Plus que de l’argent : L’essentiel des bitcoins, des chaînes de blocs et des contrats intelligents

2015

Préparé par : Foresight Gist
Préparé pour la Division de la recherche et la statistique, Ministère de la Justice

Rédigé par Dennis D. Draeger

ISBN 978-0-660-30124-2
Nº de cat. J4-91/2019F-PDF

Table des matières

Préface

En quoi consiste un rapport sur l'essentiel?

Les rapports sur l'essentiel fournissent un aperçu de l'état actuel et futur de chaque sujet et sont destinés à aider les lecteurs à évaluer rapidement et facilement l'avenir d'une question. Chaque rapport sur l'essentiel de 5 à 10 pages comprend une présentation du sujet, une revue de la littérature utilisant nos prévisions extraites automatiquement et notre propre méthode d'analyse. Les rapports sur l'essentiel mettent rapidement et facilement tous les membres de l'équipe sur la même longueur d'onde de sorte que les réunions puissent se dérouler de manière plus efficace et plus approfondie. Les rapports sur l'essentiel deviennent alors un tremplin permettant aux organisations d'élaborer leurs propres analyses et stratégies.

Méthodologie

Le système de Shaping Tomorrow est en mesure d'ajouter automatiquement des sources à sa base de données en fonction des sources et des termes de recherche clés précisés par les utilisateurs de Shaping Tomorrow. Il extrait ensuite automatiquement toute prévision contenue dans ces sources. Lorsque les utilisateurs cherchent ces prévisions, le système peut faire un résumé de celles-ci pour simplifier leur recherche. Shaping Tomorrow a extrait plus de 105 000 prévisions (des énoncés pertinents pour l'avenir en une phrase) de ses quelque 125 000 sources (*insights*) et plus. Shaping Tomorrow offre aux clients le service de recherche de ces prévisions à leur convenance, ce qui leur donne une plus grande souplesse pour l'élaboration de leurs stratégies. Les prévisions utilisées pour le présent aperçu ont été résumées en vue de tracer l'avenir des cryptomonnaies, des chaînes de blocs et des contrats intelligents. Elles ont ensuite été reformulées et éditées pour faciliter la compréhension du lecteur. Une introduction a ensuite été ajoutée pour clarifier les termes, et pour expliquer les changements que subit le marché actuel et en préciser les répercussions. Un bref scénario de référence est également présenté en vue d'ajouter une perspective sur l'évolution possible de la technologie à long terme. Le rapport se termine par des questions stratégiques, également extraites automatiquement par Shaping Tomorrow, pour donner un aperçu des questions qui font déjà l'objet de discussions en ligne.

Introduction

Ses partisans affirment que le bitcoin décentralisera le pouvoir des banques et d'autres institutions, tout en le distribuant à l'ensemble des communautés. S'il tient ses promesses, le bitcoin ne sera que le début. Les technologies qui sous-tendent le bitcoin, soit la chaîne de blocs (également connue sous le nom de registre distribué) et les contrats intelligents, sont prêtes à aller au-delà de l'argent pour passer à d'autres applications dans le monde réel. Ces technologies pourraient un jour amener l'automatisation à gravir les échelons de l'entreprise jusqu'à la haute direction, et rendre même les PDG superflus, et atteindre les organisations publiques dans un avenir lointain.

À bien des égards, ces technologies sont semblables à Internet au début des années 1990. Elles sont trop compliquées pour être comprises par les consommateurs moyens, mais les développeurs et les investisseurs les inondent de ressources. Les consommateurs moyens ne comprennent pas comment le bitcoin ou toute autre monnaie virtuelle peut réussir en l'absence de représentation physique de la valeur de la monnaie, mais les banques ont traité des opérations autres qu'en espèces d'une valeur de 410 billions de dollars (plus de cinq fois le PIB mondial) en 2013. L'année suivante, en 2014, les banques ont tiré 1,1 billion de dollars de revenus de ce genre d'opérations.

Les sommes d'argent perdues chaque année à cause de la fraude bancaire sont plus préoccupantes. En 2013, à elles seules, les opérations sans carte ont fait perdre 9 milliards de dollars en raison des cas de piratage en ligne, de fraude téléphonique ou d'escroquerie par correspondance. La somme perdue devrait atteindre 19 milliards de dollars d'ici 2018. Selon de nombreuses banques (62 % des banques interrogées par Bank Info Security en 2014), les cas de fraude passent souvent inaperçus jusqu'à ce que leurs clients les en informent.

Les partisans de la cryptomonnaie, de la chaîne de blocs et des contrats intelligents promettent que ces technologies offriront des services plus sûrs, plus efficaces et moins coûteux aux fins des opérations financières. Si ces technologies permettent de réduire la fraude bancaire, peut-être pourraient-elles éventuellement empêcher la fraude électorale, simplifier la gestion des dossiers médicaux, accroître l'efficacité du réseau électrique et brasser bien autre chose que de l'argent.

Clarification des termes

Qu'est-ce qu'un bitcoin et une cryptomonnaie?

Le bitcoin gagne en popularité depuis sa diffusion en tant que logiciel libre en 2009. À ce jour, il est l'exemple le plus réussi de monnaie numérique (monnaie virtuelle pouvant servir à acheter des biens matériels comme des biens immobiliers) et il constitue la toute première cryptomonnaie (monnaie dont la création et le transfert reposent sur le chiffrement au lieu des processus des banques centrales). Cependant, le bitcoin n'est pas la seule cryptomonnaie, et plusieurs communautés similaires font maintenant leur apparition.

À l'heure actuelle, aucune cryptomonnaie n'est soutenue par une institution centralisée. Les cryptomonnaies sont générées et régies électroniquement à l'aide d'algorithmes qui résolvent des équations mathématiques. Elles sont contrôlées par une communauté distribuée à laquelle n'importe qui peut se joindre, et sont produites électroniquement par des particuliers et des entreprises dans le monde entier. Les systèmes informatiques nécessaires à la création et à la validation des cryptomonnaies sont de plus en plus coûteux, même si la valeur de celles-ci fluctue.

Qu'est-ce qu'une chaîne de blocs?

Une chaîne de blocs est une base de données publique sur les opérations dont la nature rappelle celle d'une feuille de calcul Excel, mais dont la propriété et la surveillance ne relèvent d'aucune personne ni organisation. La propriété est plutôt répartie entre les membres décentralisés d'une communauté disparate (bitcoin ou autre).

La chaîne de blocs du bitcoin est anonyme en ce qui concerne les personnes du monde réel qui utilisent un compte, mais le compte lui-même est public. Une clé privée est attribuée à l'utilisateur de chaque compte unique pour renforcer la sécurité des mots de passe. L'élément le plus important est la capacité de la chaîne de blocs d'identifier en toute sécurité le personnage en ligne du titulaire du compte qui l'utilise avec la clé privée. Dès qu'une personne du monde réel fait connaître son identité réelle à l'aide d'une carte de crédit, d'une empreinte digitale ou de tout autre identifiant unique, la chaîne de blocs peut identifier en toute sécurité l'utilisateur de la clé. Par contre, la nature anonyme de cette technologie que beaucoup apprécient est alors perdue.

La chaîne de blocs ajoute également un autre niveau de sécurité que bon nombre d'autres technologies en ligne n'ont pas : le consensus et la permanence. La communauté de la chaîne de blocs doit parvenir à un consensus majoritaire sur chaque opération et tout autre changement apporté à la chaîne de blocs. Comme chaque mise à jour de la chaîne de blocs ne peut être supprimée, la chaîne de blocs permet de réaliser des audits avec une confiance accrue.

Qu'est-ce qu'un contrat intelligent?

Un contrat intelligent est un code qui permet un échange une fois les conditions préétablies remplies (si telle chose se produit, alors telle autre chose se produit). Les contrats intelligents sont en grande partie le moteur de ce qu'on appelle l'Internet des objets[1]. C'est ainsi que les lumières d'une maison s'allument et que la climatisation ou le chauffage est optimisé quand la voiture du propriétaire se trouve à moins de 10 km. Toutefois, les contrats intelligents peuvent également déclencher un échange en fonction des données

[1] Interconnexion par Internet de dispositifs informatiques embarqués dans des objets du quotidien, ce qui leur permet d'envoyer et de recevoir des données.

entrées dans une chaîne de blocs pour automatiser des tâches.

La chaîne de blocs permet à la gestion des données du monde réel de fonctionner davantage comme un ordinateur grâce à l'automatisation de tâches fastidieuses, comme le traitement des paiements. Lorsque le total des paiements mensuels d'un emprunteur équivaut au total de l'hypothèque, l'emprunteur est alors automatiquement inscrit comme le propriétaire à part entière de la maison. Les contrats intelligents peuvent automatiser les processus d'entiercement. Si un pari est fait, l'argent est alors détenu par un compte tiers auquel le contrat intelligent accède pour payer le gagnant. C'est donc dire que les instruments dérivés et l'assurance se prêtent très bien à l'automatisation à l'aide de contrats intelligents.

Qu'est-ce qu'une organisation autonome décentralisée (OAD)?

Puisque le modèle distribué qu'offre la chaîne de blocs se combine avec l'automatisation des contrats intelligents et d'autres technologies, il est possible pour les organisations d'automatiser leurs activités et de répartir leur gouvernance.

Même en cas de dissolution de l'entreprise centralisée, le service resterait et fonctionnerait normalement puisque tous les systèmes et processus sont distribués et autonomes. La tâche de gérer un service de plusieurs millions de dollars serait donc plus facile pour un propriétaire unique.

En quoi consiste le changement?

Les institutions financières investissent dans la chaîne de blocs pour rendre leur travail plus facile et plus sûr. R3 CEV[2] est une société spécialement créée pour aider les banques à mettre la technologie de la chaîne de blocs à l'essai. Elle dirige un consortium de 42 banques qui veulent savoir de quelle façon la technologie de la chaîne de blocs pourrait changer leur industrie. Selon R3, le potentiel de la chaîne de blocs peut se comparer au vent de changement qu'Internet a insufflé aux industries de la musique et des médias.

Le groupe Z/Yen[3] mène des recherches sur la technologie de la chaîne de blocs et ses possibles répercussions sur l'industrie de l'assurance. Il soulève un certain nombre de préoccupations, qui concernent surtout la réglementation gouvernementale ainsi que la décentralisation et le caractère évolutif du minage. Toutefois, il croit que les aspects positifs l'emportent sur les aspects négatifs, et affirme que la technologie de la chaîne de blocs permettrait d'améliorer à la fois l'intégrité et la sécurité, qui sont essentielles pour les services financiers.

Slock.it (une entreprise allemande de chaîne de blocs) tente d'être la première OAD du monde réel. Le service de Slock.it consiste à connecter l'Internet des objets à l'économie du partage à l'aide de la chaîne de blocs et des contrats intelligents. Dès qu'un utilisateur paie pour louer une bicyclette, une maison ou tout autre bien, le verrou physique du bien est automatiquement déverrouillé, et le bien est prêt à l'emploi sans intermédiaire, comme Uber ou Airbnb. Les serrures à pêne dormant, les cadenas et les portières de voiture avant peuvent tous être connectés à Internet et contrôlés par des contrats intelligents.

Cependant, la chaîne de blocs pourrait s'avérer utile pour bien d'autres choses que de simples opérations financières. Ubitquity (plateforme de tenue de documents immobiliers sécurisée par chaîne de blocs prêts à l'emploi pour les entreprises) a mis au point une plateforme de chaîne de blocs spécialement conçue pour l'industrie immobilière. La société affirme que la nouvelle plateforme améliorera le processus de transfert de titres en le rendant plus rapide, plus précis et plus transparent en vue de prévenir la fraude. Elle dit en outre que sa plateforme améliorera le processus de diligence raisonnable pour l'industrie.

Les gouvernements explorent également les avantages de la chaîne de blocs et des contrats intelligents. Le Honduras a longtemps dû faire face à la fraude des bureaucrates exploitant les failles du système pour

[2] R3 CEV ou R3 est une entreprise de technologie de bases de données distribuées. Elle dirige un consortium de plus de 200 entreprises en recherche et développement qui examine l'utilisation du registre distribué dans le système financier et d'autres domaines commerciaux.

[3] Z/Yen est un groupe de réflexion commercial, ainsi qu'une société de conseil et de capital-risque.

acquérir des propriétés en bord de mer, mais ce pays d'Amérique centrale songe à utiliser une chaîne de blocs pour les transactions immobilières similaire à Ubitquity. Le gouvernement britannique envisage de mettre en place une chaîne de blocs afin d'améliorer la transparence et l'exactitude de la tenue de ses dossiers. L'île de Man est à mener une expérience technique, le tout premier organisme gouvernemental au monde à tenter ce genre d'essai. La Chine s'est associée à Factom pour utiliser la chaîne de blocs et les contrats intelligents dans le cadre de son initiative de villes intelligentes.

Poussant l'expérience plus loin, la micronation autoproclamée du Liberland, dans les Balkans, est en pourparlers avec Pax, une « nation virtuelle » reposant sur une chaîne de blocs, composée de citoyens qui se portent volontaires pour faire respecter ses lois. Pax est un système juridique de pair à pair qui, de l'avis de certains, changera la façon dont la société conçoit le gouvernement et qui pourrait décentraliser et distribuer de nombreux services gouvernementaux dans le monde.

De nombreuses organisations s'efforcent d'utiliser la technologie de la chaîne de blocs pour rendre le vote plus sûr et anonyme. En 2014, un grand parti politique danois, l'Alliance libérale, a utilisé la technologie de la chaîne de blocs pour son propre vote interne. Puisque la chaîne de blocs repose de toute façon sur le consensus, il s'agit d'une plateforme de vote en soi et pourrait un jour être modifiée par des entités gouvernementales à cette fin.

Répercussions

Le bitcoin et d'autres cryptomonnaies représentent un idéal libertaire qui pourrait déstabiliser l'infrastructure actuelle des banques et autres puissantes institutions. La chaîne de blocs offre des architectures distribuées, sécurisées, fiables et hautement évolutives avec lesquelles les technologies conventionnelles ne peuvent rivaliser.

Bien que le secteur bancaire anticipe les perturbations en investissant dans cette nouvelle technologie, bon nombre de ses modèles d'affaires et de ses sources de revenus seront touchés, surtout par la concurrence accrue de l'industrie technologique. Les occasions sont grandes pour le secteur financier, mais les risques sont également importants, en particulier pour les petits acteurs du secteur.

Comme les ordinateurs sont maintenant en mesure de traiter les paiements, d'autres échanges contractuels pourraient s'effectuer automatiquement par l'entremise de contrats intelligents. À l'heure actuelle, si un magasin en ligne reçoit un paiement, le produit est livré, mais les humains prennent toujours part au processus. Les chaînes de blocs et les contrats intelligents pourraient entièrement automatiser le traitement, d'autant plus que les systèmes d'automatisation logistique s'améliorent grâce aux robots qui voient à l'emballage des produits et à leur expédition, laquelle se fera éventuellement à l'aide d'un véhicule sans conducteur.

Le secteur public rêve depuis des décennies d'instaurer le vote numérique, mais la chaîne de blocs peut détenir la clé de la réussite à ce chapitre si on arrive à assurer l'anonymat et à vérifier que seules des personnes votent (pour éviter le vote double). On peut y arriver de plusieurs façons en utilisant des méthodes concrètes plutôt que numériques, par exemple en fournissant à chaque citoyen une clé chiffrée à conserver en guise de numéro d'identification unique (par exemple, numéro de carte de crédit, numéro d'assurance sociale, numéro d'inscription sur les listes électorales, etc.).

Pour de nombreux partisans du vote numérique, le but ultime est une « démocratie liquide ». Ils veulent que les citoyens puissent voter sur tout ce qu'ils souhaitent ou leur permettre de faire voter à leur place quelqu'un qu'ils estiment mieux qualifié qu'eux.

Le secteur public pourrait également se servir de la chaîne de blocs pour automatiser l'allocation d'une petite somme d'argent en fonction de paramètres très précis. Ainsi, si un tremblement de terre d'une certaine magnitude était détecté dans une région donnée, l'organisme de secours d'urgence pourrait automatiquement allouer une petite somme d'argent à certaines organisations locales. Quel que soit le montant, ces fonds pourraient fournir une aide immédiate à la collectivité au moment où elle en a le plus besoin, pendant que l'organisme gouvernemental examine la façon d'intervenir le plus efficacement.

Décalage culturel

Toute nouvelle technologie connaît, à ses débuts, une période de dichotomie pendant laquelle ses partisans ont une vision idéaliste de l'avenir, tandis que ses détracteurs minimisent ses capacités ou soulignent ses aspects négatifs. Le bitcoin a déjà suscité ces deux réactions, qui commencent à s'estomper. Il y a quelques années à peine, la presse parlait surtout des utilisations du bitcoin sur le marché noir – les bitcoins servaient à payer des armes à feu, de la drogue, etc. – parce qu'il est difficile d'identifier avec certitude l'acheteur ou le vendeur dans les opérations illégales. Cette association avec le marché noir continue d'être préoccupante, mais elle ne l'est pas moins pour l'argent comptant que pour les bitcoins.

À peu près à la même époque, les économistes n'ont pas tardé à signaler les diverses faiblesses techniques du système bitcoin, et ont prédit que le bitcoin ne deviendrait jamais une monnaie. Ces économistes ont complètement passé à côté de l'utilité du bitcoin, qui n'est pas vraiment de se distinguer des autres monnaies, mais plutôt de financer la recherche et le développement d'innovations qui pourraient stimuler l'économie. Le bitcoin a beaucoup à prouver en tant que monnaie d'échange, mais il a clairement démontré qu'il a sa place sur le marché, malgré quelques problèmes techniques, que sa communauté en ligne s'emploie à résoudre.

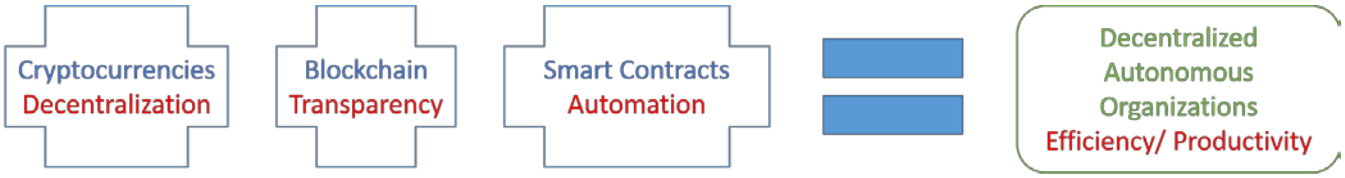

Figure 1. Les avantages fondamentaux de la chaîne de blocs et de ses technologies connexes, proposés par les techno-optimistes

Crytocurrencies Decentralization	Cryptomonnaies - Décentralisation
Blockchain Transparency	Chaîne de blocs - Transparence
Smart Contracts Automation	Contrats intelligents - Automatisation
Decentralized Autonomous Organizations Efficiency / Productivity	Organisations autonomes décentralisées – Efficacité et productivité

Pour l'instant, les entreprises et les médias grand public s'intéressent davantage aux possibilités de la chaîne de blocs et des contrats intelligents qu'à l'idée d'une monnaie virtuelle comme le bitcoin. Le scénario le plus probable est que ces technologies seront mises au pas par la réglementation, tout comme Internet l'a été au cours des 25 dernières années. Dans ce cas, la question clé est la suivante : quels paradigmes changeront entre-temps et quels secteurs seront perturbés parce qu'ils peinent à suivre la cadence?

C'est pourquoi les techno-optimistes entrevoient un avenir de décentralisation et de démocratisation endémiques, et prévoient que des entreprises entières deviendront complètement autonomes. Non seulement l'automatisation entraînera la perte d'emplois pour les employés aux échelons inférieurs, mais les OAD mettront aussi en péril les postes des cadres, des gestionnaires et de divers employés du gouvernement. Des services de plusieurs millions de dollars pourraient être exploités par un petit groupe de propriétaires – qui pourraient éventuellement devenir redondants – à l'aide d'une communauté distribuée d'utilisateurs et de développeurs.

Prévisions

Comme la préface le décrit, vous trouverez ci-dessous la liste sommaire des prévisions extraites automatiquement en ce qui concerne les cryptomonnaies, les chaînes de blocs et les contrats intelligents. Chaque liste est numérotée pour en faciliter la consultation, et chaque prévision est reliée par hyperlien à sa source, qui permet d'approfondir la question.

Cryptomonnaies

- D'ici 2027, 10 % du PIB mondial sera stocké sur un réseau de chaînes de blocs.
- De multiples entreprises de bitcoins et de chaînes de blocs réaliseront des opérations de centaines de millions de dollars et vaudront 1 milliard de dollars l'an prochain (2016).
- Plusieurs études indiquent qu'au cours des quatre prochaines années, le marché mondial des transactions numériques atteindra 9,5 milliards de dollars, tandis que les investissements mondiaux dans les technologies de chaînes de blocs atteindront 300 milliards de dollars.
- Les micropaiements devraient atteindre 13 milliards de dollars au cours des trois prochaines années, à mesure que les cryptomonnaies seront mieux acceptées.
- Les technologies de paiement décentralisées pourraient transformer l'« architecture commerciale » des transferts d'argent.
- La chaîne de blocs pourrait éventuellement réduire les coûts des services financiers comme les cartes de crédit, les envois de fonds et les transferts d'argent.
- La technologie bitcoin pourrait être aussi perturbatrice qu'Internet lui-même.
- Un tel système pourrait transformer la façon dont les gens consomment les médias en ligne et permettre aux créateurs de contenu de recevoir directement un paiement à l'utilisation.
- La valeur de la marque dans l'industrie découlera probablement de partenariats avec d'autres acteurs de l'écosystème à mesure que les banques rattraperont les grandes marques comme Google et Apple.
- Le recours à des tiers pour l'infrastructure et les talents non essentiels sera un phénomène courant à mesure que les banques seront de plus en plus connectées par un réseau complexe ou un réseau de fournisseurs et de tiers.
- L'utilisation généralisée de la technologie bitcoin dans le secteur financier pourrait finir par soutirer des dépôts aux banques commerciales et affecter les prêts dans l'économie réelle.
- La technologie de règlement qui sous-tend les monnaies numériques pourrait devenir une forme parallèle de distribution de fonds et d'exécution d'opérations financières avec la banque, pour servir de filet de sécurité.
- La Banque d'Angleterre pourrait devenir la plaque tournante d'une monnaie numérique de type bitcoin qui écarte les banques grand public et réduit les coûts des opérations financières.
- Les banques africaines pourraient vraiment devenir des pionnières dans le développement de nouvelles technologies financières comme la chaîne de blocs et le bitcoin.
- La norme API Open Banking pourrait révolutionner la façon dont les consommateurs gèrent leurs finances.
- Les cryptomonnaies distribuées par un minage concurrentiel ne supposent aucun investissement d'argent ni le risque de perdre un « achat » et n'offrent que peu de possibilités de profit aux développeurs.
- Le fait d'offrir aux commerçants vietnamiens la possibilité de recevoir des paiements par chaîne de blocs atténuera considérablement le manque de confiance et de sécurité entourant les options de paiement traditionnelles, comme les cartes de crédit, PayPal et autres offres

similaires.

- Des centaines de millions d'utilisateurs enverront de l'argent sur Internet aussi facilement qu'ils envoient des textos.

Conséquences juridiques

- Le code sera la nouvelle loi financière.
- Un tribunal américain se penchera sur la question de l'application du cinquième amendement aux clés privées bitcoin dans une affaire qui sera sans aucun doute suivie de près.
- Les échanges de bitcoins devront se conformer à une réglementation plus stricte en matière de lutte contre le blanchiment d'argent.
- Les organismes de réglementation tireront profit d'une piste de vérification améliorée et pourront voir l'activité sur le marché en temps quasi réel.
- Il semble y avoir un risque que les organisations terroristes utilisent des monnaies virtuelles pour dissimuler des opérations financières.
- Les cryptomonnaies décentralisées comme le bitcoin ne correspondent pas vraiment à la définition de « titre » et ne présentent pas les risques généralement visés par la réglementation des valeurs mobilières.
- Le FMI s'inquiète du fait que les monnaies virtuelles comme le bitcoin risquent de faciliter le blanchiment d'argent, le financement du terrorisme, l'évasion fiscale et la fraude.
- L'anonymat des utilisateurs n'est pas garanti, et la conversion des pièces en livres, en dollars ou en euros incitera les systèmes d'échange à appliquer les règlements pertinents en matière d'identité, de blanchiment d'argent et de financement du terrorisme.
- La chaîne de blocs aidera à détecter les blanchisseurs d'argent et les fraudeurs grâce à son registre distribué et à la traçabilité historique des fonds.

Chaîne de blocs

- La chaîne de blocs évoluera : de technologie dont les banques se méfient, elle passera à la technologie « perturbatrice » qui transformera totalement le système bancaire.
- Les économies liées à la chaîne de blocs auraient pu faire grimper le rendement des capitaux propres du secteur des banques d'investissement à 10,4 % en 2015, hors éléments exceptionnels.
- L'intérêt et l'investissement actuels des entreprises financières dans la technologie de la chaîne de blocs en révéleront l'incidence dans 12 à 18 mois seulement.
- Le travail sur les applications de la chaîne de blocs bénéficiera de l'adoption globale plus rapide de la technologie, ce qui exercera bientôt une pression sur les anciennes solutions financières existantes.
- La chaîne de blocs pourrait être un système de transaction universel d'une ampleur jamais imaginée auparavant qui pourrait éventuellement servir à coordonner l'ensemble de l'activité humaine et machine.
- La chaîne de blocs fera aux rapports d'entreprise et aux opérations financières ce qu'Internet a fait aux connaissances.
- Les propriétaires d'entreprise qui ont réellement à cœur de réduire les coûts et d'améliorer les fonctionnalités seront suffisamment imaginatifs pour trouver des façons d'intégrer la technologie de la chaîne de blocs dans leurs chaînes d'approvisionnement, le traitement des paiements et autres processus.

- L'utilisation de la technologie du registre distribué permettra d'améliorer l'efficacité des données ainsi que le traitement et le règlement des opérations.
- Les pratiques exemplaires de la technologie du registre distribué [pour la tenue de dossiers] émergeront certainement et créeront encore plus d'applications du concept.
- La gestion de l'identité des employés de grandes multinationales ou l'accès aux dossiers médicaux des patients pourrait se faire au moyen des chaînes de blocs pour éliminer les redondances et les entrées erronées dans les données et offrir des points d'accès à l'information par couches à des tiers sans compromettre la sécurité des données.
- La chaîne de blocs pourrait être l'innovation sociale et politique la plus importante qu'a connue l'Afrique depuis 100 ans.
- Selon M. McKinsey, la chaîne de blocs est très prometteuse pour les marchés financiers, mais il estime que les participants au marché, les organismes de réglementation et les entreprises technologiques devront coopérer pour qu'elle fonctionne.

Contrats intelligents

- Un testament numérique peut automatiquement déclencher l'exécution du contrat en faveur d'un bénéficiaire principal.
- Les contrats intelligents très partagés pourraient être reconnus comme des éléments clés de l'infrastructure et être officiellement détenus et gérés par une forme de base logicielle ouverte.
- La technologie derrière la monnaie numérique bitcoin pourrait ouvrir la voie à une ère de « contrats intelligents » et permettre la création d'une base de données cadastrale inviolable.
- Les compagnies d'assurance qui tardent à intégrer les sources de données de l'Internet des objets dans leurs modèles de souscription et de tarification risquent une sélection adverse qui pourrait exercer une pression sur leurs profits.
- On s'attend à ce que les nouvelles options FLEX offrent aux assureurs une méthode de couverture de rechange dans un environnement boursier où la transparence, la détermination des prix et la compensation centralisée sont des facteurs de différenciation intéressants.
- Avec l'automatisation croissante et l'accélération des cycles de compensation et de règlement, les marchés deviendront plus efficaces et la différenciation, difficile à trouver, mais le rôle de l'intuition humaine et des conseils stratégiques deviendra encore plus important pour servir les clients et élaborer des algorithmes.

Organisations autonomes décentralisées (OAD)

- Sur les marchés financiers, une application claire de la technologie de la chaîne de blocs est la négociation algorithmique et les activités postmarché. Les opérations haute fréquence pourraient être effectuées par des agents semi-autonomes ayant la capacité d'agir plus rapidement et de mieux explorer les sources d'information sur les prix, les nouvelles, et les changements de sentiment. De même, des pans complets d'activités postmarché, comme la compensation, qui sont actuellement gérées par des agents humains pourraient être gérées par des agents de la chaîne de blocs.
- Les registres cryptographiques pourraient coordonner les opérations au comptant (cryptomonnaie) et les interactions t+n avec les contrats intelligents et les applications autonomes décentralisées, les organisations autonomes décentralisées et les sociétés autonomes décentralisées.
- Les citoyens pourraient prendre des décisions politiques grâce à des processus numériques transparents et à des interfaces mises en place autour d'une OAD.

- Les citoyens pourraient en fait devenir actionnaires de leur gouvernement local.
- Des agents autonomes, des programmes intelligents et (plus tard) des niveaux accrus d'intelligence artificielle et d'algorithmes d'intelligence artificielle assureront l'autosuffisance des activités et la création d'une valeur au centre, aux limites et au cœur d'une organisation.
- L'idée d'une organisation ou d'une société rigide s'évaporera et laissera place à l'essence même des modèles d'interaction humaine.
- Les marchés créés ou maintenus par des organisations autonomes décentralisées ne permettront pas facilement une intervention gouvernementale. Forcer les développeurs de logiciels à introduire une fonctionnalité particulière dans le code ne fonctionnera que dans la mesure où la base utilisateur accepte réellement de passer au nouveau protocole.

Préoccupations entourant la sécurité (quantique)

La mesure dans laquelle la chaîne de blocs est sécurisée est encore examinée et débattue, mais rien ne peut être sûr à 100 %, surtout lorsqu'il s'agit d'argent. L'une des faiblesses que certains chercheurs prévoient est l'informatique quantique.

- L'informatique quantique pourrait servir au hachage.
- L'informatique quantique créera, pour la cryptomonnaie et la cryptographie en général, des problèmes qui devront être résolus à l'avenir.
- La sécurité des systèmes de cryptographie à courbe elliptique pourrait être compromise par le fait qu'un ordinateur quantique pourrait déduire la clé privée d'une adresse s'il connaît la clé publique.

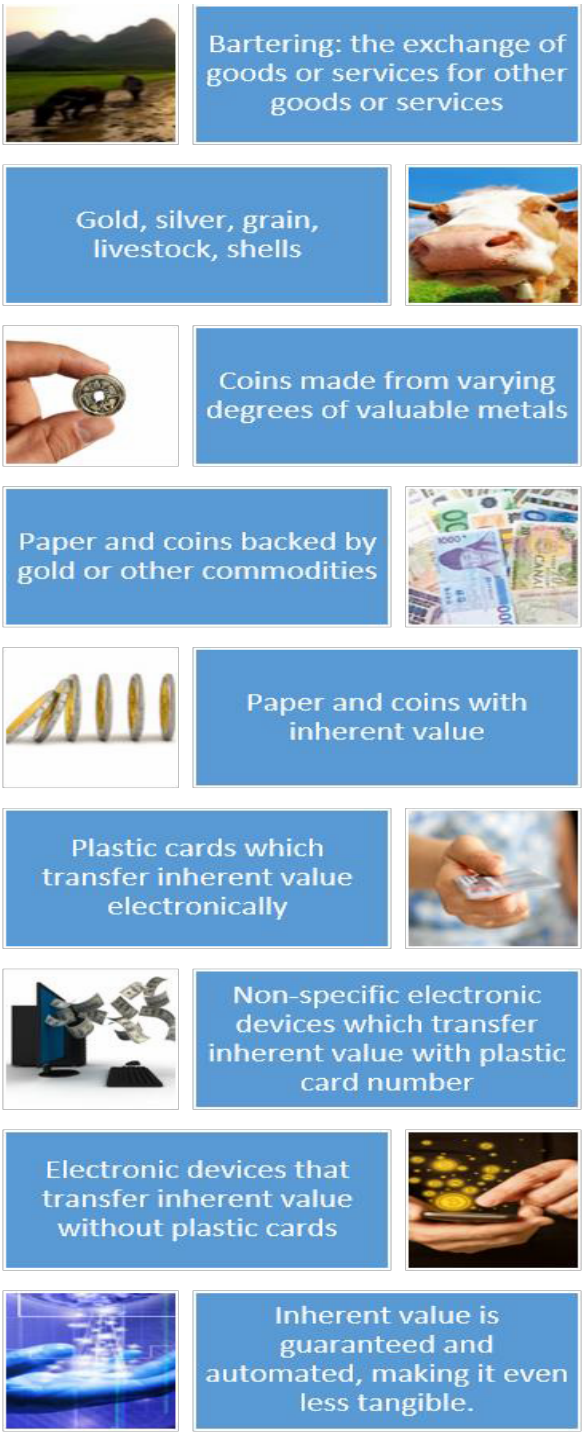

Figure 2. La monnaie fiduciaire n'a pas plus de valeur intrinsèque que la monnaie virtuelle, et la valeur de la monnaie fiduciaire est d'autant plus abstraite à l'ère des communications numériques. Internet a distribué l'information au-delà de tout cloisonnement centralisé ou décentralisé, comme les bibliothèques, et la chaîne de blocs et les technologies connexes promettent de faire de même pour la valeur. Qu'il s'agisse de monnaie ou de votes - en tant que monnaie pour le secteur public - ou d'une autre forme de valeur, la chaîne de blocs pourrait rendre cette valeur plus transparente et plus sûre, tout en suscitant une plus grande confiance pour tout système ou processus auquel elle est appliquée.

Bartering: the exchange of goods or services for other goods or services	Troc : échange de biens ou de services contre d'autres biens ou services
Gold, silver, grain, livestock, shells	Or, argent, grains, bétail, coquillages
Coins made from varying degrees of valuable metals	Pièces de monnaie fabriquées de métaux précieux à divers degrés
Paper and coins backed by gold or other commodities	Monnaie en papier et pièces de monnaie soutenues par l'or ou d'autres matières premières
Paper and coins with inherent value	Monnaie en papier et pièces de monnaie ayant une valeur intrinsèque
Plastic cards which transfer inherent value electronically	Cartes en plastique qui transfèrent électroniquement une valeur intrinsèque
Non-specific electronic devices which transfer inherent value with plastic card number	Dispositifs électroniques non spécifiques qui transfèrent une valeur intrinsèque avec numéro de carte en plastique
Electronic devices that transfer inherent value without plastic cards	Dispositifs électroniques qui transfèrent une valeur intrinsèque sans carte en plastique
Inherent value is guaranteed and automated, making it even less tangible	La valeur intrinsèque est garantie et automatisée, ce qui la rend encore moins concrète

Scénario idéal

Le scénario des techno-optimistes pour la chaîne de blocs et les contrats intelligents décrit un avenir où l'argent devient une caractéristique latente de l'interaction humaine plutôt qu'une caractéristique dominante comme c'est le cas aujourd'hui. À mesure que d'autres questions (comme le revenu de base garanti, l'Internet des objets, etc.) arrivent à maturité et convergent, les possibilités d'utilisation des chaînes de blocs et des contrats intelligents s'étendront jusqu'à couvrir presque tous les aspects de la vie numérique.

Le revenu de base garanti a gagné du terrain dans plusieurs pays du monde, surtout grâce à l'évolution de l'automatisation. Si la valeur peut être garantie et automatisée comme le suggère la figure 1, alors l'argent deviendra obsolète, et le monde numérique pourrait reposer davantage sur une sorte de système de troc numérique déterminé plus par l'économie de la réputation que par l'argent. Et à mesure que l'Internet des objets progresse, un système de réputation similaire peut même influer sur les opérations dans le monde réel.

- Si une personne manque de lait, son réfrigérateur peut commander un nouveau litre de lait qui sera livré une fois qu'elle aura répondu à un sondage en ligne.
- Quand les empreintes digitales d'une personne bien nantie sont reconnues à la porte d'un magasin, le prix de toutes les marchandises augmente.
- Si la surveillance publique s'intensifie, un acte d'indulgence pourrait être enregistré par l'appareil photo portable de quelqu'un, et une récompense (billets pour un concert pour lequel la personne a exprimé son intérêt sur Facebook) pourrait être automatiquement attribuée à la personne à partir d'un fonds philanthropique qui n'est plus surveillé par des humains.
- Si le décès d'une personne est enregistré dans un hôpital, des courriels contenant des messages d'amour, des vidéos, des photos, etc., sont envoyés à des êtres chers prédéterminés.

Tous ces scénarios sont tout à fait plausibles aujourd'hui mais, grâce à la chaîne de blocs, le processus pourrait devenir automatisé, normalisé et presque universel. L'argent et d'autres valeurs pourraient se cacher dans l'architecture numérique d'ici 20 ans tout au plus. Alors qu'une monnaie virtuelle continuerait d'exister, l'échange de valeurs de tout ordre deviendrait plus latent qu'il n'est possible aujourd'hui.

Questions stratégiques

Les questions suivantes ont été extraites automatiquement par le système de Shaping Tomorrow de la même manière que les prévisions et, comme les prévisions, chaque question comprend un hyperlien vers sa source. Certaines sources fourniront une réponse à la question, mais d'autres non. Ces questions ne sont que quelques-unes des questions entourant les cryptomonnaies, les chaînes de blocs et les contrats intelligents. Répondez-y du mieux que vous le pouvez pour votre propre organisation avant de cliquer sur les liens pour approfondir votre compréhension.

Cryptomonnaies

- Qu'est-ce qui ferait en sorte que la chaîne de blocs et les cryptomonnaies en général deviennent monnaie courante?
- Quelles nouvelles fonctionnalités la cryptomonnaie devrait-elle offrir pour avoir du succès?
- Qu'arrivera-t-il au bitcoin quand la prochaine grande récession frappera?
- S'agit-il de substituer le bitcoin ou une autre monnaie virtuelle au dollar américain [comme principale monnaie dominante]?
- Pourquoi l'adoption du bitcoin est-elle lente parmi les milliards non bancarisés?
- Comment échanger différentes monnaies ou d'autres instruments financiers entre des chaînes de blocs libellées en différentes monnaies?

Chaîne de blocs

- Comment les constructions et les systèmes créés pour traiter les litiges civils vont-ils s'adapter au bitcoin et à la chaîne de blocs?
- Que se passe-t-il lorsque les nouvelles entreprises de chaîne de blocs cessent de s'inquiéter de la conformité réglementaire et commencent à interagir avec les systèmes de la « vie réelle » existants?
- Les modes de distribution des futurs médias seront-ils également décentralisés sur la chaîne de blocs?
- Comment les États-nations pourraient-ils voter à partir de systèmes de votation fondés sur une chaîne de blocs?
- Comment une chaîne de blocs pourrait-elle perturber ou transformer les activités de vos concurrents, fournisseurs ou clients?
- Quelle est l'ampleur de la menace que la chaîne de blocs pourrait représenter pour les travailleurs humains dont les postes pourraient être automatisés en tant qu'« intermédiaires » superflus?
- D'où de nouvelles sources de risques inattendus pourraient-elles émerger dans un « monde de chaîne de blocs » qui en est encore à ses débuts et qui est si mal compris par tous, sauf par un petit groupe de pionniers et de partisans?

Contrats intelligents

- Comment les organismes de réglementation devraient-ils contrôler un processus automatisé qui se déroule sur de nombreux ordinateurs anonymes?
- Qui est réellement chargé ou responsable de l'exécution des contrats intelligents?
- Ces tonnes de choses intelligentes capables de bavarder libéreront-elles et élèveront-elles

l'humanité ou nous laisseront-elles dépendants d'un appareil et noyés dans sa complexité?
- Comment les entreprises peuvent-elles tirer parti de l'automatisation et des technologies intelligentes pour améliorer la productivité et créer un travail plus significatif et plus mobilisateur où les employés collaborent – et non compétitionnent – avec les machines »?

Organisations autonomes décentralisées

- Puisque les OAD ont pleine souveraineté sur leurs ressources et que celles-ci ne peuvent être saisies, comment peuvent-elles être tenues de payer des dommages-intérêts?
- Si vous avez utilisé le modèle d'OAD, quelles clauses pourriez-vous inclure pour vous protéger contre la possibilité d'une partie indigne de confiance?
- Les OAD doivent-elles essayer de maintenir des soldes dans d'autres monnaies, ou doivent-elles seulement récompenser les comportements en émettant leur propre monnaie interne?

Prochaines étapes

Nous vous recommandons d'élaborer plusieurs scénarios pour explorer les répercussions positives ou négatives de ces technologies sur votre organisation. Vu le rythme du changement au cours des dernières années, il est préférable d'élaborer chaque scénario sur un horizon d'au moins 10 ans, car ces changements peuvent survenir plus tôt que prévu.

Grâce à ces scénarios, vous pouvez ensuite élaborer un plan stratégique plus souple et facile à adapter en fonction de ce que l'avenir apportera.

Autres sources

Voici les sources qui ont été utilisées pour rédiger l'introduction et d'autres parties explicatives de l'aperçu.

- Global Payments 2015: The Interactive Edition
- Global Payments 2014: Capturing the Next Level of Value
- Credit card fraud and ID theft statistics
- 2014 Faces of Fraud Survey: The Impact of Retail Breaches
- Election Fraud in America
- Exhaustive Database of Voter Fraud Cases Turns Up Scant Evidence That It Happens
- U.S. voter turnout trails most developed countries
- Voter Turnout
- There is a 'game changer' technology on Wall Street and people keep confusing it with bitcoin
- What Are Smart Contracts? Cryptocurrency's Killer App
- What is Bitcoin?
- Are Smart Contracts the Future of Blockchain?
- Shift 16: Bitcoin and the Blockchain
- Forget Bitcoin — What Is the Blockchain and Why Should You Care?
- Immutability for Bitcoin and Permissioned Ledgers
- There's a Blockchain for That
- R3 completes trial of five cloud-based emerging blockchain technologies with 40 bank consortium members
- Ubitquity releases highly anticipated blockchain-powered real estate platform
- Blockchain Land Title Project 'Stalls' in Honduras
- Isle of Man Trials First Government-Run Blockchain Project
- UK Government Exploring Use of Blockchain Recordkeeping

- Factom Lands Smart-City Deal with China
- Pax and Liberland: transforming the Balkans
- A Bitcoin Technology Gets Nasdaq Test
- Bitcoin is the Sewer Rat of Currencies
- The Hutchins Center Explains: How blockchain could change the financial system (part 1)
- Hype springs eternal
- Chain of a lifetime: how blockchain technology might transform personal insurance
- How Blockchain Technology Could Revolutionize the $1.1 Trillion Insurance Industry
- Blockchain Technology: The Key to Secure Online Voting
- Five objects in which you'll soon find Blockchain
- Airbnb Co-Founder Sees Possible Integration of Blockchain Tech
- PoS forging algorithms
- Bitcoin's nightmare scenario has come to pass
- Bitcoin's Dark Side Could Get Darker
- Beyond Bitcoin: How the Blockchain Can Power a New Generation of Enterprise Software
- The History of Money and Payments
- A Typical Day in a Blockchain-Enabled World Circa 2030
- Why the blockchain will radically alter our future