1. LES FACILITATEURS D'APPROPRIATION

De façon générale, ces acteurs peuvent être comparés aux vendeurs de pelle lors de la ruée vers l'or.
La catégorie des facilitateurs d'appropriation rassemble les acteurs qui proposent un service ou un produit en lien avec l'écosystème de la blockchain. Ces acteurs sont donc peu décentralisés, puisque reposant sur une organisation traditionnelle, et situés en amont de la chaîne de valeur selon le critère de différenciation défini précédemment. Ils sont considérés comme des facilitateurs d'appropriation et de pénétration de la technologie puisqu'ils participent directement au développement et à la sécurisation de l'écosystème. Dans cette catégorie, nous distinguons quatre sous-catégories d'acteurs : les accompagnateurs, les échangeurs, les régulateurs et les coffres-forts.

2. LES PROCESS WINNERS

Les *process winners* sont les acteurs qui considèrent la technologie blockchain comme un moyen d'améliorer un certain nombre de processus internes des entreprises de l'économie traditionnelle en y apportant de l'automaticité, de la transparence et de la sécurité. Cela permet d'actionner deux leviers de croissance : celui de l'augmentation des revenus et celui de la réduction des coûts. Parmi ces initiatives, certaines sont menées par des acteurs de l'économie traditionnelle qui veulent s'approprier la technologie blockchain *via* de l'investissement en recherche et développement, des partenariats ou des acquisitions ; d'autres le sont par des startups appartenant à l'écosystème blockchain.

3. LES DAPPS ET LES BLOCKCHAINS NOUVELLE GENERATION

La catégorie des *crypto-aps'* est un ensemble plus vaste et plus complexe que celle des crypto-monnayeurs. En effet, elle rassemble les acteurs en aval de la chaîne de valeur, dont les usages dépassent largement le purement monétaire, et porte en germe un changement radical de paradigme économique. Comme nous l'expliquions précédemment, la technologie blockchain a ouvert la voie à la *token economics* où une entreprise propose un service et une crypto-monnaie permettant d'acheter ce service. Elle devient, par conséquent, à la fois une entreprise de l'économie traditionnelle dont le modèle économique repose sur le bien ou service vendu et en même temps une banque centrale qui émet sa propre monnaie.
Cette topographie distinguera donc d'une part les acteurs fournissant une infrastructure aux *crypto-aps'* (les *ChainProducers*) et ceux utilisant cette infrastructure pour développer des applications et des usages (les *ChainUsers*).

4. LES CRYPTO-MONNAYEURS OU LES BLOCKCHAINS 1.0

Les crypto-monnayeurs ou les blockchains 1.0 sont les acteurs qui ont développé des protocoles décentralisés et s'appuyant sur les couches technologiques les plus en amont de la chaîne de valeur et d'innovation de la technologie blockchain, à savoir les couches *ledger* (registres) et de transaction. Elles permettent de proposer un usage de la technologie blockchain uniquement centré autour de la monnaie. Les crypto-monnayeurs regroupent l'ensemble des acteurs ayant développé des crypto-monnaies concurrençant plus ou moins directement le Bitcoin, chef de file de cette catégorie. Notons que les projets appartenant aux crypto-monnayeurs sont ceux qui, chronologiquement, sont apparus les premiers[3].

[3] *Le projet IOTA est apparu plus tardivement que les autres mais propose un cas d'usage particulier de sa crypto-monnaie puisque uniquement centré sur les objets connectés.*

Pour cartographier la catégorie des crypto-monnayeurs, deux axes d'analyse sont proposés.

Le premier axe, celui des horizontaux, est la vitesse de transaction : plus une monnaie propose une vitesse de transaction élevée, plus elle peut se substituer aux monnaies fiduciaires qui, en pratique, ont une vitesse de transaction nulle. En effet, il est difficile d'imaginer une adoption massive des crypto-monnaies comme moyen de paiement pour les micro-transactions, s'il est nécessaire d'attendre 10 minutes pour que la validation soit effective, comme c'est le cas actuellement pour le Bitcoin. Pour améliorer la vitesse de transactions d'une crypto-monnaie, plusieurs leviers sont possibles :

- réduire le temps de validation des blocs ;
- augmenter la taille des blocs et donc le nombre de transactions pouvant y être enregistrées ;
- alléger/modifier le protocole de validation.

Dans ce qui suit, le volume de transactions – ou scalabilité – fera référence à un nombre de transactions par seconde[4] que l'on pourra comparer aux moyens de paiement actuels (comme Visa qui peut supporter plusieurs milliers de transactions par seconde). Avant de détailler les solutions permettant d'améliorer la rapidité des transactions, rappelons qu'avec la manière dont ont été construites les crypto-monnaies, il existe un compromis presque inevitable entre vitesse et sécurité. Si l'on prend le cas du Bitcoin, sa sécurité provient du fait que son algorithme de consensus, le *proof-of-work*, permet, comme nous l'expliquions précédemment, d'avoir une sécurité qui tend vers l'infini avec une altération des données historiques impossible. Cette sécurité est garantie par le temps de validation choisi par son créateur, de l'ordre de 10 minutes. Si l'on réduit ce temps de validation la sécurité en patirait puisqu'il serait plus facile de modifier l'historique des transactions. Pour dépasser ce compromis, des projets tentent d'imaginer de nouveaux moyens de validation.

Le deuxième axe, celui des verticaux, est le niveau de confidentialité : une monnaie dont le niveau de confidentialité est total n'aura pas nécessairement le même usage qu'une monnaie avec un niveau de confidentialité moindre. Les monnaies ayant un niveau de confidentialité moindre, ou pseudo-anonyme, sont des monnaies où, à chaque *wallet,* est associé un montant connu de tous sans qu'on connaisse l'identité de celui qui le détient. C'est le cas, par exemple, du Bitcoin. Ce type de monnaie propose un usage similaire à celui de la gestion d'un compte en banque où on échange des sommes d'argent *via* des virements[5]. Les monnaies ayant un niveau de confidentialité important, ou parfaitement anonyme, sont des monnaies où l'on ne connaît ni le montant associé à chaque *wallet* ni l'identité de celui qui détient le *wallet*. Ce type de monnaie propose un usage similaire à celui qu'on peut avoir de l'argent liquide et s'applique ainsi plutôt au micropaiement. Comme le cas d'usage de ces monnaies est centré autour de la notion d'argent liquide et d'anonymat, il n'est pas à exclure qu'elles puissent favoriser certaines transactions illégales comme l'achat d'armes ou de drogues.

Ces deux axes font apparaître trois catégories que nous détaillerons dans ce qui suit :

- Bitcoin *and its fellows* (Le Bitcoin et ses dérivés) ;
- *DarkWeb money* (les solutions confidentielles) ;
- *High Tech' money.*(les solutions de dernière génération)

[4] La notion du nombre de transactions par seconde ne doit pas être confondue avec celle d'immédiateté des transactions.

[5] Cet usage pourrait être utilisé par des entreprises commerciales s'effectuant des virements réguliers de montants importants nécessitant donc une sécurité maximale.

I. BITCOIN AND ITS FELLOWS

Le Bitcoin étant la première crypto-monnaie, sa technologie présente des limites que certains projets ont cherché à dépasser. Le code source du Bitcoin est open source, c'est-à-dire complètement libre d'accès en ligne. Les projets de cette catégorie se sont contentés de repartir du code source et de modifier des paramètres, à la marge. À cet égard, on peut parler de code is business puisque le code est adapté pour répondre à un besoin du marché. Les principales modifications concernent le temps de validation et la taille des blocs. Parmi les plus connues, citons le Litecoin, le Bitcoin Cash, et le Dogecoin.

Le temps de validation d'un bloc pour le protocole Bitcoin est de 10 minutes environ. Si l'on rapporte ce temps de validation par bloc en équivalent transactions, on estime que le protocole Bitcoin permet d'en valider 3 par seconde environ, contre 2 500 pour Visa. Pour obtenir une validation plus rapide des transactions, le protocole Litecoin, qui s'appuie sur le protocole Bitcoin, propose une validation de bloc toutes les 2 minutes 30 environ[6].
Le protocole DogeCoin propose de son côté une validation de blocs toutes les minutes environ. L'objectif du DogeCoin est ainsi de devenir la monnaie de pourboires d'Internet : un utilisateur ayant bien aimé une vidéo ou un tweet pourrait laisser quelques DogeCoins, dont la valeur est avant tout symbolique[7]. Le projet Dogecoin est à l'origine une plaisanterie dont le but est de montrer la facilité avec laquelle on peut créer une crypto-monnaie à partir du code source Bitcoin. Néanmoins, cette plaisanterie a reçu un accueil favorable de la communauté blockchain.

La taille maximale d'un bloc pouvant être validé par le protocole Bitcoin a été fixée par ses créateurs à 1 Mo. Cette limite peut avoir comme conséquence de saturer le réseau, ce qui entraîne un allongement du temps de transaction. L'augmentation de la taille maximale d'un bloc a longtemps fait l'objet de discussions entre les mineurs du réseau. Aucune position ne permettant de concilier les deux clans, un *fork* définitif a eu lieu au début du mois d'août 2017. Il a donné lieu à la création du protocole Bitcoin Cash qui permet de porter la taille maximale d'un bloc pouvant être validé à 8 Mo. Il est intéressant de noter que, jusqu'à la date de leur séparation (1er août 2017), les deux protocoles possédaient le même historique de transactions[8].

II. SECRET MONEY

Les monnaies complètement anonymes répondent à un besoin non adressé jusqu'à présent par les crypto-monnaies : le *cash* digital[9]. Elles s'inspirent également du code source du Bitcoin, mais changent plus radicalement sa philosophie en incluant cette notion de pur anonymat. Parmi les plus connues, citons le Dash, le Zcash, le Monero, et le Verge. Si les niveaux de confidentialité proposés sont très adaptés aux transactions illégales, et notamment du *dark web*, en réalité ce besoin dépasse largement ce cadre.

Le protocole Bitcoin assure un certain niveau de confidentialité à ses utilisateurs grâce à l'existence des clés privées et publiques. Il a néanmoins été pensé pour que l'on puisse accéder au registre des transactions et connaître, *via* la clé publique, l'origine des fonds transférés, le montant et le destinataire. C'est le principe même du protocole Bitcoin : être un registre distribué dont l'ensemble des transactions passées est consultable à n'importe quel moment et par n'importe qui.

---

[6] https://litecoin.org/fr/

[7] http://dogecoin.com/. Le DogeCoin est représenté par une tête de Shiba, très populaire dans les communautés Internet.

[8] https://www.bitcoincash.org/

[9] Cette affirmation peut paraître contradictoire puisque le titre du whitepaper du Bitcoin est, rappelons-le, A Peer-to-Peer Electronic Cash System. Cependant, pour les raisons détaillées précédemment, nous considérons que l'usage du Bitcoin ne peut être considéré comme similaire à du cash digital.

Le protocole Dash a pour ambition d'être une monnaie équivalente au *cash* mais digitalisée[10]. Pour cela, son créateur, Evan Duffield, a imaginé deux technologies venant se superposer au protocole Bictoin : l'*InstantSend* qui propose une transaction de manière immédiate et *PrivateSend* qui propose aux utilisateurs qui le souhaitent une confidentialité totale quant aux transactions[11].

Le protocole ZCash propose, grâce au concept de la preuve sans connaissance *(zero knowledge proof)*, une monnaie où l'anonymat des transactions est total. Ainsi, en utilisant le Zcash, un utilisateur peut choisir de cacher l'origine, le montant et le destinataire de la transaction. Néanmoins, grâce au concept de preuve sans connaissance, le protocole ZCash permet de garantir que l'événement (la transaction) a bien eu lieu sans fournir d'informations à son sujet (origine, destination, montant[12]).

Le protocole ByteCoin repose sur la technologie *CryptoNote*. Il n'est donc pas un fork du Bitcoin mais créée une blockchain nouvelle. L'intérêt de la technologie *CrytpoNote* est de proposer un niveau de confidentialité élevé ainsi qu'un temps de transaction d'environ 2 minutes[13]. Notons que de nombreuses autres monnaies sont nées d'un *fork* du ByteCoin, comme le Monero(qui modifie des caractéristiques de l'augmentation de la vitesse du minage, et utilise une technique dite *one time* pour les adresses publiques ce qui rend impossible de tracer le solde d'un compte[14]).

Le Verge propose « une protection de notre intimité digitale » grâce à l'utilisation de réseaux multiples axés sur l'anonymat, comme Tor et i2p où les adresses IP des utilisateurs sont complètement cachées et par, conséquent, les transactions sont intraçables.

III. HIGH TECH' MONEY

Les monnaies *High Tech'* visent à dépasser assez largement le protocole du Bitcoin ; elles proposent des usages nouveaux des crypto-monnaies tout en apportant des réponses technologiques aux principales critiques et/ou limites du BItcoin, à savoir :

- son manque de scalabilité ;
- ses frais de transaction qui peuvent s'avérer élevés ;
- le problème de la consommation d'énergie liée au *proof-of-work*.

Parmi ces initiatives, citons les plus connues : le Iota, le Nano et le OmiseGO**.**

Le Iota est une monnaie qui diffère totalement, sur un plan technologique, du protocole Bitcoin. En effet, elle a pour objectif de se passer du principe de bloc, pourtant fondamental pour une blockchain, au profit d'une dislocation des nœuds de validation. C'est une monnaie qui s'applique aux objets connectés. L'idée est de mettre à disposition la petite puissance de calcul, embarquée dans chaque objet connecté, pour valider les transactions, confondant ainsi la notion de mineur et d'utilisateur du réseau. Dès lors, il n'est plus nécessaire de concaténer l'ensemble des transactions dans un bloc pour les valider. Le nom de ce mécanisme est le *Tangle* qui s'appuie sur un *Directed Acyclic Graph* (graphe orienté acyclique) pour enregistrer les transactions[15].

---

[10] https://github.com/dashpay/dash/wiki/Whitepaper

[11] https://www.dash.org/

[12]https://www.google.fr/search?q=Zcash&oq=Zcash&aqs=chrome..69i57j0l5.1493j0j7&sourceid=chrome&ie=UTF-8

[13] https://bytecoin.org/

[14] http://whitepaperdatabase.com/monero-xmr-whitepaper/

[15] Ce concept est très technique et demande un niveau de maîtrise en mathématiques important pour pouvoir être appréhendé pleinement. Il a été formalisé par Sergei Popov, un mathématicien de renom de l'université Unicamp, au Brésil, membre actif de la communauté des crypto-monnaies. La formalisation est accessible via le lien suivant : https://iota.org/IOTA_Whitepaper.pdf

Le Nano, anciennement connu sous le nom de Railblock, est assimilable au Iota dans le sens où le concept de mineur et d'utilisateur est plus ou moins confondu[16], mais il ne s'applique pas aux objets connectés. Son cas d'usage est concentré sur une efficacité maximale autour des transactions : elles se valident en 2 secondes, sans frais de transaction et avec une scalabilité présentée comme infinie[17].

Le OmiseGO est une monnaie particulièrequi s'appuie, elle, sur la blockchain Ethereum pour être déployée et pourrait être, à ce titre, assimilée à une c*rypto-aps'* (cf. ci-dessous). Nous faisons cependant le choix de la classer dans la catégorie des crypto-monnaies, puisque son cas d'usage est essentiellement centré sur les paiements à partir des applications ou sites Internet. OmiseGO propose une technologie de stockage et de transfert d'argent en temps réel qui est agnostique aux juridictions, aux organisations et au type de monnaie traitée – monnaie traditionnelle et crypto-monnaie confondues. Le *token* OmiseGO n'est pas, à la différence des monnaies citées précédemment, un moyen d'échange, mais il est utilisé pour valider des transactions et permet d'obtenir des remises et/ou des récompenses lorsqu'on passe par lui pour effectuer un règlement.

CONCLUSION

En conlusion, la catégorie des crypto-monnayeurs rassemble les acteurs ayant développé des crypto-monnaies à usage purement monétaire. Ils ont souvent créé des initiatives dérivant légèrement du code source du protocole Bitcoin en y incorporant de légères modifications sans changer fondamentalement le produit proposé même si certaines crypto-monnaies ont été créées avec des changements plus importants dans les protocoles comme le ZCash ou le Bytecoin.

Résultat : on compte aujourd'hui plus d'une trentaine de crypto-monnaies à usage purement monétaire. Nous avons donc fait le choix de limiter les exemples à celles ayant les capitalisations boursières les plus importantes (en fin d'année 2017). Comme nous l'expliquions précédemment, il n'est pas à exclure que l'émergence des crypto-monnaies ait fait naître, presque *ex nihilo*, un grand nombre de monnaies concurrentes dont la viabilité à long terme est faible. Elles fournissent néanmoins un exemple de la théorie des monnaies concurrentes de Hayek : la sélection des bonnes et de mauvaises monnaies sera faite, sur le long terme, par les choix des consommateurs.

Les crypto-monnaies évoquées précédemment se répartissent donc de la manière indiquée sur le graphique suivant. Notons que la taille des bulles représente la capitalisation boursière, calculée comme le nombre de monnaies en circulation multiplié par le prix unitaire. Nous avons retenu les données au 31 décembre 2017. Les transactions sont exprimées en transactions par seconde avec une échelle logarithmique.

[16] Le Iota repose sur le Tangle pour ce mécanisme alors que le Nano repose sur le mécanisme dit block lattice ou « bloc tressé », qui reprend néanmoins le principe d'une implémentation d'un graphe orienté acyclique.
[17] https://nano.org/en/whitepaper

Répartition des monnaies selon leur niveau de confidentialité
et leur vitesse de transaction