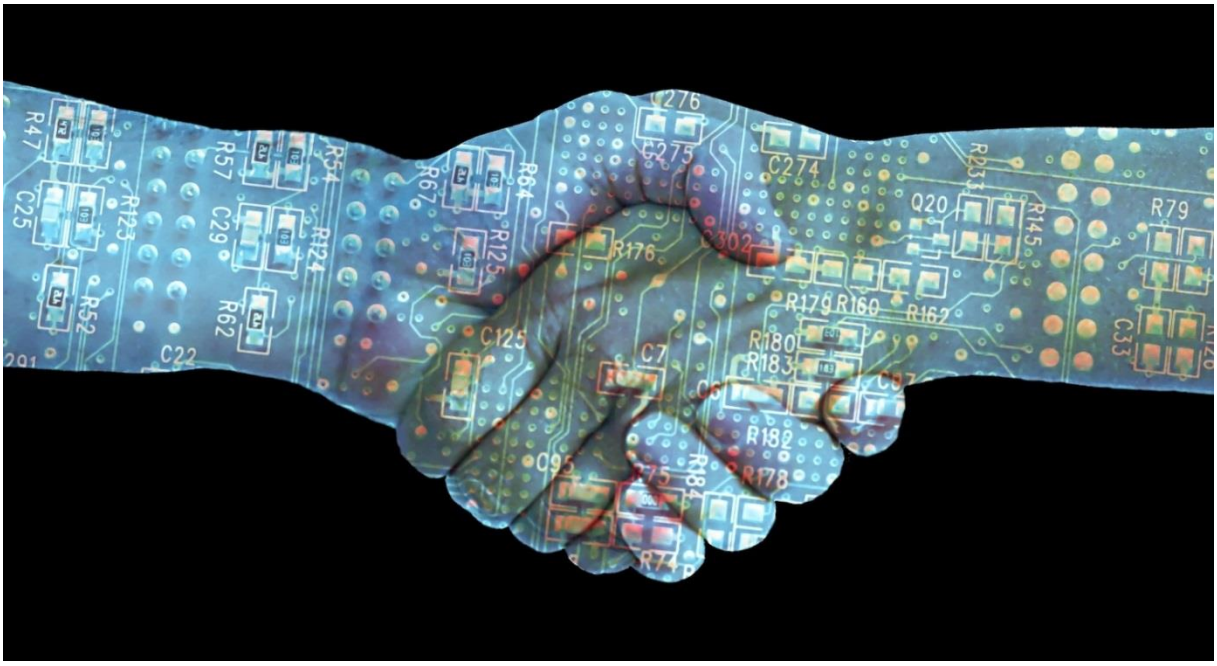
Blockchain : les multiples facettes méconnues d'une révolution qui va bouleverser nos vies

La technologie blockchain va révolutionner beaucoup plus que le seul secteur financier : elle va changer votre vie. Découvrez comment tout cela fonctionne réellement.



Dans ce PDF, nous vous proposons la traduction d'un essai de Dominic Frisby sur les nombreuses applications que nous réserve la technologie blockchain.

Dominic Frisby est un rédacteur financier basé à Londres. Spécialiste des crypto-monnaies, il est l'auteur de *Bitcoin: The Future of Money?* (2014) et *Life After the State* (2013). Il a co-écrit le documentaire *Four Horsemen* (2012).

«

L'impact de l'archivage et de la tenue de registres sur le cours de l'histoire ne doit pas être sous-estimé. Par exemple, le fait d'avoir préservé le judaïsme et le christianisme sous forme écrite leur a permis de survivre à la pléthore des autres religions contemporaines, qui ont été uniquement conservées par voie orale. Le *Domesday Book* de Guillaume le Conquérant, compilé en 1086, était encore utilisé pour régler les litiges fonciers jusqu'aux années 60. Aujourd'hui, il existe un nouveau système d'archivage numérique. Son impact pourrait être tout aussi grand. Ce système est appelé la blockchain.

Imaginez un registre numérique gigantesque. Toute personne ayant accès à Internet peut regarder l'information qu'il contient : il est ouvert à tous. Personne n'est en charge de ce registre. Il n'est pas entretenu par une personne, une entreprise, un ministère ou une organisation gouvernementale - mais par 8.000 à 9.000 ordinateurs répartis à différents endroits à travers le monde dans un réseau distribué. La participation est tout à fait volontaire. Les propriétaires des ordinateurs choisissent d'ajouter leurs machines au réseau parce qu'en échange des services de leurs ordinateurs, ils reçoivent parfois des paiements. Vous pouvez ajouter votre ordinateur au réseau, si vous le souhaitez.

Toutes les informations dans le registre sont permanentes - elles ne peuvent pas être modifiées - et chacun des ordinateurs en conserve une copie à cet effet. Si vous voulez pirater le système, vous devez *hacker* chaque ordinateur sur le réseau – et, jusqu'à présent, cela s'est révélé être impossible en dépit de nombreux efforts déployés, y compris par les meilleurs éléments de la National Security Agency. La puissance collective de tous ces ordinateurs est supérieure à celle des 500 meilleurs supercalculateurs au monde combinés.

De nouvelles informations sont ajoutées au registre toutes les minutes, mais celles-ci ne peuvent être ajoutées que lorsque tous les ordinateurs signalent leur approbation,

ce qu'ils font dès qu'ils ont une preuve satisfaisante que les informations à ajouter sont correctes. Tout le monde sait comment le système fonctionne, mais personne ne peut changer la manière dont il fonctionne. Il est entièrement automatisé. La prise de décision ou le comportement humain ne pénètre pas en lui.

Si une entreprise ou un ministère étaient en charge du dossier, il serait vulnérable - si l'entreprise faisait faillite ou l'organisation gouvernementale venait à fermer, par exemple. Mais avec un registre distribué, il n'y a aucun point de vulnérabilité. Il est décentralisé. Parfois, certains ordinateurs peuvent dérailler, mais cela n'a pas d'importance. Les copies sur tous les autres ordinateurs et leur approbation unanime pour que de nouvelles informations soient ajoutées impliquent que l'enregistrement en lui-même est en sécurité.

C'est peut-être le registre d'archive le plus important et détaillé de toute l'histoire, une mémoire permanente dans une architecture *open-source* qui se développe organiquement. Une mémoire connue sous le nom de blockchain. C'est la technologie révolutionnaire qui est derrière le système de monnaie numérique, le Bitcoin, mais son impact sera bientôt beaucoup plus vaste qu'une simple monnaie alternative.

Beaucoup de monde a du mal à comprendre ce qu'il y a de si spécial à propos du Bitcoin. Nous avons tous des comptes en ligne avec des livres, des dollars, des euros ou une autre monnaie nationale. Cet argent est entièrement numérique, il n'existe pas dans le monde réel – ce sont seulement des chiffres qui sont quelque part dans un registre comptable numérique. Environ seulement 3% de la monnaie nationale existe réellement sous forme physique ; le reste est numérique. J'ai également récolté des points de récompenses pour les courses au supermarché et des *air miles*. Ceux-ci n'existent pas physiquement non plus, mais ils s'apparentent encore à des jetons à échanger contre quelques biens ou services, quoiqu'avec une portée limitée ; ils sont donc également une forme de monnaie. Pourquoi le monde s'est tellement excité à propos du Bitcoin ?

Pour comprendre cela, il est important de faire la distinction entre la monnaie [*money*] et l'argent physique [*cash*].

Si je suis dans un magasin et que je donne au commerçant 50 pence pour une barre chocolatée, c'est une opération au comptant. L'argent passe directement de moi à lui et cela n'implique personne d'autre : c'est direct et sans friction. Mais si j'achète cette barre chocolatée avec une carte de crédit, la transaction implique un système de paiement d'un certain type (souvent plus d'un). C'est, en d'autres termes, un intermédiaire.

La même chose vaut pour les livres, les dollars ou les euros que j'ai sur les comptes en ligne. Je dois passer par un intermédiaire si je veux les dépenser - peut-être une banque, PayPal ou une société de carte de crédit. Si je veux dépenser ces points de récompenses de supermarché ou ces *air miles*, il faut passer par le supermarché ou la compagnie aérienne.

Depuis le début des années 80, les codeurs avaient essayé de trouver un moyen de reproduire numériquement la transaction en espèces - cette transaction directe, sans friction de A à B - mais personne n'avait pu trouver la solution. Le problème était connu comme le problème de la « double-dépense » [*double-spending*]. Si je vous envoie un email, une photo ou une vidéo - toute forme de code informatique - vous pouvez, si vous le souhaitez, copier et coller ce code et l'envoyer à un, ou une centaine, ou à un million de personnes différentes. Mais si vous pouviez le faire avec de l'argent, la monnaie deviendrait vite inutile. Personne n'avait pu trouver un moyen de contourner cela sans l'aide d'un intermédiaire pour vérifier et traiter les transactions, et voir à quel moment il n'y a plus d'argent. Au milieu des années 2000, les codeurs ont tous abandonné l'idée. Le problème était considéré insoluble. Puis, fin 2008, discrètement annoncé sur une liste de diffusion restreinte, le Bitcoin débarque.

> *Sur le billet d'un dollar, vous verrez les mots : « In God we trust »* - que l'on peut traduire par « En Dieu nous croyons » ou *« En Dieu nous avons confiance ». Les aficionados du Bitcoin se plaisent à dire : « In proof we trust » - « En la preuve nous croyons »*

À la fin de l'année 2009, les codeurs se réveillaient en découvrant que son inventeur, Satoshi Nakamoto, avait *craqué* le problème de la « double dépense ». La solution était la blockchain, l'enregistrement automatisé sans personne en charge. Cela

remplace l'intermédiaire. Plutôt qu'un processus de transaction bancaire, les transactions sont traitées par ces 8.000 à 9.000 ordinateurs répartis à travers le réseau Bitcoin dans la tradition collective de la collaboration en *open-source*. Lorsque ces ordinateurs ont leur preuve cryptographique et mathématique (un processus qui prend très peu de temps), ils approuvent la transaction et elle est alors finalisée. Les informations de paiement – le moment, la quantité, les adresses de portefeuille - sont ajoutées à la base de données - ou, pour utiliser la terminologie exacte, un autre bloc de données [*block of data*] est ajouté à la chaîne d'information - d'où le nom de blockchain. C'est simplement une chaîne de blocs d'informations.

La monnaie requiert la confiance - la confiance envers les banques centrales, les banques commerciales, d'autres grandes institutions, la confiance dans le papier en lui-même. Sur un billet d'un dollar, vous verrez les mots : *« In God we trust »*. Les aficionados du Bitcoin se plaisent à dire : *« In proof we trust »*. La blockchain, qui fonctionne de manière transparente via l'automatisation et la preuve mathématique et cryptographique, a supprimé la nécessité de cette confiance. Elle a permis aux personnes de payer en argent numérique directement d'une personne à l'autre, aussi facilement qu'un envoi de SMS ou d'email, sans recourir à un intermédiaire.

Donc, la meilleure façon de comprendre le Bitcoin, c'est tout simplement : le *cash* pour Internet. Il ne va pas remplacer le dollar américain, comme certains des ses partisans purs et durs vous le diront, mais il a de nombreuses applications. Et, sur un plan pratique, cela fonctionne.

Le fait est que cela a permis la montée du marché noir en ligne. Peut-être 1 million de £ de marchandises et de services illégaux sont négociés tous les jours par le biais des marchés noirs - et le moyen de paiement est le Bitcoin. Le Bitcoin a facilité cette hausse rapide. (Je tiens à souligner que, même si toutes les transactions en Bitcoin, peu importe leur importance, sont inscrites sur la blockchain, l'identité de la personne effectuant cette transaction peut être cachée si elle le désire - d'où son attrait). Dans le grand ordonnancement financier des choses, 1 million de £ par jour ce n'est pas beaucoup, mais le fait que les personnes ordinaires sur le marché noir utilisent le Bitcoin quotidiennement comme un moyen de paiement pour des biens et des services démontre que la technologie fonctionne. Je n'approuve pas les marchés noirs, mais il est intéressant de souligner que ce sont souvent les premiers à adopter

une nouvelle technologie. Ils ont été les premiers à détourner Internet pour faire du profit, par exemple. Sans pouvoir recourir à de la dette ou au capital-risque, les marchés noirs ont du faire fonctionner de nouvelles technologies de manière rapide et pratique.

Mais les utilisations potentielles de Bitcoin vont bien au-delà des marchés noirs. Il convient de se demander pourquoi nous pourrions vouloir utiliser du *cash* dans le monde physique. Vous pouvez l'utiliser pour les petits paiements - une barre chocolatée ou un journal dans votre magasin du coin, par exemple. Il existe le même besoin en ligne. Je pourrais vouloir lire un article paru dans *The Times*. Je ne veux pas prendre un abonnement annuel - mais je veux lire cet article. Ne serait-il pas agréable d'avoir un système où je pourrais effectuer un micro paiement pour lire cet article ? Cela ne vaut pas le coup de passer par un organisme de paiement pour traiter un somme aussi petite, mais avec du *cash* Internet, vous n'avez pas besoin d'intermédiaire. Vous pouvez payer au comptant et le processus ne coûte rien - il est direct. Cette utilisation potentielle pourrait ouvrir la voie à une nouvelle ère de contenu payant. Les fournisseurs de contenus en ligne ne subiront plus autant de pression, en offrant d'énorme quantité de matériel pour rien, dans l'espoir de retomber d'une façon ou d'une autre sur leurs pieds plus tard, maintenant que la technologie est là pour exécuter et recevoir le paiement pour de petites sommes, en échange de contenu.

Nous utilisons aussi du *cash* pour les paiements rapides, les paiements directs et les pourboires. Vous passez devant un musicien de rue, par exemple, et vous lui jetez une pièce de monnaie. Bientôt vous serez en mesure de payer sur le champ un fournisseur de contenu en ligne pour sa vidéo YouTube, une chanson ou un article de blog, aussi facilement et rapidement que si vous cliquiez sur [le bouton] « J'aime » à l'écran. Même si je paye mon addition au restaurant avec une carte, je vais souvent laisser un pourboire en espèces au serveur. De cette façon, je sais que le serveur va recevoir l'argent - à l'inverse de ce que font certains employeurs peu scrupuleux. J'aime bien payer comptant sur les marchés, où beaucoup de petites entreprises débutent parce que les paiements en espèces vont directement dans la poche du propriétaire de l'entreprise, sans les intermédiaires qui prennent leurs pourcentages. Ce même système de paiement direct, pas cher et rapide va s'appliquer en ligne. Les frais de traitement peu onéreux sont essentiels pour les

entreprises à faible marge. Le *cash* Internet aura son utilité là aussi. Il a également une application potentielle dans le secteur des transferts de fonds, qui est actuellement dominé par des sociétés comme Western Union. Pour ceux qui travaillent à l'étranger et qui veulent envoyer de l'argent, le virement, les commissions et autres frais de change peuvent souvent représenter jusqu'à 20% du montant transféré. Avec Bitcoin, ces coûts peuvent être supprimés.

Certains d'entre nous utilisent aussi le *cash* pour les paiements que nous voulons maintenir confidentiels. Confidentiel ne signifie pas nécessairement illégal. Vous pourriez être en train d'acheter un cadeau pour votre anniversaire de mariage et vous ne voulez pas que votre conjoint(e) le sache. Vous pourriez faire un don pour la bonne une cause ou à une organisation caritative et vous voulez garder l'anonymat. Vous pourriez faire quelque chose de vilain : beaucoup de ceux qui ont vu leurs détails personnels fuités sur Ashley Madison auraient préféré avoir été en mesure de payer leurs adhésions avec du *cash* – ce qui leur aurait permis de conserver leur anonymat.

Plus important encore, le *cash* est vital pour les 3,5 milliards de personnes - la moitié de la population mondiale - qui sont « non bancarisées », exclus du système financier et donc exclu de l'e-commerce. Avec le Bitcoin, la seule barrière à l'entrée est un accès Internet.

Le Bitcoin connaît actuellement des problèmes de gouvernance et d'évolutivité. Malgré cela, la technologie fonctionne, et les codeurs sont en train de développer des moyens d'utiliser la technologie blockchain à des fins qui vont bien au-delà d'un système monétaire alternatif. Dès 2017, vous allez commencer à voir quelques-unes des premières applications se glisser dans vos vies électroniques.

Une des applications est la messagerie décentralisée. Tout comme vous pouvez envoyer du *cash* à quelqu'un sans intermédiaire en utilisant le Bitcoin, de la même manière vous pouvez envoyer des messages - sans que Gmail, iMessage, WhatsApp, ou quel que soit le fournisseur, aient accès à ce qui est dit. La même chose vaut pour les réseaux sociaux. Ce que vous dites restera entre vous et vos amis ou *followers*. Twitter ou Facebook n'y auront pas accès. Les implications pour la

vie privée sont énormes, ce qui soulève un éventail de problèmes dans le débat actuel sur la surveillance gouvernementale en cours.

Ainsi, nous allons voir le stockage décentralisé et le *cloud computing* [l'informatique en nuage] réduire considérablement le risque de stocker des données auprès d'un seul fournisseur. Une société appelée Trustonic travaille en ce moment sur un nouveau système d'exploitation pour téléphone mobile basé la blockchain, afin de concurrencer Android et Mac OS [iOS].

Tout comme la blockchain enregistre où est un Bitcoin à un moment donné, et par conséquent à qui il appartient, la blockchain peut être utilisée pour enregistrer la propriété d'un actif - et permettre de vendre et d'acheter la propriété de cet actif. Cela a d'énormes répercussions sur la façon dont les actions, les obligations et les contrats à terme, en fait tous les actifs financiers, sont enregistrés et négociés. Pour les registraires [les bureaux d'enregistrement], les marchés boursiers, les banques d'investissement – les perturbations se trouvent juste en face de chacun d'eux. Leurs monopoles sont tous sous la menace de la technologie blockchain.

Les terres et la propriété foncière peuvent également être enregistrées et négociées sur une blockchain. Le Honduras, où les litiges fonciers sur les propriétés de bord de mer sont monnaie courante, développe déjà des moyens pour enregistrer ses registres fonciers et son cadastre sur une blockchain. Au Royaume-Uni, près de 50% des terres ne sont encore non enregistrées, d'après l'ouvrage *Who Owns Britain?* (2001) du journaliste d'investigation Kevin Cahill. Les titres de propriété des véhicules, des billets, des diamants, de l'or – d'à peu près tout – peuvent être enregistrés et *tradés* en utilisant la technologie blockchain - même le contenu de vos bibliothèques de musique et de films (bien que les droits d'auteur peuvent empêcher cela). Les jetons Blockchain seront aussi valables que tout acte de propriété - et ils seront nettement moins cher à fournir.

L'économiste péruvien Hernando de Soto Polar a remporté de nombreux prix pour ses travaux sur la propriété. Sa thèse centrale est que l'absence de titre de propriété est clairement ce qui a maintenu tant de personnes dans le tiers-monde depuis si longtemps. Qui est propriétaire de quoi doit être clair, reconnu et protégé - sinon il n'y aura pas d'investissement et le développement sera limité. Mais si la propriété est

claire, les personnes peuvent la négocier, l'échanger et prospérer. La blockchain permettra - ses plus ardents défenseurs l'espèrent - de trouver des moyens de relever ce défi.

> *Les contrats intelligents pourraient disrupter la profession d'avocat et la rendre accessible à tous, tout comme Internet l'a fait avec la musique et l'édition*

Une fois que la propriété est claire, alors les droits contractuels et les droits de propriété suivront. Cela nous amène à la prochaine vague de développement de la techno blockchain : les contrats automatisé, ou pour utiliser le jargon, « les contrats intelligents » [« *smart contracts* »], un terme inventé par le programmeur américain Nick Szabo. Avec les contrats, nous allons au-delà du titre de propriété ; les contrats représentent en même temps l'acte de propriété d'un bien foncier et les conditions liées à cette propriété foncière. Prenons, par exemple, une obligation qui appartient à une certaine personne, mais cette obligation implique certaines conditions - elle pourrait générer des intérêts, il faudra peut-être la rembourser pendant un certain temps, ou encourir des pénalités si certains critères ne sont pas respectés. Ces conditions pourraient être encodées dans une blockchain et toutes les actions correspondantes automatisées.

Que ce soit un accord initial, l'arbitrage d'un différend ou son exécution, toutes les étapes d'un contrat ont, historiquement, été évaluées et actées par des personnes. Un contrat intelligent automatise les règles, vérifie les conditions et agit sur elles, ce qui minimise l'intervention humaine - et donc les coûts. Même les accords commerciaux complexes peuvent être encodées et empaquetées sous la forme d'un contrat intelligent pour une fraction du coût de la rédaction, de la contestation ou de l'exécution d'un contrat traditionnel.

Une des critiques du système juridique actuel est que seuls les très riches ou ceux qui ont une aide juridique peuvent se le permettre : tout le monde est exclu. Les contrats intelligents ont le potentiel de *disrupter* les professions juridiques et de les rendre accessibles à tous, tout comme Internet l'a fait à la fois pour le secteur de la musique et de l'édition.

Tout cela a d'énormes implications sur la façon dont nous faisons du *business*. Il est possible que la technologie blockchain permette de faire le travail des banquiers, des avocats, des administrateurs et des registraires - avec des normes beaucoup plus exigeantes et pour une fraction du prix.

Toul comme dans le cas de la propriété, la technologie blockchain peut prouver l'authenticité. De la notarisation - l'authentification des documents [par un officier public] - à la certification, les applications sont multiples. C'est particulièrement utile pour les fabricants, surtout pour les articles griffés et les produits électroniques haut de gamme, où la valeur est dans la marque. Nous savons que c'est un véritable sac Louis Vuitton, car il a été enregistré sur la blockchain au moment de sa fabrication.

La Blockchain Tech aura également un rôle à jouer pour votre authentification. À l'heure actuelle, nous utilisons un système de noms d'utilisateur et des mots de passe pour prouver son identité en ligne. C'est un système bancal et vulnérable à la fraude. Nous n'allons pas utiliser cela plus longtemps. Une entreprise envisage même un système de technologie blockchain pour remplacer nos actuels systèmes de verrouillage pour la voiture et la maison. Une fois à l'intérieur de votre domicile, la technologie blockchain s'appuiera sur l'Internet des Objets, en reliant votre réseau domestique vers le *cloud* et les appareils électroniques autour de chez vous.

De l'identité, il n'y a qu'un petit pas qui mène à la réputation. Pensez à l'importance de la notation sur TripAdvisor ou sur eBay, ou un commentaire client positif sur Amazon. La réputation en ligne est devenue essentielle dans le business modèle d'un vendeur et elle a permis de grosses améliorations dans les normes. Grâce à TripAdvisor, ce qui était qu'un hôtel ordinaire va vous traiter comme un roi ou une reine, afin de s'assurer que vous lui donnez cinq étoiles. Le service que vous obtenez d'un chauffeur Uber est susceptible d'être bien meilleur que celui d'un chauffeur de taxi ordinaire, parce qu'il ou elle veut une bonne note.

> *Il n'y aura pas dépouillements suspects en Floride ! La blockchain permettra également d'ouvrir la voie à la possibilité d'une démocratie plus directe*

Le système de rétroaction [*feedback*] a aussi été fondamental dans le succès du marché noir en ligne. Les mauvais vendeurs obtiennent de mauvaises notes. Les bons vendeurs obtiennent de bons points. Les acheteurs vont voir les vendeurs avec de bonnes notes. Le marché noir n'est plus le magasin à arnaques, sans possibilité de recours, qu'il était autrefois. Le système de rétroaction a rendu redondant le rôle des normes commerciales, des autorités, des groupes de protection des consommateurs et des autres organismes de régulation. Ils ont l'air poussifs, lents et obsolètes.

Une fois que votre réputation en ligne peut être stockée sur la blockchain (et ainsi, non détenue par une société comme TripAdvisor, mais décentralisée) tout le monde souhaitera avoir une bonne note. La nécessité de préserver et de protéger la réputation implique simplement que les personnes vont mieux se comporter. Sony se penche sur les moyens d'exploiter ce qui permet à votre réputation en termes d'études et de formations d'être mise sur la blockchain - les notes que vous avez obtenues à l'école, votre diplôme universitaire, vos expériences professionnelles, vos compétences et qualifications, votre CV, les soutiens que vous recevez des personnes avec qui vous avez fait du business. LinkedIn est probablement en train de faire quelque chose de similaire. Il existe également une utilisation évidente de cela pour les dossiers médicaux, mais aussi pour les casiers judiciaires - pas seulement pour les individus, mais pour les entreprises. Si, par exemple, une société minière a une mauvaise réputation car elle pollue l'environnement, elle pourrait être moins à même de gagner un appel d'offres pour un projet ou d'obtenir un permis de construire.

Nous constatons également le développement de nouvelles applications pour voter. Les implications sont énormes. Les élections et les référendums sont des entreprises coûteuses - la campagne, le personnel, le dépouillement des bulletins de vote. Mais vous allez bientôt être en mesure de voter à partir de votre téléphone mobile d'une façon qui est 10 fois plus sûre que les systèmes actuels aux États-Unis ou au Royaume-Uni, le tout pour une fraction du coût et sans fraude. De plus, vous serez en mesure de vérifier votre vote pour vous assurer qu'il est comptabilisé, tout en préservant votre anonymat. Une fois en place, même un gouvernement corrompu sera incapable de manipuler un tel système. Il n'y aura pas dépouillements suspects

en Floride ! La blockchain permettra également d’ouvrir la voie à la possibilité d'une démocratie plus directe : une fois que les coûts et les possibilités de fraude sont éliminés, il y a moins d'excuses pour ne pas se présenter face à l'électorat et débattre de questions clefs.

Peu de gens l’ont vue venir, mais cette nouvelle technologie est sur le point de changer la façon dont nous interagissons en ligne. La révolution ne sera pas télévisée, elle sera *cryptographiquement* horodatée sur la blockchain. Et la blockchain, à l'origine conçue pour résoudre l'énigme de l'argent numérique, pourrait se révéler être quelque chose de beaucoup plus important : un *Domesday Book* numérique pour le 21e siècle, et bien plus encore.

»