Confiance programmée : Chances et risques de la technologie blockchain

Synthèse de l'étude «Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment»

TA-SWISS, Fondation pour l'évaluation des choix technologiques et centre de compétence des Académies suisses des sciences, entend mener une réflexion sur les répercussions – opportunités et risques – de l'utilisation de nouvelles technologies.

Cette synthèse se base sur une étude scientifique réalisée pour le compte de TA-SWISS par deux groupes de projet dirigés par Nils Braun-Dubler ainsi qu'Antoine Burret. Elle présente les principaux résultats et les recommandations de l'étude sous forme condensée et s'adresse à un large public.

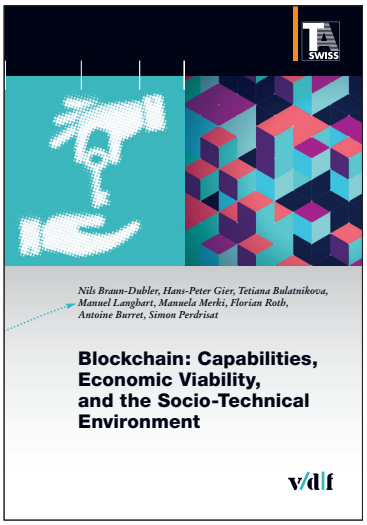
Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment

Nils Braun-Dubler, Hans-Peter Gier, Tetiana Bulatnikova, Manuel Langhart, Manuela Merki, Florian Roth, Antoine Burret, Simon Perdrisat

TA-SWISS, Stiftung für Technologiefolgen-Abschätzung (éd.)
vdf Hochschulverlag an der ETH Zürich, 2020.
ISBN 978-3-7281-4016-6

L'étude est également disponible en open access : www.vdf.ch

La synthèse peut être téléchargée gratuitement : www.ta-swiss.ch



Une brève introduction 4
La Suisse – le pays de la blockchain 4
Une machine qui crée la confiance 4
Les chances de la blockchain 5
Les risques de la blockchain 5
Double focale 6

Un regard en arrière 6

Les maillons de la chaîne 8
Un peu de cryptographie 8

La blockchain à l'épreuve de ses applications 12
Registres publics – droits de propriété garantis numériquement 12
Cryptomonnaies – la grande désillusion 12
Initial coin offering (ICO) – l'introduction en bourse virtuelle 13
Systèmes de paiement privés (private payment systems) – achats dans un camp de réfugiés 14
Preuve d'origine – de la mer à l'assiette 14
Gestion intelligente de l'énergie – du soleil sur les toits de Brooklyn 15
À la recherche de l'application tueuse (killer app) 15

La blockchain comme catalyseur 16
Confiance, contrôle et responsabilité 16
Transparence contre sphère privée 16
Dompter le tigre – mais tous ensemble 16

Une brève introduction

Libra, le système de paiement global de Facebook était sur le point d'y parvenir : pour la première fois, une application basée sur la blockchain allait devenir une réalité pour le grand public. Mais entre-temps, la perspective d'une percée majeure de la technologie blockchain s'est éloignée. Plusieurs des principaux acteurs impliqués dans ce projet, comme Visa, Mastercard ou PayPal, l'ont quitté avant son lancement prévu pour 2020. En cause : le climat défavorable et les résistances, ainsi que les appels à la prudence des banques centrales et des gouvernements à l'égard d'une solution de paiement parallèle fonctionnant sans surveillance étatique ou bancaire, une « monnaie mondiale privée » qui pourrait échapper à leur contrôle, servir au blanchiment d'argent ou au financement du terrorisme et déstabiliser le système financier bien établi.

La Suisse – le pays de la blockchain

La Suisse a décidé de miser sur la technologie blockchain et sur son potentiel, notamment en ce qui concerne les approches innovantes sur le marché financier. Et elle est bien placée pour tirer profit de cette technologie. Grâce à son cadre réglementaire libéral, une communauté très active de pionniers de la blockchain s'est déjà établie dans la « Crypto Valley » entre Zoug et Zurich. La politique d'arbitrage flexible et libérale de la Suisse devrait faire de ce pays un lieu de juridiction important pour les contrats dits « intelligents » (smart contracts). Afin de renforcer et de développer le rôle du pays en tant que centre de la blockchain, la Confédération a mis en place un groupe de travail dès 2017 qui s'efforce d'accroître la sécurité légale encadrant les applications de la blockchain en adaptant la législation de manière ciblée.

Une machine qui crée la confiance

Pour le dire très simplement, la blockchain est une base de données infalsifiable et gérée de manière décentralisée. Contrairement aux instances classiques et aux institutions (souvent légitimées démocratiquement) garantes du déroulement correct de tous les processus, la blockchain fonctionne sur le principe de la confiance de tous les participants dans un système technologique transparent et (théoriquement) absolument fiable. Plus il y a d'acteurs qui participent au consensus, plus le climat de confiance se renforce et plus la sécurité des manipulations est garantie. Ce n'est pas sans raison que la blockchain est aussi qualifiée de machine à créer la confiance. Une fabrique à confiance visant à transformer Internet en un « Internet des valeurs » dans lequel les valeurs – par exemple l'argent, les titres fonciers, les documents d'assurance ou les preuves d'identité – circulent en toute sécurité dans le monde entier.

La monnaie virtuelle Bitcoin, suivie par d'autres cryptomonnaies, a été la première application de la blockchain. Elle est certainement celle qui a le plus contribué à l'aura nébuleuse de cette nouvelle technologie. De nombreux experts en numérique et en finance débordaient d'enthousiasme à propos des opportunités qu'offrait ce qu'on qualifiait de « révolution la plus importante depuis l'invention du World Wide Web » ; mais au même moment, la plateforme commerciale illégale Silk Road, cachée dans les tréfonds d'Internet, utilisait le Bitcoin pour payer ses transactions douteuses. S'y sont ajoutées la spéculation effrénée, les fluctuations de prix et les attentes exagérées d'une part, et l'absence d'applications vraiment quotidiennes d'autre part : tout ceci a contribué à générer un hype et à créer des légendes autour de la blockchain. Par ailleurs, le système de technologie de l'information est si complexe qu'il dépasse l'entendement de la plupart des gens. Et enfin, il y a le fait que la plus grande force de la blockchain est aussi son talon d'Achille, car en éliminant les organismes de contrôle traditionnels, elle devient elle-même une instance de confiance. Mais un système technique est-il adapté pour se substituer à l'État en tant que « tiers de confiance » ou, selon le domaine d'application, pour remplacer l'autorité de surveillance financière, l'autorité électorale ou le notaire ? La blockchain peut-elle même réformer le capitalisme, comme le croient certains de ses plus ardents partisans ? La réponse à ces questions est de nature sociopolitique.

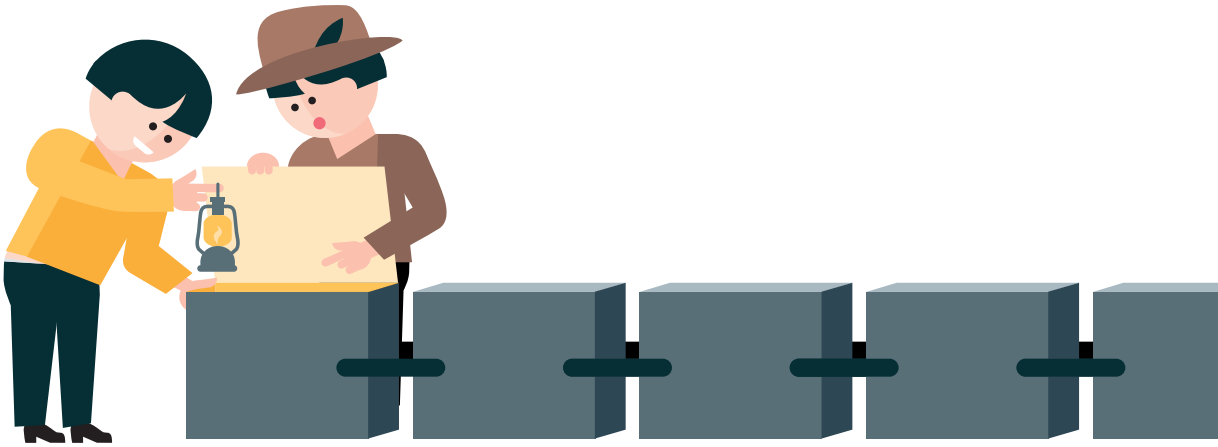
C'est dans cette optique que, conformément à son mandat, la Fondation pour l'évaluation des choix technologiques TA-SWISS a élaboré une base de connaissances complète sur les chances et les risques liés à la blockchain à l'intention du monde politique et du public.

Les chances de la blockchain

- son immuabilité, assurée par la cryptographie et un système d'incitation intelligent, qui veille à ce que tous les acteurs du réseau garantissent la légalité de toutes les transactions,
- sa nature décentralisée, qui protège l'ensemble du système des manipulations,
- sa capacité à créer un rapport de confiance entre des acteurs qui ne se connaissent pas ou peu,
- la possibilité de garantir les droits de propriété ou la preuve d'origine sous forme numérique avec une crédibilité absolue ; ceci donne à la blockchain le potentiel de renouveler de fond en comble le secteur des services financiers,
- le fait qu'en éliminant les intermédiaires, les transactions deviennent plus rapides, moins chères et moins sujettes à l'erreur,
- la transparence et l'immuabilité des informations sécurisées qui améliorent la sécurité juridique ; ceci peut être un atout considérable, surtout dans les pays qui ne disposent pas d'une autorité centrale fiable ou efficace,
- et le fait que, combinée avec les contrats intelligents et l'Internet des objets, la blockchain permet l'automatisation des processus de vérification et des preuves de validité.

Les risques de la blockchain

- le fait que certains des mécanismes de consensus, qui remplacent une instance de confiance centrale dans la blockchain et nécessitent une énorme puissance de calcul répartie sur un grand nombre d'ordinateurs, consomment de grandes quantités d'énergie,
- l'anonymat des utilisateurs qui participent à des blockchains publiques sous un pseudonyme et peuvent le faire à des fins criminelles,
- le fait que toutes les transactions jamais effectuées par une personne deviennent visibles dès que l'identité d'un pseudonyme est connue,
- l'immuabilité de la blockchain qui exclut complètement le droit à l'oubli, contrairement à ce que prévoit la protection des données,
- le fait que, bien qu'elle promette plus de transparence et une prise de décision collective, la blockchain reste complètement opaque pour le grand public en raison de sa complexité,
- et le fait que la blockchain demeure en grande partie une « solution sans problème » car il manque encore une « application tueuse » (killer app) – et que la blockchain n'est donc pas à la hauteur du battage médiatique qu'elle suscite.



Double focale

TA-SWISS présente une étude en deux parties sur la technologie blockchain. La première partie, plus technique, donne un aperçu détaillé du fonctionnement de la blockchain et analyse son potentiel économique. Elle s'appuie également sur douze études de cas pour montrer où les applications de la blockchain offrent un réel avantage par rapport aux applications traditionnelles dans un même domaine et où elles ne parviennent pas (encore) vraiment à convaincre. Les exemples vont des registres fonciers publics aux systèmes de paiement dans les camps de réfugiés, en passant par l'approvisionnement en énergie. Cette première partie a été réalisée par une équipe de projet de l'Institut d'études économiques de Bâle (IWSB) sous la direction de Nils Braun-Dubler, en coopération avec le cabinet de conseil en gestion Banking Concepts et le cabinet de droit, de fiscalité et de compliance MME. La deuxième partie de l'étude place la blockchain, sa genèse et la façon dont elle est perçue dans un contexte sociologique et culturel. Elle examine en particulier comment l'opacité du système (pour le grand public) influence le discours social autour de la blockchain, et qui a intérêt à maintenir un certain battage médiatique à cet égard. Cette deuxième partie a été rédigée par les sociologues Antoine Burret et Simon Perdrisat du Centre Universitaire Informatique de l'Université de Genève.

Ensemble, les deux parties de l'étude forment un état de l'art complet de la situation actuelle qui devrait contribuer à calmer l'excitation et à tempérer les attentes, souvent tout aussi exagérées que les craintes et les réactions défensives autour de la technologie blockchain. L'étude vise à fournir une base factuelle pour débattre de la signification économique et sociale comme des applications actuelles et futures de cette technologie.

Un regard en arrière

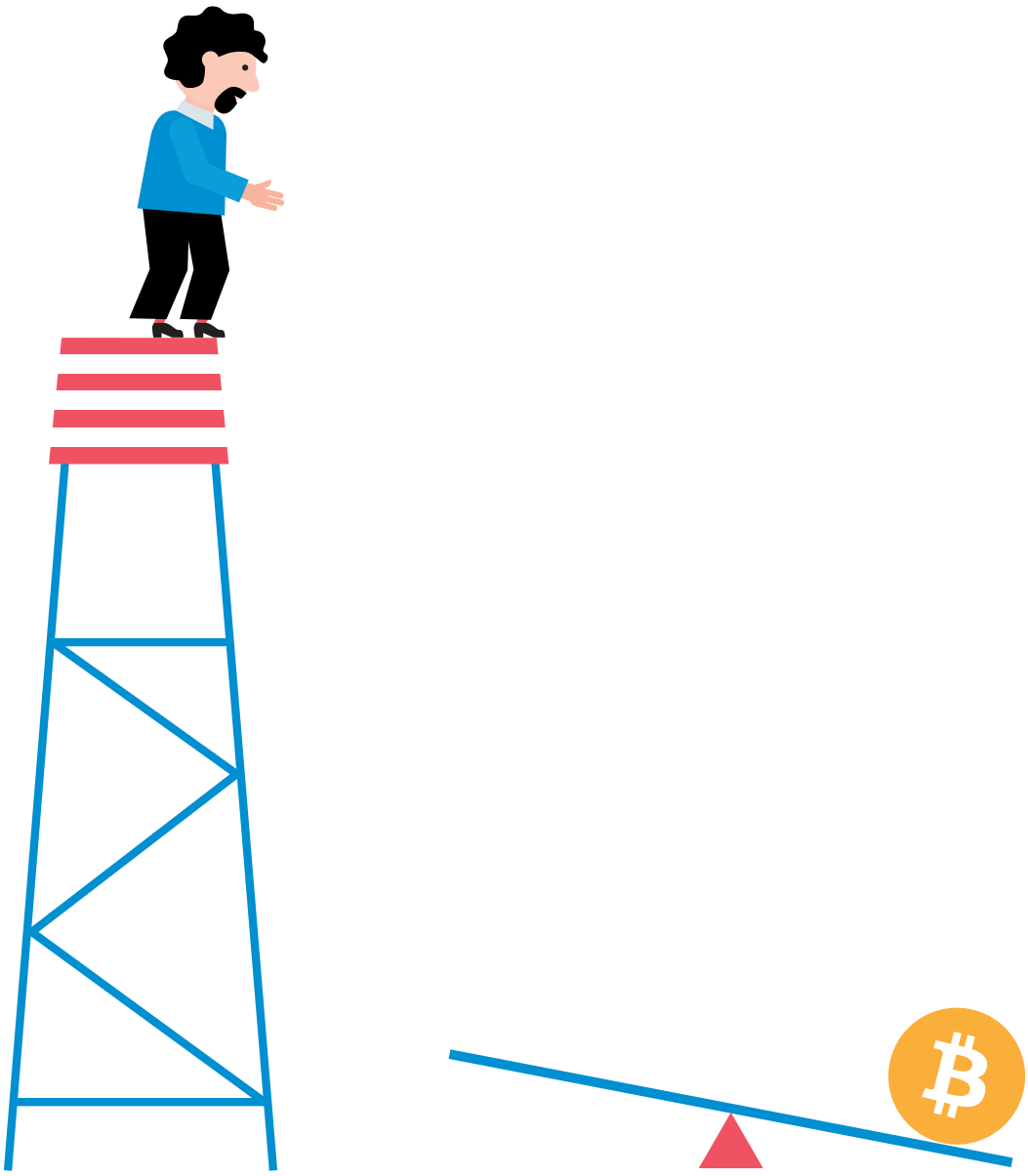
En 2008, un certain Satoshi Nakamoto – nom dont on ne sait toujours pas s'il désigne un individu ou un collectif – publie un essai scientifique sur une plateforme dédiée à la cryptographie. Cette publication porte sur un nouveau système monétaire électronique permettant de transmettre des valeurs monétaires au sein d'un système décentralisé à l'aide d'une chaîne d'ensembles de données scellés de manière cryptographique et infalsifiable. Et ce, de telle sorte que le gênant problème de la double dépense – raison pour laquelle toutes les monnaies numériques ont échoué jusqu'alors – soit résolu, à savoir que la même valeur monétaire numérique ne soit pas facturée plusieurs fois, tout en se passant de l'intervention d'une autorité de contrôle centrale. Nakamoto appelle son système Bitcoin. Grâce à un système d'incitation intelligent, tous les utilisateurs du réseau sont encouragés à participer et à valider une preuve cryptographique qui remplace l'intermédiaire de confiance. L'article, qui ne fait que neuf pages, est accueilli avec enthousiasme.

L'invention de Nakamoto n'a pas surgi de nulle part. Elle s'appuie sur des concepts et des considérations théoriques issues du domaine de la cryptographie mathématique et de l'informatique qu'elle associe à de nouvelles technologies. En même temps, elle incarne l'un des changements profonds induits par la commercialisation des technologies de l'information : les mécanismes de cryptage qui permettent d'échanger des informations de manière sûre, fiable et confidentielle sur le World Wide Web ne sont plus réservés aux gouvernements et aux grandes entreprises, mais sont devenus des outils que toute la société numérique revendique pour elle-même.

Le 3 janvier 2009, Nakamoto crée le premier bloc de la blockchain Bitcoin, le bloc Genesis. Peu de temps après, il entre dans la clandestinité et laisse à la communauté le soin de poursuivre les travaux sur le logiciel libre Bitcoin. Dans le tout premier bloc de la chaîne, le mystérieux créateur de la blockchain a inséré un titre du « Times » de Londres faisant allusion à la crise bancaire mondiale. Il est donc clair dès le départ que le projet Bitcoin n'est pas seulement un projet technique, mais aussi un projet social extrêmement critique à l'égard des institutions publiques centrales.

Le concept du Bitcoin donne lieu à de nombreuses cryptomonnaies alternatives, également appelées

« Altcoins », avec des noms comme Litecoin ou Peercoin. Cependant, dès 2009, on envisage que l'innovation fondamentale derrière le Bitcoin, la blockchain, soit étendue à d'autres domaines d'application que les devises alternatives et les transactions financières : registres de fret, titres de propriété, diplômes universitaires. En principe, « tout ce qui peut être représenté comme un bien numérique et qui ne peut être en possession que d'une seule personne à la fois » est susceptible d'être inscrit dans le registre numérique infalsifiable de la blockchain, écrit le développeur de logiciels Vitalik Buterin dans un document fondateur en 2013. Quelques années plus tard, ces considérations débouchent sur la création d'une nouvelle plateforme : Ethereum, plus qu'une cryptomonnaie, plus puissant que le Bitcoin et capable de déclencher automatiquement des actions convenues dès que certaines conditions sont remplies, comme par exemple libérer un paiement à la réception d'une livraison. Les contrats intelligents entrent en jeu.



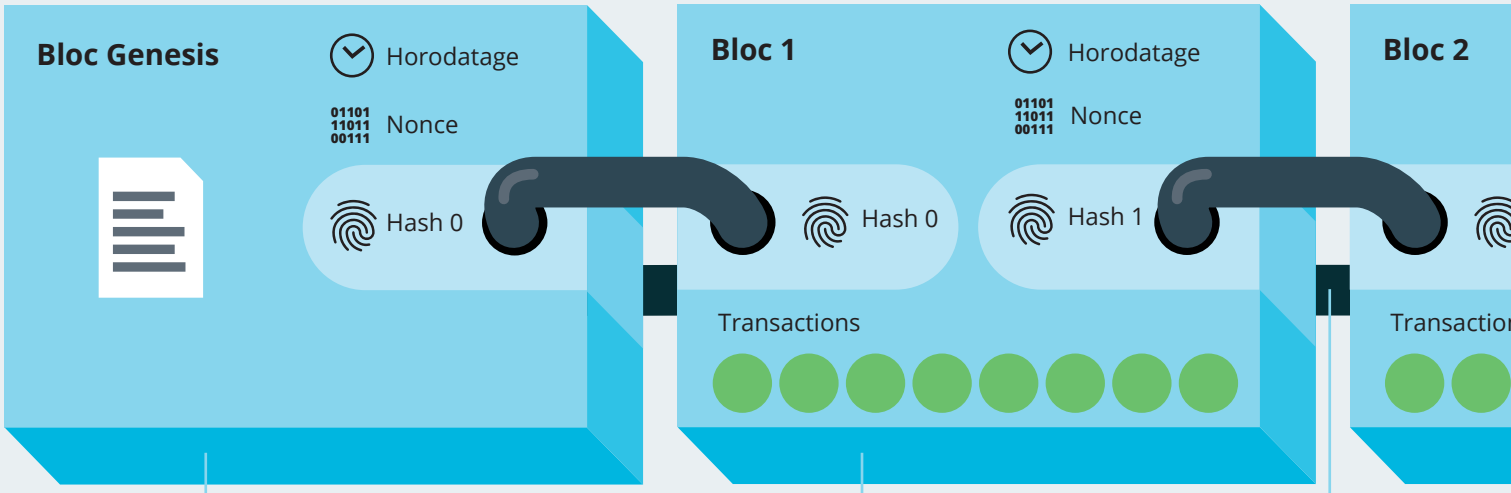
Les maillons de la chaîne

Blockchain : C'est un livre de comptes numérique infalsifiable et stocké de manière décentralisée. Elle consiste en une séquence de valeurs de hachage chronologiquement séquencées, chacune d'entre elles se référant à celle qui la précède. Il n'est donc pas possible de modifier ultérieurement les blocs ou de les introduire illégalement dans la chaîne.

Un peu de cryptographie

Cryptographie : Elle vise à sécuriser des bases de données et des informations sensibles sous une forme déterminée et à les transmettre de manière à ce que les personnes non autorisées ne puissent y accéder ou les comprendre (confidentialité). En même temps, l'identité de l'expéditeur et du destinataire doit être établie sans équivoque (authentification). Il ne doit pas être possible de modifier les informations sans s'en rendre compte pendant la transmission ou le stockage (intégrité), et enfin, l'expéditeur ne doit pas pouvoir contester ultérieurement l'authenticité des informations transmises (non-répudiation). Une clé secrète est utilisée pour crypter et décrypter les informations. Dans le cas d'un cryptage symétrique, l'expéditeur et le destinataire utilisent la même clé. Dans le cas d'un cryptage asymétrique, ils utilisent une paire de clés composée d'une clé publique et d'une clé privée que seule l'une des deux parties possède. Dans les deux cas, une clé est utilisée pour restaurer le message original.

Fonction de hachage : Il s'agit d'une procédure cryptographique qui, contrairement au cryptage, n'est pas réversible.



Bloc Genesis : Il s'agit du premier bloc d'une blockchain. Le protocole de consensus est également défini dans le bloc Genesis. Il précise qui est autorisé à valider les blocs et quelle tâche doit être effectuée à cette fin, la fréquence d'inscription d'un nouveau bloc dans la chaîne et sa taille, c'est-à-dire le nombre de transactions qui y sont stockées.

Bloc : Le contenu de chaque bloc est constitué de la valeur de hachage de toutes les transactions signées stockées dans le bloc, d'un horodatage et d'un nombre arbitraire (nonce) nécessaire pour valider le bloc. On y ajoute la valeur de hachage du bloc précédent. La valeur de hachage du nouveau bloc est calculée à partir de toutes ces valeurs.

Chaîne : Les différents blocs sont liés cryptographiquement les uns aux autres. Comme chaque bloc contient le hachage du bloc précédent, les blocs forment une chaîne dans laquelle toutes les transactions depuis le début de la blockchain sont enregistrées.

Une fonction de hachage est un algorithme qui convertit un fichier, quelle qu'en soit la longueur et la complexité (p. ex. une inscription au registre foncier, une photo ou même un fichier audio), en une chaîne de caractères de longueur fixe. Pour le SHA-256, l'algorithme le plus utilisé dans le monde de la blockchain, il s'agit de 256 bits ou caractères ou, en d'autres termes, d'une séquence de 256 zéros et uns. Les mécanismes de hachage jouent un rôle central dans la blockchain.

Valeur de hachage de l'entrée :
Bonjour le Monde

10100101100100011010011011
01010000001011111101000010
00000100000001001010000000
01000101110011001111001111
10110111101100011001000011
01011000101100011001011011
11110000101111001101101000
11001010110101011110110010
01110111110110011010110110
01111100010100011101110

Valeur de hachage de l'entrée :
Bonjour, le Monde

00000011011001110101101011
00010100111111111110011100
11010001010100110101110011
00110001111101111111001101
11111010001011000100010110
00110001010010000110000011
01110001111101000001100011
01110000010011011011110010
11010001100110101100000111
11101111101000101001 01

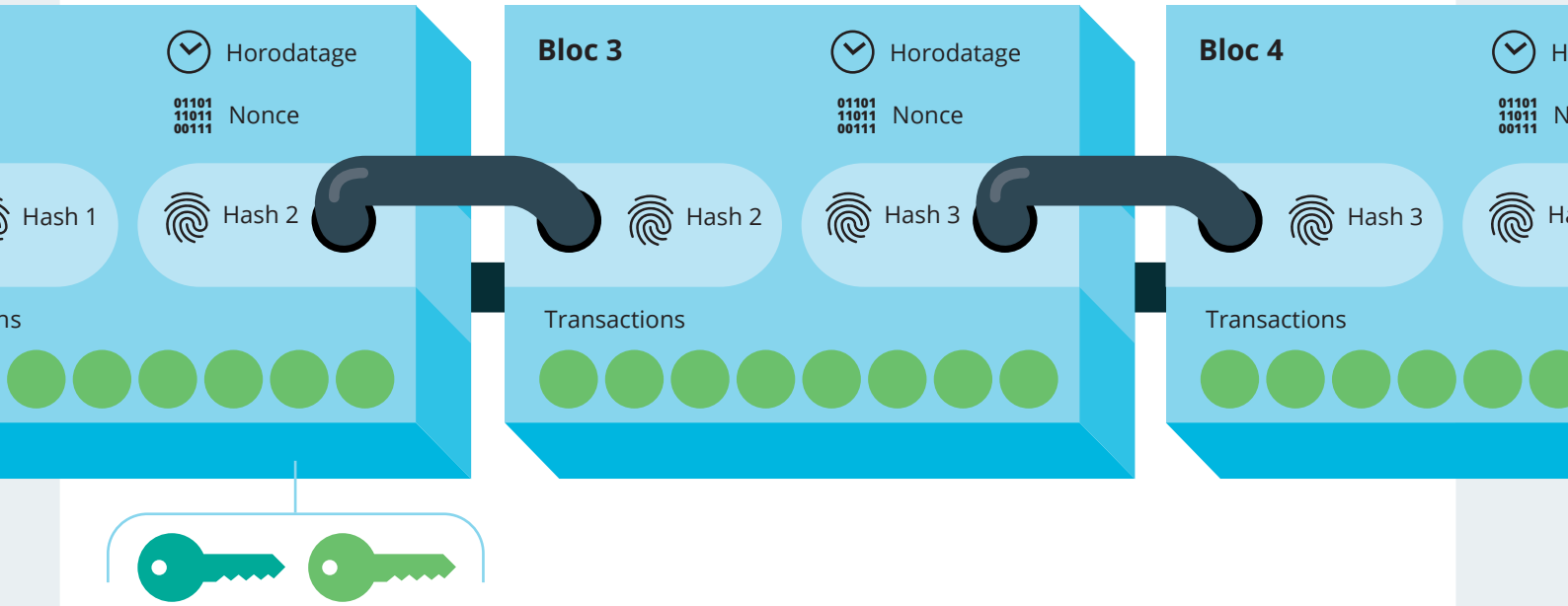
Un hachage, également appelé chiffre de contrôle, possède trois propriétés importantes :

1. Il est irréversible, c'est-à-dire qu'il est impossible à calculer à partir de la donnée de sortie et de trouver quel fichier d'entrée l'a généré. Un document « haché » ne peut donc pas être reconstitué à partir de sa valeur de hachage. Il n'est pas exclu que cela change lorsqu'un puissant ordinateur quantique sera disponible : la décomposition laborieuse de grands nombres en leurs facteurs premiers, tâche à laquelle les meilleurs superordinateurs échouent encore aujourd'hui, se ferait alors en un rien de temps.

2. La plus petite modification de la donnée d'entrée lors de la saisie donne une valeur de hachage complètement différente. Il est donc possible de vérifier si un ensemble de données a été modifié. Les valeurs de hachage permettent ainsi de détecter les manipulations.

3. La même donnée d'entrée produit toujours la même donnée de sortie. C'est pourquoi la valeur de hachage est également appelée « empreinte digitale numérique ». Si le résultat est différent, cela signifie en tous les cas que la donnée d'entrée a été modifiée.

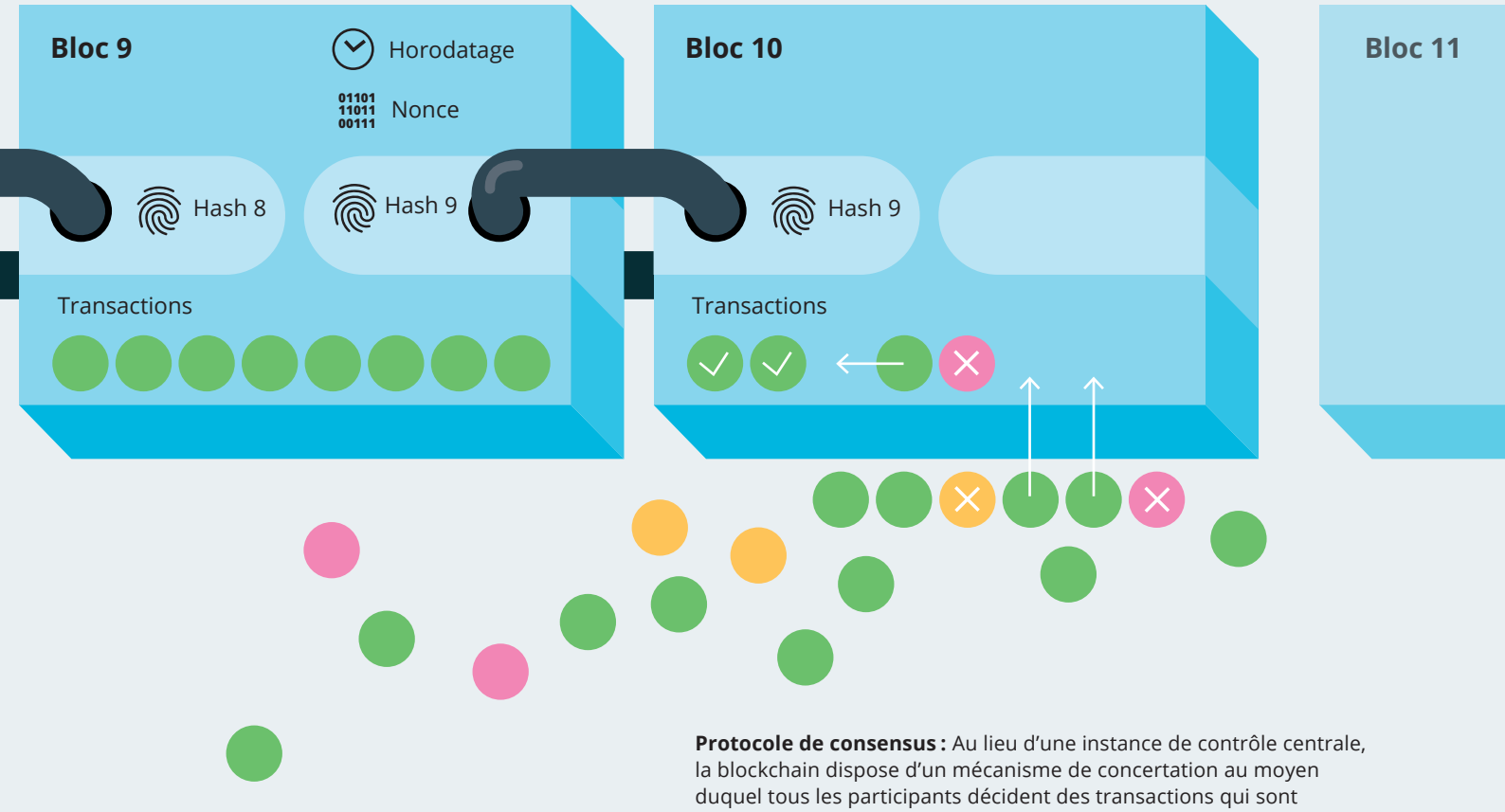
Le pouvoir des grands nombres : En réalité, le point 3 ci-dessus n'est théoriquement pas toujours correct. Il est possible en effet que différents ensembles de données soient représentés par la même valeur de hachage. Mais la probabilité d'une telle « collision » est si faible qu'elle peut immédiatement être écartée : elle correspond à la possibilité de décrocher le jackpot de l'Euromillions neuf fois de suite. De même, par exemple, la probabilité que deux utilisateurs de la blockchain se voient attribuer la même valeur de hachage comme numéro de compte est proche de zéro.



Cryptage asymétrique : Il est utilisé dans la blockchain pour sécuriser les données d'accès et pour vérifier les droits de propriété. Chaque utilisateur se voit attribuer une combinaison arbitraire de chiffres sous la forme d'une clé privée. Elle sert à calculer une clé publique et, à partir de celle-ci, un numéro de compte (adresse publique). Avec la clé privée, un utilisateur peut prouver qu'il est le seul propriétaire autorisé d'un compte. Il doit également signer chaque transaction qu'il effectue sur son compte avec sa clé privée. Grâce au lien mathématique entre les deux clés, la clé publique peut être utilisée pour vérifier si une transaction a été effectuée correctement et si une signature est valable. Si le titulaire du compte perd la clé privée, il ne peut plus accéder à ses données. Entre trois et cinq millions de Bitcoins devraient être perdus à jamais.

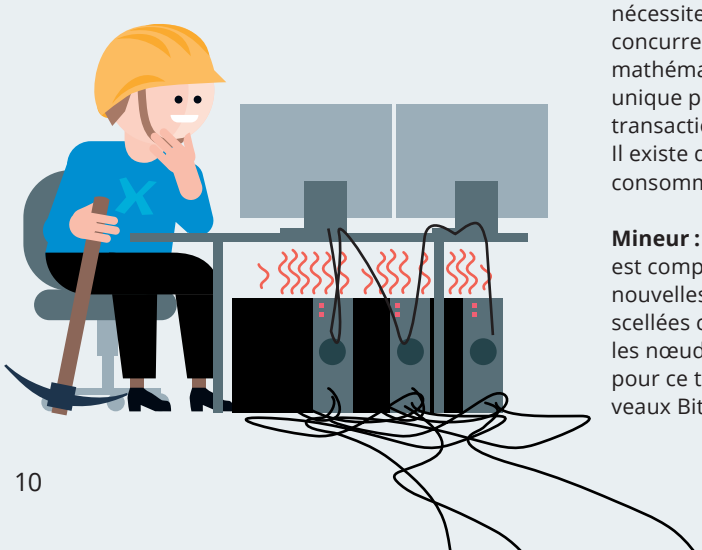
Pseudo anonymat (pseudonymat) : La blockchain étant transparente, toutes les transactions peuvent être suivies à tout moment et sont reliées à une adresse publique. Toutefois, afin de protéger la vie privée des utilisateurs, la clé publique d'un utilisateur n'est pas associée à son nom mais à un pseudonyme, ce qui ne permet pas de connaître la personne réelle qui se cache derrière. Toutefois, comme il n'est pas impossible que quelqu'un puisse deviner l'identité d'un utilisateur à partir de ses mouvements transactionnels, on parle de pseudo anonymat.

Preuve à divulgation nulle de connaissance (zero-knowledge proof) : Il s'agit d'une procédure cryptographique mathématique incroyablement complexe par laquelle une partie prouve à l'autre qu'elle connaît un secret sans avoir à révéler le secret lui-même. Les protocoles « zero-knowledge » peuvent renforcer l'anonymat sur la blockchain.



Protocole de consensus : Au lieu d'une instance de contrôle centrale, la blockchain dispose d'un mécanisme de concertation au moyen duquel tous les participants décident des transactions qui sont valables et de l'ordre dans lequel elles seront placées dans la chaîne. Ce consensus ne s'obtient pas de la même manière pour toutes les applications de la blockchain. Le protocole de consensus le plus couramment utilisé est appelé preuve de travail (proof-of-work). Il nécessite une énorme puissance de calcul, car chaque nœud est en concurrence avec les autres pour tenter de résoudre un problème mathématique complexe. La tâche consiste à calculer un hachage unique pour le nouveau bloc à inclure dans la chaîne à partir des transactions en suspens et de la valeur de hachage du bloc précédent. Il existe d'autres protocoles de consensus moins complexes et qui consomment donc moins d'énergie.

Mineur : Certains des nœuds font office de validateurs. Leur tâche est comparable à celle d'un comptable : ils vérifient la validité des nouvelles transactions, les regroupent et les placent dans la chaîne, scellées cryptographiquement dans un nouveau bloc. Pour encourager les nœuds à participer au processus de vérification, ils sont rémunérés pour ce travail. Dans le cas du Bitcoin, les mineurs reçoivent de nouveaux Bitcoins. Le processus est donc comparé à l'extraction de l'or.



Registre distribué (distributed ledger) : Comme les ensembles de données stockés dans une blockchain sont distribués de manière décentralisée à un grand nombre d'ordinateurs, la blockchain est également connue sous le nom de « base de données distribuée », ou de « registre distribué » (distributed ledger).

Nœuds (nodes) : Chaque ordinateur participant à la blockchain est un nœud. Chaque nœud conserve et tient à jour une copie complète et continuellement actualisée de la blockchain. Le fait que les données soient stockées plusieurs fois rend le réseau stable et fiable. Il est capable de faire face à la défaillance d'un ou plusieurs nœuds sans difficulté.

Blockchain publique : Tout le monde peut télécharger le protocole et rejoindre le réseau. Une preuve d'identité n'est pas nécessaire. En principe, tous les participants ont les mêmes droits. Chacun peut consulter toutes les transactions et participer au protocole de consensus. Une blockchain publique est totalement transparente pour tous les participants au réseau.

Blockchain privée : Elle s'adresse à un groupe défini de participants (par exemple, une entreprise et ses fournisseurs). Une ou plusieurs instances centrales déterminent qui peut rejoindre le réseau et qui détient quels droits d'accès. Les protocoles de consensus pour la vérification et la validation sont moins complexes et nécessitent moins de calculs dans une chaîne non publique. Il est aussi possible d'y renoncer complètement car les participants se connaissent et se font mutuellement confiance dans ce contexte. Mais cela réduit également la transparence d'une blockchain privée.

La blockchain à l'épreuve de ses applications

Registres publics – droits de propriété garantis numériquement

En tant que registre numérique infalsifiable et totalement transparent, la blockchain semble à première vue particulièrement adaptée aux registres publics tels que le registre foncier. Distribué sur un grand nombre d'ordinateurs, un registre basé sur une blockchain garantit l'immuabilité des informations qui y sont stockées et offre plus de sécurité qu'une base de données stockée sur un serveur central. Les processus deviennent plus rapides et plus efficaces. Une instance centrale n'est pas nécessaire. Cela peut devenir un atout dans un pays dont les institutions sont déficientes.

Et en Suisse ? Ici, le registre foncier, à titre d'exemple de registre public, enregistre les droits qui existent sur une parcelle. Toute modification, qu'il s'agisse de la vente du bien immobilier ou de son transfert à un nouveau propriétaire, doit être notariée et inscrite au registre foncier. En Suisse, ce sont les cantons qui tiennent ce registre pour le compte de la Confédération et qui garantissent l'exactitude de toutes les inscriptions. Il n'existe pas de registre foncier central pour l'ensemble de la Suisse. Le registre foncier est public – tout le monde peut, par exemple, demander des informations sur les propriétaires d'un bien immobilier particulier. Le marché foncier est donc largement transparent. Plusieurs des points forts de la blockchain semblent déjà présents dans le système actuel.

Il faut souligner que le droit à la protection de la sphère privée restreint l'accès au registre foncier. Il appartient aux administrateurs du registre foncier d'accorder ou non un accès supplémentaire aux personnes qui peuvent démontrer de manière crédible un intérêt particulier. Sans changer la loi, cette caractéristique ne pourrait être reproduite qu'à l'aide d'une blockchain privée définissant précisément les droits d'accès. La confiance dans l'autorité foncière cantonale serait alors remplacée par la confiance dans un groupe d'instances d'autorisation.

Le transfert intégral d'un registre public dans une blockchain n'a pas beaucoup de sens. Les solutions partielles telles que celles testées par le canton de Genève sont plus intéressantes : les extraits du registre foncier demandés par les citoyens y sont simultanément déposés sur la blockchain. Cela permet aux destinataires de vérifier que le document qui leur est envoyé est identique à l'original et donc valable. La SuisseID, preuve d'identité électronique déjà existante et juridiquement valable, pourrait servir le même objectif. Mais l'approche consistant à ajouter la fonctionnalité de contrats intelligents à un registre basé sur la blockchain semble plus prometteuse : par exemple, les modifications du registre foncier n'entreraient en vigueur qu'au moment où certaines conditions sont remplies.

Cryptomonnaies – la grande désillusion

En 2017, la valeur du Bitcoin, la plus importante monnaie numérique, a explosé en progressant de plus de 1800 % et a atteint une valeur record de près de 20 000 dollars américains à la fin de l'année. D'autres cryptomonnaies – il en existe près de 3000 aujourd'hui – connaissent elles aussi des hausses marquées suivies de chutes de prix importantes. L'attitude du grand public, des marchés financiers et des gouvernements à l'égard de cette nouvelle classe d'actifs est tout aussi volatile. On lui prédit parfois un brillant avenir ainsi que la capacité de transformer l'ensemble du système bancaire et de briser le pouvoir de ses institutions traditionnelles. Les pays technologiquement avancés, comme le Japon, les ont acceptées comme faisant partie de l'industrie émergente des technologies financières de pointe. En Suisse également, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a déjà accordé la licence bancaire à deux cryptobanques. D'autres mettent en garde contre une bulle spéculative classique, y voyant une menace pour la stabilité financière et la tentative de contourner les banques centrales et les régulateurs à grande échelle.

Force est toutefois de constater en toute objectivité que les monnaies virtuelles ont justement des performances plutôt modestes. Jusqu'à présent, elles ne sont pas vraiment une alternative valable aux devises classiques : leur valeur moyenne de transaction quotidienne reste largement inférieure, leur stabilité est déplorable et elles ne sont guère acceptées comme moyen de paiement courant. Et elles ne

remplacent pas non plus les systèmes traditionnels de paiement : avec le Bitcoin, par exemple, seules sept transactions par seconde environ peuvent être effectuées dans le monde entier, tandis que les paiements avec PayPal sont pratiquement instantanés. Enfin, les cryptomonnaies qui, contrairement à l'or, n'ont pas de valeur intrinsèque sont beaucoup trop volatiles pour être une valeur refuge.

La communauté blockchain travaille à modifier et développer le système de cryptomonnaie de manière ciblée. Par exemple, la Fondation Bitcoin s'est engagée à normaliser, sécuriser et promouvoir l'utilisation de l'argent cryptographique dans le monde entier. Mais pour l'instant, le constat demeure : les monnaies basées sur des blockchains n'ont pas encore répondu à leurs propres exigences.

Initial coin offering (ICO) – l'introduction en bourse virtuelle

La levée de capitaux peut être un processus long et difficile pour les start-ups. Il existe désormais un moyen de financement issu de la blockchain qui combine cette technologie et le crowdfunding. Contrairement à l'introduction en bourse classique (initial public offering ou IPO), les actions des sociétés ne sont pas vendues en échange de capital-risque, mais de jetons (tokens). Il s'agit d'unités numériques de la cryptomonnaie créée spécialement pour le projet en question. La FINMA distingue trois catégories de jetons basés sur la blockchain : ceux qui ont une valeur monétaire (jetons de paiement), ceux qui donnent accès à un service (jetons utilitaires) et enfin ceux qui représentent un investissement (jetons sécuritaires). L'acheteur spécule sur le fait que la valeur des jetons acquis sera multipliée grâce au succès que rencontrera le projet financé par ce biais. Les ICO sont très populaires à travers le monde et battent régulièrement des records de volume d'émission. Une ICO permet de financer une idée brillante à un stade encore précoce. Ceci peut représenter une incroyable opportunité de concrétiser rapidement une innovation – mais peut aussi être une arnaque pour soutirer de l'argent aux investisseurs de bonne foi.

Alors qu'une introduction en bourse classique prend au moins cinq mois, qu'elle implique des coûts élevés et des formalités bureaucratiques considérables, qu'elle doit se conformer à des réglementations strictes et qu'elle nécessite les services d'au moins une banque intermédiaire, la procédure d'ICO est au contraire simple, rapide et peu coûteuse. En Suisse surtout, où le capital-risque n'est pas particulièrement abondant, les ICO ont donné une forte impulsion aux start-ups du secteur fintech. Le fait que la Suisse soit devenue l'une des principales plaques tournantes pour les ICO est principalement dû à un cadre juridique et fiscal favorable, à une scène fintech active et à un remarquable réservoir de talents dans le domaine de la recherche universitaire. Afin de contrer le risque d'abus inhérent à la nature spéculative des ICO, la FINMA a publié un guide destiné à apporter des clarifications et à protéger l'intégrité de la place financière sans porter atteinte au potentiel d'innovation des ICO virtuelles.

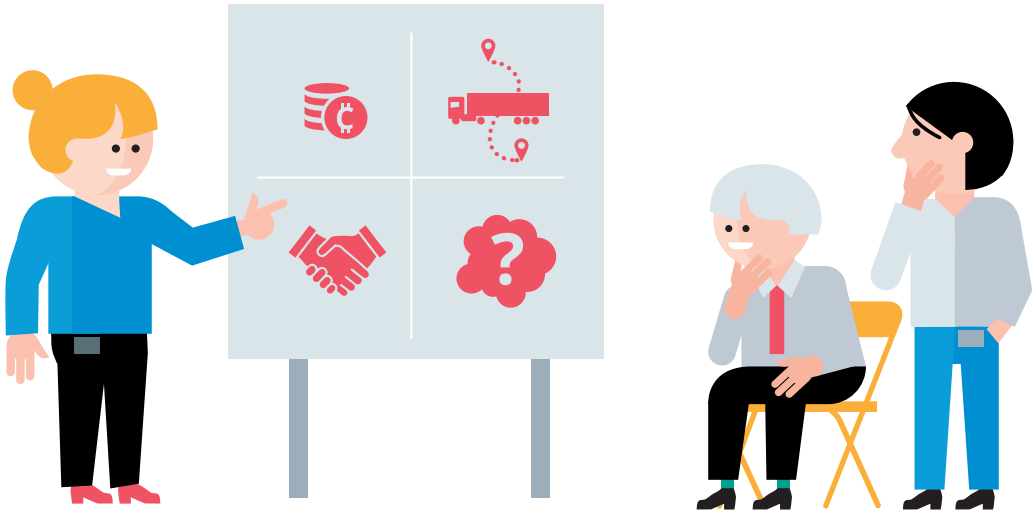
Systèmes de paiement privés (private payment systems) – achats dans un camp de réfugiés

Dans le camp de réfugiés d'Azraq, dans le désert jordanien, un projet de blockchain très remarqué est en cours. Le Programme alimentaire mondial des Nations unies (PAM) y utilise la technologie blockchain pour distribuer de la nourriture à près de 10 000 réfugiés syriens. Le PAM ne distribue plus directement de rations alimentaires depuis une dizaine d'années. À la place, les réfugiés reçoivent de l'argent ou des cartes prépayées afin de pouvoir faire leurs achats eux-mêmes. Ceci leur redonne de la dignité et une forme d'autodétermination et, fait intéressant, les conduit également à avoir une alimentation plus équilibrée. En outre, ces transferts en espèces (cash based transfers) stimulent l'économie locale et permettent de réduire les frais de logistique. Mais ces bons alimentaires peuvent être perdus, volés, accumulés ou encore revendus avec profit. Depuis mai 2017, le supermarché du camp d'Azraq utilise une procédure basée sur une blockchain qui rend le processus plus sûr, plus efficace et pour ainsi dire inviolable. Toute personne qui veut faire des achats s'identifie par un scanner de l'iris. Les données sont comparées avec la base de données du PAM dans laquelle toutes les informations sur le compte, l'identité et l'historique des achats de chaque réfugié sont stockés en toute sécurité sous forme d'ensembles de données cryptées dans la blockchain. La fonction d'intermédiaire de la banque n'est plus nécessaire, et c'est le PAM qui prend sa place en tant qu'autorité centrale, seule responsable du traitement des paiements et de la tenue des comptes. Ceci rend l'ensemble du processus plus efficace et moins coûteux, car il n'y a pas de frais.

À Azraq, il s'agit d'un réseau de blockchain privée rudimentaire avec un seul nœud. La technologie de la blockchain sert ici principalement à stocker des données sensibles de manière infalsifiable. Mais il est possible d'étendre ce projet à succès en le décentralisant et d'exploiter ainsi tout le potentiel de la blockchain : en effet, elle pourrait être utilisée pour traiter de manière transparente les achats et les dépenses des différents camps et peut-être même les services d'autres organisations d'aide dans un système unique, géré de manière décentralisée – rendant toute utilisation abusive des dons impossible, de même que leur disparition dans les poches d'intermédiaires corrompus ou le détournement des fonds d'aide.

Preuve d'origine – de la mer à l'assiette

Grâce à la blockchain, les itinéraires de livraison des biens de consommation ou des denrées alimentaires peuvent également être mieux retracés dans des chaînes d'approvisionnement complexes. La start-up britannique Provenance, par exemple, utilise la blockchain Ethereum pour documenter la provenance du thon pêché de manière équitable en Indonésie. Cela commence par le pêcheur local inscrit dans le système qui enregistre le poids et la qualité de sa prise par SMS. Les critères auxquels le poisson doit répondre pour être considéré comme durable ont été clairement définis au préalable par un organisme de certification indépendant et sont également stockés dans la blockchain. Toutes ces informations sont utilisées pour créer un jeton qui identifie clairement la prise. Cette « empreinte digitale numérique » qui accompagne le poisson à chaque étape, du débarcadère à l'usine et du grossiste au détaillant, est enregistrée et mise à jour à chaque fois, puis transmise au maillon suivant de la chaîne d'approvisionnement. Ainsi, le client final est en mesure de scanner un code QR, de retracer les informations stockées et donc de savoir exactement



ce qui se trouve dans son assiette. La gestion de la chaîne d'approvisionnement pourrait encore être perfectionnée en combinant les contrats intelligents et l'Internet des objets à la blockchain : des capteurs pourraient alors par exemple contrôler que la température pendant le transport se situe dans la plage convenue ou que les marchandises transportées n'ont pas été manipulées et, si nécessaire, déclencher automatiquement une action définie au préalable. Ceci permettrait de garantir la qualité des produits.

La surveillance et la sécurisation des chaînes d'approvisionnement sont également possibles sans la blockchain, mais les solutions qui se basent sur cette technologie optimisent la traçabilité des marchandises et le bon déroulement des processus. Là non plus, les erreurs ne sont pas exclues : dans le cas du thon, par exemple, l'organisme chargé de contrôler si les pêcheurs respectent effectivement les critères de durabilité pourrait faire un mauvais travail. La confiance dans les garants du système est donc toujours présupposée ; cela signifie que la blockchain n'est pas non plus un système totalement « sans confiance », c'est-à-dire un système dans lequel la confiance dans les intermédiaires serait totalement remplacée par un réseau décentralisé, public et transparent.

Gestion intelligente de l'énergie – du soleil sur les toits de Brooklyn

Les exemples ci-dessus montrent que c'est surtout lorsque la blockchain comble un vide que ses points forts se révèlent utiles. En d'autres termes, lorsque la confiance qui est à la base de tout transfert de services n'est pas donnée ou est difficile à établir, que ce soit parce qu'il manque une autorité centrale crédible ou parce qu'il y a trop d'instances intermédiaires susceptibles de faire des erreurs. Qu'il s'agisse d'un registre public, des achats dans le camp de réfugiés ou de l'itinéraire de livraison précisément documenté du thon pêché de manière équitable : dans tous ces cas, la blockchain est plutôt un complément aux processus analogiques ou numériques existants. Souvent, ce n'est que lorsqu'elle se limite à un contexte local qu'elle réussit à convaincre. Les toits de Brooklyn en sont le parfait exemple.

Sur une rangée de maisons « Brownstones » dans le quartier de Park Slope à Brooklyn, New York, un groupe de voisins s'est réuni pour former un micro-réseau électrique décentralisé. Ils produisent de l'énergie solaire pour leur propre consommation, mais voudraient aussi pouvoir alimenter le réseau avec leur surplus d'énergie au prix le plus juste possible et déterminer le prix qu'ils sont prêts à payer s'ils ont eux-mêmes besoin de l'électricité de leurs voisins. Cela peut être réalisé avec l'aide du micro-réseau de Brooklyn Microgrid, une plateforme de blockchain privée associée à des contrats intelligents, qui règle la distribution d'électricité en fonction de l'offre et de la demande. Les prix sont établis au moyen de contrats intelligents dans le cadre d'enchères automatiques sur la base du prix maximum qu'un consommateur connecté au micro-réseau est prêt à payer et du prix minimum auquel un producteur d'électricité est prêt à vendre. La plateforme comprend des systèmes de surveillance et de contrôle, des convertisseurs, des compteurs intelligents et le stockage d'énergie sous forme de batteries lithium-ion. Dans ce réseau, l'électricité est donc échangée et facturée directement entre les producteurs et les clients finaux, et il n'est pas nécessaire de recourir à un fournisseur d'énergie intermédiaire. Le micro-réseau de Brooklyn Microgrid n'est toutefois pas complètement déconnecté du réseau électrique. Si nécessaire, les habitants peuvent continuer à se procurer de l'électricité sur le réseau public.

Pour pouvoir réaliser de tels projets en Suisse en conformité avec la loi et, par exemple, approvisionner des villes entières en énergie via une plateforme peer-to-peer publique et décentralisée sans que le fournisseur d'énergie ne joue un rôle d'intermédiaire, il faudrait d'abord démanteler les structures du marché actuel de l'électricité. Avec les réglementations actuellement en vigueur dans le secteur de l'énergie, cela n'est pas possible : en Suisse, où le marché de l'électricité n'est toujours pas totalement ouvert, les petits consommateurs ne sont pas encore autorisés à participer au marché. En outre, les coûts d'utilisation du réseau sont soumis à une réglementation stricte et ne peuvent pas être réduits si l'électricité provient du voisinage.

À la recherche de l'application tueuse (killer app)

La révolution n'a pas encore eu lieu : on attend toujours l'application qui permettra à la blockchain de percer. La plupart de ses applications ont encore des alternatives qui fonctionnent bien. Et certaines applications innovantes qui s'appuient sur la blockchain seraient tout aussi concluantes sans elle. Néanmoins, ce n'est pas tant la technologie elle-même qui est en cause, mais plutôt le fait que la blockchain, dans sa forme la plus pure de base de données décentralisée, publique, totalement transparente et fiable, sort du cadre juridique et réglementaire actuel – remettant ainsi en question les structures économiques existantes et le rôle de toute une série d'institutions privées et publiques.

La blockchain comme catalyseur

L'utilisation de la blockchain est certes encore marginale mais constitue un phénomène social qui doit être pris au sérieux. Techniquement très complexe et difficile à appréhender par le grand public, elle est devenue une sorte d'écran sur lequel divers acteurs aux motivations différentes s'empressent de projeter leurs idées, notamment dans le domaine des cryptomonnaies. Les livres blancs rédigés pour le lancement des ICO dans un langage technique souvent impénétrable en sont un exemple éloquent. Ils relèvent souvent plus du marketing que d'une communication solide à l'intention des investisseurs potentiels – visant plutôt à masquer la valeur réelle d'utilisation finale du produit lancé et à se défausser d'emblée de leur responsabilité en cas de problèmes techniques.

Confiance, contrôle et responsabilité

Conçue dès le départ comme une alternative libertaire à un monde dans lequel les États-nations sont les instances dirigeantes centrales, la blockchain ne fait pas que dépasser le cadre réglementaire et juridique admis dans de nombreux domaines, mais remet également en question toute une série de valeurs sociales et politiques. Ses partisans rêvent souvent d'abolir les structures de l'État et de l'économie de marché dans l'espoir de pouvoir réorganiser le monde de manière plus efficace et plus équitable sur la base de blockchains et de systèmes décentralisés.

La blockchain remplace ainsi la confiance dans une instance de contrôle, garante de toutes les procédures, par la confiance dans un système cryptographique complexe et dans un mécanisme de vérification partagé par tous les acteurs. La probabilité que des erreurs se produisent dans le système est considérée comme négligeable. Si cela devait néanmoins arriver, aucun organisme n'assumerait la responsabilité du dysfonctionnement du système.

Transparence contre sphère privée

La transparence totale est la grande force de la blockchain. Par exemple, lorsqu'il s'agit d'établir une documentation sans faille des chaînes d'approvisionnement afin d'améliorer la sécurité alimentaire. Toutefois, le prix à payer pour cette transparence est une protection lacunaire de l'identité et de la vie privée des utilisateurs. Quiconque est en possession de la clé publique d'un utilisateur peut suivre toutes ses transactions. Et en associant certains schémas de comportement à d'autres ensembles de données, chacun peut être en mesure de découvrir qui se cache derrière un pseudonyme. Comme la blockchain est conçue pour stocker des données de manière indélébile et les protéger de toute manipulation, elle ne connaît pas non plus le droit à l'oubli.

Dompter le tigre – mais tous ensemble

Le fait que la blockchain fonctionne sans faire appel à des tiers de confiance remet en question toutes les institutions qui ont joué ce rôle d'intermédiaire jusqu'à présent et dont l'importance est désormais contestée. Les cryptomonnaies sont particulièrement visées par les régulateurs du monde entier et déjà interdites par certains pays. D'autres pays misent sur les « bacs à sable réglementaires » (regulatory sandbox) pour canaliser les cryptomonnaies sans exercer une trop grande pression ni mettre en danger l'innovation. Pour sa part, le World Wide Web Consortium s'efforce d'édicter des normes internationales pour clarifier le cadre d'utilisation des applications de la blockchain.

Mais pour tenter d'apprivoiser la blockchain, il n'y a pas que la réglementation et la normalisation. Depuis longtemps, les grands acteurs industriels et financiers ont commencé à adapter la technologie qui menace leur modèle commercial traditionnel à leurs propres fins et objectifs. C'est ainsi que les blockchains privées avec restrictions d'admission ont vu le jour – et ont été reprises par les administrations publiques depuis. Certains pays envisagent même de lancer une cryptomonnaie nationale.

Il est important que ces tentatives de normalisation ne soient pas dominées par les intérêts, désirs et craintes d'acteurs qui n'ont aucune légitimité démocratique à cet égard. La manière de concevoir l'utilisation d'une technologie hautement innovante qui soulève autant de questions doit être traitée dans le cadre d'un vaste débat, loin de tout battage médiatique, avec circonspection et dans l'intérêt commun. C'est l'objet du rapport en deux parties que TA-SWISS présente aujourd'hui.

Groupe d'accompagnement

- Dr. Olivier Glassey, président du groupe d'accompagnement et membre du comité directeur de TA-SWISS, Université de Lausanne
- Raphael Bucher, Office fédéral de l'environnement (OFEV)
- Prof. Christian Cachin, Université de Berne
- Hannes Gassert, crstl
- Anja Wyden Guelpa, civiclab
- Dr. Uwe Heck, Unité de pilotage informatique de la Confédération (UPIC)
- Luzius Meisser, meissereconomics
- Marine Pasquier-Beaud, Office fédéral de l'énergie (OFEN)
- Martin Rindlisbacher, UBS
- Dr. Fabian Schnell, Avenir Suisse
- Antoine Verdon, Swiss Legal Tech Association

Gestion du projet chez TA-SWISS

- Dr. rer. soc. Elisabeth Ehrensperger, directrice
- Dr. Catherine Pugin, responsable de projet

Impressum

Confiance programmée :
Chances et risques de la technologie blockchain
Synthèse de l'étude «Blockchain : Capabilities, Economic Viability, and the Socio-Technical Environment»
TA-SWISS, Berne 2020
TA 73A/2020

Rédaction : Christine D'Anna-Huber, Wissenschaft im Text, Paradiso
Traduction : Pro-Verbial, Zürich
Production : Fabian Schluep, TA-SWISS, Berne
Mise en page et illustrations : Hannes Saxer, Berne
Impression : Jordi AG – Das Medienhaus, Belp

TA-SWISS – Fondation pour l'évaluation des choix technologiques

Souvent susceptibles d'avoir une influence décisive sur la qualité de vie des gens, les nouvelles technologies peuvent en même temps comporter des risques nouveaux, qu'il est parfois difficile de percevoir d'emblée. La Fondation pour l'évaluation des choix technologiques TA-SWISS s'intéresse aux avantages et aux risques potentiels des nouvelles technologies qui se développent dans les domaines « biotechnologie et médecine », « société de l'information » et « mobilité / énergie / climat ». Ses études s'adressent tant aux décideurs du monde politique et économique qu'à l'opinion publique. TA-SWISS s'attache, en outre, à favoriser par des méthodes participatives, l'échange d'informations et d'opinions entre les spécialistes du monde scientifique, économique et politique et la population. TA-SWISS se doit, dans tous ses projets sur les avantages et les risques potentiels des nouvelles technologies, de fournir des informations aussi factuelles, indépendantes et étayées que possible. Elle y parvient en mettant chaque fois sur pied un groupe d'accompagnement composé d'experts choisis de manière à ce que leurs compétences respectives couvrent ensemble la plupart des aspects du sujet à traiter.

La fondation TA-SWISS est un centre de compétence des Académies suisses des sciences.

TA-SWISS
Fondation pour l'évaluation
des choix technologiques
Brunngasse 36
CH-3011 Berne
info@ta-swiss.ch
www.ta-swiss.ch

membre des
académies suisses
des sciences