DOCUMENT DE TRAVAIL DT/2018-01

Blockchain et pays en développement : vers une technologie maîtrisée ?

Marc RAFFINOT

Mathieu RAFFINOT

UMR DIAL 225
Place du Maréchal de Lattre de Tassigny 75775 • Paris •Tél. (33) 01 44 05 45 42 • Fax (33) 01 44 05 45 45
• 4, rue d'Enghien • 75010 Paris • Tél. (33) 01 53 24 14 50 • Fax (33) 01 53 24 14 51
E-mail : dial@dial.prd.fr • Site : www.dial.ird

Blockchain et pays en développement : vers une technologie maîtrisée ?

Marc Raffinot
Université Paris-Dauphine, PSL Research University,
IRD, LEDA [UMR 225], DIAL, 75106 Paris, France
marc.raffinot@dauphine.fr

Mathieu Raffinot
CNRS/LaBRI, Université de Bordeaux, France
mathieu.raffinot@labri.fr

9 janvier 2018

Résumé

Les technologies liées à la blockchain sont omniprésentes dans les média mais leur fonctionnement est souvent peu compris et les attentes vis-à-vis de ces technologies sont parfois déconnectées de la réalité. Le domaine du développement ne fait pas figure d'exception, nous le montrons en décrivant tout d'abord plus en détails les technologies liées aux blockchains, puis nous comparons leurs possibilités vis-à-vis des besoins dans ce domaine et faisons apparaître les limites d'application. Enfin, sans revenir sur les limites de la vision technocratique en rapport des besoins réels, nous proposons des pistes technologiques complémentaires aux blockchains mais mieux adaptées au processus de développement, en introduisant la notion d'hébergeur de blocs.

Abstract

Blockchain technologies are very popular, but the way they actually work is often not really understood. Expectations are sometimes disconnected from reality. This is true in the field of application of these technologies to developing countries. We show it by i) describing the details of the blockchain technologies ii) comparing their potentialities with the determinants of development and iii) showing the limitations of the blockchain technologies to boost development. We then present technological devices additional to blockchains better suited to the development process by introducing the notion of "blocks host".

JEL classification : G29, L14, L17, 016, 019, 031
Keywords : blockchain ; pays en développement ; crypto-monnaies ; systèmes financiers ; droits de propriétés ; hébergeur de blocs.

1 Introduction

Les technologies liées à la blockchain occupent en ce moment le devant de la scène. Il ne se passe pas une journée sans qu'un article de journal soit consacré au sujet, que ce soit à propos des cybermonnaies comme le Bitcoin, le Ripple ou l'Ether et d'autres plus confidentielles (il en existe actuellement plus de 1000) mais aussi à propos des possibilités de la blockchain en matière de disruption dans certains domaines comme l'assurance ou la gestion des droits d'auteur. Dans le domaine du développement aussi, les blockchains semblent pouvoir apporter leur lot de merveilles, comme le mythe du père Noël remis à l'heure des réseaux.

Cependant, si en apparence et dans certains contextes très spécifiques l'apport des technologies liées à la blockchain peut être déterminant, nous montrons dans cet article les limites de cette vision technocratique vis-à-vis de la réalité du développement, mais proposons aussi des pistes technologiques pour mieux en appréhender certains points critiques.

En premier lieu, pour mieux comprendre ce que cachent ces technologies nous commençons par en expliciter les principes fondateurs. Nous aurons atteint notre but sur ce point s'il ressort bien de nos explications qui se veulent simples sans être simplistes qu'il n'y a pas qu'une technologie mais un panaché de technologies et que toutes, sans exception, sont expérimentales.

Ensuite, nous tentons d'évaluer l'apport potentiel de ces technologies pour favoriser le développement des pays pauvres.

Enfin, nous proposons des pistes pour adapter/simplifier certaines de ces technologies pour obtenir un système technologique mieux adapté au monde du développement et à ses acteurs, basé sur une nouvelle notion d'hébergeur de bloc.

Mais avant d'entrer dans des considérations plus pointues, présentons tout de suite une notion technique centrale pour la cryptographie par ordinateur, la fonction de hachage. C'est une fonction qui prend un document (un article, une liste de transactions, etc) en entrée et calcule un (long) entier dit clef de hachage. En voici un exemple : `2c9c12e886bf174cd1ca183754b85c996a`, stocké sous format hexadécimal (base 16). Ce qui est important est que la fonction soit telle (a) que l'on ne sache pas créer des collisions, c'est-à-dire écrire (ou calculer) deux documents qui aient la même clef de hachage et (b) que l'univers des clefs soit suffisamment grand pour que la probabilité que deux documents pris au hasard aient la même clef soit quasiment nulle. Il existe de grandes familles de clefs de hachage, historiquement Md5, SHA-1, SHA-2, SHA-256. La première utilisée toute seule n'est plus considérée comme sûre, SHA-1 est la plus utilisée actuellement mais est en passe d'être remplacée par SHA-256 dans les prochaines années.

2 La blockchain, un panaché de technologies

La blockchain répond en apparence à des principes généraux (technologie distribuée, sécurité, confiance) qui sont issus de sa conception libertaire et qui viennent à l'esprit automatiquement lorsque la notion de blockchain est évoquée. Cependant, nous verrons par la suite que beaucoup de ces principes ne sont pas respectés ou le sont seulement très partiellement.

2.1 Une technologie distribuée

Pour échapper à une quelconque mainmise d'un acteur sur un autre, cette technologie est pensée distribuée, c'est-à-dire sans centre clairement défini, comme un réseau. Le système informatique fonctionne sur les ordinateurs (dit serveurs) de différents agents autonomes (les noeuds du réseau), qui doivent se mettre très régulièrement d'accord, c'est-à-dire obtenir un consensus, sur plusieurs points : (a) le temps (b) le codage des transactions (c) l'historique des transactions.

La difficulté du consensus dans un monde distribué est un point d'algorithmique – l'étude de la manipulation des données dans le monde informatique – étudié depuis les années soixante. Ce problème est posé dans de nombreux contextes, notamment (i) si un agent doit demander une permission pour participer au réseau ou non (ii) si les agents se connaissent entre eux ou non, (iii) la manière dont un agent peut entrer/se retirer du réseau et, point très important, (iiv) si un agent peut être malicieux ou non, notamment en mentant, mais aussi en essayant de détruire d'autre nœuds du réseau, et si c'est le cas quelle est la fiabilité de la blockchain sur ce point, ce qui est souvent traduit par un pourcentage d'agents malveillants au dessous duquel la blockchain peut continuer de fonctionner sans "casser".

2.2 Une technologie sûre d'un point de vue informatique

La blockchain est voulue sûre (ou robuste) de différents points de vue, dont voici les plus communs : (1.a) résistance aux pannes : quel pourcentage d'agents peuvent arrêter de fonctionner sans casser son fonctionnement ? (1.b) la résistance aux agents malicieux, évoquée plus haut, (1.c) la garantie que les transactions ou informations sont enregistrées de manière irrévocable, (1.d) la garantie qu'une transaction a été enregistrée avant une autre et que cet ordre perdurera.

Les points (1.a,b,c,d) sont résolus dans la plupart des technologies blockchain de la manière suivante : les transactions sont encodées à intervalles réguliers (environ 10" pour le bitcoin) dans un bloc de données qui est ensuite inséré dans une chaîne de blocs, dite "blockchain". Cette chaîne est répliquée et maintenue par tous les agents autonomes.

Pourquoi chaîne et non simple suite de blocs ? À chaque nouveau bloc, une clef de hachage (c.f. introduction) est calculée, qui sera insérée dans le bloc suivant. Ainsi, si un agent malicieux essaye de corrompre un bloc, il lui faudrait corrompre toute la suite de la chaîne sur toutes les copies des agents.

La question du consensus prend alors tout son sens : comment décider qu'un nouveau bloc proposé est valide et soit accepté comme tel par tous les autres agents ? Et comment faire pour limiter l'impact qu'un groupe d'agents malicieux aurait s'il venait à proposer un nouveau bloc corrompu ?

Pour mieux comprendre le cœur du système de sécurité en œuvre dans une blockchain, utilisons une analogie, limitée, mais qui en illustre bien le principe : un ensemble de locataires décident de sécuriser leur immeuble, en commençant par en sécuriser les entrées. Ils peuvent faire appel à une société de gardiennage spécialisée (immeuble A). Mais ils peuvent aussi choisir une solution alternative et installer un système de vidéo-surveillance réparti dans chaque appartement relié à une caméra sur l'entrée (immeuble B).

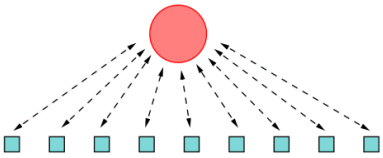

FIGURE 1 – Immeuble A, la société A (cercle rouge) est en relation bilatérale avec l'ensemble des locataires (carrés bleus). La société A ne prend pas l'information des locataires, mais directement des capteurs dans l'immeuble.

Dans le premier immeuble, la sécurité est assurée par un agent extérieur A suivant une prestation contractuelle qu'il faut rémunérer. La société A est par ailleurs soumise à des lois sociales et financières strictes qui l'obligent à facturer ses prestations au dessus d'un certain prix minimum. La confiance des locataires en leur sécurité dérive directement de leur confiance dans ce principe de sécurité ainsi que dans l'entreprise spécifique de surveillance choisie. En cas de visiteur indésirable, la réaction de la société A, typiquement envoyer quelqu'un sur place, est relativement lente, car A est une société extérieure.

Dans l'immeuble B, la sécurité est assurée par chaque locataire qui a en théorie un intérêt

propre à le faire : sécuriser ses biens et par conséquence les biens de tous car il ne peut pas savoir vers qui se dirige un éventuel malfaiteur. Le coût est bien moindre que pour l'immeuble A et provient du coût de l'installation et de son entretien.

Supposons maintenant qu'un nouveau locataire s'installe dans chacun des immeubles, appelons ces locataires LA et LB.

Le locataire LA peut dormir tranquille tant (a) qu'il a confiance dans la société A pour le protéger, indépendamment des autres locataires, et (b) qu'il peut payer les charges afférentes aux services de la société A.

Pour LB, c'est moins clair. Sa sécurité lorsqu'il n'y veille pas lui même dépend des autres locataires. C'est une sécurité distribuée. Imaginons maintenant le scénario le plus simple, tous les N locataires de l'immeuble B surveillent tout le temps l'entrée. A chaque entrant, il faut obtenir un consensus entre locataires surveillants l'entrée pour décider si un entrant est un malfaiteur ou non, c'est-à-dire un vote 0 ou 1. Comme LB ne connaît pas ses voisins, il doit se fier à leur vote. Si plus d'un certain pourcentage de ses voisins sont en fait des malfaiteurs complices d'un cambrioleur entrant, il ne sera pas dénoncé lors de son entrée et LB sera possiblement cambriolé. La sécurité de la porte d'entrée s'effondre. Quel pourcentage exactement ?

On serait tenté de dire plus de 50% simplement. Mais en fait pour répondre à cette question, il faut s'intéresser plus en détail à la technique du système de surveillance. Si l'immeuble contient un petit nombre de logements, on peut imaginer un système centralisé de l'information, sans panne possible. Tous les appartements sont reliés à un point central et l'information est directement partagée par tous. Alors 50% est juste. Mais si l'immeuble est très grand, 1000 logements par exemple, la centralisation de l'information devient problématique, et des pannes vont se produire, qui peuvent être aussi une inversion d'un vote – malveillant ou non – ainsi que la non transmission de l'information par un locataire. Les appartements, dits nœuds, sont alors reliés les uns aux autres suivant un réseau décentralisé et l'information ne peut circuler qu'à travers ce réseau. Le problème du consensus dans la plus simple des configurations distribuée est appelé en informatique le problème des généraux byzantins [12]. Il est prouvé dans ce cas de figure que le système de consensus ne résistera pas à plus de 1/3 (environ 33.3%) de locataires malveillants. C'est peu dans beaucoup de cas, notamment celui des crypto-monnaies.

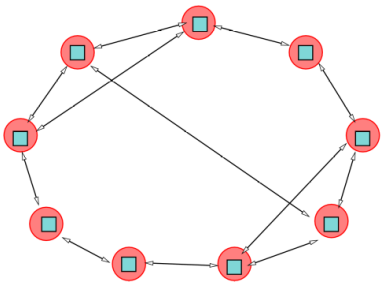

FIGURE 2 – Immeuble B. Les locataires manipulent eux-mêmes l'information qui leur arrive par le réseau.

Comment faire pour augmenter ce pourcentage ou s'en accommoder ? Différentes stratégies sont à l'œuvre dans les blockchains, et c'est pour cela qu'il est difficile de parler d'une technologie, et qu'il faudrait parler plutôt d'un ensemble de technologies.

La technologie la plus simple est de sécuriser le système en s'assurant de manière extérieure la probité relative des locataires. Par exemple, en supposant que ce soit possible, en demandant un extrait de casier judiciaire. Seul ceux qui ont un casier pas trop lourd peuvent venir habiter dans l'immeuble. C'est une blockchain que nous appellerons **privée** ou **permissioned**. Dans ce cas, le problème des 33% est moins problématique, et peut même descendre, la sécurité est assurée par un système informatique couplée à une protection extérieure. C'est le choix fait par le système montant de transactions inter-banques Ripple [18]. Il n'est techniquement résistant qu'à 20% d'agents malicieux ou en panne, mais ce n'est pas un point vraiment critique car la probité relative est fortement renforcée par la permission accordée ou non d'entrer dans le système. Le projet hyperledger [13] est un grand projet open source mis en place pour faciliter la création de blockchains privées.

Il est beaucoup plus dur de faire monter ce pourcentage dans le cas d'un système ouvert, où des agents peuvent entrer et sortir de la blockchain sans contrôle. Un premier moyen M1 est d'intéresser les agents au résultat du consensus d'une manière ou d'une autre. Un deuxième moyen M2 est de pondérer les votes en fonction de l'intérêt supposé d'un agent dans la sécurité du système. Typiquement, dans le cas des crypto-monnaies, il est raisonnable de supposer que plus un agent est riche, plus il a intérêt à ce que la blockchain perdure. Un troisième moyen M3 est d'exiger des agents une "preuve de travail" (proof of work), c'est-à-dire qu'un vote ne sera accepté que si l'agent prouve qu'il a "bien travaillé" pour voter. D'autres principes plus confidentiels ont été proposés et sont en "rodage", comme par exemple le système Tangle de la crypto-monnaie IOTA [15] ou encore Corda [4] et de nouveaux systèmes sont proposés régulièrement, à la recherche du bon compromis entre sécurité, calcul, stockage, vitesse, scalabilité et bien sûr usage.

Bitcoin se base sur un mélange de M1 et M3, et M3 consiste pour cette blockchain particulière en la résolution de calculs informatiques. Le vote du premier agent qui satisfait M3 est validé et il reçoit un intéressement en bitcoins. Cette action des agents, dite de "minage" est énergivore.

Ethereum se base sur M1 et M2. Plus un agent a d'intérêts dans le système, plus son vote sera pris en compte et sa participation au système sera rémunérée en Ethers.

Perfectionnons maintenant notre système de surveillance ! Nous installons des caméras dans chaque recoin, permettant de retracer tous les parcours d'une personne dans les couloirs, d'une porte d'appartement ou d'entrée/sortie P1 vers une porte d'appartement ou d'entrée/sortie P2. Ces caméras nous permettent aussi de compter le nombre de sacs ou de valises que transporte cette personnes, que nous appelons V.

Un parcours d'une personne de P1 vers P2 portant V valises est une transaction notée (P1,P2,V). Chaque porte de l'immeuble est bien sûr numérotée.

Nous voulons stocker l'ensemble des parcours des personnes dans le couloir à des fins de vérifications en cas d'enquête. A noter que le locataire ne connaît pas les autres locataires derrière les portes. Et pour nous défendre d'agents malveillants, qui pourraient par exemple effacer un parcours a posteriori ou rajouter un parcours qui n'a jamais eu lieu, nous voulons un stockage aussi sécurisé que possible.

Dans l'immeuble A, c'est à la société A d'assurer le stockage sécurisé de cette information. Elle utilisera la plupart du temps une base de données cryptée, qui suivant l'enjeu peut être redondante (avec copies sur plusieurs sites), sauvegardée régulièrement sur bandes, gravée sur disques inviolables (comme du pyrex) mis dans un coffre. Nous touchons à des problèmes de sauvegarde sécurisée qui sont largement étudiés depuis des années et pour lesquels des solutions pratiques existent. Le coût de ces solutions sont à la hauteur du coût de la perte des données. Les banques utilisent ce type de solutions, qui sont fournies en général clefs en main par de très grands acteurs du monde de la base de données comme Oracle ou IBM.

Dans l'immeuble B, c'est beaucoup plus dur. Chaque transaction doit être avalisée par l'ensemble des agents et les transactions passées ne doivent pouvoir ni être modifiées, ni ajoutées, ni supprimées. La solution retenue dans la plupart des blockckains et toutes les blockchains ouvertes que nous connaissons est que chaque agent possède une copie de toutes les transactions passées. C'est un premier point qui limite fortement le passage à l'échelle en terme de nombre de transactions de cette technologie.

Nous pouvons stocker toutes les transactions une après l'autre, mais cela implique beaucoup de transferts de messages, de calculs, et aussi de temps par transactions. En général, ces transactions sont agrégées sous forme de bloc.

Chaque agent stocke tous les blocs, soit. Mais cela ne suffit pas, loin s'en faut. Il faut maintenant empêcher qu'un agent ou groupe d'agents malicieux ne puisse changer le passé et pour commencer les blocs de transactions qu'il stocke ! Pour cela, la technique utilisée est quasiment la même sur toutes les blockchains. Le dernier bloc est "haché" et le code résultant, dite clef de

hachage (c.f. introduction), est stocké dans le bloc suivant, et ainsi de suite, pour former une chaîne de blocs stockée par chaque agent.

Attention, dans un système non centralisé, tous les agents qui le veulent peuvent participer à la création d'un nouveau bloc et le proposer aux autres comme le nouveau dernier bloc de la chaîne. Un agent peut donc recevoir plusieurs nouveaux "derniers" blocs encodant possiblement des transactions différentes, certains pouvant être malicieux, et il doit en choisir un. C'est à cette étape que les principes M1, M2, M3 trouvent leur importance. Le système doit garantir qu'à terme, (a) la chaîne est unique pour tous les agents et (b) que toutes les transactions ont bien été enregistrées dans un bloc, seul moyen de garantir leur validité.

Nous n'entrerons pas plus dans les détails dans le cadre de cet article. Il faut cependant bien être conscient que la complexité de ce système provient directement de la non centralisation des données, qui à son tour est à la base de la robustesse du système et de la grande confiance des utilisateurs dans le système. Les blockchains sont des points d'équilibre entre ces différents paramètres.

2.3 La confiance

Revenons sur l'aspect fondamental des blockchains, celui de la confiance. Cette technologie donne confiance pour de bonnes et de mauvaises raisons. Le fait qu'elle ait été crée en réaction à l'effondrement de la confiance dans le système traditionnel bancaire suite à la crise de 2008 est déjà un capital confiance en soi, indépendamment de la manière dont est construit le système.

Ensuite, le fait qu'elle est soit censée être contrôlée par la "société civile" est un point rassurant aussi vis-à-vis de potentiels agents malveillants gouvernementaux. Mais il est nécessaire de garder en mémoire que la sécurité d'une blockchain est assurée par ses agents à condition qu'ils y trouvent un intérêt.

La traçabilité des transactions est aussi un fort facteur de confiance. Chacun peut vérifier l'ensemble des transactions, c'est-à-dire dans notre immeuble B l'ensemble des parcours des visiteurs de porte à porte. Cette propriété, si elle est souvent perçue comme une transparence inspirant confiance, est le plus souvent utilisée comme un moyen de surveillance et d'enquête de la part des autorités (comme par exemple la douane pour les crypto-monnaies) ou par les créateurs de la blockchain, comme ce fut le cas lors du premier "casse" sur la blockchain Ethereum en 2016, pour annuler certaines opérations litigieuses [1]. Dans ce dernier cas, cette décision a fortement scindé la communauté, affaiblissant la sécurité globale de la blockchain Ethereum.

La notion de communauté de développement participe aussi à la confiance que des utilisateurs accordent aux blockchains, à l'instar de la confiance dans un logiciel libre qui dérive le plus souvent de la taille et de l'activité de ses développeurs et utilisateurs. Pourtant, une étude rapide montre que ces communautés sont loin d'être homogènes, dépendent souvent d'un petit noyau dur de programmeurs phares, parfois un ou deux seulement, sans lesquels le futur même de la blockchain devient hasardeux. Par exemple, Ethereum sans Vitalik Buterin semble avoir actuellement peu de chance de survie.

De nouvelles approches et communautés apparaissent régulièrement essayant d'améliorer la sécurisation mais aussi de formaliser la prise de décision en cas de problèmes/piratages/bugs dans le programme à la base de la blockchain. C'est le cas par exemple de la blockchain Tezos [5] qui a récemment défrayé la chronique par une ICO (Inital Coin Offering - vente publique de jetons ou tokens ayant une valeur dans la future blockchain) d'un montant record avant toute preuve de fonctionnement réel de la blockchain !

2.4 Les limites technologiques

Les limites technologiques actuelles des systèmes à base de blockchain sont nombreuses.

La première d'entre elle est le passage à l'échelle, non en nombre d'agent, mais en nombre de transactions pouvant être codées dans des blocs en un temps donné. Cette limite provient directement de la nécessité de copie distribuée des blocs sur tous les acteurs dans le cas de blockchain ouvertes.

Le pourcentage d'acteurs malveillants en est une autre, notamment le nombre d'acteurs participant au "minage". Dans le cas du bitcoin par exemple, ce nombre se réduit à cause de la consommation énergivore et du rendement de plus en plus faible de l'opération. Moins nombreux ou géolocalisés de manière proche (pour le bitcoin toujours, plus de la moitié des mineurs actuels se trouvent maintenant en Chine), ces acteurs peuvent plus facilement décider de s'entendre ou être forcés par une organisation (un gouvernement par exemple) à le faire. D'ailleurs, un calcul du prix à payer pour un gouvernement pour faire chuter le bitcoin a été estimé aux environs de 350 millions d'euros en 2016 [8].

2.5 Les limites communautaires

Les communautés qui soutiennent telle ou telle blockchain sont diverses, évoluent, se séparent, se reforment, en des temps assez courts, parfois à l'échelle d'un an par exemple. Ces communautés d'utilisateurs sont nécessaires pour assurer la sécurité de la blockchain, et parmi chacune de ces communautés les programmeurs qui contribuent au développement et à l'évolution du code sont cruciaux, d'autant plus qui sont peu nombreux. Et leur état d'esprit au moment de la création de la blockchain et son évolution sont à prendre en compte. Ce sont très souvent des sortes de divas de la programmation, animés le plus souvent par des sentiments libertaires. A ce titre ce sont souvent les premiers maillons faibles de la sécurité, non pas de la blockchain en exécution, mais de son futur ! Ce qui fait d'ailleurs penser au directeur du Media lab du M.I.T. Joichi Ito que la récupération de cette technologie dans son entier par les banques est irréaliste [11].

Il est nécessaire de garder en mémoire (a) que ces technologies sont expérimentales et (b) que l'organisation et la structuration de la communauté autour l'est aussi. Il ne se passe pas un mois sans qu'un bug soit découvert dans un smart-contrat Ethereum, avec des impacts malheureux importants en termes financiers.

3 Blockchain et aide au développement

Les opportunités (réelles ou fantasmées) créées par les blockchains, ont engendré des attentes importantes, et très diverses, dans le domaine du développement [16]. C'est notamment le cas au sein des institutions d'aide au développement. D'une manière générale, on attend des blockchains une réduction très sensible des coûts de transactions ainsi qu'une accélération de la rapidité des transactions et une amélioration de leur traçabilité permettant de développer des registres incontestables. Beaucoup d'analystes placent leurs espoirs dans l'idée que les blockchains permettront le contournement de l'Etat bureaucratique et des élites corrompues, considérées comme les principaux obstacles à la croissance de l'investissement.

Ainsi, par exemple, dans le domaine du financement des pays du Sud, on attend une réduction des coûts de transferts associée à une transparence des transactions, aussi bien de l'aide publique au développement (Le Start Network a été constitué pour exploiter les opportunités en ce domaine) que des transferts de personne à personne comme ceux des travailleurs émigrés.

La distribution de l'aide pourrait ainsi se faire directement des budgets (ou des individus) des pays industrialisés vers des personnes ciblées dans les pays en développement, ou vers certaines

lignes budgétaires spécifiques. En associant ce transfert international avec les systèmes de transferts conditionnels en espèces, cela pourrait permettre des transferts directs vers les personnes pauvres dans les pays en développement.

On éviterait ainsi les Etats, éliminant ainsi la bureaucratie et la corruption. Il existe toutefois un problème à ce niveau, puisque cela reviendrait à substituer un système piloté par les donateurs à un système contrôlé par des organismes publics du Sud, ce qui serait certainement perçu comme une pratique néo-coloniale.

Pourtant, cette idée séduisante n'est pas aussi simple à mettre en pratique qu'il pourrait le sembler. S'il s'agit de dons, le problème demeure le ciblage des bénéficiaires. La difficulté à ce niveau a déjà conduit au développement récent de l'aide distribuée au hasard, en fonction de certaines caractéristiques (du village, de la période, etc.) : c'est le cas par exemple de l'ONG GiveDirectly [10]. Mais l'utilisation de moyens électroniques de transfert n'élimine pas la nécessité d'aller sur le terrain identifier les bénéficiaires. Dans le domaine des prêts, les systèmes qui se présentent comme mettant en place des prêts de personne à personne (Kiva, Babyloan) ne sont pas capables de réaliser ce genre de transactions sans passer par des institutions de micro-finance au sud qui se chargent d'opérer le suivi de l'activité et des recouvrements.

Les blockchains sont aussi censées faciliter la constitution de systèmes financiers plus solides et plus inclusifs [2]. Certains voient dans les crypto-monnaies un moyen d'éliminer l'argent liquide, encore largement utilisé dans les pays en développement, et notamment par les commerçants et le secteur informel en général. La confiance pourrait naître ici du fait que ces monnaies ne sont pas soumises aux manipulations des banques centrales ou des États. Toutefois, des vols électroniques restent possibles, ce qui réduit l'intérêt de ces crypto-monnaies par rapport à un dépôt classique dans le système bancaire qui bénéficie d'une assurance, comme le soulignent Jérôme Mathis et Daniel Ouedraogo [9]. L'argument doit toutefois être relativisé, car les commerçants préfèrent actuellement l'argent liquide aux dépôts bancaires malgré les risques bien réels de vols ou de destruction (de nombreux marchés ont brûlé ces dernières années en Afrique de l'Ouest, consumant dans les flammes le capital de nombreux commerçants).

Les blockchains constitueraient la technique permettant d'approfondir la tendance déjà très perceptible en Afrique à l'utilisation des téléphones portables comme support de transactions financières. L'exemple le plus souvent cité est celui de Mpesa au Kenya, qui permet des paiements par téléphone portable et les remboursements d'emprunts auprès des institutions de microfinance. Les choses sont moins avancées en Afrique francophone, mais le développement d'Orange Money et d'autres systèmes similaires en Afrique de l'Ouest constituent des avancées dans le même sens. A ce niveau, les blockchains permettraient surtout de renforcer la sécurité, même avec des téléphones peu sophistiqués. Toutefois, des exemples récents ont montré que des manipulations ne sont pas impossibles, même avec cette technique [6].

Un autre domaine dans lequel on attend beaucoup des blockchains est celui de de la clarification des droits de propriété. Suite aux travaux du prix Nobel d'économie Douglass North, l'idée que le développement est lié au respect des droits de propriétés est devenue une référence dans le domaine. Cela porte aussi bien sur les droits formels que sur les droits d'occupation informels. Parmi les droits de propriété, la plus évidente lacune dans les pays en développement concerne les droits fonciers.

Ces derniers sont particulièrement importants pour les pauvres, qui ne disposent souvent d'aucun titre sur les parcelles qu'ils occupent (par exemple dans les bidonvilles, comme l'a montré De Soto dans le cas du Pérou).

C'est dans ce domaine que l'apport potentiel des blockchains est le plus souvent mentionné. Effectivement, dans beaucoup de pays africains, l'enchevêtrement des droits communautaires et de systèmes formels largement pénétrés par l'indivision rend souvent complexe l'établissement de droits de propriétés incontestables, ce qui ralentit ou décourage l'investissement.

Un système fondé sur les blockchains permettrait de constituer une base de données sur les droits fonciers qui ne pourrait pas être manipulée, et d'enregistrer les transactions sans avoir besoin d'un système public ou même de notaires. Anand, McKibbin et Pichel [3] soulignent que les avantages d'un tel système seraient aussi importants en termes d'authentification de la date de transaction, de reconstitution du registre en cas de désastre naturel (à condition que les autorités acceptent que la base de données soit détenue en dehors du pays), de preuve inviolable des droits de propriété – avantages qui pourraient être complétés par l'utilisation de "colored coins" pour enregistrer les détails qui prendraient trop de mémoire pour être enregistrés dans la blockchain.

Toutefois, la blockchain en soi ne résout pas tous les problèmes. Bien des contestations en Afrique naissent de la question de savoir qui est légitime pour attribuer des droits. L'Etat est souvent le propriétaire éminent de la terre, mais en pratique, l'attribution de droits est généralement effectuée à partir de droits traditionnels inextricablement emmêlés. Il faudrait donc commencer par clarifier cette question, qui soulève toujours des problèmes complexes, surtout quand la pression foncière fait monter la valeur potentielle des terres. Certains projets se sont attachés à effectuer cette clarification, qui montrent que les choses à ce niveau ne peuvent progresser que très lentement si l'on veut impliquer toutes les parties. C'est sans doute pourquoi les projets entrepris, notamment au Honduras et au Ghana, ne semblent pas avancer aussi rapidement qu'espéré initialement.

De plus, l'idée souvent mise en avant est qu'un registre de droits (un cadastre) bien tenu et non manipulable par les pouvoirs centraux et locaux devrait permettre le développement d'un marché de la terre. Grâce à ce marché, les producteurs les plus efficaces pourraient acheter la terre aux moins efficaces et le système bancaire pourrait alors accorder des prêts en prenant des terres comme garantie.

En soi, l'idée est un peu naïve, car le fait que les droits de propriété soient vérifiables et opposables ne signifie nullement que le système bancaire va les considérer comme des garanties suffisantes pour accorder des prêts. Pour que ce soit le cas, encore faudrait-il que les saisies de terre ne fassent pas l'objet de contestations ou de soulèvements. Les expériences menées jusqu'ici se sont révélées décevantes. Même lorsque des titres de propriété ont été distribués, pratiquement aucun crédit bancaire n'a été accordé (la valeur d'un titre de propriété situé dans un bidonville n'est pas forcément facile à valoriser). A l'extrême, comme au Cambodge, la distribution de titres de propriété a eu comme impact l'expulsion par la force des nouveaux "propriétaires" et leur relogement dans des endroits éloignés de leurs activités [16].

C'est plutôt du côté de l'assurance que des perspectives pourraient être les plus prometteuses. Dans les pays en développement, le défaut de système d'assurance est bien souvent ce qui empêche les producteurs ou les nouveaux entrepreneurs de prendre des risques en lançant de nouvelles activités. Récemment, AXA a lancé grâce aux blockchains une assurance automatique pour les billets d'avion [7]. Cela pourrait sans doute se faire aussi pour les assurances agricoles de récolte (des systèmes existent, mais ils peinent à se développer), l'automaticité du système garantissant l'absence de contestation (une application du concept de contrat intelligent).

Les opportunités offertes par les blockchains sont également potentiellement importantes dans le domaine de la gouvernance, par exemple pour déterminer le résultat des élections. Toutefois, là aussi, les choses ne sont pas aussi simples qu'il pourrait le sembler. Lors de récentes élections, les gouvernements ont purement et simplement supprimé l'utilisation d'internet dans leur pays pour quelques jours. Dans les pays où règne au mieux un autoritarisme à façade démocratique, le recours à la violence directe reste une tentation pour les détenteurs du pouvoir (généralement associée au déni de réalité ou "mensonge déconcertant").

Dans le domaine de la distribution de l'aide attribuée aux gouvernements, le fait de pouvoir suivre chaque euro depuis son point de départ jusqu'à son bénéficiaire final [17] rendrait sans doute beaucoup plus difficile la corruption qui réduit souvent les sommes qui arrivent ef-

fectivement. Bien sûr, cela renforcerait la transparence, mais il faut encore que les donateurs éventuellement mécontents aient la volonté et le pouvoir d'assainir la situation – ce qui n'est pas toujours le cas.

Par ailleurs, mettre en place des techniques à base de blockchains suppose des infrastructures adéquates, des réseaux d'ordinateurs et de serveurs mis en place par du personnel formé. Les techniques sont souvent très chères, il faudrait donc les subventionner de l'extérieur, ce qui repose le problème de la dépendance par rapport aux bailleurs de fonds.

Et puis, de manière encore plus terre à terre, les blockchains les mieux établies supposent des consommations énormes d'énergie, notamment pour le calcul de "proofs of work", une étape vitale pour la sécurité. Ceci poserait des problèmes dans des pays à faible revenu où les fréquentes coupures d'électricité créent des problèmes aussi bien aux personnes qu'au fonctionnement des entreprises. La consommation d'énergie pour le calcul et le refroidissement des serveurs peut atteindre des montants insoutenables [14] (même si par ailleurs, les blockchains trouvent de nombreuses applications dans le domaine de l'énergie, notamment pour faciliter la connexion des énergies renouvelables).

4 Vers un système adapté ?

La technologie des blockchains semble se développer inexorablement, peu importe que tous les paramètres techniques ne soient ni compris ni maîtrisés. Il apparaît cependant que seules quelques blockchains "mères" comme celle de la société privée Ethereum servent de support à la plupart des smart-contrats. Appelons les des hébergeurs de blocs.

La confiance en ces hébergeurs est grande, à la hauteur de la défiance de particuliers envers une certaine finance avide à l'origine de la crise de 2008. Cependant, si cette nouvelle confiance n'est pas censée être aveugle grâce à l'apport de la cryptographie, elle pose de nombreux problèmes, notamment de persistance. Que vont devenir le Bitcoin ou Ethereum d'ici quelques années ?

La situation dans le domaine du développement n'est pas du tout similaire à celle de la finance, sur deux points fondamentaux : (a) la confiance dans les grands acteurs du développement (par exemple ONU, FMI, Banque mondiale, Union Européenne, OCDE) reste forte, et (b) certains sont d'importants bailleurs de fonds. L'enjeu technologique des blockchains dans ce domaine n'est pas de les éviter, mais plutôt de rendre plus transparente la répartition des aides une fois versées à différents organismes, ONG, gouvernements.

Sans revenir sur la partie 3 de cet article qui illustre les limites du point de vue technocratique par rapport à la réalité et la complexité du domaine du développement, d'un point de vue technique il n'est pas nécessaire que les acteurs du développement voulant utiliser des blockchains s'en remettent à des solutions expérimentales privées du type Ethereum ou Bitcoin. Pourquoi chercher à tout prix à décentraliser dans un domaine largement centralisé du fait de la concentration des principales sources de financement, avec la complexité technique et l'absence de maîtrise des paramètres techniques qui en découlent, sans même tenir compte de la consommation énergétique qui en découle ?

On peut très bien imaginer qu'un très petit nombre de grandes institutions du développement crée un hébergeur de blocs, sous la forme technique d'une base de données sécurisée et répliquée entre ces acteurs qui auront la maintenance en charge. Les gains seront en scalabilité (économies d'échelle) et soutenabilité (persistance). En scalabilité parce qu'un système de ce type permet de gérer un nombre de transactions bien plus rapidement qu'une blockchain répartie sur un très grand nombre d'acteurs, en persistance parce que les acteurs principaux de ce service seraient des institutionnels.

Références

[1] Eric Albert : Après un "cyber-casse", la technologie blockchain se cherche un avenir, June 2016. http://www.lemonde.fr/economie/article/2016/09/26/apres-un-cyber-casse-la-technologie-blockchain-se-cherche-un-avenir_5003434_3234.html.

[2] Collomb Alexis et Sok Klara : "Blockchain" : une révolution monétaire et financière ?, 2017. https://www.cairn.info/revue-l-economie-politique-2017-3-page-70.htm.

[3] Aanchal Anand, Matthew McKibbin et Frank Pichel : Colored coins : Bitcoin, blockchain, and land administration, March 2016. https://www.ubitquity.io/home/resources/worldbank_land_paper_ubitquity_march_2016.pdf.

[4] Richard Gendal Brown, James Carlyle et Ian Grigg et Mike Hearn : Corda : An introduction, 2016. https://docs.corda.net/_static/corda-introductory-whitepaper.pdf.

[5] Benjamin Canou, Grégoire Henry, Pierre Chambart, Fabrice Le Fessant, Cagdas Bozman, Vincent Bernardoff, Guillem Rieu, Mohamed Iguernlala, Alain Mebsout Ocamlpro et Arthur Breitman : Tezos : the OCaml Crypto-Ledger. OCaml'2017, septembre 2017. https://hal.inria.fr/hal-01661696.

[6] Joseph Clark : Le détournement de 50 millions de dollars sape à la base l'émule du bitcoin, June 2016. http://www.agoravox.fr/tribune-libre/article/le-detournement-de-50-millions-de-182063.

[7] Delphine Cuny : Retard d'avion : Axa lance une assurance automatique sur la blockchain, Septembre 2017. https://www.latribune.fr/entreprises-finance/banques-finance/retard-d-avion-axa-lance-une-assurance-automatique-sur-la-blockchain-750202.html.

[8] Jean-Paul Delahaye : Une épée de Damoclès sur le bitcoin, Août 2016. http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/.

[9] Jérôme Mathis et Daniel Ouedraogo : Et si le bitcoin remplaçait le franc cfa ?, 2018. http://www.lemonde.fr/afrique/article/2018/01/05/et-si-le-bitcoin-remplacait-le-franc-cfa_5238029_3212.html.

[10] GiveDirectly : Givedirectly operating model, 2017. https://www.givedirectly.org/operating-model.

[11] Joi Ito : Why i'm worried about bitcoin and the blockchain, Février 2016. https://www.coindesk.com/joi-ito-worried-bitcoin-blockchain/.

[12] Leslie Lamport, Robert Shostak et Marshall Pease : The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, juillet 1982.

[13] The linux Foundation : Hyperledger, 2017. https://www.hyperledger.org/.

[14] Christopher Malmo : A single bitcoin transaction takes thousands of times more energy than a credit card swipe, March 2017. https://motherboard.vice.com/en_us/article/ypkp3y/bitcoin-is-still-unsustainable.

[15] Serguei Popov : The tangle, 2017. https://iota.org/IOTA_Whitepaper.pdf/.

[16] Katherine Purvis : Blockchain : what is it and what does it mean for development ?, January 2017. https://www.theguardian.com/global-development-professionals-network/2017/jan/17/blockchain-digital-technology-development-money.

[17] Association Raptim : How technology can improve humanitarian aid, Octobre 2017. https://www.raptim.org/how-technology-can-improve-humanitarian-aid/.

[18] David Schwartz, Noah Youngs et Arthur Britto : The ripple protocol consensus algorithm, 2014. https://ripple.com/files/ripple_consensus_whitepaper.pdf.