BeΔCHAIN

Fondements théoriques

Que ce soit dans le monde physique des hommes ou dans celui, numérique, des 0 et des 1, il n'existe pas de système organisationnel neutre : tout système organisationnel reflète une pensée technique, sociale, politique à l'oeuvre. Derrière chaque système il y a toujours une certaine vision du monde. Certaines visions sont plus verticales qu'horizontales (hiérarchies, strates, organisations pyramidales), d'autres plus centralisées que décentralisées (concentrations, gouvernements, élites).

Blockchain n'échappe pas à la règle. De fait il existe plusieurs blockchains (Bitcoin, Ethereum, Lisk, Hyperledger, Tendermint...) qui, toutes, proposent un mode organisationnel non-neutre, chacune présentant des variantes de structures tendant soit vers la centralisation ou la décentralisation, vers l'horizontalité ou vers la verticalité.

Dans un article récent, Vitalik Buterin, le fondateur d'Ethereum, pose en préambule que «*All blockchains have a notion of* ***history*** *- the set of all previous blocks and the order in which they took place - and the* ***state*** *- "currently relevant" data that determines whether or not a given transaction is valid and what the state after processing a transaction will be*». (fr.scribd.com/doc/314477721/Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains). Selon lui, toutes les blockchains portent à la fois les notions d'**historique** (la position et le contenu des blocks précédents) et d'**état** (les datas décrivant la validité d'une transaction et son résultat).

Reporté au monde physique des hommes, ce concept d'**historique+état** couplés est au fondement même de l'*organisation administrative comme système* : untel est à la fois *ce qu'il est* (son identité : nom, prénom, date de naissance, adresse...) et en même temps *d'où il vient* (enfant de tel et telle, eux-mêmes né-e-s de tels et telles). Pouvoir (et surtout vouloir) retracer à tout moment la généalogie d'un être, d'un objet, d'un événement, est un signe typique des systèmes organisationnels verticaux de contrôle : on doit pouvoir relier les choses entre elles non pas pour ce qu'elles sont intrinsèquement en elles-mêmes (leur *ipséité*, ce qui les distingue et les différencie les unes des autres) mais dans tout un process d'affiliation et de jeux de causes et de conséquences : ceci a produit cela.

Cette vision administrative a ses propres raisons et surtout sa propre histoire ; confronté très tôt à des volumes de populations de plus en plus importants (l'Empire romain couvrait des territoires immenses pour l'époque), le pouvoir central a nécessairement besoin d'identifier chaque être par tout un dispositif permettant de le désindividualiser : ce qu'est l'individu en soi (ipséité) n'a effectivement de sens que là où il se trouve, là où il est connu et reconnu ; sitôt qu'on s'éloigne de sa *zone de reconnaissance* (son village, sa famille, sa tribu, son activité) il est vital de pouvoir le définir autrement sous peine d'être incapable de l'intégrer dans la machinerie administrative en charge de gérer l'intégralité des êtres placés sous sa juridiction.

Avec l'industrialisation au XIXème siècle on effectue un saut à la fois qualitatif et quantitatif. Elle implique la concentration urbaine : des milliers puis des millions d'inconnus vont quitter leurs *zones de reconnaissance* pour s'agréger dans des ensembles sociaux (villes) où leur définition administrative doit muter sous peine de devenir rapidement inefficace et incapable de mener sa mission. On invente alors les pièces d'identité. La carte d'identité est un document décrivant mon ipséité (nom, prénom, sexe, date de naissance, adresse, photo...) mais, et chacun en a fait l'expérience au moins une fois, elle ne peut être obtenue que si *ma généalogie peut être reconstituée sans aucun doute*

possible : fils de untel et de unetelle, eux-mêmes né-e-s tel jour à tel endroit de untels et unetelles… Mon état est d'être ce que dit ma pièce d'identité et mon *histoire* est ce qui permet d'établir mon *état*. Comme le font Bitcoin ou Ethereum. Ainsi, en posant le couple **histoire+état** comme fondement de ce qu'est blockchain, on ne fait que reproduire un système administratif tel qu'en vigueur au moment de leur création. Sans les questionner on reproduit à l'identique les méthodes de gouvernance en cours.

Est-ce une nécessité ? Est-ce une contrainte ? Est-ce une obligation ? Oui et non.

Oui, parce que nous n'avons pas d'autres modèles pour nous guider dans nos démarches de conceptions que ceux qui nous entourent et qui ont fait la preuve de leur efficacité dans une certaine durée. Non, parce que nous pouvons aussi considérer que cette façon non-neutre d'envisager un système organisationnel est datée : elle a correspondu à une façon de voir et à une façon de faire à une époque où, probablement, il était impossible de faire autrement.

Entre temps est apparu un bouleversement mondial : l'irruption du numérique. Par ses outils, par ses méthodes, par ses protocoles (dont nous n'avons de loin pas fini d'explorer les conséquences tant au niveau technique que social ou politique) le numérique disrupte des pans entiers de nos sociétés, et en disruptera de plus en plus dans les années qui viennent. Parmi toutes ces disruptions, l'une d'elle revêt un caractère très particulier : l'abolition des *distances physiques*. Un simple exemple l'expliquera en profondeur : jusqu'à une époque très récente (moins de 20 ans) il était techniquement impossible de demander l'avis des gens sur de nombreux sujets ; on a donc inventé la démocratie représentative où des partis proposent pour un temps donné (mandature) de réaliser ceci ou cela au nom du peuple tout entier (scrutin majoritaire) ; une fois élu, ses représentants - qui sont donc aussi les nôtres - appliquent (ou pas) ce qu'ils ont promis de faire. Si la population n'est pas satisfaite elle peut changer d'équipe dirigeante au tour suivant (alternance). La *distance physique* (l'impossibilité dans ce cas de demander l'avis de tous sur chaque question) a donc produit le jeu d'outils techniques permettant de s'en affranchir. En la supprimant, le numérique pourrait permettre de le faire très facilement (e-démocratie, e-citoyenneté) et donc de rendre obsolète ce jeu d'outils techniques désormais devenu sans raison.

De la même façon, le couple **histoire+état** qui est à la base de nos identités administratives n'a plus guère d'utilité ni de sens dans la mesure où nos *identités numériques* nous permettent d'exister de plusieurs façons en différents endroits et dans différents contextes. Là aussi nous sommes loin d'avoir fait le tour des disruptions politiques, techniques et sociales que ceci induit. On peut par exemple imaginer le monde comme un immense village planétaire où chacun viendrait se définir non pas comme *né de* (histoire de notre être physique/corporel/biologique) mais comme *faisant ceci avec untel ou untel* (état social d'êtres impliqués dans des systèmes relationnels, qu'ils soient sociaux, économiques, politiques, culturels, …). C'est ce que, comme solution blockchain, se propose de faire ***beAchain***.

Un monde sans histoire ?

L'homme est un animal *aeconomicus* rationnel ; il réfléchit en permanence en terme de risque/profit. Si vous apercevez une pièce de 10 cts sur l'autoroute sous un flot ininterrompu de voitures lancées à 130 à l'heure, le profit (aller la récupérer) comparé au risque est nul. Si vous cherchez un emploi vous envoyez des CV : le risque est nul et le profit potentiellement élevé.

On ne fait certes pas que ça, mais on le fait beaucoup et souvent. Par exemple quand on détient une information on la partagera ou pas en fonction de notre évaluation du couple risque/profit : si je la partage je prends le risque de voir sa valeur - et donc mon profit - diminuer (par exemple un trader qui peut gagner des millions de dollars sur une seule information… la partager c'est ne pas les gagner) ; inversement, si je la garde elle peut me faire gagner moins qu'en la distribuant (par exemple si j'organise

un événement j'ai intérêt à le faire savoir). Il y a donc en permanence une stratégie de gestion tendant à la réduction du facteur risque et à l'augmentation du facteur profit. Rien de très nouveau... quand au néolithique un type tout seul s'attaquait à un auroch le profit était immense mais le risque aussi. Mieux valait s'y mettre à 10 ou 15, le risque était moindre et le profit le dépassait encore. En revanche, chasser l'auroch à 200 ne présente certes plus aucun risque, mais plus aucun profit non plus.

Il existe donc un ratio optimisé entre ces deux facteurs en deçà et au delà duquel toute action perd son sens. Ce ratio est à la base du process blockchain global. Pour obtenir un niveau de profit garanti, on doit tendre à un niveau de risque proche de zéro ; si le risque est égal à zéro alors le profit est immédiat. Comment maintenir le niveau de risque à zéro ? en couplant **histoire+état**. Ne pouvant modifier l'historique (chaîne de blocks se confirmant les uns les autres séquentiellement) il est inutile d'essayer d'en modifier l'état (falsifier un block) pour en tirer profit.

Le profit, dans les blockchains «classiques» (Bitcoin, Ethereum), réside donc dans la *gestion de l'histoire* ; en confirmant que la transaction en cours est conforme à l'historique, les *miners* reçoivent du profit. Ils sont payés pour ce travail. Ce faisant ils ré-historicisent en permanence le système organisationnel tout entier pour en maintenir l'administrabilité. Ceci est rendu nécessaire et obligatoire non pas parce que en soi blockchain l'exige, mais parce chaque utilisateur de la blockchain est un *homo aeconomicus* qui pèse le coût du risque et celui du profit ; quiconque tenterait, en y mettant les moyens qu'il faut, de modifier les états à son profit y parviendrait très facilement s'il n'y avait pas toute cette *gestion de l'histoire comme garantie ultime*. C'est donc parce que il y a dès le départ une «gestion de l'histoire posée comme garantie» qu'on a besoin de minage : ce n'est pas le problème qui crée sa solution mais la solution initiale qui génère son propre problème.

beAchain est une solution blockchain sans histoire... Elle n'est constituée que d'**états**. Comment est-ce possible et pourquoi est-ce possible ? Parce qu'elle est une blockchain orientée objets. Ce ne sont pas des humains qui fixent les conditions de son fonctionnement mais des machines connectées.

Une machine ne réfléchit pas en termes de risque/profit. Sans conscience de soi le risque est toujours égal à zéro et le profit sans sens : avoir telle série de 1 et de 0 plutôt qu'une autre ne signifie rien *en tant que machine*. La machine est donc honnête par définition. Ce qui est honnête ou malhonnête, c'est ce qu'on lui demande de faire : moins on peut lui en demander (et donc plus elle réalise par elle-même) plus le risque de fraude est réduit. L'idéal est d'arriver à ce que l'utilisateur humain ne puisse rien faire d'autre que *concevoir un profit* (imaginer, créer, inventer une utilisation) et *en bénéficier au final* une fois le process terminé, sans n'avoir jamais la possibilité d'intervenir directement dans le process en cours. C'est la base conceptuelle de ***beAchain***.

beAchain *pourrait* historiciser les transactions si cela avait un sens, mais ça n'en a aucun... ce qui a un sens, ce sont les états. Plus exactement l'état de chaque machine connectée en un moment T. ***beAchain*** est un «village de machines sociales» où chacun se connaît et où chacun sait déjà presque tout sur tout le monde (voir texte BEACHAIN-village-machines.pdf). Presque tout mais pas tout : les machines sont donc *contraintes de collaborer* pour réaliser une transaction. Elles sont «sociales» parce que si une machine lui parle, n'importe quelle machine répondra. Contrairement aux humains il n'y aucune évaluation du risque/profit. Si un fou furieux vous adresse la parole dans la rue il est préférable de ne pas répondre car le risque est alors très supérieur au profit. Vous tenez compte, dans la relation sociale qui s'engage à ce moment-là, de signes (d'états) qui vous permettent d'évaluer le ratio risque/profit. En revanche si un inconnu vous demande dans quelle direction se trouve la gare, tout risque est quasiment absent et le (petit) profit est supérieur : vous avez fait une bonne action en aidant un étranger perdu. Dans le monde social *il n'est pas nécessaire d'historiciser pour réaliser* : vous ne demandez ni à l'étranger - ou par curiosité ou par politesse - d'où il vient, ni au fou ce qui l'a mis dans

cet état-là. Si en revanche vous êtes un agent administratif ce n'est plus une relation sociale qui s'instaure mais une relation administrative technique : cet étranger est-il en règle, ce fou représente-t-il une menace ? La réalisation (ce qui advient ensuite) passe alors nécessairement par un faisceau de preuves validées par d'autres instances administratives. C'est donc le contexte de l'échange (qui vous êtes, qui est l'autre ?) qui fixe ses modes possibles de réalisation.

Historiciser une transaction, c'est la désocialiser. C'est lui retirer l'horizontalité décentralisée qui est dans sa nature même d'échange direct d'individu à individu pour l'inscrire dans un registre vertical centralisé. Que ce registre soit établi par un agent administratif ou par un *miner* ne fait aucune différence, l'inconnu reste un inconnu et il est dépossédé de son rôle d'acteur social transactionnel : les *miners* décident pour lui si sa requête est valide ou pas.

A l'inverse, ***beAchain*** considère une transaction comme un moment social où s'exprime une *double positivité* : la richesse collective produite équivaut aux richesses individuelles produites. Chaque machine participant de façon aléatoire (donc équitablement) aux consensus validant (ou pas) les transactions en cours, il n'y a ni centre ni lieu de pouvoir ni équation risque/profit autre que le *profit de tous* par le *profit produit par la garantie* d'un process juste, loyal et fiable. Le facteur risque/profit n'est plus individualisé, il est mutualisé : plus nous savons, moins nous risquons et plus nous bénéficions. La fiabilité de ***beAchain*** est garantie par le fait que nul utilisateur humain ne peut y trouver où réaliser un profit indu contre un risque minime.

Du néolibéralisme en blocks

La théorie néolibérale repose sur l'idée que la réussite individuelle sert le collectif *par conséquence* : elle présuppose que le profit généré par le risqueur (entrepreneur par exemple) sera indirectement redistribué après coup par la partition des richesses qu'il aura produite : la part principale du profit récompense le risqueur et la part restante, nécessairement moindre, sera allouée à la société dans laquelle il s'inscrit. De longs débats secouent régulièrement les sociétés pour discuter de la part revenant à chacun, toujours trop faible dans ce qu'il conserve pour le risqueur et bien sûr toujours trop pour le reste de la société. Trouver un équilibre satisfaisant les uns et les autres occupe donc la plus grande partie des activités sociales et politiques des sociétés. Cette répartition entre risqueurs et sociétés n'est pas naturelle, elle n'est pas liée au bon vouloir des uns et des autres : elle est régie par des règles administratives contraignantes. Trop contraignantes ou pas assez est un débat classique.

La forme économique «moderne» des échanges sociétaux n'a donc pu exister que parce que *simultanément* s'est développée une administration pour assurer que le partage sera réalisé selon les règles qu'elle institue. C'est parce que l'Etat-nation fixe les règles que le jeu est possible. L'idéal néolibéral serait que la part reversée au collectif soit la plus faible qui soit, parce que trop élevée elle accroît le rapport risque/profit : elle tend à préférer ne pas risquer et gagner peu (assistanat) que risquer et perdre gros (lire Hermando De Soto). Du coup l'économie, et, partant, toute la société, n'exploiterait pas ses potentialités au mieux. Du point de vue administratif c'est l'inverse : pour «faire société» tout groupe humain doit mettre en place des méthodes de solidarités internes quelles qu'elles soient. Personne n'a raison ni n'a tort : comme dit dans la première phrase : il n'existe pas de système organisationnel neutre : tout système organisationnel reflète une pensée technique, sociale, politique à l'oeuvre. Derrière chaque système il y a toujours une certaine vision du monde.

Le gouvernement d'une blockchain de type Bitcoin fonctionne un peu de la même façon : pour que le système organisationnel puisse assurer sa fonction, le risqueur/*miner* doit dégager un profit supérieur au risque : le risque c'est le coût d'investissement en matériel informatique toujours plus élevé, le profit ce sont les bitcoins générés qui l'enrichissent (incitation). La «part minimum» (redistribution

des profits) reversée à la société (les utilisateurs) c'est la validation de leurs transactions. On a donc un système économique parfaitement huilé où les uns gagnent sur la demande de travail des autres. La gouvernance assure que le retour minimal des profits sur la société des utilisateurs (validation) est assuré - en ce sens Bitcoin «fait société» - tout en permettant aux risqueurs (de moins en moins nombreux parce que l'investissement matériel est de plus en plus lourd) de dégager des profits de plus en plus élevés par la hausse constante du cours du Bitcoin.

Que Bitcoin ou Ethereum (fondé par un ex-bitcoiniste sur les mêmes fondamentaux idéologiques et techniques) rencontrent le succès qu'on sait est normal dans la mesure où elles reproduisent à l'identique le schéma général des sociétés desquelles elles sont issues. Pour preuve l'émergence quasi-quotidienne de start-ups dédiées à leur interfaçage avec les utilisateurs, leurs besoins et leurs attentes. Que ce schéma général soit atemporel, éternel et à validité permanente est une toute autre question.

Un autre monde est-il possible ?

beAchain s'inscrit dans un tout autre schéma, celui porté par une constellation d'expérimentations allant des fablabs aux communs et de la co-construction aux auto-organisations. Notre conviction : ce qui dorénavant fera sens et créera de la valeur (économique, humaine, sociale...) c'est le réseautage horizontal, le partage de pair à pair et la participation de tous, et que l'ensemble de l'énergie produite étant supérieur à la somme des énergies individuelles, la richesse collective partagée est supérieure à l'ensemble des richesses individuelles additionnées. Le risque est abordé collectivement et le profit redistribué intégralement. Les machines dialoguent, échangent, collaborent et valident les transactions non pour leur bien propre (ni risque ni profit) mais pour le bien commun exclusif de la collectivité des utilisateurs.

beAchain est horizontale et disponible à tout un chacun sans connaître aucun code ni aucun langage informatique, sans intermédiaires ni besoin de matériel performant. Toutes les machines connectées ont le même rôle, le même statut (pas de *miners*, pas de profits, pas de risques) et les mêmes fonctions ; toutes peuvent créer des contrats, monter des événements, construire des projets, partager des datas et valider des transactions de façon strictement égalitaire.

Bitcoin est un très beau projet. Ethereum est un autre très beau projet, notamment dans sa dimension DAO/ordinateur global. Sauf que... sauf que les organisateurs d'événements, les monteurs de projets, les expérimentateurs de nouvelles méthodes d'organisations ne toucheront jamais que la «part minime» et les *miners* la part principale de la richesse produite. Plus vous travaillez, concevez, imaginez, expérimentez, créez, plus d'autres s'enrichissent. Il y a là quelque chose de non-éthique qui n'est *économiquement réaliste* que dans une lecture purement néolibérale des systèmes organisationnels sociétaux. C'est pourtant initialement cela que blockchain, dans sa conception théorique même, a pour ambition, pour mission et pour horizon de dépasser.

Ces nouveaux tiers de confiance que sont les *miners* (vous leur faites confiance parce qu'un process consensuel s'établit entre eux lors de chaque transaction) font perdurer les anciens modèles d'organisations verticales centralisées ; si les datas ne le sont pas (DLT), l'organisation de leur gestion l'est encore. Blockchain reste donc encore entièrement à inventer.

Une communauté de machines

En tant que *communauté de machines* ***beAchain*** est plus proche, sociologiquement parlant, de la communauté villageoise que de la communauté urbaine.
Une communauté urbaine (administrée, centralisée) permet à des centaines de milliers ou de millions

d'individus de produire la possibilité de «faire société» ensemble. Elle permet à certains de ne pas produire parce que l'effet de masse assure la production collective minimale nécessaire au bon fonctionnement. A l'inverse, une communauté villageoise (tribale, familiale) auto-définit ses règles et requiert que tous travaillent - même si certains travaillent plus que d'autres - parce qu'il n'y a pas cet effet de masse dans la production minimale nécessaire. Ne pas avoir d'effet de masse ne signifie pas que cette communauté ne puisse pas atteindre ce seuil critique - et donc que ***beAchain*** ne soit limitée qu'à quelques milliers de machines - mais que l'absence d'administration centralisée contraint à répartir ses missions à l'ensemble des unités qui en assurent tour à tour les fonctions. Ce n'est pas une question de taille mais de rôles : selon leurs compétences propres (plus ou moins bien connectées, plus ou moins puissantes, plus ou moins occupées) toutes les machines donnent ce qu'elles peuvent donner. La relation risque/profit produite par la spécialisation verticale (minage) est alors remplacée par la coopération horizontale.

La façon dont on produit détermine ce qu'on produit

La spatialisation aléatoire des machines dans le volume virtuel 3D ***beAchain*** (espace social d'existence des machines) définit des *points de densité* et des *points de dilution* dans l'espace commun entraînant une temporalisation des échanges allant de quelques micro-secondes à 1 ou 2 secondes. Les *points de densité* sont des lieux où l'on trouve une grande concentration de machines : les machines approbatrices en charge de valider toute demande de transaction étant nombreuses, choisir algorithmiquement lesquelles seront concernées et lesquelles ne le seront pas se fera très rapidement. Inversement les *points de dilution*, espaces moins peuplés, nécessiteront d'aller faire appel à des acteurs plus éloignés pour boucler un cycle de validation (position en x,y et z + ou - 1, 2, 5...) ce qui retardera très légèrement le processus. Un point dense (par exemple 200 machines au même endroit) réalisera 10 ou 20 transactions simultanées alors qu'un point dilué (1 seule machine = 1 habitant/km^2) requérera un appel distant (+100 m, +1 km, +10 km) pour réunir les machines concernées. Les *relations sociales* (même lieu, même toit) entre machines, dans leurs dialogues et leurs échanges, influent directement sur la productivité du système global. Le but n'est pas d'*atteindre la plus grande vitesse* mais *la plus grande fiabilité* : n'étant pas minée, ***beAchain*** peut assurer plusieurs milliers de transactions/seconde. La fiabilité du consensus est donc entièrement celle de la confiance que les machines ont les unes vis-à-vis des autres. Ce n'est pas un point de vue conceptuel : pratiquement parlant, chaque machine fait confiance à celles qui lui sont les plus proches. *Network is Trust* : le réseau *est* la confiance.

Les blockchains «classiques» ont un tout autre fonctionnement. En l'absence de «ce que l'autre sait de moi» (fondement de ***beAchain***) les *miners* doivent donc s'assurer que untel (un inconnu par définition) a historiquement le droit d'opérer telle ou telle transaction. *Ni l'historicisation ni le Proof-of-Work ne sont donc des obligations* liées à blockchain, ce sont des obligations liées à une certaine vision sociale, politique et relationnelle de ce qu'est blockchain, ses protocoles et ses fonctionnalités.

beAchain se propose d'expérimenter ces nouveaux territoires communs et ces nouvelles façons d'envisager les relations sociales au partage, que ce soit un partage de projets, d'informations ou de richesses.