Chaîne de blocs

Libérer le potentiel révolutionnaire de la technologie des chaînes de blocs pour le développement humain

LIVRE BLANC

IDRC | CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Chercheur et auteur
Raúl Zambrano
raul@ictdegov.org
Expert international en matière de technologie et de développement, New York

Révision et soutien à la recherche
Ruhiya Kris Seward et **Phet Sayo,** administrateurs de programme principaux du programme Économies en réseaux du Centre de recherches pour le développement international (CRDI).

Conception
Claudio Mendonca
ccmdesign.ca

Les auteurs souhaitent remercier Katie Clancy et Allie Wilson pour la correction d'épreuves et le soutien à la conception de ce livre blanc.

Août 2017

Les travaux de recherche présentés dans la présente publication ont été réalisés grâce à une subvention du CRDI, établi à Ottawa, au Canada. Les opinions exprimées ne représentent pas nécessairement celles du CRDI ni de son Conseil des gouverneurs.

Table des matières

ABRÉVIATIONS

Apprép	Applications réparties
CCP	Cryptographie à clé publique
DNS	Système de noms de domaines
GLR	Technologie de grand livre réparti
OAD	Organisation autonome décentralisée
ODD	Objectifs de développement durable
PI	Propriété intellectuelle et protocole Internet
TIC	Technologies de l'information et de la communication
TIC-D	Technologies de l'information et de la communication au service du développement

FIGURES ET TABLEAUX

Résumé

Dees technologies, vieilles comme nouvelles, propulsent la vague actuelle d'innovation partout dans le monde. L'intelligence artificielle, la robotique et l'apprentissage machine gagnent du terrain et sont déployés dans une grande variété de contextes à l'échelle mondiale. Une technologie plutôt énigmatique, mais dont on entend souvent parler, est la chaîne de blocs, une technologie émergente développée dans le cadre du bitcoin, une cryptomonnaie inventée en 2008. Alors que les innovations dans les domaines de l'intelligence artificielle et de la robotique semblent avoir un côté sombre, de nombreuses personnes considèrent les chaînes de blocs comme une plateforme pour un changement positif, voire révolutionnaire.

Dans le cas des pays en développement, le degré élevé de sophistication et les exigences complexes du point de vue de l'infrastructure (bande passante, connectivité et coûts d'exploitation élevés) de cette technologie pourraient présenter un défi pour ceux qui souhaitent jouer un rôle actif au lieu de se contenter d'être des utilisateurs finaux et des consommateurs. Pour les pays de l'hémisphère Sud, il est essentiel d'étudier la pertinence des nouvelles technologies pour combler les écarts socioéconomiques et soutenir l'atteinte des cibles de développement convenues à l'échelle internationale, ce qui comprend les objectifs de développement durable (ODD). Les pays en développement doivent non seulement se demander comment ils peuvent y parvenir, mais aussi qui exploitera les technologies de chaînes de blocs afin de combler les écarts de développement, de favoriser l'inclusion sociale et de promouvoir la gouvernance démocratique.

Le présent livre blanc explore le potentiel de la technologie des chaînes de blocs pour le développement humain dans les pays en développement. La première partie (après le résumé) présente un aperçu non technique des chaînes de blocs.

On présente ensuite la gamme d'applications dans les domaines et les secteurs de développement du point de vue des biens publics et privés. La troisième partie porte sur l'utilité réelle des chaînes de blocs dans les pays en développement. Le livre blanc se termine par une série de recommandations concernant les travaux de recherche supplémentaires et les programmes de développement potentiels fondés sur les technologies de chaînes de blocs.

Dans les annexes, on décrit le cadre de Technologies de l'information et de la communication au service du développement (TIC-D) et l'on présente les technologies de chaînes de blocs selon une approche technique.

Le présent document porte sur les applications des chaînes de blocs autres que les cryptomonnaies. On y met donc l'accent sur l'utilisation de la technologie des chaînes de blocs comme plateforme d'application générique dans les pays en développement.

RÉSUMÉ

TECHNOLOGIE DES CHAÎNES DE BLOCS

La chaîne de blocs est une des technologies de base sous-jacentes du bitcoin, la première cryptomonnaie décentralisée poste à poste à avoir connu du succès dans l'histoire. Comme plateforme financière, le bitcoin nécessite l'utilisation d'un grand livre numérique pour l'enregistrement de toutes les transactions.

La chaîne de blocs est la technologie qui fournit un tel grand livre et permet d'enregistrer toutes les transactions effectuées dans le réseau de la cryptomonnaie. Les chaînes de blocs, auxquelles le bitcoin faisait initialement ombrage, se sont imposées comme une technologie autonome pouvant être déployée dans des secteurs autres que financiers.

Pour les profanes, **on peut définir les chaînes de blocs comme étant une feuille de calcul publique qui enregistre dans l'ordre les transactions entre les utilisateurs d'un même réseau poste** à poste décentralisé. Une copie à jour des données est stockée dans chaque noeud de réseau, puis est mise à jour de manière automatique dans tous les noeuds.

Complément d'information

Vous souhaitez en savoir davantage à propos des chaînes de blocs ?

Consultez l'annexe II à la page 59 pour obtenir une explication plus approfondie.

Une des grandes innovations des technologies de chaînes de blocs est la manière dont les écritures sont liées entre elles. Chaque rangée contenant un bloc de transactions est liée à la rangée précédente au moyen d'un identificateur unique. L'identificateur unique du bloc précédent est utilisé pour générer celui du nouveau bloc, ce qui crée un lien mathématique entre les blocs de la chaîne. La modification ou la suppression d'une rangée dans la base de données est pratiquement impossible, puisqu'il faudrait pour cela changer toutes les écritures de la chaîne.

L'ajout de rangées aux données nécessite le consensus des noeuds, ce qui est possible à l'aide d'un algorithme de preuve de travail que les noeuds doivent utiliser. La preuve de travail ressemble au casse-tête classique qui consiste à deviner le chiffre, avec un niveau de complexité beaucoup plus élevé toutefois. Le résultat de la preuve de travail est diffusé aux noeuds du réseau, qui le valident ensuite. Une fois la validation effectuée, le bloc est ajouté au bloc de chaînes existant.

La technologie des chaînes de blocs utilise des outils cryptographiques. Dans un premier temps, chaque identificateur unique de bloc est un hachage des entrées fournies. Le bloc de transactions compris dans chaque bloc est aussi le résultat d'une opération de hachage. Ensuite, tous les noeuds et les utilisateurs doivent se servir d'une cryptographie à clé publique pour être intégrés au réseau et interagir entre eux. Il n'est pas nécessaire de créer un profil ou de fournir des renseignements personnels, ce qui contraste fortement avec la façon dont les plateformes de médias sociaux fonctionnent.

Caractéristiques principales de la technologie des chaînes de blocs

- Confidentialité
- Pseudo-anonymat
- Intégrité
- Confiance et gouvernance réparties
- Transparence
- Sécurité
- Durabilité
- Code source ouvert

Problèmes et limitations liés aux chaînes de blocs

- Extensibilité
- Taille de bloc limitée
- Coûts d'exploitation élevés
- Impact environnemental
- Centralisation du minage
- Large bande passante nécessaire
- Utilisabilité
- Complexité
- Recours à la cryptographie
- L'immuabilité est un frein

APPLICATIONS DES CHAÎNES DE BLOCS

Il n'est pas facile de se tenir au courant des innovations et des progrès relatifs aux chaînes de blocs, car ce domaine change rapidement à l'échelle mondiale. Nous nous attarderons dans ce document à la manière dont cela se déroule dans les pays en développement. Du point de vue du développement, l'introduction des concepts de biens privés et de biens publics et leur fourniture par les secteurs public et privé sont essentielles. Le présent livre blanc met en lumière les développements de chaînes de blocs en relation avec ces deux types de biens et services.

Dans la plupart des économies en développement, les gouvernements sont, en principe, les principaux fournisseurs de biens publics, qu'il s'agisse de justice et de sécurité, ou encore de santé et d'éducation, pour ne nommer que ceux-là. Cela ne signifie pas pour autant que les gouvernements fournissent eux-mêmes ces biens.

La plupart du temps, cette mission est impartie à des partenaires privés à but lucratif et sans but lucratif. Voilà comment les technologies de chaînes de blocs sont déployées dans la plupart des pays en développement.

Les domaines et les secteurs touchés par les technologies de chaînes de blocs comprennent:

- les services gouvernementaux, particulièrement dans le cadre de programmes relatifs au gouvernement en ligne et au gouvernement branché;
- les titres fonciers, un des premiers domaines concernés par le déploiement de la technologie des chaînes de blocs;
- les services d'identité, ce qui comprend la gestion de la réputation personnelle;
- la liberté d'expression;
- la lutte contre la corruption;
- les processus électoraux;
- les nouvelles formes de gouvernance du point de vue des gouvernements virtuels et mondiaux;
- l'aide et le développement soutenus par des donateurs internationaux et des organisations multilatérales.

Les exemples et les données probantes présentés dans le présent livre blanc suggèrent que le déploiement de la technologie des chaînes de blocs pour la fourniture de biens publics dans les pays en développement en est toujours à ses balbutiements. La plupart des efforts faits en ce sens sont axés sur l'offre, et les institutions locales jouent un rôle passif et exercent un contrôle limité sur les initiatives. Les initiatives relatives à la technologie des chaînes de blocs dans le cadre de programmes de gouvernement branché et de services d'identité sont celles qui ont les meilleures chances de réussite à moyen terme.

D'autre part, la fourniture de biens privés de la technologie des chaînes de blocs présente une composante de viabilité financière interne qui fonctionne comme un aimant en attirant des fournisseurs, pourvu que les prix demeurent à un certain niveau. Des milliards de personnes dans le monde n'ont pas accès à de tels biens (p. ex., services bancaires), des biens auxquels les pauvres ont rarement un accès permanent. Par conséquent, nous examinerons les cinq domaines dans lesquels les biens et les services privés sont à la traîne. Les biens et les services en question sont les suivants:

Services bancaires pour les personnes qui n'ont pas de compte de banque;

- Envois d'argent;
- Agriculture;
- Sécurité alimentaire;
- Droits de propriété intellectuelle.

La plupart des initiatives de technologies de chaînes de blocs qui visent ce groupe de biens privés montrent du potentiel, mais n'ont pas encore pris leur envol. Certaines initiatives ont déjà pris fin ou ont été interrompues, tandis que d'autres peinent toujours à générer des revenus intéressants. Les envois d'argent et l'argent numérique sont les domaines les plus prometteurs.

Roman Arkhipov

CHAÎNES DE BLOCS ET DÉVELOPPEMENT HUMAIN

Peu importe la réussite relative des initiatives de technologie de chaînes de blocs en cours, les praticiens du développement et les chercheurs devraient au moins avoir une connaissance non technique de la capacité potentielle de la technologie à soutenir et à améliorer les programmes de développement et la gouvernance démocratique. L'analyse des répercussions de la technologie des chaînes de blocs sur le développement humain est fondée sur un cadre d'analyse à quatre piliers (reportez-vous à l'annexe I pour en savoir plus à ce sujet): l'infrastructure, le développement des capacités, les politiques et la réglementation et les institutions et la gouvernance.

En ce qui a trait à **l'infrastructure**, des données récentes indiquent que près d'un milliard de personnes n'ont pas accès à Internet et que la plupart d'entre elles vivent dans les pays en développement. Il semble donc improbable que les personnes qui n'ont pas accès à Internet deviennent des noeuds de réseau de chaînes de blocs ou exécutent des logiciels de portefeuille pour au moins profiter de la technologie en tant qu'utilisateurs finaux. Un autre problème relatif à l'infrastructure concerne ce que l'on appelle l'**infostructure**, ou l'infrastructure à clés publiques. Cela comprend les rôles, les politiques et les procédures nécessaires pour garantir le transfert électronique sécuritaire de l'information. L'infostructure n'est pas encore en place dans de nombreux pays en développement. Cela représente d'importants obstacles à l'utilisation systématique des technologies de chaînes de blocs à toutes fins, puisque ces dernières dépendent de l'utilisation d'outils cryptographiques.

En ce qui a trait au développement des capacités, on distingue deux grands problèmes. Le premier problème est l'utilisation de ces outils complexes et à multiples facettes. Des recherches récentes montrent que l'utilisation d'outils cryptographiques demeure difficile, et d'importantes améliorations sont encore nécessaires pour qu'une grande variété d'utilisateurs s'intéressent à ceux-ci et les comprennent.

Le second problème concerne la gestion des clés privées et publiques des utilisateurs finaux. Les logiciels de portefeuille et les logiciels clients peuvent fournir et ont fourni des interfaces conviviales qui facilitent la cryptographie à clé publique. Mais les utilisateurs doivent gérer leurs clés privées et les stocker de manière sécuritaire quelque part, d'une manière ou d'une autre. Ensemble, ces deux problèmes peuvent se révéler trop difficiles pour les populations relativement peu éduquées et alphabétisées, et qui font autrement face à l'exclusion socioéconomique.

Paul Morris

Comme pour d'autres technologies qui encouragent l'économie de plateforme, les technologies de chaînes de blocs sont en avance sur les politiques et la réglementation locales. Les pays industrialisés rattrapent leur retard, mais ce n'est pas le cas dans la plupart des pays en développement, où les capacités stratégiques et réglementaires sont encore naissantes.

Cet écart entraîne le déploiement désorganisé des technologies de chaînes de blocs dans l'hémisphère Sud, non seulement dans le cas des jeunes entreprises locales, mais aussi dans le cas des sociétés et autres institutions du Nord, qui contournent les priorités locales en matière de développement ou exploitent le manque de connaissances réglementaires. De plus, comme la plupart des jeunes entreprises utilisant les chaînes de blocs adhèrent au bitcoin, les politiques et la réglementation relatives aux cryptomonnaies deviennent de plus en plus importantes. Les politiques et la réglementation locales sont également essentielles pour des raisons de sécurité dans les pays où les conflits et l'extrémisme violents sont endémiques, et le financement de ces activités devrait être surveillé de plus près afin d'empêcher leur propagation dans le monde.

De la même manière que pour les technologies Internet précédentes, le déploiement des chaînes de blocs laisse entrevoir la possibilité de réduire certaines formes de gouvernement (central). La nature décentralisée de la technologie combinée à une nouvelle forme de confiance décentralisée et de consensus réparti alimentent cette opinion. Cela ne signifie pas pour autant que les chaînes de blocs sont (ou devraient être) liées de manière inextricable à ces opinions. Comme nous l'avons décrit dans la section précédente, de nombreuses jeunes entreprises dans le domaine des chaînes de blocs travaillent avec des gouvernements dans le but de déployer la technologie à une échelle nationale. Mais un des enjeux ignorés en bonne partie est le potentiel des technologies des chaînes de blocs à soutenir et à améliorer la décentralisation des gouvernements dans les États-nations. Il y a ici pour les technologies de chaînes de blocs une véritable possibilité de soutenir les gouvernements locaux, lesquels ont habituellement un accès limité à des ressources fiscales et humaines.

Pour exploiter les nouvelles technologies, les pays en développement ont besoin, outre les ressources fiscales, de capacités institutionnelles

permettant de faciliter le déploiement des technologies en question. Ces capacités ne se limitent pas à la connaissance de la technologie. Pour garantir leur viabilité à long terme, les déploiements et les initiatives de chaînes de blocs doivent renforcer les capacités institutionnelles. Il est donc essentiel de prendre en compte la manière dont les technologies de chaînes de blocs devraient être déployées dans le secteur public.

Bien que l'opinion dominante veuille que les chaînes de blocs remplacent les processus actuels, il importe davantage de voir comment la technologie peut compléter les processus de gouvernance tout en encourageant l'innovation dans le secteur public.

En ce qui concerne la gouvernance, les technologies de chaînes de blocs soulèvent toutes sortes de questions. Qui est responsable ? Qui rédige les contrats intelligents (des transactions algorithmiques qui exécutent des ententes contractuelles prédéfinies) ? Comment tous les points de vue peuvent-ils être pris en compte ? La réponse rapide du camp des chaînes de blocs est simple: personne n'est responsable puisque, par défaut, on n'a pas besoin de responsable, et tout le monde est responsable puisque la gouvernance est uniquement assurée par consensus. Ce consensus est fondé sur des algorithmes qui permettent aux utilisateurs et aux noeuds de s'entendre presque automatiquement sur les résultats du processus. Il semble donc que le logiciel prenne le contrôle et relègue les personnes, qui n'ont plus besoin d'interagir entre elles, à l'arrière-plan. Cela soulève les questions suivantes:

- **Programmeurs:** Qui s'occupe concrètement de la programmation? Comment les a-t-on choisis?
- **Compréhension du code:** Bien que le code source soit ouvert, les utilisateurs finaux doivent avoir la capacité de le lire et de le comprendre. La plupart des utilisateurs finaux en sont incapables et ont besoin d'aide pour y parvenir.
- **Extensibilité:** La technologie des chaînes de blocs n'est pas encore extensible (quoique de nombreux membres de la communauté des chaînes de blocs y travaillent). Tant que le problème de l'extensibilité ne sera pas résolu, quel sera l'impact de la croissance des technologies de chaînes de blocs à des milliards d'utilisateurs et de noeuds sur le consensus décentralisé?
- **Opposition confiance-gouvernance:** Une confiance décentralisée et dépersonnalisée ne signifie pas une gouvernance améliorée.

Malgré la répartition et la décentralisation, ces questions mettent en évidence le fait que la technologie des chaînes de blocs ne peut pas garantir que des hiérarchies et des inégalités sociales entre utilisateurs n'apparaîtront pas. Cette réalité est déjà en train de se produire dans le minage des technologies de chaînes de blocs. Il en va de même pour les programmeurs, les développeurs et les techno-entrepreneurs de chaînes de blocs, qui semblent tous jouir d'une position privilégiée dans les réseaux et qui peuvent exercer un pouvoir considérable sur les autres noeuds et utilisateurs.

L'inégalité dans un réseau décentralisé est donc possible et réelle.

CONCLUSIONS

Des défis, que les praticiens du développement des technologies de l'information et de la communication connaissent bien, menacent l'adoption et l'utilisation répandue des technologies de chaînes de blocs. La **complexité de la technologie des chaînes de blocs en tant que telle** est possiblement un nouvel ingrédient dans la recette. Cela pose de nouveaux problèmes et représente de nouveaux obstacles du point de vue du déploiement de la technologie et de sa diffusion aux utilisateurs finaux et aux parties prenantes.

La technologie des chaînes de blocs en est toujours à ses balbutiements, mais elle est soutenue par un groupe, bien que relativement petit, d'innovateurs et de techno-entrepreneurs hautement compétents. Ce groupe pourrait supprimer la plupart, sinon la totalité, des limitations et des défis soulignés dans le présent document. Par conséquent, le potentiel d'innovation des chaînes de blocs est considérable. Bien que cela en dise long sur les technologies de chaînes de blocs, il est encore tôt pour tirer des conclusions définitives sur l'évolution de la technologie dans les cinq prochaines années ou plus. Pour l'instant, la technologie des chaînes de blocs **suscite de l'engouement, mais les données probantes actuelles indiquent que les déploiements de celle-ci en sont encore à l'étape de la validation de principe.**

Le remplacement d'initiatives en cours et le lancement de nouvelles initiatives sur des plateformes autonomes de technologie de chaînes de blocs ne feront que retarder l'adoption des chaînes de blocs. Pour les pays en développement, la meilleure approche à adopter consiste à **déployer la technologie des chaînes de blocs pour compléter les programmes existants.** Cela pourrait réduire les entraves à l'accès tout en augmentant les probabilités d'investissements initiaux dans les technologies de chaînes de blocs viables à moyen terme, en répondant aux besoins locaux et en comblant les écarts de développement.

Les **initiatives de chaînes de blocs de grande ampleur qui sont liées au gouvernement branché semblent être les plus susceptibles de faire de la technologie des chaînes de blocs un catalyseur de fourniture de biens publics.** Les envois d'argent et l'argent numérique dans le secteur des biens privés montrent aussi du potentiel. Cependant, il est essentiel de comprendre comment cela pourrait ne pas promouvoir l'inclusion économique et financière des personnes qui se trouvent au bas de la pyramide.

Les problèmes d'utilisabilité peuvent aussi limiter la diffusion de la technologie des chaînes de blocs dans les pays en développement. L'utilisation répandue d'outils cryptographiques dans les pays pauvres fait face à des obstacles

Dino Reichmuth

majeurs, surtout si les initiatives de technologie des chaînes de blocs visent les segments sociaux les plus pauvres. Il n'est pas réaliste de supposer que chaque bénéficiaire doit utiliser et gérer des clés privées et publiques, et le manque d'infrastructure à clés publiques dans la plupart des pays en développement ne fera qu'aggraver la situation. La seule manière de dénouer l'impasse est de trouver des solutions de rechange qui donnent aux utilisateurs finaux un accès à des outils cryptographiques au moyen d'intermédiaires comme des organismes communautaires, des petites entreprises et des gouvernements locaux.

L'idée essentielle ici est que les **utilisateurs finaux n'ont pas besoin d'être propriétaires de la technologie ou de l'utiliser directement** pour profiter de son déploiement.

Bien que la technologie des chaînes de blocs soit florissante dans un contexte décentralisé, le présent livre blanc montre que le **minage a tendance à se centraliser et à se concentrer.** Au début des chaînes de blocs bitcoin, toute personne avec un ordinateur portatif ou un ordinateur de bureau pouvait miner le réseau. Aujourd'hui, c'est devenu l'apanage de quelques personnes qui disposent des ressources financières et du matériel nécessaires et qui peuvent payer des factures d'électricité exorbitantes.

De la même façon, en ce qui a trait aux notions de consensus, les technologies de chaînes de blocs substitueront le consensus algorithmique au consensus humain. Le **problème ici ne se limite pas à l'automatisation du consensus; il concerne également la représentation et l'échelle.** Les organisations et les réseaux de chaînes de blocs décentralisés et autonomes sont petits du point de vue du nombre de personnes qui y participent. La plupart des utilisateurs de chaînes de blocs sont

des clients qui utilisent des logiciels de portefeuille et qui ne font pas partie d'un processus de recherche de consensus algorithmique ou autre. Dans leur forme actuelle, les technologies de chaînes de blocs semblent mieux adaptées aux exploitations à petite échelle, en raison de leur manque d'extensibilité et aux autres limitations soulignées dans le présent document.

Les technologies de chaînes de blocs pourraient bientôt chambarder le développement. En effet, Internet et les technologies mobiles ont déclenché (et continuent de déclencher) des perturbations positives dans les pratiques de développement, bien qu'à un degré inférieur à celui auquel on s'attendait à leur émergence. De la même façon, les chaînes de blocs en sont toujours à leurs balbutiements, et la technologie continue d'évoluer rapidement. **La réussite du déploiement de nouvelles technologies comme les chaînes de blocs dans les pays en développement dépend de l'efficacité de ces dernières à surmonter les obstacles en matière de développement humain décrits plus haut.**

Dans ce contexte, il faut se poser une autre question pertinente: les technologies de chaînes de blocs peuvent-elles entraîner des perturbations plus profondes dans les processus de développement que les technologies précédentes ? Le potentiel est certainement là, mais des mesures mieux ciblées sont requises pour qu'il y ait un tel impact sur les processus de développement.

RECOMMENDATIONS

Au vu de l'analyse et des conclusions du présent document, nous formulons les recommandations suivantes.

RECHERCHE

Réaliser une série d'études de cas sur les initiatives de technologie de chaînes de blocs en cours dans les pays en développement. Bien qu'on puisse trouver des données anecdotiques sur de telles initiatives, peu de travaux de recherche universitaire ou de recherches de développement sont proposés pour l'instant. En effet, il existe un grand vide dans le domaine des chaînes de blocs, ce qui a favorisé l'engouement relatif à la technologie.

Réaliser de nouvelles recherches et analyses sur les chaînes de blocs pour la gouvernance et sur la gouvernance des chaînes de blocs par rapport aux gouvernements et à la fourniture de biens publics. De manière plus particulière, les liens entre la confiance, la recherche de consensus et la représentation n'ont pas été étudiés dans la littérature existante.

Lier les travaux actuels et futurs sur la technologie des chaînes de blocs à l'intelligence artificielle, puisque cette dernière est introduite de manière systématique dans la technologie et les applications décentralisées connexes. Cela nous ramène à la question de la gouvernance des technologies de chaînes de blocs et de la gouvernance des algorithmes en général, qui ne sont pas participatives ou transparentes. Les chaînes de blocs font-elles partie de la solution ?

Envisager d'entreprendre de nouvelles recherches sur la gouvernance des algorithmes et sur l'impact que ces derniers peuvent avoir sur la société, particulièrement dans les pays en développement. Ce thème est à son tour lié à la notion selon laquelle les technologies sont des produits sociaux. En fin de compte, la société finit par dicter la manière dont la technologie est exploitée. Toutefois, l'opinion dominante aujourd'hui semble se situer à l'opposé, notamment en ce qui concerne les technologies de chaînes de blocs.

Explorer des approches et des solutions novatrices pour faciliter l'accès à la technologie des chaînes de blocs des personnes qui se trouvent au bas de la pyramide, en se concentrant sur l'accès aux outils cryptographiques et à leur utilisation. Il est essentiel ici de faire une distinction entre l'utilisation et la propriété de la technologie et leurs avantages. Des déploiements technologiques précédents ont montré que les collectivités pauvres peuvent profiter des technologies sans les utiliser directement ou en être propriétaires. Les réseaux communautaires et l'utilisation partagée de téléphones cellulaires en sont des exemples bien connus.

PROGRAMMES

Explorer le rôle des initiatives d'innovation et des carrefours technologiques existants dans les pays en développement visant à soutenir le déploiement des technologies de chaînes de blocs. L'Afrique et l'Asie en particulier comptent un grand nombre de carrefours technologiques capables d'une part de fournir une expertise adéquate pour le déploiement des technologies de chaînes de blocs en s'appuyant sur les connaissances locales et, d'autre part, d'orienter la fourniture des biens publics.

Envisager de financer ou d'appuyer de petits projets pilotes ou des prototypes de technologie de chaînes de blocs axés sur les thèmes du développement, les ODD et les priorités locales des pays en développement. Il n'est pas nécessaire d'investir des sommes colossales, mais il faut porter une attention particulière à l'impact sur le développement humain. Comme nous l'avons mentionné plus tôt, les services d'identité et les services gouvernementaux qui font appel aux technologies de chaînes de blocs sont les plus pertinents à ce stade-ci et ont déjà été mis en oeuvre dans d'autres contextes.

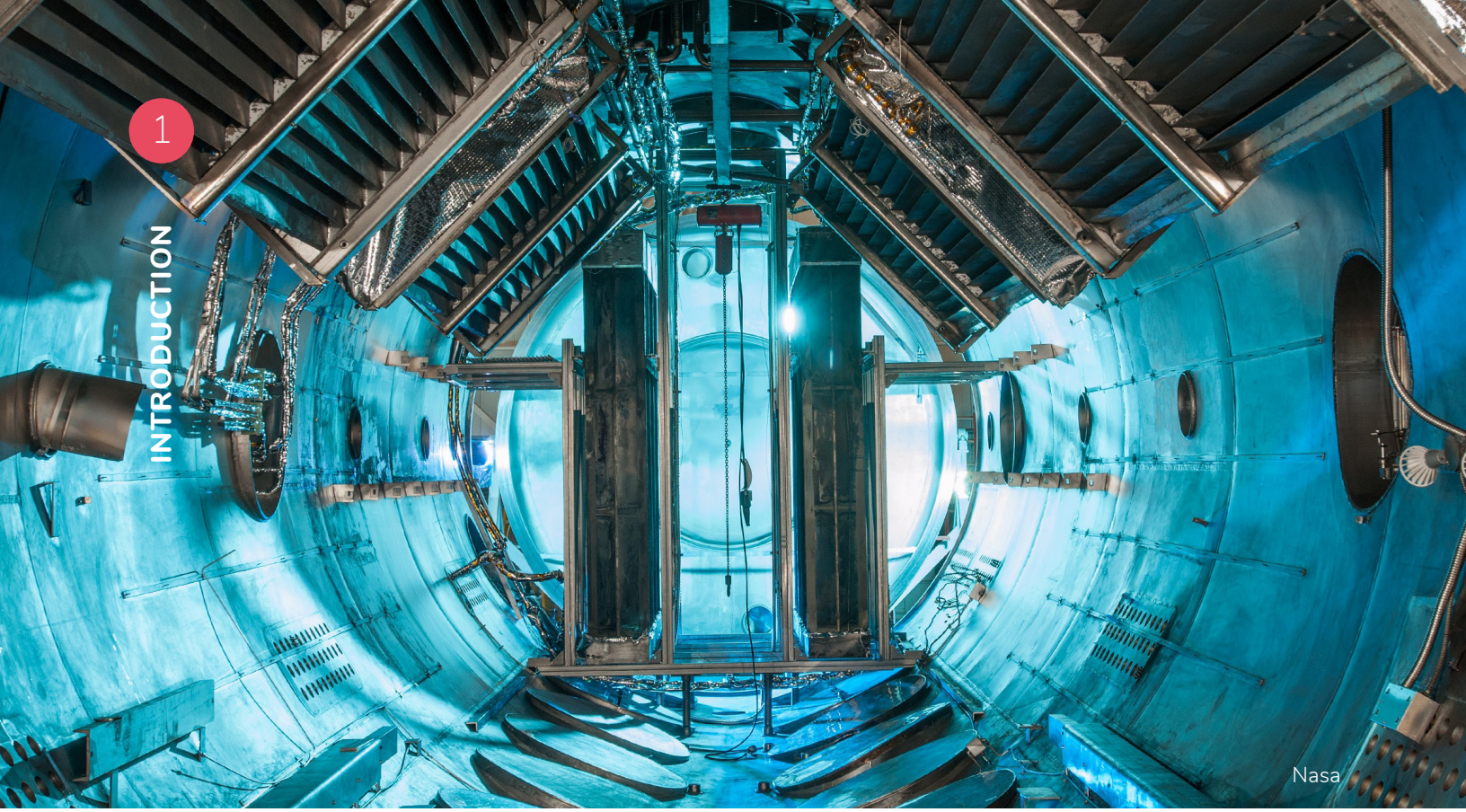
Soutenir ou aider la création d'un réseau d'innovateurs en technologies de chaînes de blocs et inciter ces derniers à soutenir les applications qui facilitent la fourniture des biens publics. Pour cela, il est essentiel d'attirer des innovateurs locaux dans les économies émergentes et en développement.

RÉSEAUTAGE ET PARTENARIATS

Soutenir la création d'une chaîne de blocs pour des projets liés aux chaînes de blocs dans les pays en développement ou envisager la création d'une base de connaissances durable connexe. L'établissement de partenariats avec des experts internationaux et d'autres innovateurs à l'échelle mondiale devrait faire partie d'une telle initiative.

Des **organismes de financement du développement multilatéraux et étrangers ont pris des mesures pour lier les technologies de chaînes de blocs à la poursuite des ODD**. Les organismes de développement et les praticiens du développement devraient conjuguer leurs efforts pour suivre les dernières avancées et réaliser d'autres recherches sur ce sujet.

Mettre en place un réseau de chaînes de blocs pour le développement ou aider à l'organisation d'un tel réseau, ou créer une organisation décentralisée autonome en partenariat avec d'importants pays et organismes donateurs. Le but premier d'un tel réseau pourrait consister à veiller à ce que le développement demeure l'enjeu principal et occupe une place plus importante que les chaînes de blocs elles-mêmes.



Nasa

Introduction

La quatrième révolution industrielle.[1] Le deuxième âge de la machine.[2] La société à coût marginal nul.[3] Voilà certaines expressions utilisées pour décrire la vague actuelle d'innovation technologique[4] qui évolue rapidement.

On constate une hausse de l'utilisation de la robotique et de l'intelligence artificielle, qui sont déployées en masse dans les processus de production par le secteur privé. Les nouvelles technologies font également partie de la vague d'innovation. Au premier plan, on trouve les chaînes de blocs, une nouvelle technologie qui constitue l'un des piliers du bitcoin, une cryptomonnaie inventée par un auteur qui demeure anonyme.[5] Alors que les innovations dans les domaines de l'intelligence artificielle et de la robotique semblent avoir un côté sombre,[6] de nombreuses personnes considèrent la technologie des chaînes de blocs comme une plateforme pour un changement positif; une plateforme qui pourrait chambarder l'économie mondiale et résoudre bon nombre des difficultés socioéconomiques et politiques auxquelles les pays se heurtent actuellement.[7] Bien que ces affirmations ne soient certainement pas nouvelles, la technologie des chaînes de blocs attire l'attention d'une grande variété d'acteurs, des gouvernements et des donateurs internationaux au secteur privé et aux investisseurs en capital-risque.

Ces technologies ont une caractéristique commune: un niveau élevé de sophistication, non seulement du point de vue des exigences logicielles et matérielles, mais aussi de celui des besoins en capital, des capacités humaines et des environnements institutionnels. Contrairement à la révolution mobile,[8] la vague d'innovation actuelle pourrait s'avérer plus compliquée pour les pays en développement qui souhaitent jouer un rôle actif au lieu de se contenter d'un rôle d'utilisateur final ou de consommateur des technologies en question. Pour les pays de l'hémisphère Sud[9], il est essentiel d'étudier la pertinence des nouvelles technologies pour combler les écarts socioéconomiques et soutenir l'atteinte des cibles de développement convenues à l'échelle internationale, ce qui comprend les ODD.

La technologie des chaînes de blocs, qui était initialement associée à des applications financières, est maintenant déployée dans de nombreux autres domaines et secteurs, y compris dans le développement et l'aide humanitaire. Les pays de l'hémisphère Sud doivent non seulement se demander comment ils peuvent y parvenir, mais aussi qui exploitera les technologies de chaînes de blocs afin de combler les écarts de développement, de favoriser l'inclusion sociale et de promouvoir la gouvernance démocratique.

Le but du présent livre blanc est d'explorer le potentiel de la technologie des chaînes de blocs pour le développement humain dans les pays en développement. On y présente tout d'abord un aperçu non technique des technologies de chaînes de blocs. On y présente ensuite la gamme d'applications des chaînes de blocs dans les domaines et les secteurs de développement du point de vue des biens publics et privés. Dans la section suivante, nous vous présenterons un examen de l'utilité réelle des chaînes de blocs dans les pays en développement, en utilisant le cadre de TIC-D décrit à l'annexe I. Le livre blanc se termine par une série de recommandations et de mesures à prendre visant des recherches supplémentaires et des programmes de développement potentiels qui font appel aux technologies de chaînes de blocs. Il est à noter que le présent livre blanc porte exclusivement sur les applications des chaînes de blocs autres que les cryptomonnaies. On y met donc l'accent sur l'utilisation des technologies de chaînes de blocs comme plateforme d'application générique dans les pays en développement.[10]

Blake Wheeler

Qu'est-ce que la technologie des chaînes de blocs ?

Tans la section suivante, vous trouverez une description détaillée de la technologie des chaînes de blocs d'un point de vue non technique.[11] La section commence par un bref historique des origines des chaînes de blocs. On y décrit ensuite ce que la technologie peut accomplir et son fonctionnement. La compréhension du fonctionnement des chaînes de blocs aidera les praticiens du développement à s'y retrouver dans le battage médiatique et à reconnaître l'utilité potentielle et les avantages des chaînes de blocs dans les recherches actuelles et futures et dans les programmes de développement.

BREF HISTORIQUE

Les chaînes de blocs sont une des principales technologies sous-jacentes du bitcoin, la première cryptomonnaie[12] décentralisée poste à poste de l'histoire.[13] Le bitcoin a été créé en 2008 par Satoshi Nakamoto, le pseudonyme d'une personne dont l'identité demeure mystérieuse.[14]

Comme plateforme financière, le bitcoin nécessite l'utilisation d'un grand livre[15] numérique pour l'enregistrement de toutes les transactions entre les utilisateurs de la cryptomonnaie. La chaîne de blocs est la technologie qui fournit le grand livre en question. La manière dont ce grand livre a été conçu est ce qui a entraîné l'émergence des technologies de chaînes de blocs.[16] Le logiciel Bitcoin créé par Nakamoto a été lancé sur Internet sous forme de logiciel ouvert, ce qui a contribué à accélérer sa diffusion à l'échelle mondiale depuis son lancement.

Au cours de ses premières années d'existence, les activités du bitcoin se déroulaient en marge de l'économie, car peu de commerçants étaient prêts à accepter la cryptomonnaie comme forme légale de paiement. Le Web invisible[17] voyait toutefois les choses d'un autre oeil.

Le bitcoin a fourni une forme de paiement anonyme qui ne peut pas être utilisée pour retrouver des acheteurs et des vendeurs. Le tristement célèbre site Web Silk Road[18], une plateforme de marché noir en ligne, utilisait largement le bitcoin, car les échanges de bitcoin facilitaient la conversion de la cryptomonnaie en dollars américains.

Complément d'information

La technologie des chaînes de blocs vous semble-t-elle encore un peu floue ?

Veuillez vous reporter à l'annexe II, à la page 59.

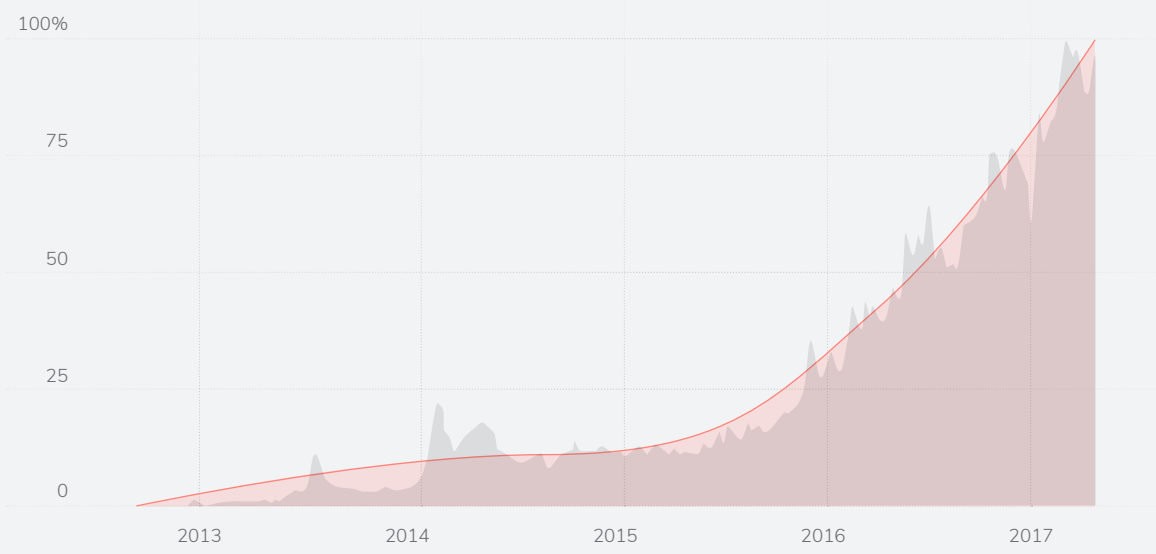
2

Le bitcoin était donc lié à différentes activités illégales comme le trafic de stupéfiants et le blanchiment d'argent. Les forces de l'ordre et les organismes de réglementation en ont eu connaissance et ont rapidement commencé à poursuivre en justice les personnes impliquées dans ces activités. La communauté du Bitcoin a ensuite dû rebâtir la réputation de la cryptomonnaie, ce qui a porté ses fruits quelques années plus tard. [19] Ce problème demeure pour le bitcoin et toutes les autres cryptomonnaies,[20] mais cela n'est pas si important pour les technologies de chaînes de blocs, car ces dernières peuvent être entièrement fonctionnelles sans le bitcoin.

Au départ, le bitcoin faisait ombrage aux chaînes de blocs, qui étaient par conséquent ignorées par les experts et les technologues. Les choses ont toutefois changé aux alentours de 2014, quand le potentiel des chaînes de blocs comme technologie autonome pour les secteurs autres que la finance a été reconnu par des innovateurs et des investisseurs en capital-risque. La figure 1 illustre cette évolution au moyen de Google Trends. Notez la croissance exponentielle à partir de 2016.

FIGURE 1 Tendances relatives aux chaînes de blocs
2012 - 2017

SOURCE: Google Trends



La figure 1 illustre l'évolution des chaînes de blocs au moyen de Google Trends, quand son potentiel comme technologie autonome pour les secteurs autres que la finance était reconnu par des innovateurs et des investisseurs en capital-risque. Il est à noter que l'axe des Y représente la part de recherches mensuelles par rapport au mois le plus élevé pour l'ensemble de la période. La valeur ne peut jamais dépasser 100 %. Veuillez vous reporter à la note de bas de page 21 pour obtenir des précisions.

2

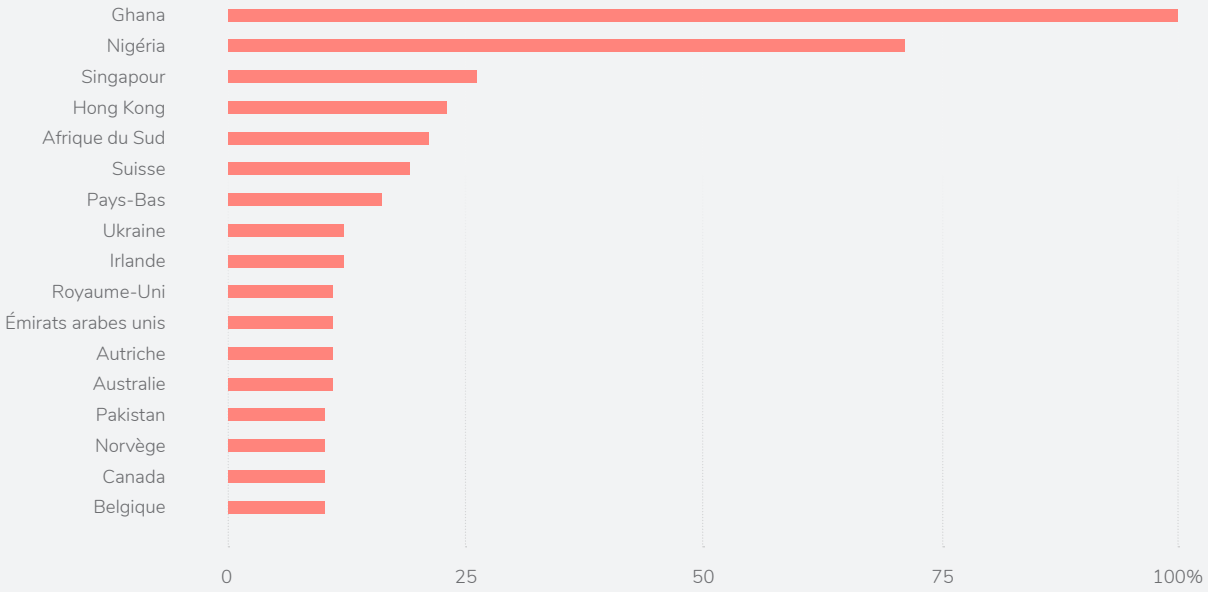
Joel Filipe

La figure 2 ci-dessous montre l'intérêt pour les technologies de chaînes de blocs par pays[21] Notez que quelques pays en développement sont en tête de peloton.

Non seulement les chaînes de blocs connaissent-elles un essor, mais elles sont également déployées dans plusieurs pays à diverses fins, comme il est décrit plus bas. Même les grandes institutions bancaires traditionnelles sont sur le point d'adopter les technologies de chaînes de blocs, non sans essayer tout d'abord de les refaçonner afin de soutenir leurs processus et leurs pratiques d'affaires actuels.

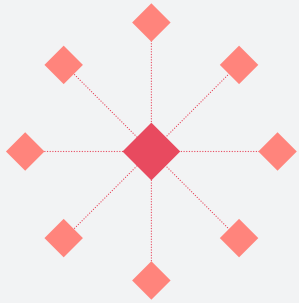
FIGURE 2 Intérêt des pays pour les chaînes de blocs
2012 - 2017

SOURCE: Google Trends

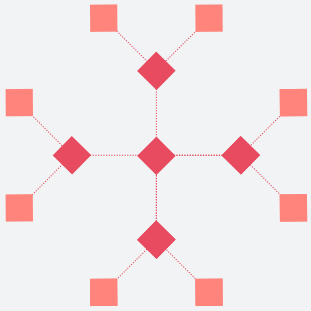


La figure 2 montre l'intérêt pour les technologies de chaînes de blocs par pays. Ce qu'il y a de paradoxal dans tout ça, c'est que si l'activité a surtout lieu dans les pays développés, la plupart des recherches sur les technologies de chaînes de blocs sont faites dans les pays en développement. Il est à noter que les chiffres de Google Trend sont relatifs et non absolus. Pour chaque recherche d'un mot-clé, Google Trend détermine le nombre maximal de recherches lors d'une journée donnée et divise tous les autres par ce nombre. Par conséquent, le maximum est toujours de 100. Il est clair que les recherches relatives aux technologies de chaînes de blocs dans Google sont toujours en hausse. Reportez-vous à la note de bas de page 21 pour de plus amples renseignements.

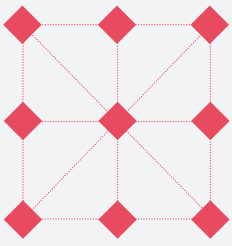
FIGURE 3 Typologies de réseaux[22]



Centralisé



Décentralisé



Réparti

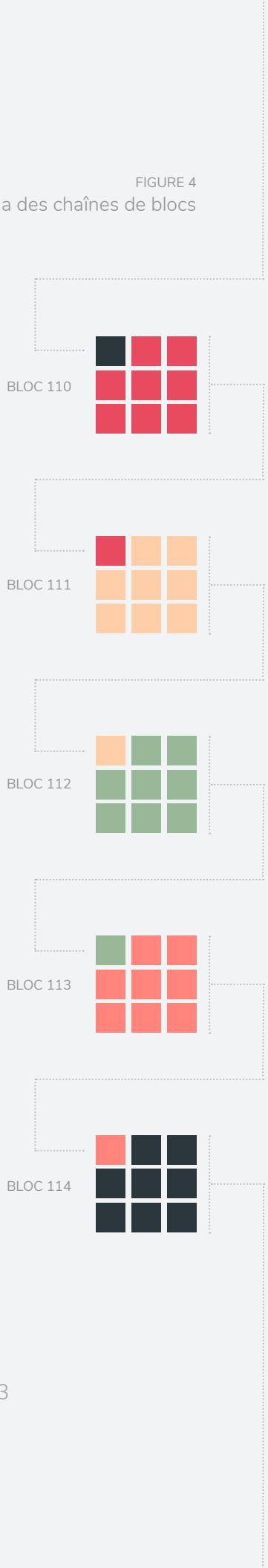
APERÇU DES CHAÎNES DE BLOCS

Pour les profanes, on peut définir les chaînes de blocs comme étant une feuille de calcul qui enregistre dans l'ordre les transactions entre les utilisateurs d'un même réseau poste à poste.[23] Par défaut, la feuille de calcul est publique: tous les utilisateurs et les noeuds du réseau ont un accès complet en temps réel aux données enregistrées dans la base de données. Il n'est pas nécessaire d'obtenir l'autorisation préalable de tiers ou d'une autorité centrale.

La feuille de calcul est également répartie.[24] Une copie des données à jour est stockée dans chaque noeud du réseau. De la même manière, les données mises à jour sont automatiquement diffusées dans le réseau chaque fois qu'une nouvelle rangée est ajoutée. Aucun ordinateur ou serveur central n'est donc requis pour gérer ou diriger le trafic.[25]

Raphael Koh

FIGURE 4
Schéma des chaînes de blocs



Une des grandes innovations des chaînes de blocs est la manière dont les écritures sont liées entre elles. Chaque écriture dans la base de données est constituée d'un bloc de transactions[26] et comporte un identificateur unique. Chaque bloc de transactions est lié au bloc précédent. En langage informatique, on dit que le nouveau bloc est l'enfant du bloc précédent, ce qui crée une chaîne logique entre les blocs.

Comment cela est-il accompli ? L'identificateur unique est utilisé pour générer l'identificateur unique du bloc suivant. Cela crée une chaîne de blocs liés entre eux. Il est donc pratiquement impossible de modifier le contenu ou l'ordre des rangées. Les blocs sont donc l'enfant mathématique du bloc qui les précède. La seule exception est ce que l'on appelle le « bloc de genèse », c'est-à-dire le premier bloc, ou la première rangée de données, qui est orphelin, puisqu'il n'a pas de parents.

La figure 4 fournit une représentation schématique de trois blocs aléatoires d'une chaîne de blocs fictive. Par exemple, le bloc 112 a son propre identificateur unique et comprend sa propre série de transactions. Il comprend aussi l'identificateur unique du bloc précédent et un horodateur unique qui enregistre la date et l'heure auxquelles l'écriture a été ajoutée à la chaîne de blocs.

Les chaînes de blocs sont évidemment beaucoup plus complexes que des feuilles de calcul ordinaires. Cela est sans doute particulièrement bien illustré dans la manière dont les écritures sont ajoutées à une chaîne de blocs.

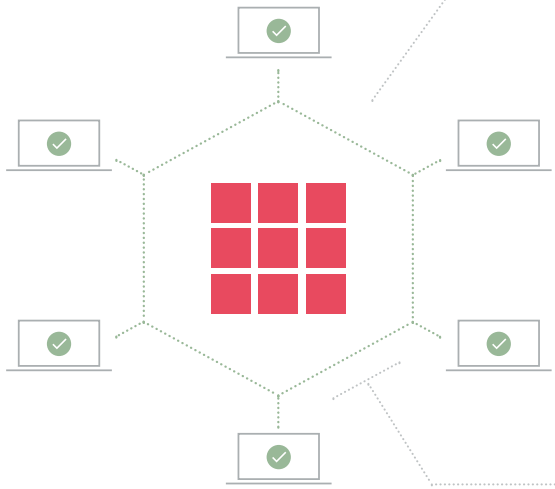
Rudiments des chaînes de blocs

Transaction
INTERACTION ENTRE LES UTILISATEURS

Les transactions sont regroupées en blocs qui seront ajoutés à la chaîne

Preuve de travail

Validation de la preuve de travail
CONFIANCE RÉPARTIE

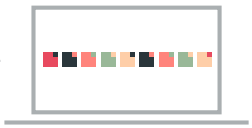


L'ajout de nouvelles rangées aux données nécessite le consensus des noeuds. Cela est accompli à l'aide de l'algorithme de preuve de travail utilisé par les mineurs du réseau qui rivalisent entre eux pour trouver le hachage d'en-tête d'un nouveau bloc de transactions (la difficulté de trouver un nouveau hachage augmente nécessairement au fil du temps du fait de l'augmentation du nombre d'écritures dans la chaîne).

Le résultat est diffusé aux noeuds du réseau, qui le valident ensuite. Une fois la validation effectuée, le bloc est ajouté au bloc de chaînes existant. Le processus compétitif de preuve de travail rend possible le consensus décentralisé. Reportez-vous à l'annexe II pour en savoir davantage à ce sujet.

Un nouveau bloc est ajouté à la chaîne

La chaîne mise à jour est diffusée au réseau



Acteurs principaux

Les principaux développeurs ont un accès en écriture au code source.

Les noeuds complets contiennent des copies à jour de la chaîne de blocs, valident les nouveaux blocs puis les diffusent dans le réseau.

Les mineurs se consacrent à la preuve de travail.

Les utilisateurs finaux se servent du réseau pour effectuer leurs transactions au moyen d'un logiciel client ou d'un logiciel de portefeuille.

Les noeuds de service comme les portefeuilles, le stockage, les échanges et les services infonuagiques.

Technologie poste à poste

Dans un réseau d'égal à égal, tous les noeuds interconnectés sont en principe égaux. Comme il n'y a pas de serveur central, il n'y a pas de point de défaillance central. Si un noeud tombe en panne, tous les autres noeuds demeurent interconnectés; les données et l'information qui circulent dans le réseau sont ainsi préservées. Exemples: BitTorrent et Napster.

Cryptographie

La chaîne de blocs utilise une cryptographie à clés publiques: une clé privée qui n'est connue que de son propriétaire, et une clé publique qui est partagée avec le reste du monde. Une clé privée est d'abord générée de manière aléatoire pour être ensuite utilisée pour créer une clé publique. La clé privée est utilisée pour chiffrer la transaction qui peut ensuite être déchiffrée par le destinataire visé au moyen de la clé publique de l'expéditeur. Il est mathématiquement impossible d'utiliser une clé publique pour déchiffrer une clé privée.

Rudiments des chaînes de blocs pour le développement

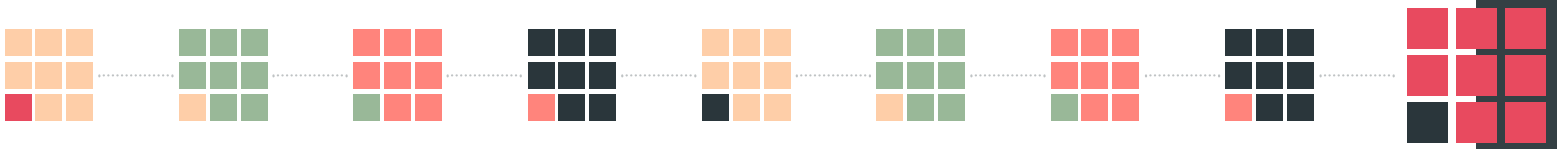
UTILISATIONS POTENTIELLES ET ACTUELLES DES CHAÎNES DE BLOCS

Services publics et gouvernementaux

Titres fonciers
Services d'identité
Lutte contre la corruption
Processus électoraux
Distribution de l'aide et développement

Services du secteur privé

Envois d'argent
Agriculture
Sécurité alimentaire
Droits de propriété intellectuelle



PRINCIPALES EXIGENCES RELATIVES AUX CHAÎNES DE BLOCS

Infrastructure et infostructure

L'écosystème des chaînes de blocs nécessite une infrastructure, des télécommunications au réseau de distribution électrique, en passant par la santé et l'éducation, et tous ces éléments nécessitent des investissements privés et publics. Cet écosystème requiert aussi une infostructure comme l'infrastructure à clés publiques, ce qui comprend les rôles, les politiques et les procédures nécessaires pour le transfert électronique sécuritaire de l'information. Dans de nombreux pays en développement, ce type d'infrastructure n'est pas encore en place.

Développement des capacités

Les pays ont besoin de capacités humaines pour développer et déployer de nouvelles technologies. Nous parlons ici non seulement de capacités techniques, mais aussi de capacités fonctionnelles transversales qui ne se limitent pas aux TIC. Les utilisateurs doivent être capables de gérer leurs clés privées et de les stocker de manière sûre, ce qui peut être difficile pour les populations peu éduquées et alphabétisées

Politiques et réglementation

La capacité de tous les ordres gouvernementaux à élaborer, à mettre en oeuvre et à appliquer des politiques sur leur territoire est essentielle. Les environnements politiques souples peuvent faciliter l'utilisation des technologies et permettre aux pays de devenir des endroits où l'on met en oeuvre des projets pilotes et où l'on déploie des prototypes, ce qui permet d'améliorer l'expertise et les avantages concurrentiels à l'échelle mondiale.

Institutions

Cela comprend les « règles du jeu » qui permettent à une personne de mener des activités dans un contexte institutionnel donné. Les mécanismes de gouvernance en font partie, particulièrement les nouveaux modèles fondés sur la participation de multiples parties prenantes. Les chaînes de blocs peuvent contribuer à améliorer ou à soutenir les institutions étatiques, ce qui facilite la décentralisation des États, une question centrale du développement.

VALEURS PRINCIPALES DES CHAÎNES DE BLOCS

Données immuables

Les chaînes de blocs garantissent l'intégrité des données et des utilisateurs. Premièrement, il est pratiquement impossible de modifier ou de falsifier les blocs d'une chaîne, ce qui offre un niveau élevé d'intégrité ou d'immuabilité des données. Deuxièmement, les métadonnées relatives aux transactions effectuées par un noeud ou un utilisateur final sont enregistrées dans la chaîne de blocs et peuvent être liées à l'utilisateur qui les effectue.

Cela signifie que les utilisateurs ne peuvent pas tromper le réseau ou tenter d'effectuer une transaction invalide. Bien que l'anonymat complet soit impossible, les chaînes de blocs ne contiennent aucun renseignement personnel et utilisent un chiffrement privé/public pour authentifier les utilisateurs qui effectuent les transactions. Les noeuds et les utilisateurs n'ont pas besoin de fournir de noms ou de renseignements personnels pour faire partie du réseau, et le minage de chaînes de blocs pour obtenir des renseignements personnels en vue de les vendre à des tiers pour réaliser un profit est impossible.

Confiance répartie

La chaîne de blocs permet de contourner la nécessité d'une autorité centrale digne de confiance. La confiance est plutôt répartie entre les éléments du réseau. Il en va de même pour les mécanismes de gouvernance; en principe, les différents types d'utilisateurs et de noeuds ont le même poids politique.

Photo via Visualhunt

AJOUTER UN NOUVEAU BLOC À LA CHAÎNE

Contrairement aux grands livres et aux plateformes de transactions traditionnels, on ne peut ajouter des blocs qu'une fois que les noeuds du réseau atteignent un consensus. On parle alors de consensus décentralisé, ce qui remplace la nécessité d'une autorité centrale digne de confiance. C'est pourquoi la chaîne de blocs se distingue comme étant une technologie où la confiance est décentralisée: le réseau lui-même assure la confiance entre les utilisateurs. Les tiers qui valident ou approuvent les transactions en cours ne sont pas nécessaires comme c'est le cas des opérations financières traditionnelles et de nombreux autres réseaux de transactions.[27]

Le consensus n'est pas atteint au moyen d'un vote, mais plutôt à l'aide de la puissance de calcul des noeuds du réseau.[28] Le consensus décentralisé est atteint à l'aide d'un algorithme de preuve de travail qui doit être exécuté sur les réseaux avant qu'un nouveau bloc soit ajouté à la base de données.[29] La preuve de travail ressemble au casse-tête classique qui consiste à deviner le chiffre [30], avec un niveau de complexité beaucoup plus élevé toutefois. Le résultat de la preuve de travail est diffusé aux noeuds du réseau, qui le valident ou le corroborent ensuite. Une fois la validation effectuée, le bloc est ajouté à la chaîne d'écritures existante et est diffusé à tous les noeuds.

Il est à noter que les noeuds doivent rivaliser entre eux pour résoudre le casse-tête. Toutefois, seuls les noeuds spécialisés qui utilisent du matériel sophistiqué ont une chance réelle de résoudre le casse-tête.

CRYPTOGRAPHIE

La technologie des chaînes de blocs utilise systématiquement des outils cryptographiques.

En premier lieu, l'identificateur unique de chaque bloc est un hachage des entrées fournies.[31] Le bloc de transactions compris dans un enregistrement de chaînes de blocs est également le résultat d'une opération de hachage. Toutefois, la fonction de hachage utilisée dans cette opération diffère de celle qui est utilisée pour générer l'identificateur unique de bloc.[32] Les renseignements sur les transactions sont chiffrés et révèlent donc peu leur contenu réel à l'oeil nu, autres que certaines métadonnées élémentaires.[33]

Ensuite, tous les noeuds et les utilisateurs doivent se servir d'une cryptographie à clé publique pour être intégrés au réseau et interagir entre eux. Les utilisateurs et les noeuds doivent générer des clés privées et publiques. Ces dernières sont partagées par tout le réseau aux fins d'identification. La création d'un profil et la transmission de renseignements personnels ne sont pas nécessaires. Une clé publique valide suffit. Dans ce contexte, la technologie des chaînes de blocs est pseudo-anonyme, ce qui contraste fortement avec les plateformes de médias sociaux existantes.

INCITATIFS INTÉGRÉS

Les technologies de chaînes de blocs comportent des incitatifs financiers intégrés pour les noeuds qui rivalisent pour la preuve de travail ainsi que pour ceux qui souhaitent fournir des services supplémentaires propres au bitcoin, aux chaînes de blocs ou aux deux.

Par exemple, les noeuds qui résolvent la preuve de travail dans la chaîne de blocs du bitcoin obtiennent des bitcoins fraîchement frappés. En outre, les noeuds peuvent également facturer des frais pour chaque transaction payée en bitcoins par les utilisateurs. En principe, ces incitatifs devraient suffire à payer le matériel, l'énergie et les autres coûts associés à la preuve de travail.

La conversion de bitcoins en dollars américains et autres devises était l'un des premiers services fournis par les noeuds. Étant donné que le prix courant du bitcoin a augmenté rapidement au fil du temps, les échanges sont devenus une des sources principales de revenus pour les noeuds du réseau.

La chaîne de blocs a créé un écosystème sophistiqué de services qui se sont montrés profitables jusqu'à maintenant. La récente hausse du prix du bitcoin et d'autres plateformes de chaînes de blocs accélérera cette croissance.

ES CHAÎNES DE BLOCS ET LA GOUVERNANCE

La nature décentralisée de la technologie des chaînes de blocs combinée à l'émergence d'une confiance réseau répartie pourraient entraîner des perturbations majeures dans les processus de gouvernance traditionnels,[34] notamment en encourageant l'apparition de formes de gouvernance plus horizontales et personnalisées. D'autres idées proposées dans la littérature comprennent:[35]

- De nouvelles formes de démocratie directe permettant à tous les membres du réseau de participer aux processus décisionnels. Un exemple est la « démocratie liquide » qui précède la chaîne de blocs et qui y a trouvé sa plateforme idéale.[36]
- L'autonomisation des personnes en décentralisant et en partageant le pouvoir entre elles. Pour y parvenir, on peut utiliser des agents logiciels qui agissent au nom des personnes, en s'appuyant sur des protocoles convenus et programmés dans la chaîne de blocs.[37] Les organisations décentralisées autonomes[38] sont de bons exemples, tout comme les autres formes d'organisations décentralisées qui fonctionnent au moyen de contrats intelligents.[39]
- Des services publics mondiaux personnalisés et offerts aux clients peu importe l'endroit où ils se trouvent et leur nationalité. Les différentes variantes de cette idée ne nécessitent pas toutes la disparition de l'État-nation. En fait, les chaînes de blocs peuvent compléter les services gouvernementaux tout en améliorant la transparence et la responsabilité.[40]
- La création d'États-nations fondés sur les chaînes de blocs comme la Bitnation.[41]
- La passation d'un nouveau contrat social plus inclusif.[42]

Thomas Kvistholt

Ferdinand Stohr

TYPES DE CHAÎNES DE BLOCS

Bien que la chaîne de blocs du bitcoin soit publique et ouverte à tous, les chaînes de blocs n'ont pas besoin de posséder ces caractéristiques pour être déployées et utilisées de manière efficace.

Premièrement, les chaînes de blocs peuvent être publiques ou privées.[43] Dans ce dernier cas, seul un ensemble de noeuds présélectionnés peut constituer le réseau et traiter les transactions. Deuxièmement, les chaînes de blocs peuvent avoir un statut sans permission ou avec permission.

Les chaînes de blocs avec permission nécessitent l'authentification des noeuds au moyen de mots de passe, de condensés ou de signatures numériques pour lire ou ajouter de nouvelles écritures à la chaîne de blocs.

Par conséquent, une chaîne de blocs privée peut être sans permission, tandis qu'une chaîne publique peut nécessiter une authentification préalable avant qu'une permission d'écriture soit accordée à la chaîne de blocs. Dans ce cas, seuls les noeuds authentifiés peuvent ajouter de nouvelles écritures à la base de données. L'information ci-dessus est résumée dans le tableau 1.

Tableau 1: Types de chaînes de blocs

	Sans permission	Avec permission
Public	Tous les noeuds du réseau d'égal à égal doivent avoir un accès complet à la chaîne de blocs.	Les noeuds doivent être authentifiés pour avoir un accès en écriture à la chaîne de blocs.
Privé	Tous les noeuds d'un réseau privé préalablement défini ont un accès complet à la chaîne de blocs.	Les noeuds doivent être authentifiés pour avoir un accès en lecture et en écriture à la chaîne de blocs privée. Dans d'autres cas, seuls certains noeuds autorisés peuvent ajouter des écritures à la chaîne de blocs, tandis que les autres n'y ont qu'un accès en lecture.

Les chaînes de blocs privées avec permission sont soutenues par certains acteurs du secteur privé. Par ailleurs, les gouvernements pourraient envisager l'utilisation de chaînes de blocs publiques avec permission pour fournir des services précis à leurs citoyens, tout en évitant l'utilisation coûteuse et insoutenable d'algorithmes de preuve de travail.[44]

Il est à noter que l'utilisation de chaînes de blocs hybrides publiques-privées est aussi possible.[45] Enfin, certains observateurs ont qualifié la technologie des chaînes de blocs de « technologie de grand livre réparti » (GLR) pour souligner sa nature non monétaire.[46] Cependant, les GLR ne font pas tous appel aux chaînes de blocs. Corda[47] et Ripple[48] sont des exemples de GLR qui ne font pas appel à des chaînes de blocs.[49] La figure 5 réunit toutes les possibilités ci-dessus et fournit une représentation schématique de toutes ces variantes.

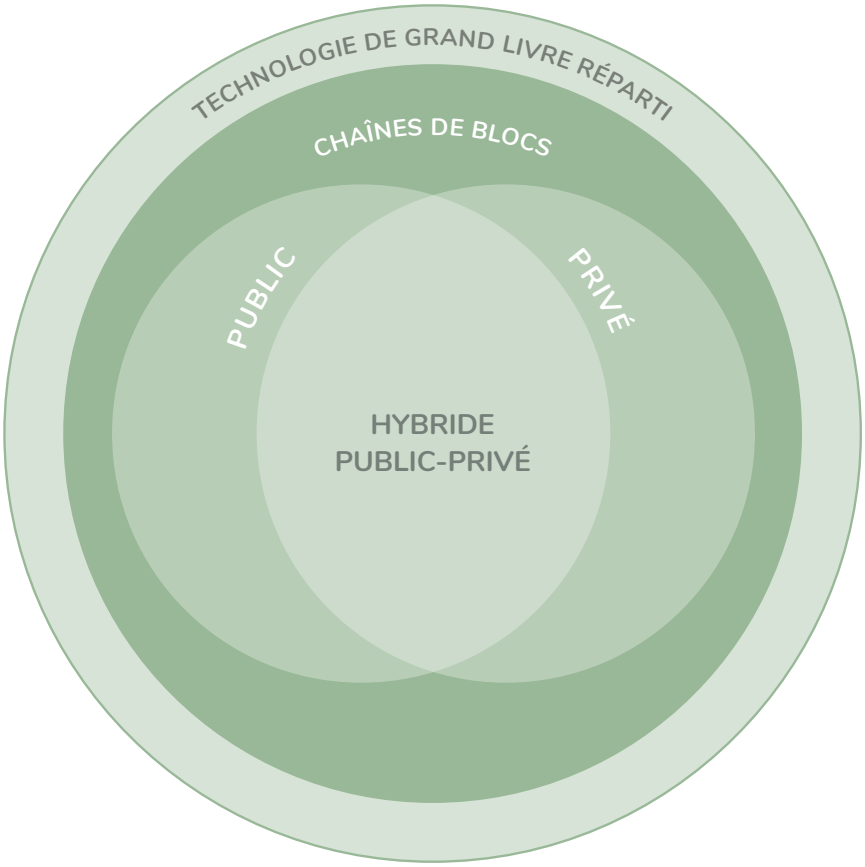


Figure 5: Technologie de grand livre réparti et de chaînes de blocs

CARACTÉRISTIQUES PRINCIPALES DES CHAÎNES DE BLOCS

La présentation ci-dessus fournit les renseignements généraux pour définir les caractéristiques principales et les grands principes des chaînes de blocs. Les voici:

Confidentialité: Les chaînes de blocs ne contiennent aucun renseignement personnel et utilisent un chiffrement privé/public pour authentifier les utilisateurs qui effectuent les transactions. Le minage de chaînes de blocs dans le but d'obtenir des renseignements personnels pouvant être vendus à des tiers pour réaliser un profit est impossible.

Pseudo-anonymat: Les noeuds et les utilisateurs n'ont pas besoin de fournir de noms ou de renseignements personnels pour faire partie du réseau. Toutefois, l'anonymat complet n'est pas assuré, car il est possible de lier les utilisateurs à l'activité sur le réseau, ce qui peut révéler leur identité.[50]

Intégrité: Elle fonctionne de deux manières. Premièrement, il y a l'intégrité des données: il est pratiquement impossible de modifier ou de falsifier les blocs d'une chaîne. On nomme aussi cette caractéristique « immuabilité ». Deuxièmement, il y a l'intégrité des utilisateurs: les métadonnées relatives aux transactions effectuées par un noeud ou un utilisateur final sont enregistrées dans la chaîne de blocs et peuvent être liées à l'utilisateur qui les effectue. Les utilisateurs ne peuvent pas tromper le réseau ou tenter d'effectuer une transaction invalide.

Confiance et gouvernance réparties: La chaîne de blocs permet de contourner la nécessité d'une autorité centrale digne de confiance. La confiance est plutôt répartie entre les éléments du réseau. Il en va de même pour les mécanismes de gouvernance; en principe, les différents types d'utilisateurs et de noeuds ont le même poids politique.

Transparence: Toutes les métadonnées relatives à la chaîne de blocs sont accessibles à tous les noeuds et utilisateurs en temps réel. Il est impossible de cacher ou de caviarder l'information de la chaîne de données.[51] La transparence répartie est ainsi possible, mais cela pose de nouveaux problèmes.[52]

Sécurité: Pour utiliser une chaîne de blocs, tous les participants (noeuds et utilisateurs finaux) ont besoin d'outils cryptographiques et de clés publiques et privées.

Viabilité: Des incitatifs financiers intégrés fournissent une voie claire pour la viabilité économique du réseau.

Code source ouvert: Les logiciels requis pour utiliser les chaînes de blocs, ce qui comprend les outils cryptographiques, sont gratuits pour tous. En outre, les utilisateurs dotés des capacités adéquates peuvent en fait aider à améliorer et à perfectionner les technologies des chaînes de blocs, en plus de trouver des bogues éventuels. Cela peut également faciliter la propagation des innovations en matière de chaînes de blocs.

LIMITES DES CHAÎNES DE BLOCS

En tant que technologie émergente, les chaînes de blocs comportent des limites qui peuvent empêcher leur adoption généralisée par le secteur financier, mais aussi par d'autres secteurs. On peut résumer les limites en question comme suit:

Extensibilité: Dans sa forme actuelle, la chaîne de blocs du bitcoin ne peut ajouter qu'un nouveau bloc de transactions toutes les dix minutes environ. Cela se traduit par un faible volume de transactions par secondes (moins de cinq), ce qui est très loin des volumes déclarés par les réseaux de transactions traditionnels.

Taille des blocs: Le problème ci-dessus est causé par la petite taille des blocs définie dans le code source original du bitcoin. La taille maximale de chaque bloc est d'un mégaoctet, ce qui permet 2 200 transactions. L'augmentation de la taille des blocs fait actuellement l'objet de discussions, mais aucune décision finale n'a encore été acceptée.[53]

Coûts élevés: Les noeuds de minage utilisent du matériel sophistiqué et coûteux pour les algorithmes de preuve de travail. Par conséquent, seuls certains noeuds du réseau peuvent l'emporter dans ce processus même si, en théorie, tous les noeuds disposent des logiciels requis pour miner le réseau. Le concept une unité centrale - un vote, de Nakamoto, n'existe plus, car les coûts du matériel et d'électricité empêchent la plupart des noeuds de participer à ce processus.

Impact environnemental: « L'inefficacité de la preuve de travail du point de vue des ressources énergétiques est un sous-produit des coûts élevés. Certaines estimations de la consommation d'électricité indiquent qu'au printemps de 2017, l'utilisation d'électricité pour le bitcoin était comparable à celle de 280 000 foyers américains par année.[54]

Centralisation: Le minage est désormais centralisé, et seuls quelques noeuds contrôlent une grande part du marché.[55] La figure 6 ci-dessous montre la part de marché des principaux noeuds ou entreprises de minage. Notez que les cinq entreprises principales contrôlent plus de la moitié du marché.[56]

Bande passante: Pour être actifs sur le réseau, les noeuds complets doivent avoir accès à la bonne bande passante. Les connexions lentes et peu fiables ne sont pas souhaitables, surtout si l'on tient compte de la taille actuelle de la chaîne de blocs qui s'élève à 120 gigaoctets.[57]

Utilisabilité: La technologie des chaînes de blocs nécessite la gestion sécuritaire des clés publiques et privées par les utilisateurs finaux et les noeuds. Bien que les logiciels de portefeuille aient fait beaucoup de progrès, la perte de clés privées demeure un risque sérieux. Aucune des solutions existantes n'est à l'épreuve du vol physique, et seules quelques solutions peuvent protéger les utilisateurs contre les logiciels malveillants.[58]

Complexité: Les technologies de chaînes de blocs semblent incompréhensibles pour la plupart des gens, et le jargon technologique qui s'y rapporte n'aide pas. Seules quelques personnes semblent comprendre la technologie.

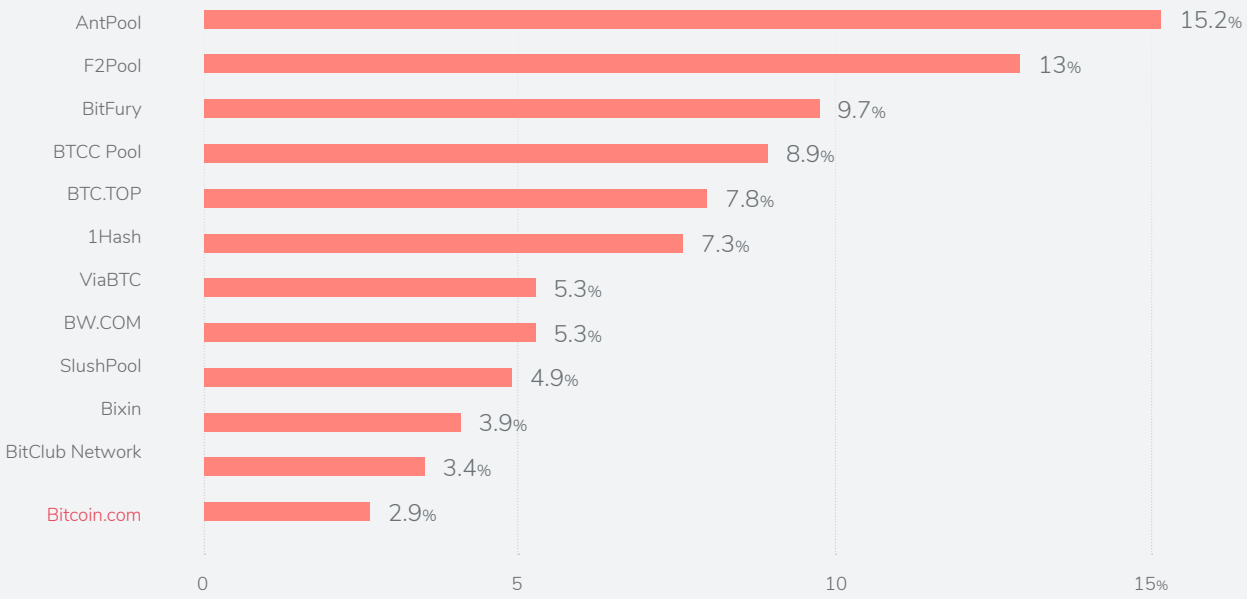
Cryptographie: L'utilisation d'outils cryptographiques ne fait que commencer, et l'on ne peut pas s'attendre à ce que l'internaute moyen l'adopte à court terme.

L'immuabilité comme frein: Si la chaîne de blocs est piratée ou si le code du logiciel comporte un bogue qui permet un exploit particulier, l'immuabilité peut devenir un frein. Ce fut par exemple le cas du piratage Ethereum de l'année dernière, quand un noeud rebelle a pu s'emparer de près de 64 millions de dollars.[59]

L'écosystème de la technologie des chaînes de blocs est proactif et s'efforce déjà de contourner ces limites. Le fait qu'on utilise un code source ouvert est déterminant. D'autre part, on ne peut apporter de modifications au code et aux opérations de la chaîne de blocs qu'en atteignant un consensus ou un accord de la majorité des noeuds sur la marche à suivre.

FIGURE 6 Part de marché des meilleurs mineurs de chaînes de blocs de bitcoins

1er avril , 2017



Source: blockchain.info

Applications des chaînes de blocs

Malgré le fait qu'elles s'avèrent être une couche de base, les chaînes de blocs n'ont pas besoin du protocole Bitcoin pour être fonctionnelles. Les technologies de chaînes de blocs peuvent être utilisées dans d'autres domaines et secteurs où des transactions, des interactions et des événements entre les acteurs peuvent avoir lieu. Cela comprend les biens corporels et incorporels.

Il n'est pas facile de se tenir au courant des innovations et des progrès relatifs aux chaînes de blocs, car ce domaine change rapidement à l'échelle mondiale.[60] Ce qui nous importe ici est toutefois la manière dont cela se déroule dans les pays en développement.

Du point de vue du développement, l'introduction des concepts de biens privés et de biens publics et leur fourniture par les secteurs public et privé sont essentielles.[61] Dans le présent livre blanc, nous mettons l'accent sur la relation entre ces deux types de biens et services.

Avant d'entrer dans le vif du sujet, il est essentiel d'établir une distinction entre la prestation du service et l'enregistrement et le stockage des transactions dans les chaînes de blocs. La technologie de grand livre réparti (GLR) n'est pas conçue pour fournir le service en tant que tel. Elle permet plutôt un enregistrement sécuritaire, privé, transparent et immuable des transactions effectuées durant la prestation du service.[62] Par exemple, le Royaume-Uni se sert déjà de chaînes de blocs pour verser des prestations d'aide sociale. De plus, le gouvernement britannique a mis en place un service infonuagique auquel seules les institutions publiques ont accès.[63] Cette solution pourrait être considérée comme une pratique exemplaire pour les pays en développement. En ce qui concerne les titres fonciers, l'organisme public concerné ne délivre pas encore les titres aux propriétaires. La délivrance et une empreinte ou un hachage numériques des titres fonciers peuvent être enregistrés dans la chaîne de blocs pour fournir la preuve de propriété ou la légitimité des titres. On peut prévenir la fraude et l'altération de titres par des tiers de cette manière.

Dans les sous-sections suivantes, nous explorerons cette évolution en utilisant les catégories susmentionnées de biens privés et publics et de leur prestation par les secteurs privé ou public

Guillaume Bolduc

PUBLIC GOODS

Dans la plupart des économies en développement et des économies émergentes, les gouvernements sont, en principe, les principaux fournisseurs de biens publics, qu'il s'agisse de justice et de sécurité, ou encore de santé et d'éducation, pour ne nommer que ceux-là.[64] Cela ne signifie pas pour autant que les gouvernements fournissent eux-mêmes ces biens. La plupart du temps, cette mission est impartie à des partenaires privés à but lucratif et sans but lucratif.

C'est le cas en ce qui concerne la conception et la mise en oeuvre actuelles de technologies de chaînes de blocs dans l'hémisphère Sud. L'important retard accusé par la réglementation locale sur les nouvelles technologies s'est avéré en bonne partie la cause de ce phénomène, lequel s'est déjà produit avec d'autres technologies.[65]

SERVICES GOUVERNEMENTAUX

En principe, les technologies de chaînes de blocs pourraient être utilisées pour fournir des services gouvernementaux qui nécessitent le traitement et la gestion de documents publics auxquels les personnes ont difficilement accès, dans les pays en développement du moins. De manière plus générale, on peut se servir des chaînes de blocs pour appuyer la prestation générale de la plupart des biens publics aux citoyens et aux parties prenantes, particulièrement ceux qui exigent une interaction personnelle et une identification individuelle.[66]

Il existe un lien implicite entre la technologie des chaînes de blocs et le gouvernement électronique[67], et ce lien est exploré par un petit groupe de jeunes entreprises du domaine des chaînes de blocs. Procivis,[68] une jeune entreprise suisse, lancera bientôt une boutique d'applications relatives aux chaînes de blocs pour la prestation de certains services gouvernementaux au public. L'entreprise offrira également des services d'identité à ses clients.[69] L'Ukraine a récemment conclu une entente avec BitFury[70] pour le soutien de la prestation

BitFury

Fondée en 2011 comme exploitation minière de bitcoins, BitFury offre aujourd'hui une gamme complète de services de matériel et de logiciels pour l'écosystème des chaînes de blocs. L'entreprise est devenue très rentable et a affiché des revenus estimés à 93,7 millions de dollars américains pour l'exercice financier 2017. BitFury travaille avec différents acteurs des secteurs privé et public depuis son siège social à Amsterdam et ses bureaux de San Francisco, de Washington, DC, de Riga, en Lettonie et de Hong Kong.

BitFury travaille actuellement avec le ministère de la Justice de la Géorgie, le National Agency of Public Registry et l'économiste Hernando DeSoto pour gérer des titres fonciers et des services de notariat au moyen de chaînes de blocs, afin de permettre aux Géorgiens d'enregistrer plus rapidement et facilement les titres fonciers d'une manière juste et responsable. La nouvelle initiative de chaînes de blocs du gouvernement ukrainien est également appuyée par BitFury, qui mène des projets pilotes visant les registres, les services publics, la sécurité sociale, la santé publique et l'énergie de l'État.

BitFury a commencé à mettre au point une intelligence artificielle sur les chaînes de blocs pour l'industrie des soins de santé.

de services publics à ses citoyens, entre autres choses.[71] Dubai s'est aussi jointe à la vague des technologies de chaînes de blocs et a l'intention de devenir une ville de chaînes de blocs à part entière d'ici 2020 dans le cadre de l'initiative Smart Dubai.[72]

Les services de santé, qui sont un secteur riche en information, pourraient particulièrement profiter des technologies de grand livre réparti.

De nombreuses jeunes entreprises du domaine des chaînes de blocs soutiennent maintenant ces secteurs et travaillent dans des pays comme les Philippines et l'Estonie, pour ne nommer que ceux-là.[73] Comme nous l'avons mentionné plus tôt, la santé est l'une des cibles principales d'Hyperledger. En revanche, le secteur de l'éducation n'est pas parvenu à susciter beaucoup d'intérêt de la part des jeunes entreprises et des consortiums du domaine des chaînes de blocs.[74] La plupart des exemples qui suivent montrent comment les technologies de chaînes de blocs pourraient soutenir une grande variété de programmes et d'initiatives de gouvernement branché.

TITRES FONCIERS

Les titres fonciers ont peut-être été le premier domaine où la planification et le déploiement potentiel de la technologie des chaînes de blocs ont eu lieu dans un pays en développement. En 2015, le gouvernement du Honduras a conclu une entente avec Factom,[75] une jeune entreprise américaine, pour l'utilisation de chaînes de blocs visant à gérer l'enregistrement des titres fonciers et à empêcher la fraude et la corruption.[76]

Comment cela s'est-il produit ? Une fondation locale faisant la promotion des valeurs libertariennes a initialement approché Factom et a ensuite établi le lien de manière proactive entre cette dernière et le gouvernement central. Une entente confidentielle a

ensuite été signée. Toutefois, quelques mois plus tard, le projet a été interrompu pour des raisons qui demeurent nébuleuses.

L'année dernière, des initiatives similaires ont été lancées en Géorgie[77] et au Ghana.[78] Dans le cas de la Géorgie, l'économiste de renommée mondiale Hernando de Soto participe au projet en tant que membre du comité consultatif de BitFury, la jeune entreprise du domaine des chaînes de blocs qui met en oeuvre l'initiative.[79] Le cas du Ghana est possiblement plus intéressant, puisqu'une jeune entreprise sans but lucratif, BitLand,[80] utilise la chaîne de blocs du bitcoin pour gérer les titres fonciers et régler les différends. BitLand travaille en étroite collaboration avec les institutions locales dont la mission consiste à délivrer des titres fonciers et qui sont prêtes à essayer de nouvelles technologies pour résoudre des problèmes qui existent depuis des dizaines d'années. BenBen[81] est une autre jeune entreprise du Ghana qui travaille sur ce sujet.

Bien que les initiatives menées au Ghana semblent tomber à l'eau, la Suède va de l'avant avec son propre projet de titres fonciers et va au-delà de la validation de principe.[82] Quoi qu'il en soit, cela semble indiquer que les déploiements de chaînes de blocs dans les pays en développement font face à des défis de taille.

BitLand

Bitland est une plateforme expérimentale mise en place au Ghana pour combler le fossé entre le gouvernement et les régions non documentées où il n'y a pas de titres fonciers. Bitland, qui est une organisation bénévole, cherche à obtenir le consentement et l'approbation des personnes et des communautés, des horodateurs, et l'approbation gouvernementale. Malgré la bonne presse, le projet a rencontré divers obstacles qui ont retardé son déploiement. Il reste à voir si l'initiative réussira à mettre en place ses services, bien qu'un lancement mondial ait été prévu à l'automne 2017.

SERVICES D'IDENTITÉ

Comme nous l'avons mentionné plus tôt, Namecoin a mis au point une technologie de clé qui pourrait permettre de protéger et de vérifier l'identité personnelle, de promouvoir la liberté d'expression et d'empêcher la surveillance.

Plusieurs jeunes entreprises travaillent déjà sur les services d'identité fondés sur les chaînes de blocs.[83] Par exemple, OneID[84] fournit des services d'authentification à facteur multiple et d'authentification unique entre autres choses.[85] Cela semble être un des domaines les plus prometteurs pour l'utilisation réussie des chaînes de blocs, comme en fait foi le nombre grandissant de jeunes entreprises qui oeuvrent dans le domaine.

L'identité fondée sur la technologie des chaînes de blocs peut être utilisée de manière efficace pour gérer les passeports, les actes de naissance et de mariage et les pièces d'identité électorales, ainsi que pour s'occuper des programmes de résidence électronique, entre autres choses.

Toutefois, certains détracteurs soutiennent que les technologies d'identité numérique actuelles fonctionnent bien et sont bien plus extensibles que celles qui ont recours aux plateformes de chaînes de blocs.[86] Les limites à l'extensibilité de la technologie de chaînes de blocs pourraient empêcher le déploiement massif de ces dernières dans des pays populeux comme la Chine et l'Inde.[87]

LIBERTÉ D'EXPRESSION

De jeunes entreprises comme FlorinCoin[88] et Publicism[89] encouragent la liberté d'expression de différentes manières.[90] FlorinCoin a créé une application de GLR appelée Alexandria qui est censée être une banque de connaissances et d'information décentralisée administrée directement par les utilisateurs finaux.

Namecoin

L'administration des adresses et des noms de protocole Internet, le système de noms de domaine (DNS), a entraîné des problèmes relatifs à la gouvernance d'Internet. Pour le moment, la gouvernance d'Internet est assurée par une coalition réunissant de nombreuses parties prenantes. Elle est actuellement fortement centralisée, tout en étant répartie à l'échelle mondiale. La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), joue un rôle clé dans cette structure.

Namecoin, qui a été créée en 2012, est la première chaîne alternative dont l'objectif consistait à décentraliser la gestion du DNS. En modifiant le code source original du bitcoin, en créant sa propre chaîne de blocs et en permettant la saisie systématique de paires de clés et de noms, Namecoin a fourni les outils nécessaires à la gestion des noms de domaines et des identités personnelles. Toutefois, sa réussite a été plutôt limitée par rapport aux grands registraires de nom de domaine. La plateforme ne s'occupe que des domaines.bit, qui ne sont accessibles qu'au moyen de fonctions complémentaires particulières ou d'extensions ajoutées aux navigateurs habituels.

De plus, et ce point est peut-être encore plus important, Namecoin a eu peu ou pas d'influence sur les débats entourant la gouvernance d'Internet.

En raison de l'immuabilité inhérente aux chaînes de blocs, des problèmes relatifs au squat du DNS, des noms de domaine sans adresse de protocole Internet pertinente, et aux saisies possibles de nom, Namecoin semble être en difficulté.


Avel Chuklanov

Une des applications des chaînes de blocs est la conservation de contenu numérique censuré qui disparaît habituellement rapidement d'Internet. Floricoin a amélioré la chaîne de blocs en introduisant la possibilité de joindre des commentaires aux blocs de la chaîne. Publicism offre du soutien aux journalistes qui sont menacés de censure dans de nombreux pays en leur permettant d'utiliser des pseudonymes pour protéger leur identité.[91] MazaCoin,[92] dont le but est de soutenir les communautés autochtones des États-Unis, a récemment commencé à utiliser sa plateforme pour protéger la liberté d'expression et stocker des photos de protestation.[93]

LUTTE CONTRE LA CORRUPTION

Le National Democratic Institute des États-Unis s'est associé à BitFury,[94] l'entreprise qui travaille sur les titres fonciers en Géorgie, afin d'encourager les efforts de lutte contre la corruption au moyen d'une plateforme appelée Blockchain Trust Accelerator.[95] Le but est de promouvoir le développement d'applications de chaînes de blocs qui encouragent le gouvernement ouvert et la transparence. Pour l'instant, on a peu d'information sur l'accélérateur, qui a été lancé en juin 2016.

PROCESSUS ÉLECTORAUX

Des processus électoraux de toutes sortes ont également profité du déploiement et de l'utilisation des technologies de chaînes de blocs. Follow My Vote[96] est une jeune entreprise qui utilise des GLR pour mettre en oeuvre des processus de vote et empêcher la fraude et le vol d'identité. Un des avantages potentiels est que les votants qui utilisent les chaînes de blocs peuvent vérifier leur choix de vote au moyen de leur clé privée à tout moment.[97] L'Ukraine fait partie des pays qui se sont lancés dans ce domaine. L'Ukraine se servira de E-vox,[98] un GLR fondé sur Ethereum pour les élections locales. La mise en oeuvre a déjà commencé dans quelques villes.[99]

L'accès aux clés privées, que les pirates pourraient obtenir de différentes manières, est toutefois un des principaux problèmes de cette application[100]. Les votants pourraient aussi tenter de louer ou de vendre leur clé privée pour des raisons pécuniaires. Quand le vote au moyen de la chaîne de blocs aura fait ses preuves comme méthode viable, il sera intéressant de le comparer au vote en ligne, qui est déjà utilisé en Estonie.[101]

NOUVELLES FORMES DE GOUVERNEMENT

Certaines plateformes de chaînes de blocs visent à remplacer le gouvernement, ou à l'émuler, du moins. Bitnation[102], qui permet aux utilisateurs de créer leur propre pays sans frontière offrant une gamme de services à ses citoyens, en est le meilleur exemple. Les pays ainsi créés ont leur propre constitution. Certains offrent même un revenu de base à leurs citoyens.[103]

AIDE ET DÉVELOPPEMENT

Aid:Tech, une entreprise basée à Londres, est peut-être la première jeune entreprise de technologie de chaînes de blocs à avoir soutenu les efforts humanitaires et les projets de développement au Moyen-Orient.[104] L'entreprise propose un système de bons qui peut être utilisé dans les circonstances les plus difficiles et qui aide à garantir que les ressources financières se rendent à leur destination finale de manière sécuritaire. Bitnation offre également du soutien aux réfugiés.[105]

Du côté de l'ONU, l'UNICEF (le Fonds des enfants des Nations Unies) a déboursé 100 000 dollars américains en appui à la jeune entreprise 9Needs[106] et prévoit faire la même chose pour cinq à dix autres jeunes entreprises.[107] 9Needs travaille sur des innovations dans les domaines de la santé et du développement.

Le PNUD (Programme des Nations Unies pour le développement) soutient les transferts de fonds et

Bitnation

BitNation, founded in 2014, is a "Virtual Nation", a decentralized nation not linked to any territory and only existing in the blockchain. BitNation aims to provide the same services as a traditional government, but in a way that is not bound by geography – rather, education, health services, and notary services are provided through the chain or through local contractors. BitNation has developed agreements with Estonia to support notary services for their e-Residents project. In 2015, BitNation developed a "Blockchain Emergency ID" as a response to the refugee crisis, allowing refugees who could not get other identity documents to receive an ID recorded on their identification documents and to receive Bitcoin Visa cards with funds that can be used in Europe. Bitnation has received a significant amount of media coverage since its inception, and represents a very libertarian position towards statehood.

9Needs

9needs, based in South Africa and started in 2012, uses blockchain and identity technology to tackle post-Apartheid social issues. Their most developed project is Amply, with aims to help the government use blockchain to manage Early Childhood Development Services. In 2016, 9needs received funding from the UNICEF Innovation Fund, and is being piloted at 50 centres in South Africa to help strengthen registration, contracting, and information management systems.

les outils financiers en Serbie et en Moldova, et a l'intention d'étendre ses activités à d'autres pays sous peu.[108]

Le PAM (Programme alimentaire mondial des Nations Unies) a annoncé un projet pilote de chaînes de blocs au moyen d'Ethereum pour fournir de l'aide financière aux personnes dans le besoin en Jordanie, en s'appuyant sur les résultats d'une initiative plus modeste menée au Pakistan.[109] Selon un rapport, sept agences des Nations Unies explorent ou utilisent des technologies de chaînes de blocs pour soutenir leurs activités et leurs programmes.[110]

RÉCAPITULATION

Les déploiements de technologies de chaînes de blocs dans les pays en développement n'ont pas encore causé de perturbations majeures d'une manière soutenue. La plupart des déploiements sont axés sur l'offre et fonctionnent comme des initiatives autonomes qui ne sont pas liées à des programmes en cours; les institutions locales ne jouent qu'un rôle passif dans ces déploiements et leur participation soutenue est limitée. Les défis économiques et politiques locaux demeurent ardus, ce qui ne changera pas à moins que les responsables des déploiements de technologies de chaînes de blocs adoptent une approche plus globale.

Par conséquent, les initiatives relatives à la technologie des chaînes de blocs dans le cadre de programmes de gouvernement branché et de services d'identité plus vastes sont celles qui ont les meilleures chances de réussite à moyen terme.

BIENS PRIVÉS

La fourniture de biens privés de la technologie des chaînes de blocs comporte une composante de viabilité financière interne qui fonctionne comme un aimant en attirant des fournisseurs, pourvu que les prix demeurent compétitifs. Malgré tout, des milliards de personnes dans le monde n'ont pas accès à ces biens, particulièrement en ce qui a trait aux services bancaires. Lorsque ces personnes, qui sont pauvres, ont un accès minimal à de tels biens, elles doivent payer des frais extraordinairement élevés pour utiliser des services privés comme des envois d'argent.[111] L'agriculture est un autre secteur où les biens privés sont omniprésents. Il s'agit aussi d'un secteur qui fournit un moyen de subsistance à la plupart des pauvres du monde.[112] Les droits de propriété intellectuelle sont un autre domaine où les technologies de chaînes de blocs pourraient protéger efficacement les biens numériques et non numériques et garantir que les redevances sont acheminées aux créateurs et aux innovateurs.

Clark Young

SERVICES BANCAIRES POUR LES PERSONNES QUI N'ONT PAS DE COMPTE DE BANQUE

M-Pesa, un produit d'innovation mobile du Kenya, a été la première tentative fructueuse visant à fournir des services bancaires de base aux personnes qui se trouvent au bas de la pyramide. Aujourd'hui, plus de 90 pays emploient des stratégies similaires pour offrir des services à près d'un demi-milliard

de personnes. Toutefois, près de deux milliards de personnes n'ont toujours pas accès à des services bancaires de base.[113]

C'est à ce chapitre que les entrepreneurs espèrent que la chaîne de blocs, par l'intermédiaire de BitPesa.[114] BitPesa, qui est une jeune entreprise basée au Kenya et administrée par des expatriés, soutienne les transactions et les paiements entre les entreprises africaines et le reste du monde au moyen de la chaîne de blocs du bitcoin. En principe, la plateforme est ouverte à tous, ce qui comprend les petites entreprises et les microentreprises qui pourraient utiliser ces services pour accroître leur chiffre d'affaires. BitPesa est donc nettement différente de M-Pesa. Pourtant un litige oppose les deux entreprises depuis quelques mois.[115] BitPesa est active en République démocratique du Congo, au Kenya, au Nigéria, en Tanzanie et en Ouganda, et a des partenaires aux États-Unis et en Chine. Outre les paiements, BitPesa convertit des bitcoins en devises locales, ainsi qu'en dollars américains et autres devises.

BitSoko[116] est une autre jeune entreprise kenyane qui propose un portefeuille de bitcoin Android afin de réduire les coûts de transaction plutôt élevés des autres plateformes d'argent mobile, comme M-Pesa. Ces coûts oscillent entre quatre et dix pour cent, et BitSoko cherche à réduire ces frais à moins d'un demi pour cent. Elle offre aussi une plateforme plus sûre et transparente en tirant parti des avantages de la chaîne de blocs du bitcoin. En 2015, BitSoko a reçu l'appui de la Fondation Bill et Melinda Gates pour créer essentiellement le portefeuille de services qu'elle offre aujourd'hui.[117] Bien que BitSoko ait l'intention de prendre en charge les téléphones polyvalents dans un avenir rapproché, la plateforme d'application n'est offerte que pour les téléphones intelligents, ce qui limite la couverture et l'utilisabilité pour les personnes qui peuvent se payer le téléphone intelligent plus coûteux. Dans ce contexte, BitSoko

BitPesa

Bitpesa, a quickly growing company, has merged mobile money and blockchain technology. From the early pilot in 2013, it has received significant startup funding to serve emerging markets that include Nigeria, Kenya, Tanzania, Uganda, the Democratic Republic of the Congo and Senegal, as well as the UK. Bitpesa takes Bitcoin payments and exchanges them for local currencies which are then deposited into bank accounts or mobile money wallets. Bitpesa promises to be a cheap way to transmit money and remittances internationally, especially for underserved markets in the mobile money space in Africa.

accuse toujours un retard important sur M-Pesa et les autres plateformes d'argent mobile. Il convient de noter que BitPesa et BitSoko permettent également les envois d'argent.

En avril 2017, la Fondation Bill et Melinda Gates a lancé sa propre initiative pour soutenir la prestation de services financiers aux pauvres. L'initiative fournira aux gouvernements des cadres pour l'utilisation de la technologie des chaînes de blocs; toutefois, cette initiative comporte également des limites du point de vue de l'extensibilité et de la gouvernance.[118]

ENVOIS D'ARGENT

Les envois d'argent sont probablement l'un des domaines les plus compétitifs de l'écosystème des chaînes de blocs, sans doute en raison de la taille du marché et de leur rentabilité. En 2015 seulement, les envois d'argent se sont élevés bien au-delà de 500 milliards de dollars américains. À eux seuls, les États-Unis étaient responsables du quart des envois.[119] Cette année, le coût moyen des transactions d'envoi d'argent était de près de sept et demi pour cent, et c'est en Afrique que le coût était le plus élevé. L'utilisation de banques traditionnelles entraîne des coûts beaucoup plus élevés (jusqu'à 11 pour cent), tandis que les cartes prépayées, à un taux moyen de 1,75 pour cent[120], demeurent les plus abordables

Il s'agit certainement d'un domaine où la compétition relative à la technologie des chaînes de blocs est déjà intense. En effet, une trentaine de jeunes entreprises et d'entreprises établies offrent déjà des services d'envoi d'argent dans de nombreux pays.[121] Abra,[122] une jeune entreprise basée aux Philippines qui a récemment obtenu du soutien financier de la part d'investisseurs en capital-risque internationaux, en est un bon exemple. Abra a maintenant l'intention d'étendre ses activités à d'autres pays en utilisant la chaîne de blocs du bitcoin. Il est à noter que l'application actuelle n'est offerte que pour les téléphones intelligents. Les utilisateurs qui n'ont pas accès à un tel appareil doivent donc utiliser un ordinateur ou un appareil similaire pour avoir accès aux services.

Un autre exemple est Rebit,[123] également basée aux Philippines, qui est soutenue par une plus grande société dont le but est de promouvoir le bitcoin dans le pays,[124] et qui permet d'envoyer de l'argent à n'importe quel pays depuis les Philippines. Rebit prétend ne pas facturer de frais d'utilisation, mais exige que

les utilisateurs achètent des bitcoins pour utiliser le service. Les destinataires reçoivent la devise locale, car Rebit s'occupe de la conversion (et garde ainsi les bitcoins), et sont avisés par courriel et par message texte.

Du point de vue du développement, le Programme des Nations Unies pour le développement (PNUD) a récemment annoncé le lancement d'un projet pilote d'envoi d'argent au moyen de la chaîne de blocs en Serbie,[125] alors que l'UNICEF explore les technologies de chaînes de blocs pour les transferts de fonds.[126]

En raison de la part de marché plutôt importante du secteur, les envois d'argent semblent être l'un des secteurs les plus intéressants, et par le fait même compétitifs, en ce qui a trait au déploiement des technologies de chaînes de blocs. Abra et BitPesa[127] sont deux des six principales entreprises d'envoi d'argent au moyen de la technologie des chaînes de blocs, mais elles pourraient être facilement délogées par d'autres entreprises qui commencent à croître et à s'accaparer une plus grande part du marché.

AGRICULTURE

Bien que le secteur agricole dans les pays industrialisés dépende en grande partie de l'utilisation de technologies de toutes sortes, ce n'est certainement pas le cas de la plupart des pays en développement. En fait, le secteur a l'un des plus bas niveaux d'investissement technologique, surtout chez les petits exploitants agricoles. Les technologies mobiles ont changé un peu la donne en fournissant de l'information et des services aux producteurs, y compris pour l'établissement des prix. Il ne manque donc pas de jeunes entreprises dans le domaine des chaînes de blocs qui émergent pour soutenir ce secteur. Les applications courantes comprennent: les produits de suivi et les chaînes d'approvisionnement, la facilitation des paiements aux producteurs, la surveillance des prix pour s'assurer d'obtenir un juste prix pour un produit et l'amélioration de l'agriculture soutenue par la communauté.[128] À titre d'exemple, Skuchain[129] utilise des contrats intelligents pour le suivi des chaînes d'approvisionnement agricole (qui sont aussi utilisés dans de nombreux autres secteurs).[130] Toutefois, ce service semble aussi exiger un haut niveau de sophistication qui n'est peut-être pas à la portée de la plupart des petits exploitants agricoles plus pauvres de l'hémisphère Sud.

Farmshare[131] soutient l'agriculture communautaire qui encourage les formes de propriété collective et les processus de travail collectif pour le développement des économies locales. Farmshare utilise également des contrats intelligents et des applications réparties pour promouvoir les produits locaux et s'assurer que les paiements sont distribués entre les communautés participantes.[132]

Bitmari[133], un autre service de portefeuille de bitcoins africain pour l'envoi d'argent, soutient un accélérateur et une fiducie pour les cultivatrices du Zimbabwe.[134] Le projet utilise le sociofinancement pour recueillir des bitcoins afin de financer une centaine d'agricultrices qui sont censées recevoir de l'assistance technique de la part d'experts

SÉCURITÉ ALIMENTAIRE

Pour ce qui est de la sécurité alimentaire et du soutien des petits exploitants et des petites coopératives agricoles, AgriLedger[135] semble être le chef de file incontesté. Grâce à la chaîne de blocs et à une application mobile qui fonctionne sur les téléphones intelligents, AgriLedger permet aux agriculteurs de surveiller toutes leurs transactions, tout en fournissant un identificateur unique à chaque utilisateur final. Nul besoin de dire que l'application nécessite l'accès à des réseaux mobiles avec un accès aux données. À l'heure actuelle, on ne peut pas affirmer avec certitude que AgriLedger prévoit offrir un accès hors ligne.

Zbysiu Rodak

DROITS DE PROPRIÉTÉ INTELLECTUELLE

En tant que plateforme immuable, répartie et transparente comportant des jetons financiers intégrés, la technologie des chaînes de blocs semble être dans une position idéale pour soutenir la protection des droits de propriété intellectuelle. Un bon exemple en est la création de registres de propriété intellectuelle fondés sur la technologie des chaînes de blocs où les propriétaires de propriétés intellectuelles peuvent conserver des certificats numériques hachés de leurs propriétés intellectuelles et même utiliser la plateforme pour obtenir des redevances auprès de ceux qui utilisent leurs inventions en se servant de contrats intelligents.[136] Curieusement toutefois, il s'agit d'un domaine qui a reçu relativement peu d'attention de la part de l'écosystème des technologies de chaînes de blocs.

Jenny Hill

Ascribe[137] est l'une des jeunes entreprises qui travaillent dans ce domaine. Elle se concentre sur la protection de la propriété intellectuelle des artistes. Elle utilise la chaîne de blocs du bitcoin, mais a mis au point un protocole à source ouverte qui interagit avec la chaîne et permet aux utilisateurs d'enregistrer leur propriété intellectuelle.[138] Les artistes peuvent obtenir des certificats d'attribution et des certificats de propriété et gérer l'exploitation sous licence de leurs oeuvres par des tiers.

On pourrait s'attaquer efficacement aux problèmes de piratage de cette manière, mais la protection de la propriété intellectuelle fondée sur la chaîne

de blocs doit être coordonnée avec les gouvernements et les législateurs pour pouvoir être appliquée d'un point de vue juridique. C'est peut-être cette situation qui dissuade les intervenants de développer et de déployer les chaînes de blocs dans ce domaine. D'autre part, les questions relatives à l'utilisation juste de la propriété intellectuelle pourraient être compromises par un régime de propriété intellectuelle fondé sur la chaîne de blocs.[139]

RÉCAPITULATION

La plupart des initiatives de chaînes de blocs qui visent ce groupe de biens privés montrent beaucoup de potentiel, mais n'ont pas encore pris leur envol.[140] Certaines ont déjà cessé ou ont été interrompues, alors que d'autres ont du mal à générer des revenus intéressants. Cette condition peut être un symptôme de la compétition intense entre jeunes entreprises dans un marché qui en est encore à ses balbutiements et où le précieux capital de risque se fait rare. Les progrès attribuables à la technologie des chaînes de blocs dans des domaines comme les services bancaires pour les pauvres et l'agriculture sont limités et sont éclipsés par d'autres technologies comme les services mobiles. Dans ce contexte, les envois d'argent et l'argent numérique semblent être les domaines les plus prometteurs à ce stade.

CONCLUSION

L'examen des applications de la technologie des chaînes de blocs révèle que les barrières à l'entrée demeurent élevées comparativement aux autres technologies comme les applications mobiles. L'innovation dans le domaine des services mobiles s'est étendue rapidement aux pays en développement malgré les niveaux plus faibles de compétence en matière de technologie et l'accès limité à Internet, et l'émergence de plus de 100 carrefours technologiques sur le continent africain en est une preuve solide.[141]

L'innovation dans le domaine de la technologie des chaînes de blocs semble exiger des connaissances et des capacités plus importantes. Bien que les carrefours technologiques et les techno-entrepreneurs soient actifs dans les pays en développement depuis de nombreuses années, l'adoption locale des chaînes de blocs s'est révélée plutôt lente, et certainement pas aussi impressionnante que celle des technologies mobiles. Cela ne signifie pas pour autant que les initiatives de chaînes de blocs soient vouées à l'échec dans l'hémisphère Sud. Au contraire, dans la plupart des cas, on met à l'essai la technologie dans plusieurs secteurs, et ce, pour la première fois. Certaines jeunes entreprises de l'hémisphère Sud ont en effet tiré parti des technologies de chaînes de blocs, mais déploient des formes conventionnelles mises au point dans le Nord, et bien que les tendances actuelles indiquent que l'innovation dans le domaine des chaînes de blocs se produit surtout dans le Nord, le déploiement a lieu à l'échelle mondiale, ce qui aura rapidement une incidence sur les écosystèmes d'innovation du Sud.

Chaînes de blocs et développement humain

Dans la section précédente, nous avons eu un aperçu d'applications de la technologie des chaînes de blocs qui pourraient être utiles au développement. Bien que l'on puisse conclure que la gamme d'applications est vaste, la profondeur globale demeure faible. Bon nombre des initiatives décrites plus haut en sont encore au stade sur papier ou sont sur le point de débuter, alors que d'autres sont pleinement opérationnelles, mais ne servent que très peu de clients et de parties prenantes, et de nombreuses initiatives ont mordu la poussière. C'est peut-être en raison du fait que la technologie en est toujours à ses balbutiements et qu'elle commence à peine à prendre son envol.

Quoi qu'il en soit, les praticiens du développement qui cherchent des solutions novatrices pour combler les lacunes traditionnelles doivent avoir une connaissance non technique adéquate du potentiel que les technologies de chaînes de blocs pourraient avoir pour le soutien et l'amélioration des programmes de développement. Dans la présente section, nous explorons le cadre analytique présenté à l'annexe I, en adoptant aussi le point de vue de la gouvernance pour déterminer de manière plus précise le potentiel de la chaîne de blocs pour l'amélioration de la gouvernance démocratique.

INFRASTRUCTURE ET INFOSTRUCTURE

Les données récentes indiquent que près de quatre milliards de personnes n'ont pas d'accès Internet, et que la plupart d'entre elles vivent dans les pays en développement.[142] De plus, les personnes qui vivent dans les centres urbains de l'hémisphère Sud ont accès aux plus récentes technologies et à une bande passante adéquate, tandis que les communautés rurales et marginalisées de même que les personnes trop pauvres pour acheter l'accès ou les outils technologiques ne l'ont pas. Il semble donc peu probable que les personnes qui vivent dans ces conditions puissent devenir des noeuds d'un réseau de chaînes de blocs ou puissent utiliser efficacement des logiciels de portefeuille pour au moins profiter de la technologie en tant qu'utilisateurs finaux.[143] Il est vrai que cela ne concerne pas seulement les chaînes de blocs. Cependant cet état de fait a une incidence sur la manière dont la technologie devrait être déployée et exploitée si le but ultime des interventions consiste à encourager le développement humain des personnes qui sont exclues de la société.

Les chaînes de blocs sont uniques en raison de l'utilisation obligatoire d'outils cryptographiques qui nécessitent la mise en place d'une infrastructure différente, que l'on appelle aussi infostructure: une infrastructure à clés publiques.[144] L'infrastructure à clés publiques, qui englobe les rôles, les politiques et les procédures nécessaires pour assurer le transfert électronique sécuritaire de l'information, n'est pas encore en place dans de nombreux pays en développement. Cette circonstance pose de sérieux obstacles à l'utilisation systématique de la technologie des chaînes de blocs. C'est particulièrement vrai en ce qui a trait à la fourniture efficace et transparente de biens publics d'une manière répartie. Il n'est donc pas surprenant que les défenseurs de la technologie aient déjà recommandé le déploiement d'une infrastructure à clés publiques décentralisée au moyen de la technologie des chaînes de blocs, pour ainsi contourner le modèle centralisé traditionnel.[145]

DÉVELOPPEMENT DES CAPACITÉS

Du point de vue des utilisateurs finaux, l'utilisation d'outils cryptographiques de manière régulière peut représenter un défi redoutable. Une étude récente réalisée auprès d'étudiants américains, dont un bon nombre étaient natifs du numérique, indique que même chez cette population, d'énormes obstacles doivent être surmontés avant que les outils cryptographiques deviennent

courants.[146] De la même manière, le lanceur d'alerte Ed Snowden a eu de la difficulté à communiquer avec les journalistes en raison de l'incapacité de bon nombre de ces derniers à utiliser ces outils et encore moins à installer les logiciels nécessaires sur leur ordinateur portatif.

On se bute à deux problèmes ici. Le premier concerne l'utilisation de ces outils. Le second concerne la gestion des clés privées et publiques des utilisateurs finaux. Comme nous l'avons mentionné plus tôt, les portefeuilles de chaîne de blocs peuvent et ont certainement fourni des interfaces conviviales qui facilitent la création et l'utilisation de la cryptographie à clés publiques, même si l'utilisateur n'en comprend pas très bien son fonctionnement.[147]

Mais les utilisateurs doivent pouvoir gérer leurs clés privées et les stocker de manière sécuritaire quelque part, d'une manière ou d'une autre. Ensemble, ces deux problèmes peuvent se révéler trop difficiles pour les populations relativement peu éduquées et alphabétisées, et qui font face à l'exclusion sociale.

Comme nous l'avons mentionné dans la section 3 ci-dessus, quelques jeunes entreprises des pays en développement ont connu un certain succès dans l'exploitation des chaînes de blocs, malgré l'adoption limitée de ces dernières par les clients. La plupart d'entre elles utilisent la chaîne de blocs du bitcoin.

Toutefois, aucune de ces jeunes entreprises ne propose d'innovations permettant d'adapter le code aux contextes locaux ou de mettre au point de nouvelles fonctions et, contrairement aux applications de technologie mobile, on ne développe pas d'applications réparties. Cela laisse fortement supposer que des compétences techniques plus pointues sont requises pour l'implantation au niveau local.

Des pays comme le Ghana et le Kenya ont profité des carrefours technologiques et des réseaux existants pour tirer parti des chaînes de blocs et disposent donc d'un écosystème d'innovations naissant qui pourrait soutenir le développement local. À moyen terme, cet écosystème pourrait devenir une rampe de lancement pour l'innovation dans le domaine des chaînes de blocs dans l'hémisphère Sud, particulièrement si du capital de risque ou d'autres mécanismes financiers externes sont proposés, ce qui comprend l'aide au développement.

POLITIQUES ET RÉGLEMENTATION

Comme pour de nombreuses autres technologies qui encouragent ce que l'on appelle l'« économie de partage[148], les technologies de chaînes de blocs dont le bitcoin est le fer de lance sont en avance sur les politiques et la réglementation locales. Les pays industrialisés ont déjà commencé à rattraper leur retard, mais ce n'est certainement pas le cas dans la plupart des pays en développement, où les capacités stratégiques et réglementaires sont encore naissantes. Cet écart entraîne l'utilisation des technologies de GLR dans l'hémisphère Sud, non seulement par les jeunes entreprises locales, mais aussi par celles du Nord. Les pays du Nord peuvent devenir des lieux où l'on met en oeuvre des projets pilotes de validation de principe et où l'on déploie des prototypes, ce qui permet d'améliorer l'expertise et les avantages concurrentiels à l'échelle mondiale. En fait, cela est déjà en train de se produire dans plusieurs pays en développement.

L'absence de politiques relatives à l'infrastructure à clés publiques dans ces pays peut aussi être considérée au départ comme un moteur pour les chaînes de blocs, mais, d'autre part, elle peut aussi devenir un frein si des problèmes de sécurité liés à la gestion des clés publiques, comme le vol ou le trafic de clés, apparaissent.[149]

Advenant de tels problèmes, il devient nécessaire de mettre en place des politiques relatives à l'infrastructure à clés publiques, même si la mise en oeuvre est accomplie selon des modèles décentralisés fondés sur des technologies de chaînes de blocs.

L'adhésion exclusive au bitcoin par la plupart des jeunes entreprises qui utilisent les chaînes de blocs fait en sorte que les politiques et la réglementation relatives aux cryptomonnaies soient si importantes. Cela comprend les services qui offrent la conversion de bitcoins ou d'autres cryptomonnaies en devises locales, ainsi que l'utilisation de cryptomonnaies comme monnaie légale. En outre, les politiques et la réglementation locales sont également importantes pour des raisons de sécurité dans les pays où les conflits et l'extrémisme violents sont endémiques, et le financement de ces activités devrait être surveillé de près afin d'empêcher leur propagation dans le monde.

Zi Jian Lim

INSTITUTIONS

LES RÉSEAUX RÉPARTIS ET L'ÉTAT

Comme ce fut le cas pour certaines des technologies Internet précédentes, les chaînes de blocs peuvent aussi contribuer à réduire davantage certaines formes de gouvernement central, sinon toutes. En effet, une des raisons pour lesquelles Nakamoto a mis au point le bitcoin était la réaction des gouvernements à la crise économique mondiale de 2007-2008.[150] Bon nombre des premiers tenants de la chaîne de blocs du bitcoin étaient des libertariens qui considéraient la nouvelle technologie comme étant l'outil le plus efficace pour éliminer l'interventionnisme étatique pour de bon.[151] La nature répartie de la technologie combinée à une nouvelle forme de confiance décentralisée et de consensus réparti alimentent cette opinion.

Toutefois, cela ne signifie pas forcément que la chaîne de blocs est liée de manière inextricable à ce point de vue. En fait, et comme nous l'avons décrit dans la section précédente, de nombreuses jeunes entreprises du domaine des chaînes de blocs travaillent directement avec les gouvernements pour déployer la technologie au niveau de l'État. Plus récemment, le créateur d'Ethereum a changé de point de vue en ce qui a trait à la pertinence de la philosophie libertarienne dans la conjoncture politique actuelle.[152]

Un des enjeux ignorés en bonne partie jusqu'à maintenant est le potentiel des chaînes de blocs pour le soutien et l'amélioration de la décentralisation gouvernementale dans les États-nations. La décentralisation de l'État, aussi appelée gouvernance locale, est un des grands enjeux du développement, et de nombreux pays en développement se sont déjà dotés de politiques générales de décentralisation. Toutefois, les gouvernements locaux sont aux prises avec des problèmes majeurs de fiscalité et de capacités et sont incapables de fournir des biens publics.

La technologie des chaînes de blocs pourrait par conséquent présenter des avantages réels pour les gouvernements locaux. L'argument en faveur des services gouvernementaux décentralisés ou répartis que les experts des chaînes de blocs avancent pourrait se révéler une occasion très avantageuse pour toutes les parties concernées.

CAPACITÉS INSTITUTIONNELLES

L'exploitation des nouvelles technologies par les pays en développement nécessite non seulement des ressources fiscales, mais aussi des capacités institutionnelles qui en facilitent le déploiement de manière soutenue. Ces capacités ne se limitent pas au savoir technologique. Elles comprennent aussi les capacités administratives et des règles du jeu claires entièrement établies et applicables de manière légale. De nombreux pays en développement sont toujours en train de développer ces capacités, ce qui limite sérieusement leur capacité à profiter eux aussi de l'apparition d'innovations technologiques comme les chaînes de blocs, notamment. Comme nous l'avons vu dans les exemples de la section 4, cette condition n'a toutefois pas empêché ces pays d'utiliser les technologies les plus récentes. Au contraire, les institutions des pays en développement peuvent adopter l'utilisation des chaînes de blocs en important le savoir-faire et l'expertise nécessaires ou en faisant appel à l'expertise locale, si elle est offerte, à l'extérieur du gouvernement. Le véritable problème est que ces initiatives ne sont pas nécessairement viables à moyen terme. Elles sont habituellement menées en vase clos, sans lien avec les autres institutions publiques, et en dehors des processus de politiques qui servent à allouer des ressources fiscales aux institutions publiques.

D'un point de vue institutionnel, il est également important de tenir compte de la manière dont les chaînes de blocs devraient être utilisées dans le secteur public. Bien que l'opinion actuelle suggère que les technologies de chaînes de blocs devraient remplacer entièrement les processus existants, il est aussi possible de voir la technologie comme un complément aux processus[153] et comme une source d'innovation dans le secteur public.

Enfin, il est essentiel de faire une distinction entre la conception et la mise en oeuvre des initiatives de chaînes de blocs. Bien que les institutions publiques doivent participer à la conception, la mise en oeuvre peut être réalisée par des partenaires privés (à but lucratif et sans but lucratif), qui sont mieux qualifiés pour cette tâche.

En fait, c'est ce qui s'est produit dans le cas du développement des applications mobiles dans les pays en développement. Cependant, il semble que ce ne soit pas le cas des projets pilotes actuels en matière de technologie des chaînes de blocs. Et cette situation pourrait avoir une incidence négative sur la mise à l'échelle et sur la viabilité à long terme des projets pilotes en question.

LA GOUVERNANCE DES CHAÎNES DE BLOCS

Les appels en faveur d'un nouveau contrat social soulèvent d'importantes questions concernant la chaîne de blocs: Qui est responsable ? Qui rédigera ce contrat ? Comment tous les points de vue peuvent-ils être pris en compte ?[154] La réponse rapide du camp des chaînes de blocs est simple: personne n'est responsable puisque, par défaut, on n'a pas besoin de responsable[155]. En fait, tout le monde est responsable puisque la gouvernance est assurée uniquement par consensus. Ce consensus est à son tour fondé sur des algorithmes[156] qui permettent aux utilisateurs et aux noeuds de s'entendre presque automatiquement sur les résultats du processus.

Une des idées centrales de la gouvernance par consensus algorithmique est l'organisation décentralisée autonome. Des groupes de personnes qui cherchent à promouvoir un résultat commun, un objectif stratégique ou une intervention politique se réunissent et s'entendent sur une série de principes qui sont programmés dans des logiciels. Le logiciel prend ensuite le contrôle de l'ensemble de l'opération et relègue les personnes, qui n'ont plus besoin d'interagir entre elles, à l'arrière-plan. Ce scénario soulève plusieurs questions qui peuvent être résumées comme suit:

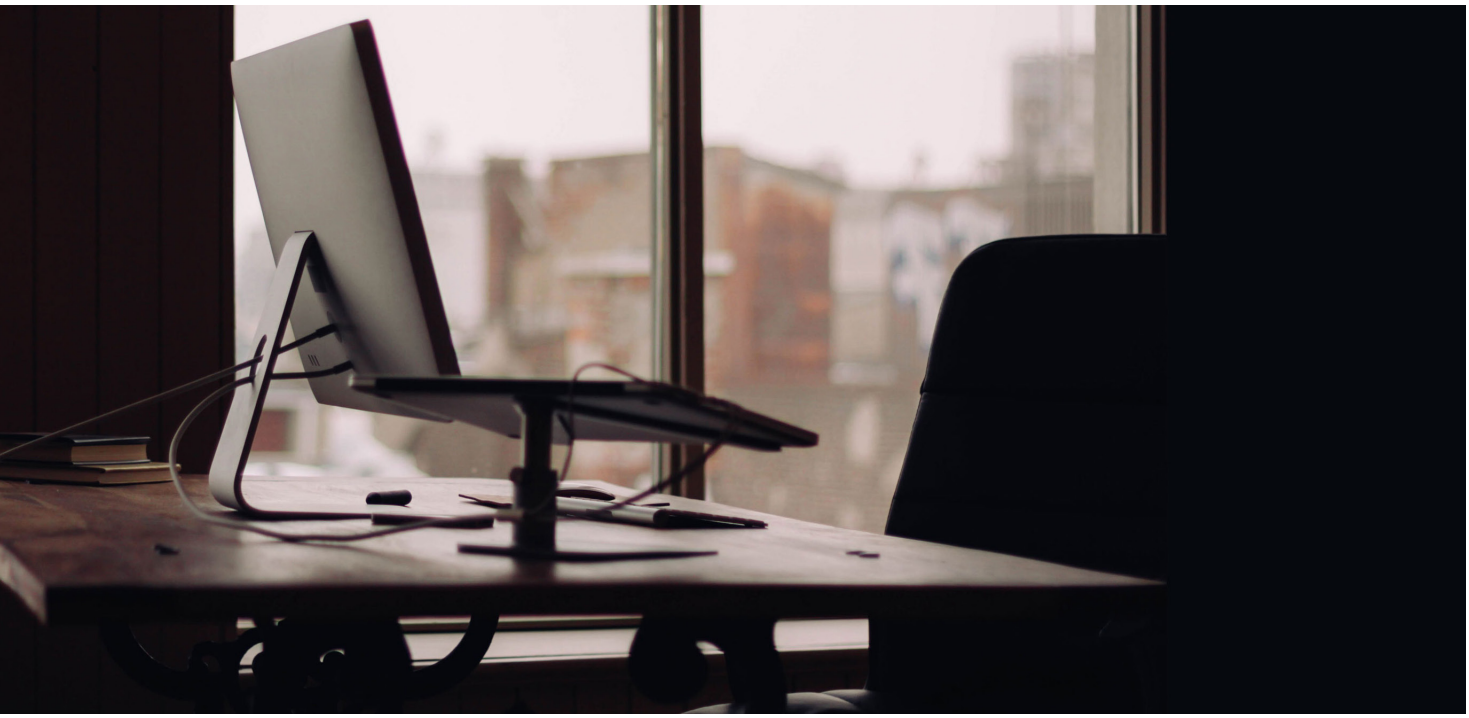
Programmation: Qui s'occupe concrètement de la programmation ? Comment les a-t-on choisis? La programmation prévoit la traduction des ententes entre les membres des organisations décentralisées autonomes dans un certain langage de programme, ce qui comprend l'apprentissage machine, qui exécute le contrat intelligent et déclenche automatiquement des événements particuliers lorsque certaines conditions sont réunies.

Compréhension du code: Qui peut vraiment lire et vérifier le code ? La plupart des chaînes de blocs font appel à un logiciel à source ouverte, ce qui veut dire que tout le monde a accès au code. Mais les utilisateurs doivent être capables de le lire et de le comprendre. Par analogie, pour pouvoir lire un livre gratuit en chinois, il faut connaître la langue.

Sinon, le livre gratuit est sans utilité pour le lecteur potentiel, peu importe son coût. Les personnes qui ne peuvent pas lire le code devront alors trouver un tiers digne de confiance qui peut s'assurer que le code correspond à ce qui a été convenu.[157]

Extensibilité: Comme il a été décrit dans la section 2, les chaînes de blocs comportent des limites bien connues en ce qui a trait à leur extensibilité. Même si des innovations dans le secteur peuvent éventuellement aider à résoudre ce problème, la poussée pour limiter le nombre de chaînes de blocs à un minimum pourrait être contre-productive.

Mais si le nombre augmente, l'interopérabilité entre les chaînes de blocs devient un problème plus important.[158] En outre, quelle sera l'incidence de l'extension de



Luke Chesser

la technologie des chaînes de blocs à des milliards d'utilisateurs et de noeuds sur l'atteinte d'un consensus décentralisé ? Des problèmes de représentation démocratique pourraient survenir dans le réseau dans un avenir rapproché.

Opposition confiance-gouvernance: Le fait que la confiance soit décentralisée et dépersonnalisée pour incomber plutôt à un réseau réparti ne signifie pas automatiquement une gouvernance améliorée.[159] À titre

d'exemple, les noeuds et les utilisateurs qui ne faisaient pas partie de la conception originale de la chaîne de blocs n'ont pas participé au processus et aux décisions de gouvernance prises par ceux qui en faisaient partie. Les utilisateurs se joignent au réseau dans des conditions données ou passent à autre chose s'ils ne sont pas satisfaits.

Malgré la répartition et la décentralisation des chaînes de blocs, ces questions mettent en évidence le fait que ces dernières ne peuvent pas garantir que des hiérarchies et des inégalités sociales entre utilisateurs n'apparaîtront pas. En fait, c'est exactement ce qui semble se produire en ce moment dans le minage des chaînes de blocs.160 Il en va de même pour les programmeurs, les développeurs et les techno-entrepreneurs de chaînes de blocs, qui semblent tous jouir d'une position privilégiée dans le réseau et qui peuvent exercer un pouvoir considérable sur les autres noeuds. L'inégalité dans un réseau décentralisé est donc possible.

Enfin, certains enthousiastes des chaînes de blocs semblent croire que des algorithmes programmés par quelques personnes compétentes pourraient ou devraient diriger la société, voire remplacer les interactions personnelles.161 Toutefois, les algorithmes ne sont pas neutres ou immédiatement transparents pour la plupart des gens.162 Ce qu'il faut peut-être davantage, c'est un réseau décentralisé qui garantit la transparence et la gouvernance démocratique des algorithmes.

Du point de vue de la gouvernance et du développement, la plupart des points abordés plus haut supposent un niveau considérable de développement des institutions et des valeurs démocratiques. L'utilité réelle pour un pays en développement donné devrait être évaluée au cas par cas. Cependant, en principe, plus le niveau de développement humain est faible, plus il sera compliqué de mettre en oeuvre la technologie des chaînes de blocs de manière systématique.

Conclusions

Des défis, que les praticiens du développement des technologies de l'information et de la communication connaissent bien, menacent l'adoption et l'utilisation répandue des technologies de chaînes de blocs. La complexité de la technologie des chaînes de blocs en tant que telle est possiblement un nouvel ingrédient dans la recette. Cela pose de nouveaux problèmes et représente de nouveaux obstacles du point de vue du déploiement de la technologie et de sa diffusion aux utilisateurs finaux et aux parties prenantes. C'est certainement le cas dans les situations où le développement de l'infrastructure et les capacités locales sont inférieurs à la moyenne mondiale.

La technologie des chaînes de blocs en est toujours à ses balbutiements, mais elle est soutenue par un groupe, bien que relativement petit, d'innovateurs et de techno-entrepreneurs hautement compétents. Ce groupe pourrait supprimer la plupart, sinon la totalité, des limitations et des défis soulignés dans le présent document. Par conséquent, le potentiel d'innovation des chaînes de blocs est considérable.

Bien que cela en dise long sur les technologies de chaînes de blocs, il est encore tôt pour tirer des conclusions définitives sur l'évolution de la technologie dans les cinq prochaines années ou plus. Pour l'instant, c'est l'engouement qui domine. Mais les données probantes actuelles relatives à la technologie des chaînes de blocs indiquent que les déploiements de celle-ci en sont encore à l'étape de la validation de principe.[163]

Bon nombre des applications de la chaîne de blocs examinées dans le présent document sont déjà déployées. Cependant, la plupart d'entre elles sont mises en oeuvre à une petite échelle, ont peu de clients ou s'adressent à peu de parties prenantes, particulièrement dans les pays en développement. Quelques gouvernements ont déjà franchi le pas et essaient de tirer parti de la technologie des chaînes de blocs pour combler les lacunes dans la fourniture des biens publics. Toutefois, il s'agit dans la plupart des cas de projets pilotes, et l'on constate un manque de stratégies claires à long terme.

Le remplacement d'initiatives en cours et le lancement de nouvelles initiatives sur des plateformes autonomes de chaînes de blocs ne feront que retarder l'adoption des chaînes de blocs. Pour les pays en développement, la meilleure approche à adopter consiste à déployer la technologie des chaînes de blocs pour compléter les programmes et les initiatives existants. Cela pourrait réduire les entraves à l'accès tout en augmentant les probabilités d'investissements initiaux dans les technologies de chaînes de blocs viables

à moyen terme, en répondant aux besoins locaux et en comblant les écarts de développement.

Les problèmes d'utilisabilité peuvent aussi limiter la diffusion des chaînes de blocs dans les pays en développement. L'utilisation répandue d'outils cryptographiques dans les pays pauvres fait face à des obstacles majeurs, surtout si les initiatives de technologie des chaînes de blocs visent les segments sociaux les plus pauvres. Il n'est pas réaliste de supposer que chaque bénéficiaire doit utiliser et gérer des clés privées et publiques. Le manque d'infrastructure à clés publiques dans la plupart des pays en développement ne fera qu'aggraver la situation. La seule manière de dénouer l'impasse est de trouver des solutions de rechange qui donnent aux utilisateurs finaux un accès à des outils cryptographiques au moyen d'intermédiaires comme des organismes communautaires, des petites entreprises et des gouvernements locaux.

L'idée essentielle ici est que les utilisateurs finaux n'ont pas besoin d'être propriétaires de la technologie ou de l'utiliser directement pour profiter de son déploiement.

Les initiatives de technologies de chaînes de blocs de grande ampleur qui sont liées au gouvernement branché semblent être les plus susceptibles de faire des chaînes de blocs un catalyseur de fourniture de biens publics. Les envois d'argent et l'argent numérique dans le secteur des biens privés montrent aussi beaucoup de potentiel. Cependant, ils pourraient ne pas promouvoir l'inclusion économique et financière des personnes qui se trouvent au bas de la pyramide.

Bien que la technologie des chaînes de blocs soit le porte-étendard de la décentralisation, le présent livre blanc montre que le minage a tendance à se centraliser et à se concentrer. Au début des chaînes de blocs bitcoin, toute personne avec un ordinateur portatif ou un ordinateur de bureau pouvait miner le réseau. Aujourd'hui, c'est devenu l'apanage de quelques personnes qui disposent des ressources financières et du matériel nécessaires et qui peuvent payer des factures d'électricité exorbitantes. Il en va de même pour la notion de consensus. Les technologies de chaînes de blocs substituent le consensus algorithmique au consensus humain. Le problème ici ne se limite pas à l'automatisation du consensus; il concerne également la représentation et l'échelle. Les organisations et les réseaux de chaînes de blocs décentralisés et autonomes sont petits du point de vue du nombre de

personnes qui y participent.[164] La plupart des utilisateurs de chaînes de blocs sont des clients qui utilisent des logiciels de portefeuille et qui ne font pas partie d'un processus de recherche de consensus algorithmique ou autre. Dans leur forme actuelle, les technologies de chaînes de blocs semblent mieux adaptées aux exploitations à petite échelle, en raison de leur manque d'extensibilité et des autres limitations soulignées dans le présent document.

Les technologies de chaînes de blocs pourraient bientôt chambarder le développement. Toutefois, les chaînes de blocs en sont toujours à leurs balbutiements, et la technologie continue d'évoluer rapidement. La réussite dans les pays en développement dépendra de la capacité des chaînes de blocs à améliorer le développement humain. Cela dépendra de la manière dont les thèmes soulignés dans la section précédente sont abordés. Les algorithmes seuls ne suffiront pas.

Internet et les technologies mobiles ont déclenché des perturbations positives dans les pratiques de développement, bien qu'à un degré inférieur à celui auquel on s'attendait à leur émergence. Dans ce contexte, il faut se poser une autre question pertinente: les technologies de chaînes de blocs peuvent-elles entraîner des perturbations plus profondes dans les processus de développement que les technologies précédentes ? Le potentiel est en place, mais des mesures mieux ciblées sont requises pour qu'un tel impact se produise sur les processus de développement.

Recommendations

Au vu de l'analyse et des conclusions du présent document, nous formulons les recommandations suivantes.

RECHERCHE

Réaliser une série d'études de cas sur les initiatives de technologie de chaînes de blocs en cours dans les pays en développement. Bien qu'on puisse trouver des données anecdotiques sur de telles initiatives, peu de travaux de recherche universitaire ou de recherches de développement sont proposés pour l'instant. En effet, il existe un grand vide dans le domaine des chaînes de blocs, ce qui a favorisé l'engouement relatif à la technologie.

Réaliser de nouvelles recherches et analyses sur les chaînes de blocs pour la gouvernance et sur la gouvernance des chaînes de blocs par rapport aux gouvernements et à la fourniture de biens publics. De manière plus particulière, les liens entre la confiance, la recherche de consensus et la représentation n'ont pas été étudiés dans la littérature existante.

Lier les travaux actuels et futurs sur la technologie des chaînes de blocs à l'intelligence artificielle, puisque cette dernière est introduite de manière systématique dans la technologie et les applications décentralisées connexes. Cela nous ramène à la question de la gouvernance des technologies de chaînes de blocs et de la gouvernance des algorithmes en général, qui ne sont pas participatives ou transparentes. Les chaînes de blocs font-elles partie de la solution ?

Envisager d'entreprendre de nouvelles recherches sur la gouvernance des algorithmes et sur l'impact que ces derniers peuvent avoir sur la société, particulièrement dans les pays en développement. Ce thème est à son tour lié à la notion selon laquelle les technologies sont des produits sociaux. En fin de compte, la société finit par dicter la manière dont la technologie est exploitée. Toutefois, l'opinion dominante aujourd'hui semble se situer à l'opposé, notamment en ce qui concerne les technologies de chaînes de blocs.

Explorer des approches et des solutions novatrices pour faciliter l'accès à la technologie des chaînes de blocs des personnes qui se trouvent au bas de la pyramide, en se concentrant sur l'accès aux outils cryptographiques et à leur utilisation. Il est essentiel ici de faire une distinction entre l'utilisation et la propriété de la technologie et leurs avantages. Des déploiements technologiques précédents ont montré que les collectivités pauvres peuvent profiter des technologies sans les utiliser directement ou en être propriétaires. Les réseaux communautaires et l'utilisation partagée de téléphones cellulaires en sont des exemples bien connus.

PROGRAMMES

Explorer le rôle des initiatives d'innovation et des carrefours technologiques existants dans les pays en développement visant à soutenir le déploiement des technologies de chaînes de blocs. L'Afrique et l'Asie en particulier comptent un grand nombre de carrefours technologiques capables d'une part de fournir une expertise adéquate pour le déploiement des technologies de chaînes de blocs en s'appuyant sur les connaissances locales et, d'autre part, d'orienter la fourniture des biens publics.

Envisager de financer ou d'appuyer de petits projets pilotes ou des prototypes de technologie de chaînes de blocs axés sur les thèmes du développement, les ODD et les priorités locales des pays en développement. Il n'est pas nécessaire d'investir des sommes colossales, mais il faut porter une attention particulière à l'impact sur le développement humain. Comme nous l'avons mentionné plus tôt, les services d'identité et les services gouvernementaux qui font appel aux technologies de chaînes de blocs sont les plus pertinents à ce stade-ci et ont déjà été mis en oeuvre dans d'autres contextes.

Soutenir ou aider la création d'un réseau d'innovateurs en technologies de chaînes de blocs et inciter ces derniers à soutenir les applications qui facilitent la fourniture des biens publics. Pour cela, il est essentiel d'attirer des innovateurs locaux dans les économies émergentes et en développement.

RÉSEAUTAGE ET PARTENARIATS

Soutenir la création d'une chaîne de blocs pour des projets liés aux chaînes de blocs dans les pays en développement ou envisager la création d'une base de connaissances durable connexe. L'établissement de partenariats avec des experts internationaux et d'autres innovateurs à l'échelle mondiale devrait faire partie d'une telle initiative.

Des **organismes de financement du développement multilatéraux et étrangers ont pris des mesures pour lier les technologies de chaînes de blocs à la poursuite des ODD**. Les organismes de développement et les praticiens du développement devraient conjuguer leurs efforts pour suivre les dernières avancées et réaliser d'autres recherches sur ce sujet.

Mettre en place un réseau de chaînes de blocs pour le développement ou aider à l'organisation d'un tel réseau, ou créer une organisation décentralisée autonome en partenariat avec d'importants pays et organismes donateurs. Le but premier d'un tel réseau pourrait consister à veiller à ce que le développement demeure l'enjeu principal et occupe une place plus importante que les chaînes de blocs elles-mêmes.

NASA

ANNEXE I

Cadre analytique

Le domaine des Technologies de l'information et de la communication au service du développement (TIC-D) fournit le cadre analytique de base du présent document en soumettant ces quatre différents points de vue à une même analyse. Pour les besoins du présent document, l'accent est mis sur la partie « développement » du cadre des TIC-D.

L'aspect le mieux connu des TIC-D est peut-être le soi-disant fossé numérique qui demeure considérable dans de nombreux pays en développement. Sans surprise, le fossé numérique n'est que le reflet des disparités socioéconomiques et des disparités entre les sexes dans l'hémisphère Sud. Toutefois, le lien entre ces fossés apparemment différents n'est habituellement pas reconnu. Ainsi, les tentatives visant à combler le fossé numérique sans tenir compte des disparités socioéconomiques et intersectionnelles se traduisent habituellement par des efforts qui ne peuvent pas être soutenus à moyen ou à long terme.

Et même si ces tentatives sont réussies, comme on pourrait le penser dans le cas des technologies mobiles dans les pays en développement, elles ne favorisent pas nécessairement l'inclusion sociale des personnes qui se trouvent au bas de la pyramide ou ne fournissent pas non plus de nouveaux débouchés économiques à ces mêmes personnes. Des recherches récentes sur le sujet[165] ont révélé que la diffusion horizontale des nouvelles technologies dans le monde s'est accélérée au cours des 15 à 20 dernières années, mais que la pénétration verticale de celles-ci dans les pays en développement ne fait que commencer. Cette distinction fondamentale démontre que l'exploitation efficace des nouvelles technologies dans de nombreux pays en développement est une question plus complexe qui transcende le fossé technologique traditionnel.

La plupart des pays en développement n'ont pas d'autre choix que d'importer ou d'utiliser des technologies développées ailleurs (habituellement dans des

pays industrialisés). Ils doivent mobiliser une grande variété de ressources pour adopter les nouvelles technologies et les adapter au contexte et aux besoins locaux. C'est certainement le cas du secteur de la production (ce qui comprend le secteur des services) de l'économie et des investissements gouvernementaux dans la technologie, comme le gouvernement électronique par exemple.

Les chaînes de blocs, qui sont une nouvelle technologie et qui pourraient causer des perturbations, ne pourront pas se soustraire aux schémas de diffusion que d'autres technologies perturbatrices ont suivis dans la plupart des pays en développement. Bien sûr, il se pourrait que les chaînes de blocs se répandent aussi rapidement, voire plus rapidement, que les technologies mobiles au cours des 20 dernières années, par exemple. Mais même si c'était le cas, les conditions et l'environnement dans lesquels cette distribution serait possible doivent être examinés. Par conséquent, le présent document met l'accent sur les piliers suivants puisqu'ils sont reliés à la diffusion des nouvelles technologies:

Infrastructure: Des investissements publics et privés qui soutiennent le développement général de l'infrastructure dans un pays, ce qui ne se limite pas aux TIC. Par exemple, l'accès au réseau électrique et l'infrastructure de santé et d'éducation sont aussi inclus.

Capacités: Les capacités humaines que les pays devraient posséder afin de développer et de déployer de nouvelles technologies. Cela comprend non seulement les capacités techniques, mais aussi les capacités fonctionnelles qui sont transversales et qui ne se limitent pas aux TIC.

Politiques et réglementation: La capacité de tous les ordres gouvernementaux à élaborer, à mettre en œuvre et à appliquer des politiques sur leur territoire est essentielle.

Institutions: L'environnement des « règles du jeu » qui permettent à une personne de mener des activités dans un contexte institutionnel donné, ce qui comprend le secteur privé et les organisations de la société civile. Les mécanismes de gouvernance en font partie, particulièrement les nouveaux modèles fondés sur la participation de multiples parties prenantes.

Cargo Cult

ANNEXE II

Technologies de chaînes de blocs

APERÇU

Les technologies de chaînes de blocs sont fondées sur quatre technologies différentes que le créateur du bitcoin a réunies. Les technologies en question sont les suivantes:

- Réseaux poste à poste;
- Bases de données décentralisées et réparties;
- Cryptographie;
- Algorithme de preuve de travail (pour résoudre le soi-disant problème de la double dépense).

RÉSEAUX D'ÉGAL À ÉGAL

Dans un réseau poste à poste, tous les noeuds interconnectés sont en principe égaux.

Il n'y a pas de serveur central, puisqu'on n'en a pas besoin. Ces réseaux se caractérisent donc par l'absence de point de défaillance central. Si un noeud tombe en panne, tous les autres noeuds demeurent interconnectés; les données et l'information qui circulent dans le réseau sont ainsi préservées. Par conséquent, les noeuds sont à la fois des clients et des serveurs.

Dans l'ère Internet, le défunt site de partage de musique Napster, créé en 1999, est peut-être le meilleur exemple de réseau poste à poste. En effet, on se servait de Napster pour le partage d'un fichier décentralisé: sur le réseau, on pouvait trouver un même fichier dans des milliers de noeuds, voire plus encore. Aujourd'hui, BitTorrent est l'un des plus importants réseaux poste à poste d'Internet.[166] Napster et BitTorrent utilisent leurs propres protocoles pour la communication et l'interaction sur le réseau.[167] InterPlanetary File System[168] est l'incarnation la plus perfectionnée du réseau poste à poste fondé sur l'utilisation de tables de hachage distribuées.[169]

QUI FAIT PARTIE DES CHAÎNES DE BLOCS: LES TYPES D'UTILISATEURS ET DE NOEUDS

Les chaînes de blocs sont accessibles sous forme de logiciels à source ouverte à tous ceux qui les téléchargent dans un dispositif computationnel. Une fois le logiciel lancé, le dispositif devient un noeud ou un utilisateur de plus dans le réseau poste à poste. En principe, toute personne disposant d'un dispositif branché à Internet peut se joindre au réseau. On trouve les cinq grands types d'acteurs suivants dans un réseau poste à poste de chaînes de blocs:

Développeurs principaux: Le groupe de personnes qui a un accès en écriture au code source des technologies de chaînes de blocs. Les modifications apportées au code doivent toutefois être approuvées par la communauté du réseau.

Noeuds complets: Il s'agit des noeuds qui contiennent des copies à jour de la chaîne de blocs, valident les nouveaux blocs puis les diffusent dans le réseau.

Mineurs: Les noeuds qui s'occupent de la preuve de travail, en rivalisant entre eux pour trouver le hachage d'en-tête requis pour ajouter un bloc de

transactions à la chaîne de blocs. Utilisateurs finaux: Les utilisateurs qui se servent du réseau pour effectuer leurs transactions en se connectant à un noeud du réseau au moyen d'un logiciel client ou d'un logiciel de portefeuille. Les utilisateurs finaux doivent avoir une copie complète de la chaîne de blocs pour être actifs sur le réseau.[170]

Noeuds de service: Les noeuds qui fournissent des services à d'autres noeuds comme des services de portefeuille, de change, de mixeur, de stockage et infonuagiques, pour ne nommer que ceux-là.

Dans le cas du bitcoin, on a créé une fondation[171] pour sensibiliser le public et influencer les politiques et la réglementation gouvernementale, entre autres choses.

BASES DE DONNÉES DÉCENTRALISÉES ET RÉPARTIES

En termes simples, une base de données utilisée dans un réseau poste à poste est décentralisée, car une copie des données structurées est stockée par défaut dans les noeuds. On dit que les bases de données sont « réparties » pour désigner la manière dont leur traitement est effectué par le réseau. Une base de données est répartie si les calculs requis pour modifier les données sont exécutés par un ensemble de noeuds de réseau, au lieu d'un serveur central (Raval, 2016).[172]

Il est à noter qu'une base de données centralisée peut également être répartie. En fait, il s'agit du modèle le plus utilisé par les grands fournisseurs d'accès Internet.[173]

CRYPTOGRAPHIE

L'utilisation massive d'outils cryptographiques est l'une des caractéristiques distinctives des technologies de chaînes de blocs, qui ont recours à la cryptographie à clés publiques. La cryptographie à clés publiques utilise des paires de clés: une clé privée qui n'est connue que de son propriétaire, et une clé publique qui est partagée avec le reste du monde. Elle permet la création

asymétrique de clés privées et publiques. Une clé privée est d'abord générée de manière aléatoire. Celle-ci est ensuite utilisée pour créer une clé publique. La clé privée est utilisée pour chiffrer la transaction qui peut ensuite être déchiffrée par le destinataire visé au moyen de la clé publique de l'expéditeur. Il est à noter qu'il est mathématiquement impossible d'utiliser une clé publique pour déchiffrer une clé privée.

Dans Bitcoin, on utilise la clé publique pour créer une adresse Bitcoin.[174] Bitcoin et d'autres logiciels de portefeuille (client) permettent habituellement de créer facilement ces clés, ainsi que de stocker des clés privées dans des dispositifs numériques et dans d'autres noeuds qui fournissent ces services, ou encore de les conserver sur papier. Les utilisateurs finaux peuvent générer de multiples clés publiques Bitcoin pour traiter leurs transactions.[175]

HACHAGE

Les données sont stockées de manière structurée dans les chaînes de blocs. Chacun des blocs d'une chaîne comporte une structure définie qui comprend quatre colonnes, ou champs. L'en-tête de bloc fait partie de ces colonnes. Celui-ci comporte lui-même six champs. L'en-tête de bloc est utilisé pour générer un identificateur unique, ou hachage de bloc, pour le bloc actuel et comprend l'identificateur unique du bloc précédent.

Le hachage est une fonction cryptographique qui peut convertir une entrée de n'importe quelle longueur dans une sortie à longueur fixe. La probabilité que le résultat du hachage de deux entrées différentes soit identique est presque nulle: toute entrée a un résultat de hachage unique. Il est impossible de deviner le résultat du hachage de l'entrée initiale. La rétro-ingénierie du hachage est impossible.

Toutefois, il est facile de s'assurer que le hachage est le résultat d'une entrée: le hachage est efficace d'un point de vue computationnel. Il s'agit de la propriété de hachage qui permet aux noeuds du réseau de valider ou de corroborer le résultat du processus compétitif de preuve de travail, ce qui rend par conséquent possible le consensus décentralisé.

Le hachage d'un bloc est en fait le condensé des six champs qui constituent l'en-tête de bloc et sert d'identificateur unique pour le bloc en question. Le calcul du hachage de bloc aux fins d'utilisation pour le hachage du bloc précédent crée ainsi un lien mathématique entre les deux blocs.[176]

Pour hacher un bloc, on encode l'en-tête de bloc à l'aide d'une fonction de hachage cryptographique[177] qui génère une chaîne de caractères alphanumériques présentée sous forme hexadécimale[178], au lieu de la notation décimale habituelle. La lecture d'un fichier de chaîne de blocs ne révélera pas beaucoup d'information à l'oeil nu, puisque le contenu a été haché.[179]

Bref, la fonction de hachage cryptographique encode des données ou du texte, peu importe leur taille, et produit un résultat dont la longueur est fixe et qu'on appelle un condensé[180] ou l'empreinte numérique de l'entrée fournie. Les chaînes de blocs utilisent SHA-256[181, 182] qui génère un condensé constitué de 256 bits ou 32 octets ou caractères.

En principe, il est pratiquement impossible que deux entrées différentes aient le même condensé. De la même façon, il est impossible de choisir à l'avance un condensé particulier pour une entrée donnée. Enfin, il est impossible de deviner ou de déchiffrer du contenu soumis à une fonction de hachage à partir du condensé obtenu.

On peut aussi identifier les blocs par leur position dans la chaîne de blocs ou par le numéro de rangée. On appelle cette position la hauteur de bloc, laquelle ne fait pas partie de la structure de données du bloc en tant que tel, mais qui est plutôt générée de manière dynamique.[183]La hauteur de bloc permet d'indexer les entrées d'une chaîne de blocs afin de chercher et de récupérer plus rapidement des entrées de blocs particulières.

Exemples de hachage

Par exemple, en utilisant SHA-256 pour hacher la phrase « Blockchain: Disrupting Development ? » on obtient le condensé suivant en format hexadécimal:

a86b5ca5e16b840d152779b7c8378a01ae441d211

En ajoutant la lettre s à la fin du mot « Blockchain », on obtient

66a1cc69b0dbb6d7d0ae27c18c87a8c5648dc5af1b3091ed093bb02437dd50aa

ce qui est totalement différent du premier condensé, bien qu'on ait ajouté un seul caractère.

ALGORITHME DE PREUVE DE TRAVAIL

La preuve de travail est un algorithme de force brute utilisé par les noeuds de minage de réseau qui rivalisent entre eux pour trouver le hachage d'en-tête d'un nouveau bloc de transactions. En raison de la conception de la technologie, la difficulté de trouver un nouveau hachage augmente au fil du temps, puisque le nombre d'entrées dans la chaîne augmente lui aussi. De la même façon, la récompense, sous la forme de nouveaux bitcoins, que reçoivent les mineurs, tend à diminuer au fil du temps.

Comme nous l'avons mentionné à la section 2 (et dans le résumé), la preuve de travail présente certaines similitudes avec le casse-tête classique auquel les enfants jouent qui consiste à deviner le chiffre. Toutefois, la preuve de travail est certainement beaucoup plus complexe.

Premièrement, la preuve de travail consiste à trouver un nombre hexadécimal qui comporte 256 caractères alphanumériques. Deuxièmement, les huit ou neuf premiers caractères du nombre doivent tous être des zéros. Troisièmement, le nombre cherché doit être inférieur à un seuil préalablement défini. Finalement, les mineurs doivent utiliser comme entrée la solution trouvée au terme du processus de preuve de travail précédent, ainsi qu'un nombre qui est utilisé pour effectuer le calcul.[186]

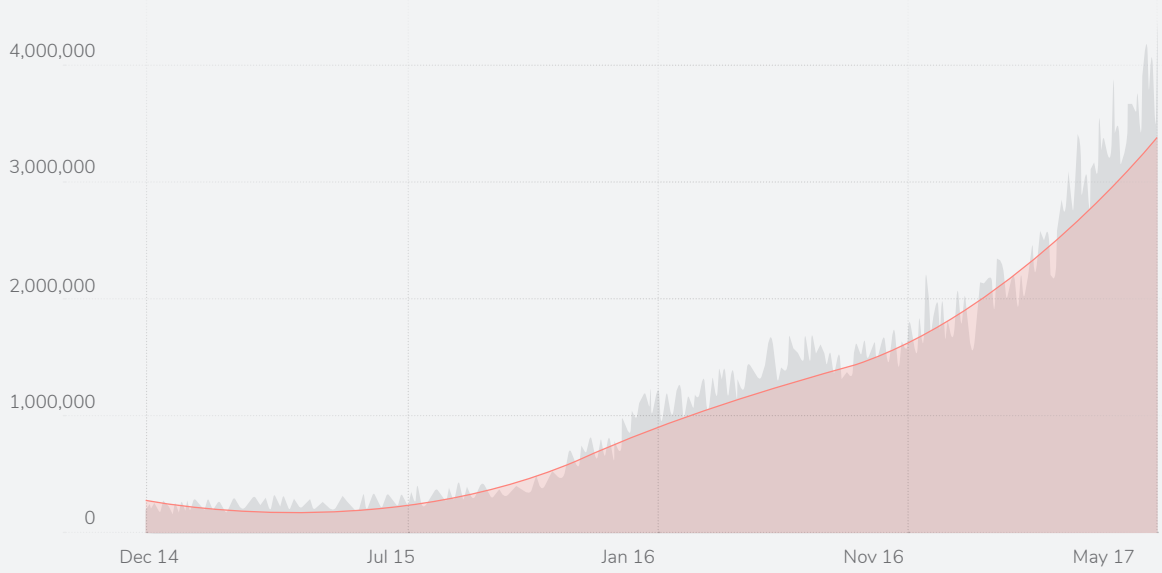
Il faut une puissance de calcul considérable pour participer à cette course, et encore, il faut parfois des milliards d'itérations pour trouver le résultat. On a mis au point du matériel spécialisé et coûteux pour l'algorithme de preuve de travail des technologies de chaînes de blocs.[187] Dans la même veine, le minage est surtout effectué par des bassins miniers qui utilisent essentiellement un traitement réparti poste à poste pour trouver une solution au casse-tête. Des mineurs de toutes tailles peuvent faire partie d'un bassin et distribuer des récompenses en fonction du travail accompli s'ils remportent la compétition.

La figure 7 montre la croissance absolue des taux de hachage au cours des trois dernières années. Bien que la croissance réelle semble ralentir, la valeur réelle demeure considérable et nécessite une immense puissance de calcul de même que d'importantes ressources énergétiques. La preuve de travail n'est donc pas synonyme d'algorithmes des plus efficaces ou des plus intelligents.

FIGURE 7

Taux de hachage de chaînes de blocs de bitcoins
De janvier 2015 à avril 2017

Source: blockchain.info



Quoi qu'il en soit, la preuve de travail résout des problèmes de longue date comme la double dépense[188] et le problème des généraux byzantins.[189] Elle protège en outre le réseau poste à poste contre les attaques Sybil.[190]

INNOVATIONS EN MATIÈRE DE CHAÎNES DE BLOCS

Les innovations dans le domaine des chaînes de blocs vont au-delà des nouvelles cryptomonnaies.[191] Cela ne signifie pas que ces applications n'entraînent pas la création de nouvelles cryptomonnaies. En fait, la plupart des innovations utilisent les cryptomonnaies comme mesure pour inciter les mineurs à résoudre la preuve de travail ou d'autres algorithmes similaires. Les noeuds qui offrent des services aux utilisateurs finaux et aux autres noeuds du réseau peuvent aussi profiter de ces incitatifs en chargeant des frais ou en prenant d'autres arrangements.[192]

Comme tant d'autres technologies, l'innovation est le moteur de l'évolution des chaînes de blocs. De manière générale, trois types d'innovations ont eu lieu:[193]

1. **L'innovation en matière de cryptomonnaie,** qui vise à améliorer les fonctions et les limites du bitcoin dans leur ensemble. Les applications qui visent à trouver des solutions de rechange au bitcoin comme cryptomonnaie sont appelées monnaies alternatives. Les pièces colorées répondent aussi à cette définition. La plupart de ces plateformes utilisent la chaîne de blocs du bitcoin.

2. **L'innovation en matière de consensus**, qui vise à réduire les coûts élevés et l'inefficacité apparente des algorithmes de preuve de travail. La preuve d'enjeu et les variantes de l'algorithme de preuve de travail original en font également partie.

3. **L'innovation en matière de chaînes de blocs**, qui vise à répandre l'utilisation de la chaîne de blocs au-delà des cryptomonnaies et à d'autres domaines. Les exemples comprennent Namecoin[194] et Ethereum.[195] Certains auteurs ont nommé cet ensemble d'applications chaînes alternatives, puisqu'elles utilisent des chaînes de blocs indépendantes de bitcoin.[196]

De nos jours, de nombreuses monnaies alternatives sont en circulation.[197] Au fil du temps, l'innovation générale en matière de chaînes de blocs s'est déplacée des cryptomonnaies à l'amélioration et à l'augmentation de l'utilisation de l'ensemble des technologies de grand livre réparti (GLR). Les chaînes auxiliaires[198] sont une innovation complémentaire dont l'objectif initial était de promouvoir l'interopérabilité de la chaîne de blocs du bitcoin avec d'autres monnaies alternatives. Les tendances actuelles portent à croire que les innovations en matière de GLR continueront de mener la danse, tandis que les monnaies alternatives poursuivront leur déclin à moyen terme.[199] Quoi qu'il en soit, un examen plus approfondi des premières plateformes de chaînes alternatives peut révéler la manière dont les chaînes de blocs ont changé au fil du temps.

NAMECOIN

L'administration des adresses et des noms de protocole Internet, le système de noms de domaine (DNS), a entraîné des problèmes relatifs à la gouvernance d'Internet, qui est pour l'instant assurée par une coalition réunissant de nombreuses parties prenantes. Le système actuel est fortement centralisé, tout en étant réparti à l'échelle mondiale. ICANN,[200] la Société pour l'attribution des noms de domaine et des numéros sur Internet, joue un rôle clé dans cette structure.

Namecoin, qui a été créée en 2012, est la première chaîne alternative dont l'objectif consistait à décentraliser la gestion du DNS.[201] En modifiant le code source original du bitcoin, en créant sa propre chaîne de blocs et en permettant la saisie systématique de paires de clés et de noms, Namecoin a fourni les outils nécessaires à la gestion des noms de domaines et des identités personnelles.

Toutefois, sa réussite a été plutôt limitée par rapport aux grands registraires du DNS. La plateforme ne s'occupe que des domaines.bit, qui ne sont accessibles qu'au moyen de fonctions complémentaires ou d'extensions ajoutées aux navigateurs habituels.[202] De plus, et ce point est peut-être encore plus important, Namecoin a eu peu ou pas d'influence sur les débats entourant la gouvernance d'Internet.[203]

En raison de l'immuabilité inhérente aux chaînes de blocs, des problèmes relatifs au squat du DNS, des noms de domaine sans adresse de protocole Internet pertinente et des saisies possibles de nom, Namecoin semble être en difficulté.[204]

ETHEREUM

Ethereum est habituellement associée étroitement aux contrats intelligents. Cela n'est toutefois vrai qu'en partie, car la plateforme peut prendre en charge une vaste gamme d'applications où l'interaction et la coordination entre pairs dans un réseau donné peuvent être programmées et automatisées.[205] Ce qu'il faut bien comprendre ici, c'est que les pairs conviennent eux-mêmes de la marche à suivre et programment ensuite la chaîne de blocs en conséquence. C'est ce que l'on appelle un contrat intelligent, et celui-ci est soutenu par une organisation décentralisée autonome. En réalité, Ethereum est une chaîne de blocs programmable[206] qui peut servir d'assise au développement d'une multitude d'applications décentralisées.[207]

Ethereum offre aussi une solution de remplacement à la centralisation potentielle inhérente à l'algorithme de preuve de travail du protocole Bitcoin qui ne peut être calculé efficacement que par des mineurs munis de matériel sophistiqué. Ethereum utilise plutôt un algorithme de preuve d'enjeu.[208] En bref, la preuve d'enjeu exige que les noeuds qui souhaitent participer au processus compétitif de minage doivent fournir un cautionnement ou un dépôt de garantie dans la monnaie d'Ethereum, l'ether. Cela peut éliminer la nécessité de recourir à du matériel coûteux et les coûts énergétiques afférents à son utilisation.

Ethereum peut également comporter des composants d'intelligence artificielle, dont des algorithmes d'apprentissage profond, pour la mise en oeuvre de contrats intelligents et le soutien du développement d'applications décentralisées. Ces dernières semaines, Ethereum a gagné beaucoup de terrain et est en passe de devenir l'un des principaux concurrents de Bitcoin, bien que les deux plateformes aient des fonctionnalités et des buts différents.

Lee Ferrell

HYPERLEDGER

Hyperledger

Hyperledger est un espace collaboratif interindustriel servant à l'élaboration de normes et de protocoles ouverts pour les technologies de GLR. Il vise à améliorer le rendement et l'extensibilité des chaînes de blocs. Hyperledger soutient actuellement des applications dans les domaines de la finance et des soins de santé.

Hyperledger n'est pas seulement une innovation en matière de chaînes de blocs; c'est un espace collaboratif interindustriel servant à l'élaboration de normes et de protocoles ouverts pour les technologies de GLR. Hyperledger, qui a été créé par la Fondation Linux en 2015, compte aujourd'hui plus de 100 membres industriels, dont des entreprises de partout en Asie. Hyperledger vise aussi à améliorer le rendement et l'extensibilité des chaînes de blocs.

Pour l'instant, Hyperledger soutient des applications dans les secteurs de la finance et des soins de santé, mais il commencera bientôt à travailler sur les chaînes d'approvisionnement.[209]

RECAP

In contrast with Namecoin, Ethereum has had a relatively greater impact on the blockchain ecosystem, while Hyperledger is one of the many new blockchain technology consortia that have recently emerged.[210] In any event, these examples show the quick evolution of distributed ledger technology in recent years. The pace has barely slowed since and innovation in this space continues to take place at a rapid pace.

ENDNOTES

1 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2 http://secondmachineage.com/

3 http://thezeromarginalcostsociety.com/

4 Dans le présent document, « technologie » est synonyme de « technologies de l'information et de la communication » (TIC) et exclut toutes les autres technologies.

5 Nakamoto (2008).

6 Le côté négatif, du point de vue des répercussions négatives sur les emplois et les revenus, et de la soi-disant singularité voulant que des machines intelligentes finissent par contrôler l'humanité. Vous trouverez un exemple à l'adresse http://time.com/3614349/artificial-intelligence-singularity-stephen-hawking-elon-musk/.

7 Vous trouverez un exemple dans Tapscott (2016 : 25) : « Le résultat pourrait être une économie de pairs où les institutions sont réellement réparties, inclusives et responsabilisantes et, par le fait même, légitimes. En changeant profondément ce que nous pouvons faire en ligne, la nouvelle plateforme peut même créer les conditions technologiques pour résoudre certains de nos problèmes les plus difficiles. » [traduction libre]

8 Des nations en développement ont participé à la vague d'innovation mobile de la dernière décennie. On a commencé à déployer à l'échelle mondiale des applications mobiles créées au Kenya et dans d'autres pays en développement. On peut considérer les applications mobiles comme étant des applications micro-informatiques dont les entraves à l'accès sont moindres et qui nécessitent des compétences techniques et des compétences en programmation de base, tandis que les anciennes applications Web nécessitaient un niveau plus élevé de connaissance et un ensemble de compétences plus pointues. Reportez-vous au Programme des Nations Unies pour le développement, 2013.

9 Reportez-vous à Ashish Gadnis, Opinion: Blockchain offers poorest a real economic identity — and a shot at the SDGs, Blogue Devex, 7 novembre 2016. http://bit.ly/2hP8HdT

10 On peut considérer les technologies de chaînes de blocs comme étant une technologie d'application générale. Reportez-vous à Kane (non daté).

11 Vous trouverez les détails techniques plus loin à l'annexe II.

12 https://fr.wikipedia.org/wiki/Crypto-monnaie

13 L'histoire générale des monnaies numériques et du bitcoin en particulier n'entre pas dans le cadre du présent document. Reportez-vous à Popper (2016) pour en savoir plus à ce sujet.

14 Il convient de noter que Nakamoto (2008) n'a pas employé le terme « chaîne de blocs » dans son article novateur. Il a plutôt fait allusion à une chaîne de blocs qui fonctionne sur un « serveur d'horodatage ».

15 https://fr.wikipedia.org/wiki/Grand_livre

16 Swan (2015) soutient que la chaîne de blocs constitue la couche de base du bitcoin et de tous les protocoles similaires qui sont suivis par le logiciel Bitcoin.

17 https://fr.wikipedia.org/wiki/Dark_web

18 https://fr.wikipedia.org/wiki/Silk_road

19 Reportez-vous à Popper (2016) pour des détails supplémentaires.

20 L'attaque pirate récente contre plus de 100 pays au moyen d'un logiciel rançonneur est un exemple : des pirates informatiques demandent qu'on les paye en bitcoins pour « libérer » l'information qu'ils ont chiffrée. Reportez-vous à Gautham, Bitcoin Ransomware Makes Global IT Infrastructure 'WannaCry', NewsBTC, 13 mai 2017. http:// www.newsbtc.com/2017/05/13/bitcoin-ransomware-makes-global-infrastructure-wannacry/.

21 Les chiffres de Google Trend sont relatifs et non absolus. Pour chaque recherche d'un mot-clé, Google Trend détermine le nombre maximal de recherches lors d'une journée donnée et divise tous les autres par ce nombre. Par conséquent, le maximum est toujours de 100. Quoi qu'il en soit, il est évident que les recherches relatives aux technologies de chaînes de blocs dans Google sont toujours en hausse.

22 https://fr.wikipedia.org/wiki/Pair_%C3%A0_pair

23 Il semble y avoir une certaine confusion concernant la différence entre un réseau décentralisé et un réseau réparti. Pour une définition conceptuelle claire, reportez-vous à l'article classique de Baran (1962). La chaîne de blocs peut donc être qualifiée de réseau décentralisé et réparti.

24 Comparons cela au paradigme actuel d'information et de services sur Internet, où la centralisation est une caractéristique essentielle qui génère une valeur substantielle pour les entreprises qui fournissent les services en question.

25 L'information provient de Baran (1962).

26 Dans Bitcoin, un nouveau bloc de transactions est ajouté toutes les dix minutes environ. Les blocs ajoutés à la chaîne ne peuvent pas contenir plus de 2 200 transactions, à quelques transactions près.

27 Certains auteurs ont qualifié les chaînes de blocs de « protocole de la confiance ». Reportez-vous à Tapscott (2016: 3 & ff.)

28 One-CPU-one vote, à Nakamoto (2008: 3); et la majorité des unités centrales prévalent.

29 D'autres algorithmes peuvent donner le même résultat. Par exemple, Ethereum a proposé la preuve d'enjeu. Reportez-vous à l'annexe II pour obtenir des précisions techniques supplémentaires.

30 http://www.abcya.com/guess_the_number.htm

31 Vous trouverez des détails techniques à l'annexe II.

32 Dans ce cas, on utilise un hachage binaire ou un arbre de Merkle. Pour en savoir plus, consultez l'annexe II. Il convient de noter qu'il est également possible de hacher un hachage, et que ce procédé est utilisé couramment dans les chaînes de blocs.

33 Vous pouvez voir les dernières transactions Bitcoin ici.

34 Reportez-vous à Swam (2015) pour un exemple. Les références à Hayek et coll. sont également courantes dans cette littérature.

35 Cela repose en partie sur les travaux d'Atzori (2015). Futarchy et Franchalutes ne sont pas inclus ici, car ils ne semblent pas pertinents dans le contexte des pays en développement.

36 Consensys, Liquid democracy and emerging governance models, 24 août 2016. https://media.consensys.net/2016/08/24/liquid-democracy-and-emerging-governance-models/.

37 En fait, il s'agit de la définition de « contrat intelligent ».

38 Pour la typologie sommaire des organisations décentralisées, reportez-vous à Raval (2016).

39 Les contrats intelligents (qu'on appelle aussi contrats d'application automatique, contrats de chaîne de blocs ou contrats numériques) sont des transactions algorithmiques qui appliquent des ententes contractuelles prédéfinies. Les conditions de l'entente sont programmées dans une chaîne de blocs et sont appliquées de manière automatique par le logiciel. Certains contrats intelligents font appel à une intelligence artificielle afin d'avoir une certaine adaptabilité. Les contrats intelligents permettent à au moins deux parties pseudo-anonymes de faire affaire ensemble (habituellement par le truchement d'Internet), sans avoir besoin d'une autorité centrale. Pour en savoir plus, rendez-vous à l'adresse https://blockgeeks.com/guides/smart-contracts/.

40 Pour un exemple, rendez-vous à l'adresse http://www.reform.uk/reformer/government-in-blockchains-ii-disrupting-bureaucracy/.

41 https://bitnation.co/

42 Il s'agit d'un des appels généraux de l'ouvrage de Tapscott.

43 On peut voir les chaînes de blocs comme étant le troisième type. Dans ce cas, un nombre prédéterminé de noeuds mène le processus, le rendant ainsi privé. Reportez-vous à Buterin, V. On public and private blockchains, Ethereum, 7 août 2016. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

44 On assiste en ce moment à des débats sur la faisabilité des chaînes de blocs centralisées. Reportez-vous à Buntinx, JP, A centralized blockchain solution will not solve financial fraud, The Merkle, 22 mai 2016. http://themerkle.com/a-centralized-Blockchain-solution-will-not-solve-financial-fraud/.

45 Les chaînes de blocs hybrides sont des GLR qui combinent les caractéristiques des chaînes de blocs publiques et privées, et de chaînes de blocs de consortiums.

46 Reportez-vous à Walport (2016) pour un exemple.

47 https://www.corda.net/

48 https://ripple.com/

49 Reportez-vous au livre blanc de Corda pour des détails supplémentaires.

50 Des services de mixeur élaborent des initiatives visant à garantir l'anonymat complet. Pour en savoir plus à ce sujet, reportez-vous à Novetta, Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins, Novetta, septembre 2015. https://www.novetta.com/wp-content/uploads/2015/10/ NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.

51 Cela ne s'applique qu'aux chaînes de blocs publiques et aux chaînes de blocs sans permission.

52 Brenig, C., Transparency through Decentralized Consensus: The Bitcoin Blockchain and Beyond, Albert-Ludwigs-Universität Freiburg, dissertation de Ph.D. non publiée, 2017. https:// freidok.uni-freiburg.de/fedora/objects/freidok:11559/datastreams/FILE1/content.

53 Pour en savoir davantage sur le débat entourant la taille des blocs, reportez-vous à Coleman, L., Extension Block Proposal Stumbles In Attempt to End Bitcoin Block Size Debate, Cryptocoins News, 4 avril 2017. https://www. cryptocoinsnews.com/extension-block-proposal-stumbles-trying-end-block-size-debate/.

54 Deetman, S., Bitcoin Could Consume as Much Electricity as Denmark by 2020, Motherboard, 29 mars 2016. http://motherboard.vice.com/read/bitcoin-could-consume-as-much- electricity-as-denmark-by-2020.

55 Zambrano, R., Blockchain mining: Competition and (de)centralization, 24 avril 2017. http:// blog.raulza.me/blockchain-mining-competition-and-decentralization/.

56 Les données relatives à Ethereum révèlent des tendances similaires : https://etherscan.io/stat/miner?range=7&blocktype=blocks.

57 La taille de la chaîne de blocs d'Ethereum est environ deux fois moins importante. Le téléchargement d'un fichier aussi volumineux au moyen d'une connexion lente peut être laborieux. https://bitinfocharts.com/

58 The Morning Paper (2017).

59 Pour en savoir plus, reportez-vous à Coleman, L., Ex-Ethereum Developer: How the DAO Hack Happened and What Comes Next, Cryptocoins News, 30 juillet 2016. https://www.cryptocoinsnews.com/ex-ethereum-developer-dao-hack-happened-comes-next/ ou à Ore, J., How a $64M hack changed the fate of Ethereum, Bitcoin's closest competitor, CBC News, 28 août 2016. http:// www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009

60 Un rapport indique qu'au début de l'année, plus de 1 200 jeunes entreprises dans le domaine des chaînes de blocs étaient en activité. Reportez-vous à Michalik, V. et L. Lundy, Frost & Sullivan identifies the 2017 global blockchain startup map, Marginalia, 31 mars 2017 Pour la liste des 250 plus grandes sociétés de chaînes de blocs en 2017, reportez-vous à Blockchain Daily News, Top 250 blockchain companies and startups, 2017. http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html.

61 Reportez-vous à Kaul (2003) pour une définition des biens publics qui est mieux adaptée à l'ère de la mondialisation que la définition traditionnelle.

62 Higgins, S., UK Government Trials Blockchain Welfare Payments System, Coindesk, 7 juillet 2016. http://www.coindesk.com/uk-government-trials-Blockchain-welfare-payments-system/.

63 Prisco, G. (2016).

64 Cela est fondé sur la définition des biens publics de Kaul. Kaul (2003).

65 The Economist, Uberworld: The world's most valuable startup is leading the race to transform the future of transport, 3 septembre 2016. http://www.economist.com/news/leaders/21706258-worlds-most-valuable-startup-leading-race-transform-future.

66 Mougayar, W., The Blockchain is Perfect for Government Services, Coindesk, 3 septembre 2016. http://www.coindesk.com/Blockchain-perfect-government-services-heres-blueprint/

67 Cela comprend la cybergouvernance, le gouvernement ouvert et le gouvernement branché.

68 https://procivis.ch/

69 Ngo, D., Procivis Set to Release Blockchain-Powered e-Government 'App Store' This Year, Bitcoin Magazine, 8 février 2017. https://bitcoinmagazine.com/articles/procivis-set-release-blockchain-powered-e-government-app-store-year/.

70 http://bitfury.com/

71 Chavez-Dreyfuss, G., Ukraine launches big blockchain deal with tech firm Bitfury, Reuters. 19 avril 2017. http://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2.

72 Lohade, N., Dubai Aims to Be a City Built on Blockchain, Wall Street Journal, 24 avril 2017. https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080.

73 Dyrda, L., 8 blockchain healthcare startups to know, Becker's Health IT & CIO Review, 30 août 2016. http://www.beckershospitalreview.com/healthcare-information-technology/8-Blockchain-healthcare-startups-to-know.html. Healthcoin, une jeune entreprise néerlandaise, ne s'intéresse qu'à la santé personnelle.

74 Reportez-vous à Watters, A., The Blockchain for Education: An Introduction, Hackeducation.com, 7 avril 2016. http://hackeducation.com/2016/04/07/Blockchain-education-guide et Tierion (2016).

75 https://www.factom.com/

76 Reportez-vous à Colindres (2016) pour en savoir plus.

77 Forbes (2016) Vous trouverez une mise à jour récente à l'adresse suivante : https://www.forbes.com/sites/laurashin/2017/02/07/ the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands- project/#1281b034dcdc.

78 Mwinsuubo, N., Bitland Ghana Land Title Protection News, Bitland Global, 7 mars 2017. http://bitlandglobal.com/cadastral-land-registry-news-ghana/.

79 Rendez-vous à l'adresse suivante : http://bitfury.com/team.

80 Rendez-vous à l'adresse suivante : http://www.bitland.world/oracle/index.php.

81 Rendez-vous à l'adresse suivante : http://benben.com.gh/.

82 Vous trouverez les plus récents développements ici : Keane, J., Sweden Moves to Next Stage With Blockchain Land Registry, Coindesk, 30 mars 2017. http://www.coindesk.com/sweden-moves-next-stage-blockchain-land-re gistry/

83 Mesropyan, E., 21 Companies Leveraging Blockchain for Identity Management and Authentication, Let's Talk Payments, 13 février 2017. Et ici : https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/.

84 http://www.oneid.com/

85 Reportez-vous à Swan (2015), chapitre 3, pour en savoir plus à ce sujet.

86 Cooper, A., Does digital identity need blockchain technology?, Gov.uk., 15 août 2016. https://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-Blockchain-technology/.

87 Le programme d'identification nationale de l'Inde (Aadhaar) place la question de l'extensibilité à l'avant-plan.

88 http://florincoin.org/

89 https://steemit.com/blockchain/@pieterhaasnoot/publicism-blockchain-based-free-press

90 Une jeune entreprise a récemment annoncé un nouveau routeur Internet qui utilise les chaînes de blocs pour empêcher la surveillance et renforcer la sécurité. Reportez-vous à Young, J., Blockchain Router Solution to Government Surveillance, Nodio Believes, Coin Telegraph, 4 novembre 2016. https://cointelegraph. com/news/Blockchain-router-solution-to-government-surveillance-nodio-believes.

91 Cobben, I., Blockchain technology to improve press freedom, World News Publishing Focus, 2 août 2016. http://blog.wan-ifra.org/2016/08/02/Blockchain-technology-to-improve-press-freedom.

92 https://www.mazacoin.org

93 Rogoff, Z., Blockchain versus pipeline: uncensorable protest against fossil fuel development, Medium, 16 octobre 2016. https://medium.com/@zakkai/Blockchain-versus-pipeline-uncensorable-protest- against-fossil-fuel-development-bc03412f9229#.sgdbxd24a.

94 http://bitfury.com/

95 Swislow, D., What the blockchain could mean for democracy in the digital age, National Democratic Institute, 23 juin 2016. https://www.demworks.org/what-Blockchain-could-mean-democracy-digital-age.

96 https://followmyvote.com/

97 Follow My Vote utilise Bitshares, une plateforme financière de chaîne de blocs, comme technologie principale.

98 http://e-vox.org/

99 Reportez-vous à http://e-vox.org/e-vox-memo/ and http://e-vox.org/balta-installs-e-voxnarada/.

100 Burns Koven, J., Block The Vote: Could Blockchain Technology Cybersecure Elections?, Forbes, 30 août 2016. http://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-Blockchain-technology-cybersecure-elections/.

101 Vous trouverez une évaluation de la plateforme de l'Estonie, dans Springall, D. et coll., Security Analysis of the Estonian Internet Voting System, ACM, novembre 2014. https://estoniaevoting.org/findings/paper/.

102 https://bitnation.co/

103 Une analyse comparative de Bitnation et de la plateforme Second Life, parue en 2004, pourrait être le point de départ d'une étude de cas sur les formes alternatives de gouvernement national.

104 Clark, A., Blockchain In Humanitarian Efforts Leads To Award Nomination, Aid:Tech, 2 août 2016. https://aid.technology/charity-digital-news-Blockchain-in-humanitarian-efforts-leads- to-award-nomination-for-aidtech/.

105 Reportez-vous à https://refugees.bitnation.co/.

106 Reportez-vous à http://9needs.net/this-is-results-lab/.

107 Higgins, S., UNICEF Just Invested in its First Blockchain Startup, Coindesk, 15 novembre 2016. http://www.coindesk.com/unicef-just-invested-first-blockchain-startup/.

108 Begovic, M. et coll., UNDP Alternative Financing Lab - the next big thing is a lot of small (and smart things)!, PNUD Croatie, 19 septembre 2016. http://www.hr.undp.org/content/croatia/en/home/blog/2016/9/19/UNDP-Alternative-Financing-Lab-the-next-big-thing-is-a-lot-of-small-and-smart-things-.html.

109 del Castillo, M., The UN Wants to Adopt Bitcoin And Ethereum – And Soon, Coindesk, avril 2017. http://www.coindesk.com/the-united-nations-wants-to-accept-ethereum-and-bitcoin-and-soon/.

110 Higgins, S., Seven United Nations Agencies Are Now Investigating Blockchain Applications, Coindesk, 27 avril 2017. http://www.coindesk.com/7-united-nations-agencies-are-now-investigating-blockchain-applications/ et https://www.blockchain-expo.com/2017/04/blockchain/un-launches-request-information-blockchain-based-international-assistance/.

111 Comme nous l'avons mentionné plus tôt, le présent document ne porte pas sur les services financiers. Pour trouver une analyse approfondie de l'innovation et de l'utilisation des chaînes de blocs dans ces services, reportez-vous à Skinner (2016).

112 Le secteur agricole emploie 40 pour cent de la population active mondiale, et jusqu'à 75 pour cent de la population active des pays pauvres d'Afrique et d'Asie. http://www.momagri.org/UK/agriculture-s-key-figures/With-close-to- 40-%25-of-the-global-workforce-agriculture-is-the-world-s-largest-provider-of-jobs-_1066.html.

113 Données tirées du rapport mondial 2015 Mobile Money de GSMA : http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf.

114 https://www.bitpesa.co/

115 Reportez-vous à https://www.bitpesa.co/blog/bitpesa-v-safaricom/.

116 https://bitsoko.wordpress.com/about/

117 Caffin, G., Meet the Kenyan Startup Trying to Change Bill Gates' Mind on Bitcoin, Coindesk, 23 juillet 2015. http://www.coindesk.com/meet-the-kenyan-startup-trying-to-change-bill-gates-mind-on-bitcoin/.

118 Woyke, E., How Blockchain Can Bring Financial Services to the Poor, MIT Technology Review, 18 avril 2017. https://www.technologyreview.com/s/604144/how-blockchain-can-lift-up-the-worlds-poor/ et la Fondation Gates, Financial Services For The Poor - Strategy Overview, (non daté). http://www. gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor.

119 Pew Research, Remittance Flows Worldwide in 2015, 31 août 2016. http://www. pewglobal.org/interactives/remittance-map/.

120 Banque mondiale, Remittance Prices Worldwide, 19 septembre 2016. https://remittanceprices.worldbank.org/sites/default/files/rpw_report_sept_2016.pdf. Les ODD comprennent une cible de réduction des frais maximaux d'envoi d'argent à trois pour cent. Rendez-vous à l'adresse suivante : https:// sustainabledevelopment.un.org/sdg10.

121 Reportez-vous à : http://themoneywiki.com/wiki/alternative-currency-rebittance-bitcoin-remittance. Il est à noter que certains des liens proposés sont désormais inactifs.

122 https://www.goabra.com/

123 https://rebit.ph/

124 Satoshi Citadel Industries : http://sci.ph/about.html.

125 Begovic et coll., cité plus haut, 2016.

126 Higgins, S., UNICEF Eyes Blockchain as Possible Solution to Child Poverty Issues, Coindesk, 3 février 2016. http://www.coindesk.com/unicef-innovation-chief-Blockchain-child-poverty/.

127 Buntinx, JP, Top 6 Bitcoin and Blockchain Remittance Companies, The Merkle, 18 avril 2017. https://themerkle.com/top-6-bitcoin-and-blockchain-remittance-companies/.

128 Vous trouverez d'autres exemples à l'adresse suivante : http://www.ccgrouppr.com/practical-applications-of- Blockchain-technology/sectors/agriculture/.

129 https://www.skuchain.com/

130 Alisson, I., Skuchain: Here's how blockchain will save global trade a trillion dollars, International Business Times, 8 février 2016. http://www.ibtimes.co.uk/skuchain-heres-how-Blockchain-will-save-global-trade-trillion-dollars-1540618#.

131 http://farmshare.us/

132 Vous trouverez le livre blanc de Farmshare ici : https://www.academia.edu/16673793/FarmShare_Blockchain_ Community-Supported_Agriculture. Selon le site Web de Farmshare, le projet a été interrompu, ce qui signifie probablement qu'il ne sera pas mené à bien.

133 http://bitmari.com/

134 Campbell, R., BitMari's Farmers Accelerator Program Aims to 'Decolonize African Agricultural Economies, Bitcoin Magazine, 8 novembre 2016. https://bitcoinmagazine.com/articles/bitmari-s-farmers-accelerator-program-aims-to-decolonize-african-agricultural-economies-1478638863.

135 http://www.agriledger.co/

136 Cawrey, D., How Bitcoin's Technology Could Revolutionize Intellectual Property Rights, Coindesk, 8 mai 2014. http://www.coindesk.com/how-block-chain-technology-is-working-to-transform-intellectual-property/.

137 https://www.ascribe.io/

138 Higgins, S., Blockchain Startup Raises $2 Million for Intellectual Property Solution, Coindesk, juin 2015. http://www.coindesk.com/blockchain-startup-2-million-intellectual-property/.

139 Rogers, B., How the Blockchain and VR Can Change the Music Industry, Part 1, Medium, 24 novembre 2015. https://medium.com/cuepoint/bc-a-fair-trade-music-format-virtual- reality-the-blockchain-76fc47699733.

140 Le microfinancement et le microcrédit sont un autre domaine où les chaînes de blocs pourraient être utiles, comme c'est le cas en Birmanie. Reportez-vous à Dhaliwal, S., Blockchain Makes Microfinance Accounting Foray in Burma Led by Infoteria and Tech Bureau of Japan, Cointelegraph, 28 juin 2016. https://cointelegraph.com/news/Blockchain-makes-microfinance-accounting-for-ay-in-burma-led-by-infoteria-and-tech-bureau-of-japan.

141 Kelly, T., Tech hubs across Africa: Which will be the legacy-makers?, Banque mondiale, 30 avril 2014. http://blogs.worldbank.org/ic4d/tech-hubs-across-africa-which-will-be-legacy-makers.

142 ITU (2016), http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx. Ce chiffre inclut les personnes qui ont accès à Internet au moyen d'un téléphone cellulaire.

143 Par exemple, il convient de noter que M-Pesa n'était pas limitée par la connectivité Internet. Cela permettait aux utilisateurs munis d'un téléphone polyvalent de profiter de l'argent mobile au moyen de la messagerie texte. Les portefeuilles fondés sur la messagerie texte seront probablement un peu plus difficiles à mettre en oeuvre, puisqu'ils nécessitent l'utilisation d'une cryptographie à clés publiques par le client. En outre, les risques pour la sécurité pourraient être beaucoup plus importants.

144 https://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques

145 Allen, C. et coll., Decentralized Public Key Infrastructure: A White Paper from Rebooting the Web of Trust, 23 décembre 2015. https://danubetech.com/download/dpki.pdf.

146 Routi, S. et coll., Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client, Arxiv, 29 octobre 2015. https://arxiv.org/pdf/1510.08555v1.pdf.

147 Reportez-vous à The Morning Paper (2017).

148 The Economist. The Rise of the Superstars, Special report, 16 septembre 2016. http://www.economist.com/news/special-report/21707048-small-group-giant-companiessome-old-some-neware-once-again-dominating-global.

149 Un marché noir pour les clés privées, par exemple.

150 Popper (2015).

151 Idem.

152 Pearson, M., Ethereum's Boy King Is Thinking About Giving Up the Mantle, Motherboard, 24 avril 2017. https://motherboard.vice.com/en_us/article/ethereums-boy-king-is-thinking-about-giving-up-the-mantle.

153 Werback (2016) fournit des précisions.

154 Cette discussion porte sur les technologies de GLR dont on pourrait se servir pour améliorer le développement humain. Elle ne tient donc pas compte du bitcoin et des autres monnaies alternatives.

155 N'oubliez pas le principe « une unité centrale, un vote » de Nakamoto.

156 Comme la preuve de travail, qui est un algorithme de force brute, inélégant et inefficace.

157 Le bail tous frais compris est un bon exemple de contrat intelligent. On peut facilement ajouter le contrat à une chaîne de blocs, puis, chaque mois, les paiements de location seront effectués automatiquement jusqu'à ce que le contrat arrive à échéance. Toutefois, on ne devrait pas s'attendre à ce que les locataires soient capables de lire le code machine pour signer le contrat. Par défaut, ils doivent donc se fier à l'algorithme. Dans ce cas, l'opacité l'emporte sur la transparence.

158 On peut voir les chaînes auxiliaires comme une solution partielle à ce problème.

159 La technologie des chaînes de blocs n'élimine pas vraiment le besoin de confiance. Elle change plutôt la manière dont la confiance agit dans un réseau réparti.

160 Reportez-vous à https://blockchain.info/pools

161 Cette perspective et la réapparition de l'intelligence artificielle à l'ère des données massives sont en train de déclencher la création de ce que l'on appelle la « société de la boîte noire » (black box society). Reportez-vous à Pasquale (2015).

162 O'Neall (2016) plonge dans ce sujet particulier et présente des exemples réels qui illustrent comment les algorithmes peuvent détruire la vie des gens.

163 Pour connaître les problèmes liés à la mise en oeuvre de ces questions à cette étape, reportez-vous à : Harris, P. Despite the Success of Blockchain POCs, Deploying Pilots Won't be Easy (Part One), Distributed, 4 mai 2017.

164 À titre d'exemple, M-pesa compte plus de 20 millions d'utilisateurs au Kenya. Facebook a plus d'un milliard d'utilisateurs. Une application de chaînes de blocs pourrait-elle compter autant d'utilisateurs ?

165 Comin (2013).

166 Vous trouverez un résumé de l'histoire de BitTorrent et des détails sur cette organisation ici : Johnsen, J.A. et coll., Peer-to-peer networking with BitTorrent, NTNU, Department of Telematics, décembre 2005. http://web.cs.ucla.edu/classes/cs217/05BitTorrent.pdf.

167 BitTorrent utilise des tables de hachage distribuées.

168 https://ipfs.io/

169 https://fr.wikipedia.org/wiki/Table_de_hachage_distribu%C3%A9e

170 La vérification de paiement simplifiée est utilisée pour ces clients. La vérification de paiement simplifiée faisait partie de la conception initiale de Bitcoin de Nakamoto.

171 https://bitcoinfoundation.org/

172 La preuve de travail par un bassin minier est donc répartie.

173 De nombreux observateurs des technologies de chaînes de blocs ne font pas de distinction entre « réparti » et « décentralisé ».

174 Il s'agit d'un processus plutôt complexe qui est résumé dans le wiki Bitcoin : https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

175 Bitcoin utilise une cryptographie sur les courbes elliptiques.

176 L'en-tête de bloc est en fait haché deux fois à l'aide de SHA-256. Autrement dit, le condensé qui découle de la première opération SHA-256 sur l'en-tête de bloc devient une entrée pour la seconde opération de hachage. Cela réduit le risque d'attaque en augmentant la sécurité du condensé final.

177 https://fr.wikipedia.org/wiki/Fonction_de_hachage_cryptographique

178 https://fr.wikipedia.org/wiki/Syst%C3%A8me_hexad%C3%A9cimal

179 La plupart des chaînes de blocs stockent des métadonnées, ou des données sur les données. Les métadonnées sont chiffrées à leur tour.

180 Le condensé chiffré devient une signature numérique.

181 SHA signifie « algorithme de hachage sécurisé », un algorithme créé par la National Security Agency des États-Unis.

182 https://fr.wikipedia.org/wiki/SHA-2

183 On peut jeter un coup d'oeil en temps réel à la chaîne de blocs du bitcoin ici: https://Blockchain.info/. Pour voir la structure de données du bloc 436132, par exemple, rendez-vous à l'adresse http://bit.ly/2e040Pm.

184 La signature numérique comporte en fait 64 caractères hexadécimaux. Il faut garder à l'esprit qu'un caractère ordinaire est représenté par deux symboles hexadécimaux contigus. Par conséquent, la signature compte réellement 32 caractères.

185 Des outils de hachage sont offerts en ligne. Reportez-vous à la page http://www.fileformat.info/tool/hash.htm pour un exemple. On peut également hacher des fichiers, des documents, des photos, etc.

186 Ce nombre est appelé nonce.

187 Pour connaître l'évolution du matériel de minage de bitcoins, reportez-vous à Szmigielski (2016).

188 https://en.bitcoin.it/wiki/Double-spending

189 http://www-inst.eecs.berkeley.edu/~cs162/fa12/hand-outs/Original_Byzantine.pdf

190 https://fr.wikipedia.org/wiki/Attaque_Sybil

191 L'«embranchement » du logiciel Bitcoin est ce qui, dans une large mesure, a entraîné ces innovations. Le fait que le logiciel original soit à source ouverte signifie que les embranchements doivent le demeurer.

192 Les innovateurs font face à un grand dilemme qui porte sur l'endossement du bitcoin ou sur la création d'une monnaie rivale. Bien qu'on ait créé de nombreuses nouvelles cryptomonnaies, le prix élevé du bitcoin est devenu un pôle d'attraction pour son utilisation. Le bitcoin est également devenu un précieux actif financier.

193 Ces affirmations sont fondées sur les travaux d'Antonopoulos (2015).

194 https://namecoin.org/

195 https://www.ethereum.org/

196 Antonopoulos (2015).

197 Vous trouverez une liste complète des données financières à l'adresse https://bitinfocharts.com/index_v.html. Il est à noter qu'il y a de nombreux petits joueurs qui rivalisent ensemble avec quelques joueurs importants et dominants. Toutefois, l'augmentation rapide du prix du bitcoin s'est répandue à toutes les autres cryptomonnaies et chaînes de blocs.

198 Les chaînes auxiliaires peuvent améliorer l'utilisabilité, l'extensibilité et l'interopérabilité des chaînes de blocs. Nous n'approfondirons pas ce sujet d'une manière systématique ici puisqu'il ne correspond pas à la portée initiale du présent document. Reportez-vous à Back, A. et coll. Enabling Blockchain Innovations with Pegged Sidechains, 22 octobre 2014.

199 Cela ne signifie pas pour autant que l'innovation relative aux cryptomonnaies autres que le bitcoin soit sur le point de disparaître. Zcash, une nouvelle cryptomonnaie qui promet un anonymat total, est un exemple récent.

200 https://www.icann.org/

201 Il ne faut pas oublier que Namecoin peut être utilisée à d'autres fins, comme la protection de l'identité.

202 Namecoin est également parvenue à résoudre le problème du triangle de Zooko, que l'on croyait insoluble auparavant.

203 Namecoin a été invitée à la dernière réunion d'ICANN, tenue en mars dernier, à Copenhague.

204 Vous trouverez plus d'information dans Kaldoner (non daté).

205 Cela peut entraîner des bogues logiciels dans la chaîne de blocs, comme l'a montré le piratage d'Ethereum, quand un noeud a volé plus de 64 millions de dollars. Reportez-vous à Siegel, D., Understanding the DAO attack, Coindesk, 25 juin 2016.

206 Reportez-vous au document de présentation d'Ethereum : http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html.

207 Ethereum est un système Turing-complet, ce qui signifie qu'il est applicable de manière universelle, en langage informatique. Reportez-vous à Buterin (2013).

208 Ethereum est en train de mettre au point la preuve d'enjeu Casper : https://blog.ethereum.org/2015/08/01/ introducing-casper-friendly-ghost/. Ethereum étudie aussi d'autres possibilités.

209 Rendez-vous à l'adresse https://www.hyperledger.org/industries.

210 On dénombre plus de 25 consortiums mondiaux de technologie de chaînes de blocs. Reportez-vous à Mougayar, W., The State of Global Blockchain Consortia, Coindesk, 11 décembre 2016. http://www.coindesk.com/state- global-blockchain-consortia/

Chaîne de blocs

Libérer le potentiel révolutionnaire de la technologie des chaînes de blocs pour le développement humain

LIVRE BLANC

IDRC | CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada