Une crypto de plus
ou plus qu'une crypto ?

Septembre 2019

Introduction

Dans l'âpre monde des blockchains, plusieurs cryptomonnaies se sont développées pour répondre à des besoins différents de ceux couverts, plus ou moins bien, par l'ancêtre Bitcoin qui domine encore largement les esprits et les marchés.

Parmi ces cryptomonnaies, Dash semble sortir du lot pour avoir résolu, bien avant tous les autres, un problème que peu d'autres ont analysé et encore moins tenté de résoudre, à savoir celui de la **gouvernance** dans un domaine où, quasiment par définition, il n'y a pas de chef clairement désigné[1]. C'est un problème d'autant plus aigu qu'il a amené la communauté Bitcoin à se scinder en 2017 et a entraîné la création de Bitcoin Cash, communauté qui s'est à nouveau divisée lors de la scission avec l'équipe en charge de Bitcoin SV. C'est aussi un problème de gouvernance qui a amené à l'existence parallèle d'Ethereum Classic en plus d'Ethereum.

Pourtant, tous les jours, la cryptomonnaie Dash et sa communauté prouvent que ce problème de gouvernance peut être résolu. Et si, bien évidemment, Dash n'est pas exempt de défauts et connaît, lui aussi, son lot de soucis à résoudre, c'est une cryptomonnaie apte à fournir de nombreuses opportunités de croissance saine.

Ce dossier sera l'occasion de revenir sur l'histoire de Dash, d'explorer ses caractéristiques, de regarder comment lui et sa communauté fonctionnent, d'en étudier les forces et les faiblesses.

Dans l'univers impitoyable des cryptomonnaies, quels sont les atouts de Dash ? Quel peut être son avenir ?

[1] On pourrait ici reprendre la proposition de Jacques Favier qui a trouvé le terme de "monnaie acéphale" (cf https://bitcoinlamonnaieacephale.fr/).

La cryptomonnaie pour les nuls, en quelques mots

L'objet de ce dossier n'est pas d'expliquer par le détail le fonctionnement et les concepts d'une cryptomonnaie, tant ce sujet peut à lui seul faire l'objet d'un ouvrage à part (qui, du reste, existe, par exemple sous la plume d'Andreas Antonopoulos, *Mastering Bitcoin*[2]).

Mais pour poser le contexte, revenons tout de même sur les grands principes de base. Le lecteur intéressé pourra toujours retrouver facilement sur Internet de nombreuses ressources pour le détail des concepts abordés ici.

Qu'est-ce qu'une cryptomonnaie ?

Une monnaie électronique

Il s'agit d'une **monnaie électronique** dont il n'y a pas *a priori* d'équivalent physique et qui n'a besoin d'aucun pendant physique pour fonctionner, par opposition à la monnaie électronique traditionnelle, d'abord assise sur une réalité physique tangible (les pièces et les billets) qui s'est progressivement dématérialisée avec l'avènement de l'informatisation de nos sociétés.

À ce titre, une cryptomonnaie existe d'abord et avant tout de façon numérique et ne sera représentée sous forme physique que de façon anecdotique.

Une monnaie sans besoin d'intermédiaire de confiance

Par construction, là où les monnaies électroniques traditionnelles ne sont que la représentation d'une monnaie nationale garantie par un État et des institutions financières entièrement encadrées par celui-ci, une cryptomonnaie fonctionne **sans tiers de confiance**, c'est-à-dire sans avoir besoin d'un intermédiaire qui garantisse les transactions ou les valeurs échangées.

Ceci n'est pas une mince affaire : une monnaie qui peut fonctionner sans tiers de confiance, c'est une monnaie qui se passe de banque et d'intermédiaire dans les transactions. De ce point de vue,

[2] https://www.amazon.fr/Mastering-Bitcoin-Programming-Open-Blockchain/dp/1491954388

c'est quelque chose qui est très proche de l'échange physique, du troc ou de l'utilisation de monnaies métalliques comme on le pratiquait il y a quelques centaines d'années, avec des caractéristiques essentielles : la matière étant ce qu'elle est dans notre univers, elle ne peut exister en même temps dans deux endroits différents ; quand une pièce de monnaie change de mains, il n'y a aucun besoin d'un tiers de confiance pour s'assurer que la valeur transportée dans cette pièce change de propriétaire.

Historiquement, le tiers de confiance n'est apparu que lorsqu'il s'est agi d'échanger de la valeur sans échanger physiquement de la matière, pour des raisons de praticité, de distance, de sécurité, de rapidité, etc. Là où les pièces de monnaie pouvaient conserver une valeur intrinsèque par leur contenu de métal rare (or ou argent, essentiellement), l'effet de commerce, la créance ou le billet papier ne sont utiles que lorsqu'on peut accorder de la confiance à l'institution qui le produit.

De nos jours, toutes les opérations financières reposent sur le principe de confiance : confiance dans l'établissement bancaire dans la tenue des comptes qui lui sont confiés (on espère, parfois naïvement, que la banque ne fasse pas n'importe quoi avec notre argent), et confiance dans l'État que les euros, les dollars ou la devise qu'on manipule soient *in fine* assis sur une richesse suffisamment concrète pour valoir quelque chose (et sinon, c'est le Vénézuéla[3] ou le Zimbabwe[4]).

Les cryptomonnaies se sont affranchies de ce problème en trouvant une solution élégante à la non-rivalité[5] des biens numériques : au moyen d'un algorithme encapsulant une série de principes simples, Bitcoin, la première cryptomonnaie, a permis de prouver qu'on pouvait fort bien échanger un bien numérique, *a priori* non rival, de façon rivale, c'est-à-dire garantissant un unique propriétaire à la fois. Bitcoin a prouvé qu'il était possible de réaliser un **transfert numérique sans permettre sa déduplication**.

Une monnaie publique

Comme on l'a vu, une cryptomonnaie est donc une monnaie électronique, sans tiers de confiance, capable de garantir le suivi de son propriétaire de façon sûre et certaine dans le temps, comme un bien physique, et surtout, de façon **publique**.
Cette publicité des transactions est réalisée au travers d'un "grand livre de comptes" qui contient l'ensemble de toutes les transactions effectuées, depuis le début de la mise en place de la cryptomonnaie. Par construction, ce grand livre de compte est constitué de blocs de transactions chaînés les uns aux autres (d'où le nom de chaîne de blocs, ou *blockchain*).

Ainsi, à n'importe quel moment, il est possible de vérifier les transactions effectuées et garantir, de façon mathématiquement sûre, que les transferts sont bien réalisés sans erreur, des sources vers les destinations toutes connues sans opacité, et ce d'autant plus que les procédés utilisés pour construire cette chaîne de blocs en rendent sa modification impossible *a posteriori*.

Comme on va le voir plus loin, cette publicité des transactions n'impose pas (ou n'impose plus, disons) une levée complète de l'anonymat des propriétaires ; elle autorise seulement une

[3] https://www.lemonde.fr/international/article/2019/05/29/venezuela-l-inflation-a-ete-de-130-060-en-2018_5469091_3210.html
[4] https://fr.wikipedia.org/wiki/Hyperinflation_au_Zimbabwe
[5] https://fr.wikipedia.org/wiki/Rivalit%C3%A9_(%C3%A9conomie)

“auditabilité” des comptes publics ce qui permet notamment de connaître avec précision la masse monétaire en circulation, chose que les banques centrales ont le plus grand mal à réaliser pour les monnaies traditionnelles.

Une monnaie décentralisée

Pour garantir que les transactions sont bel et bien enregistrées et incorruptibles dans le temps, il faut cependant que le grand livre de compte, cette chaîne de blocs décrite précédemment, disponible publiquement au su et au vu de tous, ne soit pas conservé en un unique endroit qui constituerait un point unique de défaillance possible.

Dès lors, une cryptomonnaie digne de ce nom doit être **décentralisée**, c’est-à-dire garantir que la chaîne de blocs est gérée et conservée à plusieurs endroits du globe, indépendants les uns des autres, n’appartenant pas tous au même propriétaire, et de la façon la plus large possible pour éviter toute collusion des multiples propriétaires des équipements l’hébergeant.

C’est ce qu’on réalise en créant des nœuds, c’est-à-dire des serveurs qui, chacun, contiennent une copie de l’ensemble de la chaîne de blocs. Ces nœuds sont constamment reliés les uns aux autres afin de se synchroniser. Ce sont ces nœuds qui ont la tâche de confirmer les transactions, vérifier et verrouiller les blocs de transactions dans la chaîne et tenir l’ensemble des soldes comptables de tous les participants au réseau. Plus le nombre de ces nœuds est élevé, plus ces serveurs sont répartis dans le monde, plus la redondance d’information est forte, et plus la perte d’information devient improbable.

Un peu de jargon

Avant d’aller plus loin, il sera utile d’introduire un peu de jargon concernant les blockchains.

Confirmation de transaction

La confirmation d’une transaction est le moment où la transaction a été vue (i.e. placée dans la liste des transactions à insérer dans le prochain bloc de transactions) par un nombre raisonnablement élevé de nœuds du réseau cryptomonétaire. Cette opération est généralement très rapide puisqu’en quelques secondes (moins de 5), on estime que l’ensemble des nœuds du réseau a pu voir la nouvelle transaction arriver.

Confirmation de bloc

La confirmation d’un bloc est le moment où l’ensemble des transactions de ce bloc sont inscrites dans la chaîne de blocs. Le bloc étant confirmé, les transactions qui le composent sont alors impossibles à annuler (il faut pour cela annuler tout le bloc, ce qui nécessite des moyens exponentiellement plus importants à mesure que d’autres blocs sont enchaînés à sa suite).

La double dépense

Toute cryptomonnaie est confrontée à un problème inhérent à sa nature purement numérique.

On l'a vu : dans le monde numérique, toute information peut être recopiée à l'identique sans que l'information de base ne soit touchée. De ce point de vue, une information est un **bien non rival**, dont la possession peut être étendue à plusieurs propriétaires sans aucun souci d'accès concurrent (i.e. le fait que j'accède ou que je manipule telle information n'empêche personne d'accéder ou de manipuler la même information ailleurs, la copie étant toujours possible et parfaite).

Bitcoin puis toutes les cryptomonnaies ensuite ont élégamment résolu ce problème en rendant la possession d'un jeton numérique (= une pièce numérique intangible) rivale, c'est-à-dire en imposant que ce jeton ne puisse être présent qu'une fois unique dans la chaîne de blocs. On peut le déplacer, on peut le scinder (ce qui détruit l'ancien jeton et donne naissance à deux ou plusieurs autres jetons), on peut additionner deux jetons pour n'en donner qu'un au final, mais, à aucun moment, un même jeton ne peut être impliqué dans deux transactions simultanées.

La double dépense, c'est l'occurrence d'un tel cas. Lorsqu'elle survient, c'est tout l'enjeu du protocole de décision au cœur de la cryptomonnaie de déterminer laquelle des deux dépenses est jugée légitime, l'autre étant rejetée.

Bitcoin a permis d'introduire le "consensus Nakamoto" qui permet justement de trancher celle des deux transactions qui sera choisie. Les autres cryptomonnaies, Dash y compris, ont appliqué les mêmes principes permettant de construire la chaîne de blocs en se prémunissant de façon efficace de ce problème de double dépense.

Preuve de travail (proof of work, PoW)

Pour valider un bloc, il faut que l'opération soit coûteuse (en temps, en ressources, en capital, …) : c'est ce qu'on appelle la preuve de travail. Ce coût permet de garantir économiquement que chaque participant du réseau a un intérêt bien compris d'une part à garantir la validité des blocs et d'autre part à tout faire pour éviter des attaques de tiers ou d'autres participants, visant à remanier le registre à leur profit.

C'est tout le génie du "consensus Nakamoto" d'avoir permis l'émergence d'un équilibre entre les différents acteurs du réseau, ni altruistes, ni forcément honnêtes, qui assure que la production et la validation des blocs se déroule comme prévu, dans l'intérêt du réseau même.

La preuve de travail est, de loin, la méthode la plus employée parmi les cryptomonnaies pour garantir le processus décisionnel lors de l'ajout de transactions dans un bloc.

Preuve d'enjeu (proof of stake, PoS)

Dans certains cas, et typiquement pour les cryptomonnaies qui ont intégré dans leur protocole de fonctionnement des mécanismes de prise de décision décentralisée pour la gouvernance de leur écosystème complet et de leur communauté, la preuve d'enjeu remplace ou s'ajoute à la preuve de travail.

Cette preuve d'enjeu est basée sur la possession d'une partie des jetons du réseau (les cryptomonnaies) ; à l'instar d'un cens qui autorise un suffrage censitaire, la preuve d'enjeu permet aux participants d'un réseau qui sont investis dans celui-ci de disposer d'un poids de vote

proportionnel à leur investissement. L'idée est que, sur le long terme, les décisions d'investisseurs impliqués dans la monnaie et son futur soient plus judicieuses que celles de tierces parties qui n'ont pas mis "leur peau en jeu".

Plusieurs cryptomonnaies proposent cette preuve d'enjeu, soit dans un futur proche (comme Ethereum), soit d'ores et déjà (comme Tezos). Notons que Dash propose ce mécanisme au travers des Masternodes, ce qui sera détaillé plus loin.

L'histoire de Dash

Pourquoi il fut créé

Dash n'a pas toujours existé sous ce nom.

Le 18 janvier 2014, lorsque Evan Duffield, son créateur, lance officiellement sa cryptomonnaie, elle s'appelle alors XCoin, appellation qu'elle ne gardera qu'une poignée de jours avant de changer pour DarkCoin.

À la différence de la plupart des passionnés de Bitcoin de la première heure, qui sont surtout des développeurs, codeurs dans l'âme et "geeks"[6] au savoir pointu dans leur domaine mais manquant souvent d'ouverture sur les autres disciplines, Evan Duffield est à la fois un développeur informatique, ayant travaillé dans plusieurs entreprises spécialisées dans l'intelligence artificielle et les réseaux sociaux, et aussi un conseiller en investissements financiers diplômé qui a développé son expérience dans ce domaine pendant plusieurs années. Cette double compétence informatique et financière offre au fondateur de Dash un point de vue un peu différent de celui pris par les premiers suiveurs de Satoshi Nakamoto, le créateur de Bitcoin, qui sont surtout des informaticiens et des cryptographes.

Avec cette nouvelle cryptomonnaie, Evan Duffield veut en effet résoudre plusieurs problèmes qu'il a identifiés pour Bitcoin[7] : outre les éventuels problèmes de croissance et de mise à l'échelle, la première cryptomonnaie souffrait à ses débuts d'instabilités de réseau et Duffield pressent une difficulté générale de gouvernance chez Bitcoin. Dans une communauté qui refuse ouvertement tout chef incontestable, les prises de décision sont parfois complexes : comment évaluer les options de développement qui s'offrent à la communauté, qui décide en dernier recours, que faire en cas de désaccord profond ?

[6] https://fr.wikipedia.org/wiki/Geek
[7] https://www.youtube.com/watch?v=0Jw5Gk-iuy0&feature=youtu.be&t=1510

L'avenir lui donnera globalement raison sur ces différents points : la croissance de Bitcoin a effectivement posé des problèmes quelques années plus tard avec la limitation de la taille des blocs de transactions qui fait actuellement plafonner le réseau de cette cryptomonnaie à 4 transactions à la seconde. Quant à la gouvernance de la première cryptomonnaie, elle est suffisamment problématique pour n'avoir pas pu éviter différents contentieux ayant abouti à des scissions de la communauté, entraînant la création de Bitcoin Cash en 2017 puis Bitcoin SV en 2018.

Dès le départ, Duffield a clairement fixé les objectifs de sa cryptomonnaie : une gestion la plus performante et efficace possible de la monnaie. Au contraire par exemple d'Ethereum, une autre cryptomonnaie créée à la même époque et qui ambitionne de fournir bien plus qu'un moyen de paiement, le but de Darkcoin — qui, afin de se débarrasser de la mauvaise image de marque véhiculée par le mot "dark", deviendra officiellement Dash (mot valise pour "digital cash", "argent liquide numérique") le 25 mars 2015 — est de devenir une sorte de Bitcoin nouvelle génération, une monnaie électronique pair-à-pair fonctionnelle et résolvant certains problèmes inhérents à Bitcoin : l'absence d'anonymat des transactions, la lenteur de ces dernières et les problèmes de gouvernance de la cryptomonnaie.

Pour Dash, l'objectif est bel et bien de devenir avant tout "le Paypal de la cryptomonnaie", se rapprocher du concept d'argent liquide numérique, notamment en éliminant complètement toute sa complexité technique pour l'utilisateur final et en lui offrant une interface simple et efficace, tout en conservant ses principes essentiels, à savoir la décentralisation, l'auditabilité aisée, la résistance à la censure (i.e. personne ne peut empêcher une transaction légitime d'être écrite dans la chaîne de blocs), des frais de transaction aussi faibles que possible, …

Par extension et une fois ce but réalisé, Dash ambitionne ensuite de permettre ce que Bitcoin envisageait dès le départ et qui fut rapidement réalisé au travers d'Ethereum, à savoir aussi servir de plateforme à des applications décentralisées, ce qui devrait être possible avec une série de mises à jour du code de Dash rassemblées sous le nom d'"Evolution", déjà entamées et dont la version 1.0 est prévue pour 2020.

Les premiers jalons

Après un début assez mouvementé (le chapitre sur les faiblesses sera l'occasion de détailler ces débuts), XCoin rapidement renommé Darkcoin va voir son utilisation notoirement décoller[8] au sein de certains darknets[9]: les fonctions assurant l'anonymat de cette nouvelle cryptomonnaie rendent en effet bien plus aisé son usage pour des transactions où la plus grande discrétion est de mise ("privacy coin") et, typiquement, certaines organisations y trouveront leur intérêt.

Cependant, cette première innovation de cette cryptomonnaie sur Bitcoin, amenant l'anonymat et avec lui, attirant une faune pas forcément fréquentable, sera bientôt dépassée par d'autres avancées techniques plus importantes, dès mai 2014.

[8] https://99bitcoins.com/darkcoin-darknet-markets/ , https://tinyurl.com/y5npwy78
[9] https://fr.wikipedia.org/wiki/Darknet

C'est ainsi que l'apparition des Masternodes (un réseau de second niveau sur lequel nous reviendrons en détail dans quelques paragraphes) apportera de nouvelles fonctionnalités déterminantes et caractéristiques de la nouvelle cryptomonnaie, en offrant par exemple des possibilités de transactions quasi instantanées.

À l'automne 2015, la mise en place d'un système de budget décentralisé et d'une gouvernance complète associée permet à Darkcoin renommé depuis Dash (en mars de cette année) de devenir **la première cryptomonnaie à disposer d'une "organisation autonome décentralisée"[10] ou DAO[11]**.

La DAO

Cette forme d'organisation très particulière permet, grâce à l'instauration de règles de gouvernance dans la blockchain sous-jacente, de faire fonctionner des organisations sans désigner de chef ou de responsable direct, tout en conservant la possibilité à chaque participant de faire valoir son opinion, de financer ou pas des projets proposés au sein de l'organisation, et de faire évoluer l'organisation elle-même en fonction des opportunités et des menaces qui se présentent à elle.

Quelques beaux succès

Depuis ces premières années, la communauté Dash ne s'est pas reposée sur ses lauriers et peut même s'enorgueillir de quelques beaux succès.

Au Vénézuela

C'est le cas par exemple avec le déploiement de Dash au Vénézuéla : pays ravagé par un effondrement économique typique de la mise en place d'une économie socialiste, la monnaie locale, rongée par une inflation galopante, s'est rapidement dépréciée à tel point qu'elle n'est plus réellement utilisée par personne. Les Vénézuéliens, réduits au troc et au système D pour leur vie quotidienne, ont pu mesurer l'importance d'une monnaie solide et indépendante du gouvernement dès que les cryptomonnaies ont été disponibles.

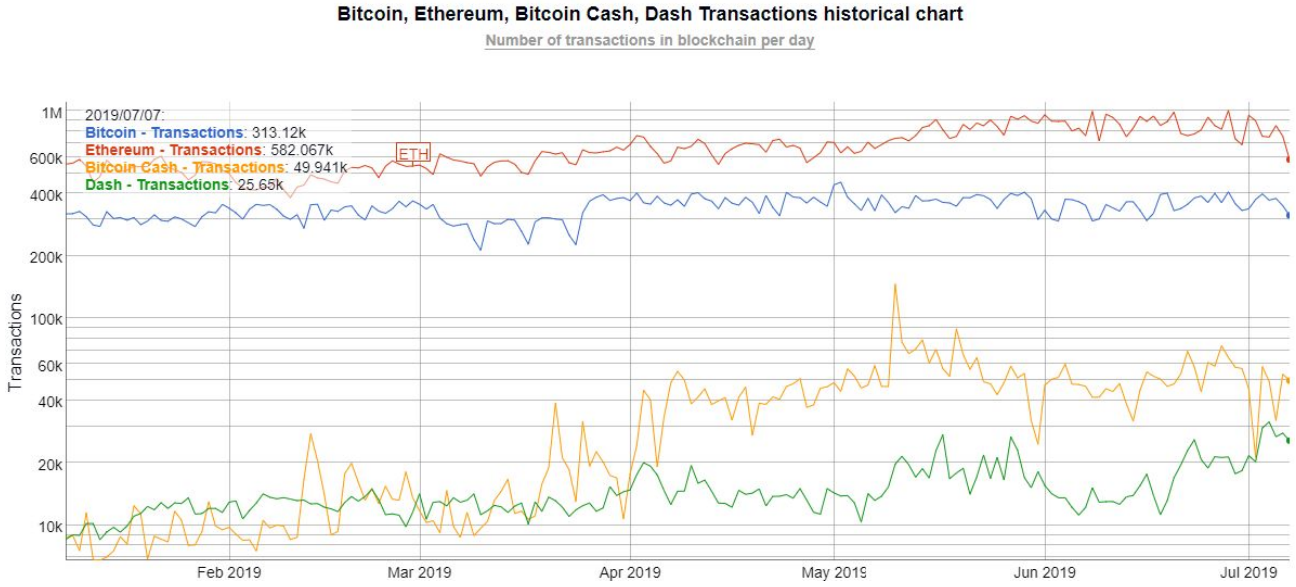
Bénéficiant de compatriotes expatriés qui leur envoient, outre des devises (souvent du dollar américain), des cryptomonnaies qui ont l'énorme avantage de transiter d'un pays à l'autre de façon instantanée, sans frais et sans se soucier des frontières, un nombre croissant de Vénézuéliens pratique maintenant des transactions sur diverses blockchains.

Si Bitcoin est évoqué, il est relativement peu utilisé : les frais de transaction, prohibitifs pour le Vénézuélien moyen, empêchent de considérer cette cryptomonnaie comme réellement praticable dans ce pays en pleine déconfiture.

[10] https://fr.wikipedia.org/wiki/Organisation_autonome_d%C3%A9centralis%C3%A9e
[11] https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

La relève “cryptomonétaire” est donc assurée par d’autres jetons comme Ethereum, Bitcoin Cash et Dash[12] qui bénéficie sur place d’une bonne presse et d’une communauté enthousiaste. Avec une inflation locale de plus de 80.000% sur le bolivar, on comprend aisément que le Vénézuélien cherche fébrilement un refuge à la richesse qu’il peut produire ; de ce point de vue, la volatilité naturelle des cryptomonnaies n’est pas un frein tant elle paraît supportable face à la perte de pouvoir d’achat du bolivar d’un jour à l’autre. On comprend dès lors que les deux années passées ont vu l’usage des cryptomonnaies exploser dans ce pays, et notamment celui de Dash[13].

Si, bien sûr, connaître la pénétration de Dash est difficile, il n’en reste pas moins que le nombre de transactions effectuées avec cette blockchain progresse de mois en mois comme en atteste le graphique suivant qui permet de mettre en relation ce nombre de transaction avec celui d’autres cryptos populaires.



Record du nombre de transactions à la journée

Un autre beau succès au crédit de la blockchain Dash est sa capacité maintenant prouvée à encaisser un nombre important de transactions dans une même journée. En septembre 2018, Bitcoin Cash avait prouvé que le principe général proposé par Satoshi Nakamoto permettait de traiter un nombre intéressant de transactions à la seconde en atteignant 2,1 millions de transactions enregistrées dans une période de 24 heures, soit environ 25 transactions à la seconde.

La communauté Dash parviendra quant à elle à atteindre 3 millions de transactions en novembre de la même année (soit 34 transactions par seconde)[14]. Ces pics atteints tant pour Dash que pour Bitcoin Cash en créant un grand nombre de transactions sur le réseau pour en tester les capacités effectivement “en grandeur réelle” ont permis de mesurer la réaction des différents acteurs, des nœuds de chaque chaîne, et de déceler les points d’étranglement éventuels et les améliorations à apporter.

[12] https://cfxmagazine.com/en/crypto-en/venezuela-adopts-dash/
[13] https://www.inverse.com/article/54641-venezuela-cryptocurrency
[14] https://dashnews.org/fr/le-stress-test-dash-depasse-3-millions-de-transactions/

Ces tests ont aussi permis de montrer que l'organisation du réseau, les redondances mises en place et le principe général d'augmentation de la taille des blocs en fonction de la demande réelle couvrent bien les besoins, au moins dans un avenir proche, et tout indique que les efforts seront raisonnables pour la mise à l'échelle des infrastructures afin de pouvoir, un jour, se comparer avec les niveaux de performances atteints par des réseaux traditionnels de paiements bancaires mondiaux (typiquement, Visa ou Mastercard, dont le taux moyen tourne autour de 4000 transactions à la seconde).

Les spécificités de Dash

Si Dash est une cryptomonnaie bâtie au départ sur les mêmes principes que Bitcoin et qui a initialement repris dans sa conception le code informatique de Litecoin, un clone proche de Bitcoin, elle s'est néanmoins assez vite attachée à résoudre certaines problématiques présentes sur la première cryptomonnaie en introduisant différentes techniques.

Au niveau de la blockchain

Ainsi, là où chaque bloc Bitcoin est généré toutes les 10 minutes, les blocs Dash sont, eux, générés toutes les 2 minutes et 30 secondes. Ceci, couplé à une limite de taille de bloc plus large (à 2 Mo à la place de 1 Mo pour Bitcoin), permet de stocker plus de transactions dans chaque bloc, de produire plus de blocs dans une période donnée, et donc de traiter plus de transactions au total.

Ceci est cohérent avec le but officiel de Dash qui ambitionne de devenir la monnaie électronique du futur et doit donc être capable de traiter progressivement un grand nombre de transactions à la seconde.

Masternode

Notion introduite très vite peu après le lancement du projet, les Masternodes ("nœuds maîtres") sont des serveurs particuliers qui fournissent plusieurs services additionnels aux nœuds de base qui se contentent de répliquer la blockchain et d'en assurer la cohérence.

Les Masternodes permettent entre autres de fournir deux services particuliers qui seront détaillés dans les paragraphes suivants : InstantSend et PrivateSend. Ces services sont accessibles indépendamment de la production d'un bloc, c'est-à-dire que, grâce à la création de ce réseau en deux niveaux, l'un chargé de produire les blocs, l'autre d'assurer des services orientés paiement en ligne, on peut facilement garantir une montée en charge harmonieuse du moyen de paiement dans son ensemble.

Ces services sont rémunérés : chaque Masternode reçoit une partie des dashs générés à chaque bloc comme récompense et pour garantir la qualité des services ainsi fournis. En échange du verrouillage de 1000 dashs par Masternode comme caution, son propriétaire est alors à même de

voter sur les financements de projets qui sont proposés par la communauté. Cette rémunération explique le nombre élevé de masternodes sur le réseau Dash (environ 5000) proportionnellement aux nœuds du réseau Bitcoin, non rétribués.

Cette dernière possibilité est une spécificité de Dash qui rend son fonctionnement relativement rare dans le monde des cryptomonnaies où la gouvernance n'est généralement pas ou peu prise en compte.

La présence, dans certaines cryptomonnaies, de mécanismes de Preuve d'Enjeu permet en effet aux participants de voter (de façon censitaire[15] ou comme le ferait une assemblée d'actionnaires) pour les évolutions de protocole, de l'écosystème ou sur n'importe quel sujet compatible avec le protocole de la blockchain considérée. Ceci permet d'éviter les écueils rencontrés par les communautés où l'absence de vote clair entraîne des scissions au sein des équipes en fonction des préférences et intérêts de chacun.

Avec Dash, ce mécanisme est maintenant robuste puisqu'il est en place depuis ses tout débuts, et a déjà permis d'accompagner favorablement les évolutions de la cryptomonnaie et d'orienter ses nouveaux développements. En outre, il s'ajoute au mécanisme de Preuve de Travail qui continue d'être utilisé pour le consensus établissant les transactions dans les blocs.

InstantSend

On l'a vu : au travers des Masternodes, Dash permet deux services.

Le premier d'entre eux, InstantSend, est un mécanisme qui permet le verrouillage des transactions et permet ainsi d'éviter toute double dépense, ce qui permet au commerçant de finaliser la transaction en toute sécurité.

Dans un réseau comme Bitcoin, une transaction n'est effectivement validée et impossible à annuler qu'une fois validé le bloc dans lequel elle apparaît. Ceci peut prendre une dizaine de minutes, voire plusieurs heures à plusieurs jours si le réseau des mineurs est engorgé. Pour Dash, la validation d'un bloc ne prend certes qu'un peu plus de deux minutes, mais c'est encore beaucoup trop pour toute opération de paiement électronique où on estime qu'au-delà de 5 secondes, le client et le commerçant s'impatientent.

Dash a résolu ce problème en proposant de verrouiller la transaction, c'est-à-dire que, par protocole, cette transaction bénéficiera d'un mécanisme de consensus rapide, indépendant du consensus de l'intégralité du bloc, qui permettra de garantir que cette transaction ne pourra pas être altérée une fois validée.

En outre, ce protocole est maintenant activé par défaut, sans frais supplémentaires, pour une grande majorité de transactions, et permet que les fonds concernés soient immédiatement réutilisés dans une nouvelle transaction, en cascade. Pour l'utilisateur final (qu'il soit client ou commerçant),

[15] https://fr.wikipedia.org/wiki/Suffrage_censitaire

cela revient à reléguer l'ensemble du processus de confirmation en coulisse et lui fournit un système de paiement quasi instantané et très proche de la version physique de la monnaie : l'argent liquide.

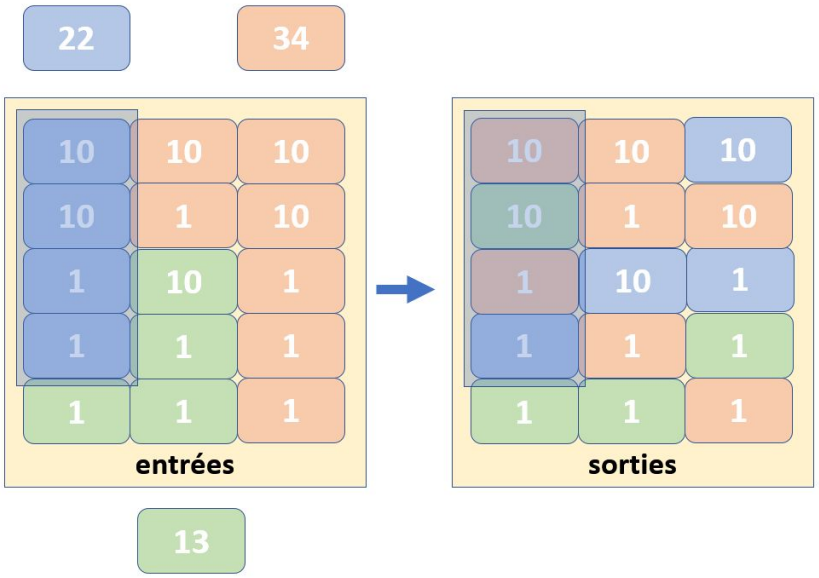
Concrètement, cela veut aussi dire que certaines applications spécifiques de la monnaie deviennent possibles alors qu'elles sont notoirement plus complexes à mettre en œuvre sur d'autres cryptomonnaies, comme les micro-transactions (transactions nombreuses mais de très faible montant[16]).

PrivateSend

Une seconde innovation de Dash est l'introduction de PrivateSend, algorithme qui permet de garantir la confidentialité des transactions en mélangeant intelligemment les transactions entre elles.

Pour y parvenir, cet algorithme va essentiellement découper les transactions en petites transactions de dénomination fixe (en transactions de 0,01, 0,1, 1 et 10 dashs par exemple) et faire savoir aux Masternodes qu'un utilisateur demande une transaction "PrivateSend". Ces Masternodes vont ensuite apparier cette demande avec celles d'autres utilisateurs (au moins deux) afin d'échanger de façon aléatoire les différents montants entre eux. Dans ce procédé, les Masternodes se chargent simplement de mettre en relation les utilisateurs désireux d'anonymiser leurs transactions et ne sont jamais dépositaires des fonds concernés.

Le schéma ci-dessous présente un cas d'utilisation très simple, avec trois utilisateurs, et pour un premier passage (nommé "cycle de mélange") : une transaction de 22 dashs (encadrée en bleu) sera mélangée avec d'autres transactions pour aboutir à la fin à une transaction de même montant, mais dont les dashs proviennent de sources différentes.



[16] https://cryptobriefing.com/dash-celebrating-smaller-transactions/

En réalisant cette opération spécifique plusieurs fois de suite avec à chaque fois d'autres utilisateurs, on garantit de façon statistiquement très sûre qu'il sera très difficile de retrouver l'origine des fonds. Il s'agit là de réaliser une propriété fondamentale de toute monnaie : la fongibilité. Chaque unité de compte doit avoir la même valeur que toutes les autres.

Notons que ce procédé de mélange ("mixing") des transactions est en application dans d'autres cryptomonnaies (avec des technologie comme CoinJoin, mais aussi Bitcoin Cash avec CashShuffle[17] typiquement, qui ne sont pas exactement similaires mais reposent sur le même principe général) et pouvait être mis en pratique sur Bitcoin lui-même[18] avant que les frais de transaction ne deviennent prohibitifs, rendant l'opération bien trop coûteuse. Une différence essentielle est que ce procédé ne dépend pas de tierces parties, et se fait directement au niveau du protocole du réseau Dash (les fonds ne sont confiés à personne le temps du mélange).

Après quelques années d'utilisation, la sécurité de ce procédé, qui dépend bien évidemment du nombre de cycles effectués, n'est plus à mettre en doute. Bien que des récompenses soient régulièrement offertes à qui parviendrait à retracer l'origine de fonds d'une transaction "PrivateSend", l'opération semble suffisamment complexe pour que personne n'ait pu pour le moment prétendre remporter ces récompenses.

[17] https://cashshuffle.com/
[18] Avec des conséquences juridiques identiques : https://tinyurl.com/yyj24434

Forces et faiblesses

Maintenant que nous avons une meilleure idée des différentes caractéristiques de Dash, nous pouvons regarder plus en détail ses forces et ses faiblesses.

Forces

Un modèle économique unique et solide

L'une des forces évidentes de cette cryptomonnaie est la structure même de son écosystème économique. Très rapidement, les développeurs de Dash ont compris tout l'intérêt qu'il pouvait y avoir à consacrer à la communauté elle-même une partie des fonds produits par le minage.

Comme on l'a vu, le minage permet de sécuriser la chaîne de blocs en garantissant que les blocs inscrits ne seront plus modifiés une fois ajoutés aux précédents. Le minage nécessitant des ressources (de temps, de calcul, d'électricité, etc.), il est rémunéré avec des jetons (des dashs) qui sont produits à un rythme prévu dans le protocole, dès le départ.

Ce rythme diminue progressivement, assurant à terme que la production de Dash est limitée : il n'y aura jamais plus de 18 millions de dashs en circulation, à l'instar de Bitcoin (dont la production maximale sera de 21 millions). Ceci garantit la cryptomonnaie contre l'inflation qui représente dans ce cas un amoindrissement de la valeur de la monnaie dans le temps ; en garantissant une limite maximale au nombre de jetons produit, on garantit aussi une période de déflation des prix et d'accroissement de la valeur de chaque jeton.

Ce choix économique n'est pas neutre. Choisi par Satoshi Nakamoto pour Bitcoin, dans le respect d'une compréhension de l'économie suivant plutôt l'école autrichienne[19], il fournit une garantie plus solide que son inverse, l'inflation, et permet de favoriser l'épargne sur la consommation, au contraire de la monnaie fiat actuelle (i.e. produite par l'État) qui favorisent la consommation et

[19] https://www.wikiberal.org/wiki/%C3%89cole_autrichienne

même l'endettement. De ce point de vue, on peut comprendre que conserver ce choix pour Dash fut une bonne chose.

D'autre part, et cela fait la spécificité de Dash, il a rapidement été décidé qu'au contraire de Bitcoin qui dirige 100% des jetons issus du minage vers les mineurs eux-mêmes, les jetons seraient répartis de la façon suivante :

- 45% vont aux mineurs et rémunèrent leur travail de sécurisation
- 45% vont aux Masternodes et rémunèrent les services offerts
- Les 10% restants financent la DAO, cette organisation décentralisée qui va permettre à la communauté Dash de réaliser sa propre gouvernance.

Ceci permet à la fois de garantir la sécurité du réseau, la fourniture de services à valeur ajoutée, et de trouver des fonds pour sécuriser les développements, les innovations et les équipes d'informaticiens[20] qui maintiennent le code.

En outre et comme on l'a évoqué à plusieurs reprises dans les précédents paragraphes, la façon dont les fonds sont ventilés (à qui, pourquoi et comment) est votée par la communauté des Masternodes qui ont tout intérêt, ayant au moins 1000 dashs de caution par nœud, à diriger la communauté vers les options les plus profitables, les moins risquées et celles qui offrent le meilleur avenir sur le long terme.

Une communauté plus sereine

Cette "architecture technico-économique" et la façon dont les problèmes de gouvernance ont été résolus par l'introduction de ces Masternodes et du pouvoir décisionnel censitaire, essentiellement capitaliste par nature (on reproduit ici une société en copropriété avec des actionnaires), ont largement contribué à créer une communauté plus sereine que d'autres, et clairement tournée vers le but fixé au départ, c'est-à-dire faire de Dash une monnaie mondiale, décentralisée et indépendante des États ou du système bancaire actuel.

Les dissensions, liées à des choix techniques ou politiques, étant résolus de façon établie dès le départ, il a été constaté une agressivité bien plus faible qu'ailleurs au sein de la communauté Dash qui résout bien ses éventuels conflits internes.[21] En pratique, l'agressivité existe bien sûr toujours : des luttes pour l'attention, des prises de positions radicales et l'intransigeance sont aussi de mise dans cette communauté comme les autres. Cependant, ces conflits intestins ne se traduisent pas sur la gouvernance globale de la cryptomonnaie et n'entraînent pas de graves scissions dont les effets économiques sont toujours négatifs.

Une core team compétente et rémunérée

Dès lors qu'un budget existe, il est possible de rémunérer correctement et régulièrement des développeurs de qualité qui n'ont alors pas de mal à s'investir sur le long terme dans le projet (la

[20] https://www.dash.org/fr/lequipe/

[21] Un exemple type de la gouvernance de Dash est la résolution par vote, en moins de 24 heures dès janvier 2016, du débat sur l'accroissement de la taille des blocs, une question technique qui déchire la communauté Bitcoin depuis des années.

passion, aussi forte soit-elle, ne suffisant pas toujours à remplir les frigos). Cet auto-financement permet aussi bien de se mettre à l'abri d'un bénévolat aléatoire que d'une prise de contrôle par des entités centralisées tierces.

Ce principe de la DAO permet en outre de fidéliser des compétences de manière durable. C'est ainsi que Ryan Taylor, directeur de la principale entité de la DAO, Dash Core, a rejoint Evan Duffield de manière informelle dès 2014 pour ensuite professionnaliser durablement son engagement auprès de Dash alors qu'il occupait précédemment des postes plus rémunérateurs dans le secteur de la finance.

En outre, cette budgétisation attire les talents : le fait de savoir, d'entrée de jeu, que le système a été pensé pour tenir la route économiquement permet plus facilement à des personnalités de rejoindre la communauté. Outre les développeurs, cruciaux pour implémenter les innovations et maintenir le code de Dash, on peut aussi penser aux communicants dont la fonction d'évangélisation est indispensable pour pénétrer le marché des paiements, et permettre de recruter spontanément dans des pays fort éloignés des fondateurs ou des principaux responsables (Vénézuéla, Nigéria, Turquie, …)

Enfin, soulignons l'importance de cette méthode de rémunération des projets, essentiellement méritocratique par la mise en concurrence des propositions soumises au réseau, qui permet naturellement l'émergence, par sélection naturelle, d'acteurs de qualité sur le long terme.

Faiblesses

Une communauté trop peu agressive ?

On l'a vu : la communauté Dash est décidément orientée vers le développement de son produit, et l'absence de drames épicés comme on peut en trouver du côté de Bitcoin, Bitcoin Cash ou même Ethereum rend plus difficile la partie médiatique que doivent pourtant jouer les cryptomonnaies pour se faire connaître.

Là où les différentes communautés tournant autour de Bitcoin sont régulièrement parcourues de spasmes plus ou moins violents, la communauté Dash semble avoir su contenir intelligemment les inévitables conflits internes. Sur le long terme, c'est probablement une excellente chose qui évite le développement de personnages toxiques dont les dégâts peuvent être important pour ce qui s'apparente essentiellement à des startups dont la fragilité joue surtout comme un handicap sur un marché (celui de la monnaie et des paiements) où aucun cadeau, aucune latitude ne sera permise. Sur le court terme, cela rend plus difficile pour les équipes et la communauté Dash de faire connaître les innovations, les avancées pourtant notables de cette cryptomonnaie.

De façon plus pragmatique, on ne pourra s'empêcher de noter le choix assez moyennement judicieux du nom "Dash" pour ce nom de cryptomonnaie. S'il est évident que "DarkCoin" était un choix désastreux en termes d'image, le mot "Dash" en lui-même, même s'il est court donc facile à retenir et relativement générique, entre en collision avec d'autres noms, depuis la lessive jusqu'à des équipes de sport en passant par un super héros de bande dessinée.

Une crypto PoW

Dash est une cryptomonnaie qui utilise de fait la "preuve de travail" (PoW) : cela sécurise les blocs produits et garantit notamment que les échanges ne peuvent être falsifiés.

Cependant, tout comme Bitcoin qui utilise un procédé très proche, cette sécurisation représente un coût énergétique important. On ne compte plus le nombre d'articles, généralement très mal étayés, qui s'enhardissent à comparer la consommation électrique nécessaire pour maintenir la sécurité sur les chaînes cryptographiques en preuve de travail, Bitcoin en tête, et arrivent à la conclusion que bouffer autant d'énergie que (au choix) le Lichtenstein ou l'Irlande est totalement déraisonnable.

En pratique, la plupart des calculs faits, généralement fantaisistes (pour ne pas dire foutaisistes), s'évertuent à vouloir comparer ces cryptomonnaies avec un système de paiement et seulement ça, ce qui ruine bien évidemment tout le sens de l'exercice ; Dash, tout comme Bitcoin, n'est pas qu'un système de paiement. C'est aussi un système de compensation, de gestion de compte, de distribution de moyens de paiement, de sécurisation des transactions et de valorisation.

Si Bitcoin ou Dash doivent être comparés aux systèmes déployés actuellement, il faut alors prendre en compte l'ensemble du système bancaire tel qu'il existe, qui comprend aussi la production des pièces, des billets, des cartes à puce, des terminaux de paiement, des distributeurs automatiques, mais aussi des chambres de compensation, des data-centres des banques, et leur indispensable réseau de guichets, de personnel derrière, et de l'inévitable plante verte dans le bureau du directeur.

Autrement dit, si on peut clairement faire le reproche aux cryptomonnaies, comme Dash, utilisant la preuve de travail d'être fort gourmandes en électricité, la comparaison avec les autres formes de monnaie dans le monde donne en réalité un avantage écrasant à cette technologie et la preuve de travail, bien qu'imparfaite, reste incroyablement compétitive et économe en énergie…

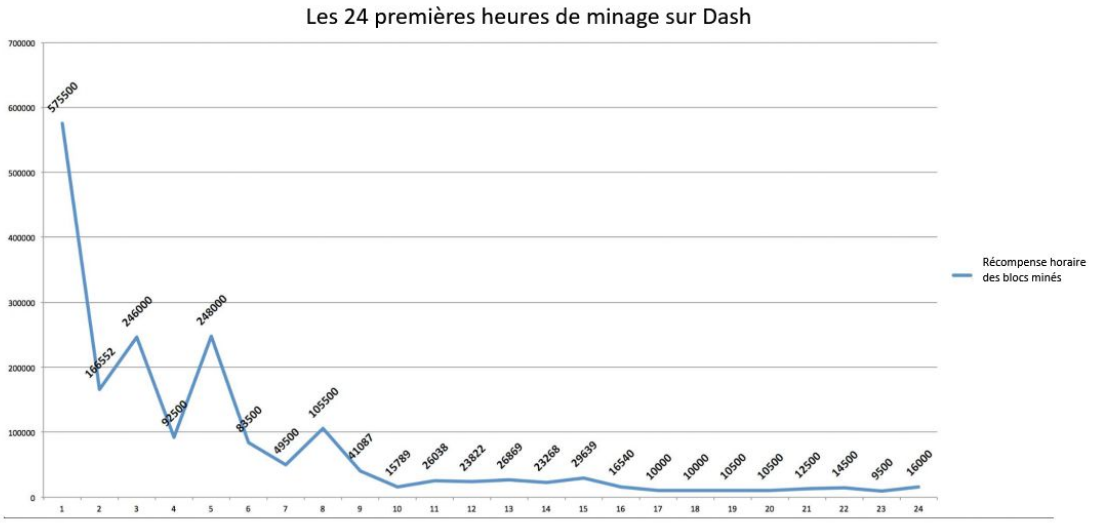
Néanmoins, on peut admettre que l'argument principal, à savoir qu'il existe possiblement un moyen plus efficace énergétiquement de sécuriser une chaîne, est raisonnable. Il reste bien sûr à trouver un tel moyen, d'autant que dépenser de l'énergie pour obtenir ce résultat est économiquement parfaitement sensé.

L'Instaminage du lancement

Un des principaux reproches qui est fait à Dash porte sans aucun doute sur son lancement.

Lorsqu'en janvier 2014, Evan Duffield lance ce qui s'appelle XCoin pour devenir rapidement DarkCoin, les premières heures qui suivent la mise à disposition du premier client de minage ne se passent pas exactement comme prévu.

Au lieu d'une émission raisonnée de jetons, à raison de quelques dizaines par blocs produits, ce sont plusieurs centaines de milliers qui déboulent d'un coup comme en atteste le petit graphique suivant ; c'est ce que beaucoup, par la suite, appelleront "instaminage", "fastminage" ou "minage instantané" pour signifier la découverte trop rapide de blocs trop généreux dans leur dotation…



En fait, le code source du mineur, essentiellement issu du code d'une autre cryptomonnaie (Litecoin), comporte plusieurs erreurs qui ont provoqué cette production intempestive de monnaie à un rythme prévu ni par les développeurs, ni par la communauté.

Le lancement, qui a bénéficié d'une certaine exposition sur les réseaux sociaux, démarre donc un peu trop sur les chapeaux de roue et sur une fort mauvaise image de marque : là où chacun s'attendait à pouvoir miner à son rythme, avec une probabilité d'obtenir des jetons à peu près équitable entre les différents mineurs, on se retrouve avec une production incontrôlée et une répartition assez biaisée de la cryptomonnaie.

Il s'en suivra de longs débats (qu'on pourra éplucher avec plus ou moins de bonheur, sur Bitcointalk par exemple[22]) pour savoir si, finalement, ces ratages au lancement étaient ou non calculés, si l'enrichissement des premiers mineurs est ou non scandaleux, si tout cela tient d'une arnaque ou pas.

Au passage, on pourra noter que Litecoin, dont le code Dash fut issu initialement, a souffert du même problème[23] avec une production de blocs erratique pendant ses premiers jours, sans qu'aucune publicité ne soit faite de ce démarrage lui aussi tumultueux, là où Dash supportera longtemps cette critique. Charlie Lee, fondateur de Litecoin, finira par le reconnaître au cours de l'été 2019[24].

Ici, mon point n'est pas de déterminer si, effectivement, tout ceci s'apparente ou non à une arnaque, tant la question, plus de 5 ans après, apparaît sans intérêt : d'une part, la répartition actuelle des jetons Dash est nettement moins concentrée que dans d'autres cryptomonnaies, d'autre part, ce lancement délicat est maintenant une donnée connue que la communauté a officiellement accepté. Enfin, l'historique des développements postérieurs parle de lui-même : s'il y a eu arnaque, on peine à voir qui a été floué (les jetons produits ces premières heures ne valaient presque rien sur

[22] https://bitcointalk.org/index.php?topic=421615.0
[23] https://old.reddit.com/r/dashpay/comments/a7vt1d/if_dash_had_a_fast_mine_due_to_a_bug_in_the/ec6cie7/
[24] https://beincrypto.com/charlie-lee-stirs-dash-instamine-controversy-attracts-scrutiny-to-litecoins-own-misgivings/

les marchés, et le cours est resté faible très longtemps) et comment l'ensemble du système a pu tenir aussi longtemps…

Mais en fait, peu importe : ce lancement fut fort négativement connoté puisqu'il a durablement associé ces erreurs à un concept qui a, lui, plutôt démontré ses atouts depuis. Sur les forums consacrés aux cryptomonnaies, il n'est pas rare que les discussions sur Dash reviennent régulièrement sur ce démarrage, montrant à quel point l'aspect marketing de ces cryptomonnaies est important.

Concentration des Masternodes

Par construction, nous avons vu que Dash est composé d'un réseau primaire de nœuds en charge du minage (sécurisation des transactions et de la blockchain) ainsi que d'un réseau secondaire de Masternodes qui fournissent des services supplémentaires.

L'existence de ces masternodes peut, en elle-même, poser problème dès lors qu'elles permettent — au moins en théorie — la concentration de pouvoir (de vote et donc budgétaire, notamment). Avec cette concentration technique viennent naturellement des éventuels jeux de pouvoir sur le renouvellement des décideurs, et ce, d'autant plus que le ticket d'entrée pour un masternode est maintenant élevé ; à 1000 dashs pour disposer d'un masternode, cela signifie environ 100.000 euros immobilisés, ce qui élimine de fait beaucoup de nouveaux entrants potentiels.

Très concrètement cependant, si ces craintes sont fondées et si une collusion reste toujours possible sur le papier, les faits historiques et la situation actuelle montrent qu'il n'en est rien : la concentration des avoirs au sein de Dash[25] est bien plus faible que pour Bitcoin[26] par exemple (i.e. il y a 7 fois moins de très riches en Dash qu'en Bitcoin, indépendamment des cours respectifs de ces deux cryptomonnaies), ou pire encore, Litecoin[27].

Des opérateurs de Masternodes pas toujours au niveau

Un autre souci lié aux masternodes tient dans le droit de vote des propriétaires sur les budgets fournis à des projets soumis par la communauté.

Si l'idée est économiquement intéressante, elle se heurte parfois à certains aspects pratiques : avec la multiplication des projets d'une communauté très active, il est en effet difficile pour un opérateur de se faire une idée précise de la valeur de chacun des projets sur lequel son vote sera demandé. Pire : certains projets, fort techniques, nécessitent des compétences dont les opérateurs ne disposent pas toujours.

Inévitablement, cela entraîne donc des pertes, tant du côté de projets qui reçoivent des financements alors qu'une étude plus approfondie aurait probablement réduit ou annulé leur budget, ou inversement et plus souvent, des projets qui se retrouvent sans budget faute de votes favorables.

---

[25] https://bitinfocharts.com/top-100-richest-dash-addresses.html , https://tinyurl.com/yy9er3gv
[26] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html
[27] https://twitter.com/WeissRatings/status/1070019958908903424

Ce problème d'attribution budgétaire se double d'un autre problème, plus organisationnel celui-ci : pour le moment, la formule choisie pour le financement d'un projet consiste à payer tout ou partie du financement du projet et espérer que ce projet aboutisse. Inévitablement, certains projets n'aboutiront pas (ambitions trop grandes, incompétence, escrocs…) et se solderont par une perte sèche pour la communauté. Évidemment, lorsque certains cas limites se présentent, toute action en justice pour recouvrer les fonds indûment dépensés s'avère particulièrement complexe, la DAO de Dash n'ayant pour le moment pas d'existence juridique en tant que telle.

Ce problème devrait être au moins partiellement résolu avec la mise en place récente[28] de la Dash Investment Foundation[29] qui aura, elle, une personnalité juridique et pourra donc à la fois contracter et suivre les projets. Quant à la principale entité de la DAO Dash, une entreprise de droit américain nommée Dash Core, elle est déjà la propriété légale du réseau décentralisé et anonyme des masternodes, par l'intermédiaire d'un trust établi pour servir ses intérêts. Le personnel de Dash Core, dont son directeur Ryan Taylor, peut donc être révoqué par les masternodes.

Il est à noter que cette fondation et ce trust, entités réellement responsables des investissements auprès de ses actionnaires (la communauté Dash au travers de la DAO), établissent un lien entre le monde numérique des cryptomonnaies et le monde réel, gouverné par les lois communes et les codes juridiques habituels. Dash suit en cela la tendance qu'on peut observer dans certaines autres cryptomonnaies de fournir un socle concret à ses activités ; on peut évoquer ici Tezos, dont la fondation[30] est elle aussi bâtie afin d'offrir à la fois un véhicule juridique pratique pour la gestion des fonds qui lui sont confiés et une personne morale capable d'ester en justice ou, le cas échéant, d'y être poursuivie, ce qui —il faut être honnête — rassure l'investisseur particulier.

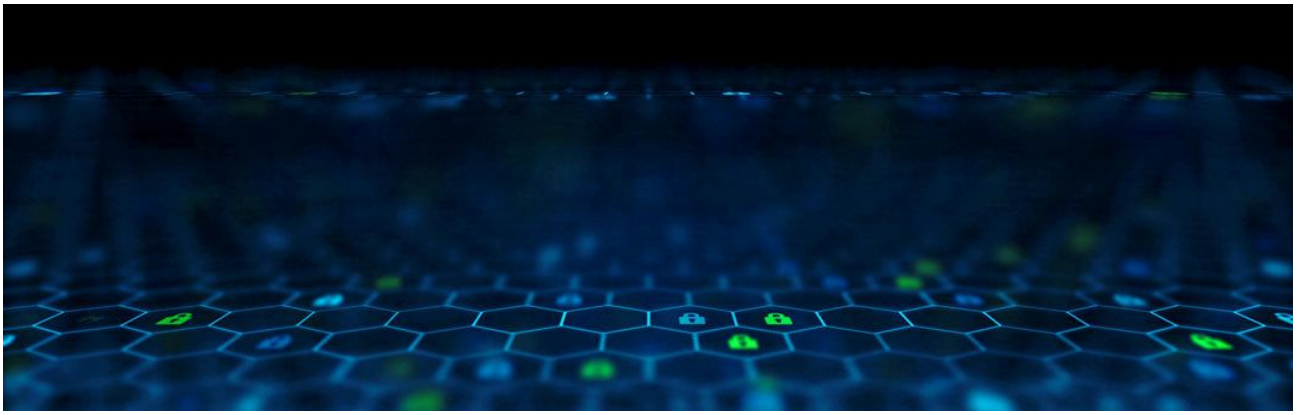
Des mises à jour parfois lentes

Comme toute organisation décentralisée, la mise à jour du réseau dépend essentiellement du bon vouloir de chacun des opérateurs.

Ceci aboutit parfois à des lenteurs dans la mise à jour, ces dernières devant se faire au rythme du plus lent des opérateurs, ce qui peut provoquer (comme ce fut le cas pour le passage à la version 0.12) l'interruption momentanée de certains services proposés par les nœuds. Si cela n'entraîne qu'une gêne temporaire pour un réseau qui est encore relativement jeune et faiblement utilisé, il en sera différemment lorsque Dash représentera une portion notable des paiements en cryptomonnaie dans le monde.

On notera cependant que la mise à jour vers la version 0.13 puis la version 0.14 se sont déroulés sans délai (à tel point que la vitesse de mise à jour a surpris même les habitués du réseau). Il est vrai qu'un opérateur trop lent à mettre à jour le nœud dont il a la charge court le risque de ne plus être rémunéré à court terme.

[28] https://twitter.com/DashFrance/status/1169177969882992640
[29] https://dashnews.org/fr/dash-lance-dash-investment-foundation-pour-etendre-les-opportunites-de-croissance/
[30] https://tezos.foundation/



Le futur de Dash

Une feuille de route déjà définie

Si le but global de Dash est clair, devenir une monnaie électronique globale, voire “la” monnaie mondiale de référence, les objectifs de plus court terme sont aussi relativement bien définis : une véritable feuille de route (roadmap) existe et peut même être consultée en ligne[31].

On y découvre ainsi que les prochains mois seront consacrés à améliorer encore le système de paiement pour permettre l’utilisation d’adresses nominatives de paiement, tendant à rendre un paiement sur internet aussi simple qu’un échange d’e-mail. Le prochain jalon, nommé Evolution, vise à faire de Dash “la cryptomonnaie la plus simple à utiliser de toutes”, afin que — je cite — « même ta grand-mère puisse s’en servir ».

Le marché potentiel est évidemment énorme, puisqu’on permettra notamment de “bancariser” de façon extrêmement simple tous ceux qui n’ont pour le moment pas les moyens ou les capacités d’obtenir un compte bancaire traditionnel (on pense ici à tous les pays en voie de développement, ou à tous les individus, mouvements ou entreprises privés de services bancaires pour raisons politiques par exemple).

Cette évolution devrait aussi permettre de fournir une alternative crédible aux solutions actuelles de transferts d’argent depuis les pays riches vers les autres (le mécanisme des “remittances internationales”, ces transferts effectués par les expatriés de pays pauvres dans les pays riches qui renvoient dans leur pays natal et à leur famille le produit de leur travail). On parle ici de sommes colossales qui deviennent instantanément plus simples et moins coûteuses à transférer, comparé à l’usage de transferts bancaires généralement complexes ou aux transferts via Western Union ou ses concurrents dont les services sont particulièrement coûteux.

Citons enfin l’introduction, dans les prochaines versions du protocol, de possibilités techniques de développer des applications décentralisées (les Dapps) à l’instar de ce qui se fait sur Ethereum. Ces

[31] Feuille de route officielle en français : https://www.dash.org/fr/feuille-de-route/

DApps[32] permettent de mettre à profit la puissance de calcul fournie par le réseau des noeuds participants soit pour des opérations spécifiques, soit pour l'établissement et la gestion de contrats "intelligents" (smart contracts)[33], soit pour le stockage d'informations décentralisé. Autant d'éléments qui, chacun, ouvrent de vastes opportunités de création de richesse et de services à forte valeur ajoutée.

Aperçu économique de Dash

Les principales forces et faiblesses de Dash ayant été parcourues, il est à présent utile de revenir sur les principes économiques sous-jacents aux cryptomonnaies en général et ceux de Dash en particulier, ce qui permettra de faire un peu de prospective.

Pour qu'une monnaie fonctionne dans le monde réel, elle doit couvrir trois besoins essentiels :

1. Permettre l'échange et servir de moyen de transaction.
2. Servir de mesure de compte.
3. Être capable de stocker durablement de la valeur.

On comprend aisément que si le point 1 et 2 sont actuellement faciles à remplir par les cryptomonnaies, le point 3 reste problématique en ce que la profondeur du marché concerné (i.e. la capacité de ce marché d'absorber des ordres d'achat ou de vente importants) est trop faible, ce qui entraîne de possibles manipulations, et une volatilité encore bien trop forte.

Un marché qui doit s'approfondir

Pour que ce troisième point puisse tenir, i.e. que la volatilité actuelle du marché s'amenuise et que la valeur soit convenablement stockée dans le temps, il faut que ce marché s'approfondisse, c'est-à-dire que la valeur stockée soit progressivement plus importante que la valeur présente dans les transactions au jour le jour. L'actuelle stabilité relative des monnaies en circulation est obtenue précisément parce que toute la monnaie n'est pas en circulation : une grande partie de la richesse créée n'est pas liquide et consiste en foncier, en capitaux investis durablement, en savoir-faire et en organisations dont les valorisations, vastement supérieures aux valeurs échangées quotidiennement sur les marchés, ont été établies grâce à l'épreuve du temps.

De la même façon, il faudra encore beaucoup d'investissement **sur la durée** et **dans l'économie réelle** pour donner au marché des cryptomonnaies une certaine profondeur.

On pourra arguer que les performances de Bitcoin sont assez problématiques dans ces deux points de vue : sur la durée, il n'est pas dit du tout que cette cryptomonnaie passe l'épreuve du temps compte tenu de ses limitations actuelles en terme de temps de traitement et du coût des transactions moyennes ; en terme d'économie réelle, on peine à voir comment une monnaie qui coûte si cher et prend autant de temps à se déplacer peut participer à édifier des entreprises et créer de la richesse…

[32] https://blog.dash.org/an-introduction-to-dash-platform-dapi-and-drive-9d080d6e89c9
[33] https://fr.wikipedia.org/wiki/Contrat_intelligent

Cet “approfondissement du marché Bitcoin” reste possible si la première cryptomonnaie abandonne toute velléité de devenir un jour une vraie monnaie mondiale pour ne plus se concentrer que sur une simple réserve de valeur, échangée exclusivement sur les plateformes de trading, ce qui modifie complètement sa nature même : puisque l’échange direct de Bitcoin (sans tiers centralisé, en pair à pair) devient progressivement trop lent et trop coûteux, il n’est plus directement échangeable qu’au sein de ces plateformes, et donc directement dépendant de ces systèmes éminemment centralisés, et qui deviennent de fait des tiers de confiance. Bitcoin peut, dans ce cadre, jouer le rôle d’une réserve de valeur et ces plateformes deviendraient alors l’équivalent de banques centrales. Mais on comprend qu’on est, dans ce cas de figure, aux antipodes du projet de Satoshi Nakamoto.

De ce point de vue, Dash compte en revanche parmi le fort petit nombre de cryptomonnaies capable de s’inscrire de façon effective sur ces deux tableaux : sur la durée d’abord, en ayant une vision de long terme claire et un parcours évolutif déjà clairement établi (la “feuille de route” joue ce rôle sur le court et le moyen terme et le but de devenir une vraie monnaie globale pour le long terme), et au plan de l’économie réelle en participant déjà à l’édification de projets concrets[34], grâce à son ingénieuse infrastructure financière.

Un nouveau modèle économique, équilibré ?

Et justement, la façon dont l’écosystème Dash est construit est, on l’a vu dans les paragraphes précédents, intéressante à plus d’un titre : permettant à la fois de résoudre les problèmes de gouvernance en fournissant la possibilité à différents acteurs et investisseurs de définir clairement les directions qu’ils désirent voir prendre par la cryptomonnaie, et à la fois de fournir un moyen de subventionner les projets, les développements et la maintenance de l’écosystème en lui-même, Dash réalise une intéressante performance économique qu’aucune autre cryptomonnaie n’a pour le moment réalisée.

Ce résultat est bâti sur l’expérience et les développements réalisés sur la cryptomonnaie de Satoshi Nakamoto : en termes économiques, Bitcoin représente en effet un équilibre très particulier entre les intérêts des différents acteurs. D’un côté, les utilisateurs de la monnaie ont intérêt à ce que celle-ci soit simple d’usage, sans tiers de confiance pour en conserver le prix d’usage le plus faible possible, et décentralisée pour éviter collusion et censure. D’un autre, les mineurs ont intérêt à miner les blocs pour à la fois bénéficier de la récompense par blocs, et assembler les transactions entre elles pour toucher les frais de transaction demandés pour les enregistrer. Mieux encore : les incitations des différents acteurs sont prises en compte dans l’établissement du consensus, rendant les attaques par collusion (attaques 51%)[35] très improbables.

On le comprend : dès sa conception, Bitcoin a bénéficié d’un rare équilibre entre les différentes incitations qui aboutissent à un système efficace sur lequel on peut effectivement bâtir une économie, l’échange de valeur devenant possible sans tiers de confiance.

Cependant, avec l’introduction d’un niveau supplémentaire, Dash introduit une part d’incertitude : s’il semble assez clair que l’équilibre du premier niveau n’est pas remis en question, quelles sont les

[34] https://twitter.com/DashFrance/status/1161515351949139968 , https://twitter.com/DashFrance/status/1155606012767944704
[35] https://fr.wikipedia.org/wiki/Attaque_des_51%25

garanties que l'introduction du second niveau, celui où opèrent les Masternodes, ne provoque pas des effets de bords dommageables ? On a vu dans les paragraphes précédents qu'avec les années écoulées, les menaces possibles (collusion de nœuds, typiquement[36]) ne se sont pas produites. Il semble pour le moment que non seulement ce second niveau n'a pas eu d'effet de bord détrimental sur Dash, mais a permis de découpler la production de blocs qui sécurisent les informations échangées des services spécifiques de paiement (rapidité de la transaction, fongibilité, anonymat).

Pour le moment, force est de constater que les résultats obtenus sont plutôt encourageants, et depuis, l'apparition d'autres cryptomonnaies utilisant elles aussi le principe de Masternodes (comme ZCoin, PIVX, Blocknet ou — de façon plus surprenante — la cryptomonnaie Monero avec son projet Tari[37]) tend à montrer que l'idée de base est séduisante et opérationnelle au-delà du simple cas Dash.

[36] https://www.youtube.com/watch?v=bz6rFZQywOE
[37] https://tinyurl.com/y4ppldu3

Conclusion

L'étude de Dash, son écosystème et sa communauté donnent un bon aperçu de ce qu'il est possible de réaliser dans le domaine des cryptomonnaies, en allant bien au-delà du schéma initial de l'expérience Bitcoin.

Pour autant qu'on puisse le dire au moment où ces lignes sont écrites (à l'été 2019), Dash a démontré possible l'émergence d'un écosystème équilibré, capable à la fois de résoudre ses problèmes de gouvernance et de s'autofinancer tout en respectant les règles de base des cryptomonnaies, à savoir la décentralisation, l'absence de tiers de confiance, la transparence des transactions et l'impossibilité de les censurer.

D'autres cryptomonnaies tentent actuellement de résoudre les différents problèmes qui se posent depuis l'avènement de Bitcoin : outre la gouvernance de ces projets décentralisés et sans leader clair, on retrouve ainsi les problèmes de montée en charge, d'anonymat, de fongibilité, de financement de la maintenance et de la R&D. Pour le moment, si Dash n'a bien sûr pas encore résolu intégralement chacun de ces problèmes, il a apporté des solutions crédibles et innovantes qui laissent penser que cette cryptomonnaie est globalement sous-évaluée.

Nul ne peut dire quelle sera "la" crypto de demain ; Dash a cependant de bons atouts et sa communauté en est un vrai : une structure permettant de jeter des passerelles juridiques et économiques entre réseau décentralisé et monde réel, un esprit plus positif que bien d'autres communautés de cryptos, un modèle économique pertinent qui permet d'envisager une évolution avec beaucoup moins d'à-coups que d'autres.

Dash est peut-être une crypto de plus, mais c'est certainement plus qu'une crypto : c'est un écosystème aux solides perspectives d'avenir.