, Leibniz Institute for Financial Research SAFE.
37. Lakomski-Laguerre, O. (2020). Monnaie et immortalité : une autre histoire du Bitcoin, *Œconomia. History, Methodology, Philosophy* (10-1), pp. 145-154.
38. Lakomski-Laguerre, O. et Desmedt L. (2015). L'alternative monétaire Bitcoin : une perspective institutionnaliste, *Revue de la régulation*, 18, 2e semestre, https://doi.org/10.4000/regulation.11489.
39. Lalucq, A. (2023). Les cryptos : la bienveillance coupable des régulateurs, *Revue d'économie financière*, pp 19-31.
40. Laurent A. et Monvoisin, V. (2015). Les nouvelles monnaies numériques : au-delà de la dématérialisation de la monnaie et de la contestation des banques, *Revue de la régulation*, 18-1, pp. 1-24.

41. Liu, Y., Tsyvinski, A. and Wu, X. (2022). Common Risk Factors in Cryptocurrency, *The Journal of Finance*, vol 77(2), pp. 1133-1177.
42. Lo, S. and Wang, C. (2014). Bitcoin as Money, *Current Policy Perspectives* 14-4, Federal Reserve Bank of Boston.
43. Loignon, S. (2017). *Big Bang Blockchain*, Tallandier.
44. Malherbe, L. et Montalban, M. (2022). Cryptocurrencies, Big Techs, central bank digital currencies and the changing role of banks in the payment industry: old wine in new bottles?, In: *Central Banking, Monetary Policy and the Future of Money*, pp. 76-93, Edward Elgar Publishing.
45. Mishkin, F. (2004). *The Economics of Money and Financial Markets*, Pearson, 7th edition.
46. Narain, A. et Moretti M. (2022). Réglementer la crypto, *Finances & Développement*, FMI, Septembre, www.imf.org/fr/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti.
47. Nakamoto, S. (2009). *Bitcoin : un système de paiement électronique pair-à-pair*, Traduction française de bitcoin.org/bitcoin.pdf par Arnaud-François Fausse, accessible via https://blog.octo.com/wp-content/uploads/2016/01/bitcoin_fr.pdf.
48. Oliver Wyman - J.P. Morgan & Co. (2021). *Unlocking $120 Billion Value In Cross-Border Payments - How banks can leverage central bank digital currencies for corporates*, https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/unlocking-120-billion-value-in-cross-border-payments.pdf;
49. Pavel, I. (2017). La blockchain – Les défis de son implémentation, *Annales des Mines - Réalités industrielles* (3), pp. 20-24.
50. Perrot, E. (2021). Enjeux anthropologiques et politiques des cryptomonnaies, *Études*, pp. 55- 64, Avril.
51. Perrot, E. (2018). Les cryptomonnaies, *Études*, pp. 41-52, Juin.
52. Sockin, M. and Wei Xiong (2020). A model of cryptocurrencies, NBR Working Paper Series, https://www.nber.org/system/files/working_papers/w26816/w26816.pdf, March.
53. Yang Q., Zhao Y., Huang H., Xiong Z., and Kang J. (2022). "Fusing Blockchain and AI With Metaverse: A Survey", IEEE Open Journal of the Computer Society, https://www.computer.org/csdl/journal/oj/2022/01/09815155/1EJBce8LdBe.
54. The White House (2022). *Technical Evaluation for a US Central Bank Digital Currency System*, Washington, Septembre.
55. Valence, A. (2019). Les cryptomonnaies sont-elles vraiment décentralisées ? : quelques leçons de l'écosystème bancaire, *Revue d'économie financière*, 133 (1), pp. 285-300.
56. Wachtel, P., Blejer, M.I. (2020). A Fresh Look at Central Bank Independence, *Cato Journal*, 40, 105-130, https://www.cato.org/sites/cato.org/files/2020-02/cj-v40n1-7.pdf.
57. Wallcrypt – Agence Internationale de Vulgarisation Web 3 (2023). *La convergence de la Blockchain avec l'IoT*, https://wallcrypt.com/la-convergence-de-la-blockchain-avec-iot-objets-connectes/, visité de 02 Août.
58. Walsh, C.E. (2010). Central Bank Independence, In: Monetary Economics, *The New Palgrave Economics Collection*, Palgrave Macmillan, Durlauf, S.N., Blume, L.E. (eds), London.