EXPLICATION DE LA TECHNOLOGIE BLOCKCHAIN

GUIDE ULTIME DU DÉBUTANT AU SUJET DU PORTEFEUILLE BLOCKCHAIN, MINES, BITCOIN, ETHÉRÉUM, LITECOIN, ZCASH, MONERO, RIPPLE, DASH, IOTA ET LES CONTRATS INTELLIGENTS

ALAN T. NORMAN

Alan T. Norman

Explication De La Technologie Blockchain

«Tektime S.r.l.s.»

Norman A.

Explication De La Technologie Blockchain / A. Norman — «Tektime S.r.l.s.»,

"Au lieu de parler d'investissement, ce livre se concentrera sur le fonctionnement de la technologie chaîne de blocks et comment elle pourrait être utilisée à l'avenir. Au lieu de parler d'investissement, ce livre se concentrera sur la façon dont la technologie chaîne de blocks fonctionne et comment elle pourrait être utilisée à l'avenir. Les sujets que vous pouvez vous attendre à voir dans ce livre comprennent: • Quel problème la technologie chaîne de blocks résout-elle? • Comment la technologie peut-elle rendre nos institutions plus rapides et moins coûteuses? • La technologie pourrait-elle remplacer totalement nos institutions (comme les gouvernements, les banques, etc.) ? • Comment la chaîne de blocks crée-t-elle la confiance entre étrangers? • Comment la chaîne de blocks augmente-t-elle la sécurité des transactions et des contrats? • Peut-on utiliser la chaîne de blocks en dehors des finances? • Qu'est-ce qu'un bloc? • Qu'est-ce qu'une chaîne de blocks et pourquoi en avons-nous besoin? • Qu'est-ce qu'une explication technique de ce qui se passe dans la chaîne de blocks ? • Qu'est-ce que l'exploitation minière et pourquoi en avons-nous besoin? • Existe-t-il des solutions de rechange à l'exploitation minière pour créer une chaîne de blocks? • Quelle est l'histoire de Bitcoin? • Bitcoin a-t-il des problèmes? • Qu'est-ce que Ethereum, et qu'est-ce qu'un contrat intelligent? • Y a-t-il d'autres technologies chaîne de blocks que je devrais connaître? • Comment les entreprises adoptent-elles la chaîne de blocks? • Quels obstacles réglementaires pourraient ralentir l'adoption de la chaîne de blocks? Voilà beaucoup de questions. Si tu es prêt à les attaquer, je suis prêt. "

Содержание

Alan T. Norman
Explication De La Technologie Blockchain

Explication De La Technologie Blockchain

Guide Ultime Du Débutant Au Sujet Du Portefeuille Blockchain, Mines, Bitcoin, Ethéréum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA Et Les Contrats Intelligents

Alan T. Norman

Traductrice: Yves Champagne

Obtenez votre livre **Bitcoin Whales** gratuitement en Bonus
(Trouvez-le à la fin du livre)

Pourquoi Vous Devriez Lire Ce Livre

Si vous n'avez jamais entendu parler de Blockchain ou vous avez seulement une vague idée de la façon dont cette nouvelle technologie fonctionne, c'est le livre pour vous. Dans ce court guide, je vais vous expliquer l'essentiel de la façon dont la technologie de la chaîne de blocs fonctionne, en utilisant des explications simples et en donnant des exemples en cours de route. J'ai présenté beaucoup de gens à Blockchain, donc je sais où les débutants sont généralement confus et les principales questions qu'ils ont. Tous les principes de base sont abordés étape par étape dans ce livre, vous n'avez pas besoin de connaissances ou de compréhension spéciales de la technologie pour comprendre les concepts dans ce livre. Blockchain est une technologie, comme l'Internet ou l'ordinateur personnel, qui est destiné à être utilisé par les masses. Il détient le potentiel de révolutionner presque chaque interaction dans nos vies. Beaucoup de lecteurs auront entendu parler de Bitcoin et crypto monnaies. Il s'agit d'une application importante de la technologie Blockchain et de la première application. Cependant, la chaîne de blocs n'est pas limitée à l'utilisation dans les systèmes de financement et de paiement. Bien que nous allions certainement couvrir Bitcoin et d'autres cryptomonnaies dans ce livre, nous allons également examiner les applications potentielles de Blockchain à travers de nombreuses industries différentes.

Ce N’est Pas Un Livre Sur L’investissement Dans Bitcoin Ou Autres Crypto-Monnaies

Au cours des dernières années, des centaines de nouvelles devises ont été créées, tous vivant en ligne, sur la chaîne de blocs. Pour les nouveaux arrivants à la technologie, il peut venir comme une surprise que les gens investissent sérieusement dans les devises numériques nouvellement inventées comme Bitcoin. Pour ceux d’entre vous qui sont nouveaux à Blockchain, l’idée d’investir dans la crypto-monnaie pourrait sembler attrayant. Un mot d’avertissement : investir dans la crypto-monnaie est un marché très volatile et extrêmement risqué. Faites vos recherches avant d’investir dans un crypto-monnaie pour s’assurer qu’il est légitime, et ne pas investir plus d’argent que vous pouvez vous permettre de perdre. Blockchain et les crypto-monnaies sont encore dans leurs premiers jours, et tout peut arriver à tout moment. Pendant que ces devises sont intéressantes et ont le potentiel de gagner une large utilisation, ce n’est pas un livre sur la crypto-monnaie. Si vous cherchez des conseils d’investissement ou des renseignements d’initiés sur les devises qui connaîtront le plus de succès, vous ne les trouverez pas dans ce livre, vous liriez mon autre livre – “Cryptocurrency Investing Bible”.

Ce Que Vous Apprendrez Dans Ce Livre

Au lieu de parler d'investissement, ce livre se concentrera sur la façon dont la technologie Blokchainfonctionne et comment elle pourrait être utilisée à l'avenir. Les sujets que vous pouvez vous attendre à voir dans ce livre comprennent :

- Quel problème la technologie Blokchainrésout-elle?
- Comment la technologie peut-elle rendre nos institutions plus rapides et moins coûteuses?
- La technologie pourrait-elle remplacer totalement nos institutions (comme les gouvernements, les banques, etc.) ?
- Comment la Blockchain crée-t-elle la confiance entre étrangers?
- Comment la Blockchain augmente-t-elle la sécurité des transactions et des contrats?
- Peut-on utiliser la Blokchainen dehors des finances?
- Qu'est-ce qu'un bloc?
- Qu'est-ce qu'une Blockchain et pourquoi en avons-nous besoin?
- Qu'est-ce qu'une explication technique de ce qui se passe dans la Blockchain?
- Qu'est-ce que l'exploitation extraction et pourquoi en avons-nous besoin?
- Existe-t-il des solutions de rechange à l'extraction pour créer une Blockchain ?
- Quelle est l'histoire de Bitcoin?
- Bitcoin a-t-il des problèmes?
- Qu'est-ce que Ethereum, et qu'est-ce qu'un contrat intelligent?
- Y a-t-il d'autres technologies Blokchain que je devrais connaître?
- Comment les entreprises adoptent-elles la Blockchain ?
- Quels obstacles réglementaires pourraient ralentir l'adoption de la Blockchain?

Voilà beaucoup de questions. Si tu es prêt à les attaquer, je suis prêt.

Que Fait La Blockchain?

Avant d'entrer dans les détails techniques de la technologie Blockchain, il est important de comprendre les problèmes que la Blockchain résout. Pourquoi avons-nous besoin de la Blockchain, et que fait notre technologie actuelle? Les premiers utilisateurs de la technologie Bitcoin et de la Blockchain ont repéré ce qu'ils percevaient comme une faille fondamentale dans notre façon de penser les transactions, la confiance et les institutions sociales. Les premières versions de la Blockchain sont venues à peu près au même moment que la crise financière de 2007 aux États-Unis, lorsque de nombreuses personnes ont perdu confiance dans les institutions sociales qui étaient censées protéger les intérêts de l'homme ordinaire. Bien sûr, les gens ont été déçus par le système bancaire à la suite de la crise, mais ils ont également perdu confiance dans le gouvernement pour réglementer les marchés financiers et dans la presse pour enquêter sur les crises potentielles. En fait, les sondages Gallup et le baromètre Edelman Trust montrent tous deux une baisse constante de la confiance du public dans les institutions – banques, gouvernement, médias, universités et organismes sans but lucratif – au cours de la dernière décennie. La confiance dans les institutions est à un niveau historiquement bas dans l'histoire américaine, et des problèmes similaires affligent l'UE. (Brexit, ascension de Marine Le Pen, indépendance de la Catalogne, crise de la gouvernance en Grèce). L'idée fondamentale derrière les institutions est de créer la confiance entre étrangers dans la société. Nous avons des lois et des systèmes en place pour permettre à des millions de personnes qui ne se connaissent pas de vivre dans le voisinage les unes des autres. Cependant, les créateurs de Blockchain ont estimé que ces institutions ont échoué.

Le Problème Avec Les Institutions

Pour voir pourquoi les créateurs de Blockchain veulent remplacer les institutions, il est utile de réfléchir à la façon dont nous en sommes arrivés au point où la confiance institutionnelle est si faible. Quelles sont les faiblesses des institutions et comment la Blockchain pourrait-elle les résoudre?

La Lenteur

La première et la plus grande faiblesse institutionnelle est la rapidité. Les institutions, de par leur nature même, sont lentes. Elles nécessitent des approbations et plusieurs cycles de vérification pour chaque relation, contrat et transaction. Les changements de politique au niveau institutionnel sont également lents. La création de nouvelles lois ou la mise en œuvre de nouvelles procédures peuvent prendre des mois ou des années. Par exemple, la production de votre déclaration de revenus prend des heures de travail et de maux de tête. Ensuite, le gouvernement doit vérifier les informations que vous avez soumises dans la déclaration avant de recevoir votre remboursement. Des mois, voire des années plus tard, le gouvernement peut choisir de vous auditer, auquel cas vous aurez besoin des copies d'exemplaires d'anciennes transactions financières datant de plusieurs années.

Un autre exemple est la durée des transactions bancaires. Il n'y a aucune raison, sur le plan technologique, pour qu'un transfert bancaire prenne plus de quelques minutes. Cependant, il faut généralement quelques jours ouvrables pour qu'une transaction soit compensée en raison d'une combinaison de systèmes périmés, de politiques internes et de règlements gouvernementaux qui exigent que la transaction soit analysée et traitée. La technologie de la chaîne de blocs est régie par ses utilisateurs et utilise la cryptographie pour protéger la vie privée des utilisateurs. Selon la façon dont le système est conçu, il peut être incroyablement rapide. Les nouveaux contrats intelligents peuvent automatiquement calculer et débourser quelque chose comme une déclaration de revenus ou même une facture d'entreprise une fois que certaines conditions sont remplies. Comme elle est fondée sur le consensus, la collectivité peut décider collectivement de mettre en œuvre un changement dans la façon dont le système fonctionne et de régler les problèmes au fur et à mesure qu'ils surviennent.

La Chèreté

Les institutions traditionnelles sont également chères. Il est facile de désigner les taxes comme une dépense des institutions, mais tous les frais de transaction et les abonnements d'utilisateurs que vous payez chaque mois sont d'autres formes de dépenses institutionnelles. Au fil du temps, ces dépenses s'additionnent. Par exemple, les banques facturent des frais pour traiter les virements électroniques, convertir des devises ou même gérer votre compte. Les agences d'assurance exigent des frais administratifs intégrés à vos primes d'assurance. De nombreux détaillants en ligne facturent des frais de transaction par carte de crédit. Si vous dirigez une petite entreprise, vous trouverez des frais partout, du marketing au traitement des paiements. Nous sommes devenus si habitués à ces petits frais que le coût de la vie dans la société, mais la Blockchain espère remettre en cause cette hypothèse. Les contrats et les transactions de la Blockchain ont lieu sur un réseau partagé. Les utilisateurs du réseau interviennent également pour vérifier les transactions des autres. Au lieu qu'une autorité centrale facture des frais pour vérifier votre transaction, vous vérifiez une autre transaction sur le réseau en échange du traitement de votre propre transaction. Toutes les technologies de Blockchain ne fonctionnent pas exactement de cette façon, mais l'idée est la même pour la plupart d'entre elles. En participant au réseau, vous vous retrouvez avec moins de frais que si vous auriez payé à une institution traditionnelle.

Susceptibilité Aux Attaques

La cybercriminalité est en hausse, et il est maintenant courant d'entendre parler des grandes institutions qui se font pirater ou qui ont des atteintes aux données personnelles. La vulnérabilité aux attaques est l'une des raisons pour lesquelles la confiance envers les institutions diminue. Lorsque vous centralisez des données, vous êtes sûr de trouver de mauvais acteurs qui cherchent à tirer parti de cette information.

Le piratage d'Equifax de 2017 aux États-Unis est un exemple majeur. Equifax recueille des renseignements sur le crédit des consommateurs aux États-Unis, y compris les numéros de carte de crédit, les renseignements sur la sécurité sociale, les noms complets, les adresses et l'historique des paiements. L'atteinte à la protection des données en septembre 2017 a touché 143 millions de consommateurs, mettant en évidence les dangers de faire confiance à la sécurité des données à une grande institution. Certaines technologies de la chaîne de blocs sont plus sécuritaires que d'autres, et chaque technologie a sa propre méthode pour assurer la confidentialité. Cependant, étant donné que chaque relation, contrat et transaction est chiffrée individuellement, même si vous deviez violer un élément de renseignements personnels, vous n'auriez pas accès à l'information de quelqu'un d'autre dans le processus.

Remplacer Les Institutions Par La Technologie

La plupart des gens conviendraient que nos institutions ont des défauts et ne sont pas des solutions parfaites. Mais ils résolvent les problèmes de confiance, et ils le font depuis des centaines d'années. En fait, nous vivons probablement à l'ère la plus paisible et la plus confortable de l'histoire humaine. Toute alternative à nos institutions actuelles doit avoir des avantages et une force clairs. L'idée derrière la Blockchain est de remplacer les institutions par une technologie qui peut mieux faire le travail et autonomiser les individus. Si vous pouviez créer un moyen pour les étrangers de se faire confiance sans avoir besoin d'une banque ou d'un gouvernement comme intermédiaire, vous vous attaqueriez à l'un des plus gros goulots d'étranglement de la société. Mais pour ce faire, vous auriez besoin d'un système puissant pour créer un consensus entre étrangers, et les créateurs de Blockchain croient que le pouvoir réside dans la décentralisation. Toutes les applications de la Blockchain (et d'autres technologies cryptographiques) reposent essentiellement sur le concept de décentralisation . Au lieu d'une autorité centrale rigide et lente à prendre des décisions et à régir les relations, la Blockchain cherche à rendre le pouvoir réglementaire aux individus. Au lieu de faire confiance à une grande institution, la Blockchain renforce la confiance par le consensus.

Un Nouveau Paradigme Technologique

La base de toute la chaîne de blocs et de la technologie cryptographique est le réseau pair-à-pair. Traditionnellement, lorsque nous pensons à la confiance, nous considérons les institutions comme des intermédiaires. À l'heure actuelle, si je voulais vous envoyer $100, nous aurions besoin d'un virement bancaire:

1. Premièrement, je soumettrais le transfert à la banque.
2. Ensuite, ma banque exigerait des frais en pourcentage pour traiter la transaction
3. Ma banque vérifie que j'ai $100 dans mon compte
4. Ma banque demande à votre banque si votre compte est valide et ouvert pour les dépôts
5. Ma banque met à jour son grand livre de comptes pour soustraire $100 de mon compte
6. Votre banque met à jour son grand livre pour ajouter $100 à votre compte.

Une interconnexion de réseaux de pair-à-pair n'a pas besoin d'intermédiaire. Il utilise plutôt un grand livre distribué pour traiter les transactions. Tous les ordinateurs qui font partie du réseau tiennent à jour une copie du grand livre, et les transactions sont systématiquement ajoutées au grand livre. Il est incroyablement difficile de changer le registre une fois qu'il est rédigé, parce que cela exigerait de changer la copie du registre sur des milliers d'ordinateurs dans le réseau de pairs. «Voici comment le même transfert de $100 fonctionnerait sur un réseau de pairs avec un grand livre distribué:

1. Premièrement, je présente la demande de transfert au réseau
2. Ensuite, les ordinateurs les plus proches de moi sur le réseau vérifient que j'ai suffisamment de monnaie dans mon compte et que votre compte de réception est valide
3. Une fois qu'ils ont vérifié la transaction, ils l'ont transmise à tous les ordinateurs près d'eux sur le réseau
4. À leur tour, ces ordinateurs vérifient à nouveau la transaction et la transmettent, ce qui donne lieu à un effet cascade jusqu'à ce que la transaction soit ajoutée à chaque registre du réseau de pairs.

Puisque les ordinateurs du réseau de pair à pair sont à la fois des utilisateurs et des vérificateurs, les transactions de la chaîne de blocs peuvent être sans coût. L'effet cascade de la vérification des transactions signifie qu'une transaction peut être traitée en minutes ou en heures plutôt qu'en jours.

Edifier La Confiance

La nature peer-to-peer de la Blockchain renforce la confiance sans les institutions. Étant donné que tous ceux qui utilisent le réseau ont une copie du grand livre, la Blockchain promet une nouvelle ère de transparence dans la comptabilité. Je peux facilement voir si vous m'avez envoyé $100 et que la transaction a été vérifiée. Une fois que vous l'avez fait, je sais que vous ne pourrez pas annuler la transaction ou annuler les frais, car ils ont été vérifiés par le réseau. Les nouvelles avancées de la Blockchain signifient également que je peux créer un contrat entre nous qui ne paie qu'une fois certaines conditions sont remplies, ce qui nous permet de faire des affaires en sachant que le contrat est financé et ne sera payé que si les travaux sont terminés.

Augmenter La Connexion

L'un des plus grands avantages potentiels de la technologie Blockchain est une connexion mondiale accrue. Lorsque vous pouvez facilement envoyer des devises à n'importe qui dans le monde, les frontières nationales et régionales commencent à s'effondrer. Il devient plus facile de faire confiance à des étrangers, où qu'ils se trouvent dans le monde. De la même manière que l'Internet connecte le monde, la Blockchain promet désormais de créer la confiance entre les gens dans le monde. La Blockchain peut être utilisée pour créer des contrats entre étrangers, permettre aux citoyens de voter de manière anonyme et mettre fin à la falsification des élections, et connecter des appareils intelligents qui assurent la sécurité des citoyens. Il est même possible que la Blockchain puisse être utilisée pour des référendums publics quotidiens ou hebdomadaires sur de nouvelles lois où vous pouvez voter depuis votre ordinateur personnel. La véritable démocratie populaire changerait définitivement le fonctionnement du gouvernement, donnant le contrôle des lois et des politiques à la population.

Augmenter La Productivité

Un avantage de deuxième niveau de la Blockchain est une productivité accrue. Actuellement, les institutions pèsent sur l'économie, car les gouvernements prélèvent des impôts pour gérer la bureaucratie et les banques facturent des frais pour le transfert et la détention d'argent. Une économie et une société basées sur la Blockchain peuvent être nettement plus efficaces. Comme effet secondaire, le même niveau de confiance sociétale pourrait être maintenu avec une diminution significative de la quantité de travail requise.

La Sécurité Et La Confidentialité

Ainsi, la Blockchain a le potentiel de vérifier les relations, les contrats et les transactions plus efficacement que les grandes institutions. Mais l'efficacité est inutile si le système n'est pas également hautement sécurisé. Bien que la technologie peer-to-peer existe depuis la création de l'Internet, ces réseaux n'étaient pas sécurisés de la manière dont nous nous attendons à ce que les institutions financières et les gouvernements le soient. Une banque traditionnelle protège la vie privée en limitant l'accès aux informations aux seules parties concernées. Les livres de banque sont des documents internes, et lorsque vous vérifiez l'historique de vos transactions, vous ne pouvez voir que les transactions dans lesquelles vous êtes impliqué. Ce rôle de tiers de confiance, le maintien d'un livre de comptes non public est le rôle principal d'une banque. Le grand livre public est le fondement de la sécurité de la Blockchain, mais un grand livre public signifie que la confidentialité est compromise. C'était l'un des problèmes fondamentaux des transactions peer-to-peer avant 2008. Personne ne pouvait comprendre comment garantir la confidentialité lors de l'utilisation d'un grand livre public. Les avantages du grand livre distribué étaient énormes en termes de rapidité, de coût et de fiabilité. Cependant, les consommateurs n'étaient pas susceptibles d'adopter un système permettant de retrouver toutes leurs transactions.

La Cryptographie

Le premier niveau de protection de la sécurité et de la vie privée dans la chaîne de blocs est la cryptographie. L'information sur les transactions est regroupée. Cela comprend l'identification de la transaction, l'heure, le montant, l'adresse de l'expéditeur et l'adresse du destinataire. Les renseignements sur la transaction sont ensuite passés par une fonction de hachage cryptographique avant d'être ajoutés au grand livre. Lorsque l'information sur la transaction a été chiffrée, elle ressemble à ceci (exemple d'une transaction Bitcoin du 20 octobre 2017) :

aba128d3931e54ce63a69d8c2c1c705ea9f39ca950df13655d92db662515eacf

Une fonction de hachage cryptographique raccourcit et normalise le nombre de caractères dans une description de transaction, ce qui signifie que plus de transactions peuvent être envoyées sur le réseau à tout moment. Si je regarde la liste des transactions, il est impossible de dire quoi que ce soit au sujet de l'expéditeur, du destinataire et du montant. Cependant, puisque les normes de chiffrement de Bitcoin sont accessibles au public est encore possible de déchiffrer la transaction et d'apprendre plus de détails, y compris la clé publique de l'expéditeur, la clé publique du destinataire, et le montant envoyé.

De nouveaux concurrents Bitcoin utilisent différents types de cryptographie pour brouiller davantage l'information sur la transaction, ce qui rend impossible d'apprendre des informations sur la transaction une fois qu'il a été inclus dans le grand livre.

Nous discuterons plus en détail du chiffrement et du hachage dans un prochain chapitre.

Le Grand Livre Distribué = Difficile A Changer

Le grand livre distribué, l'un des principaux défis de la confidentialité, est également un élément clé de la sécurité de la Blockchain. Un grand livre traditionnel géré par une banque est protégé par de nombreuses couches de sécurité pour empêcher les modifications non autorisées. Cependant, si un attaquant était en mesure d'accéder au grand livre, il pouvait instantanément apporter des

modifications. Les livres à propriétaire unique font également l'objet de transactions frauduleuses. Si un voleur d'identité ou un fournisseur malveillant envoie une demande de transaction à la banque en votre nom, il est possible que la transaction soit approuvée à votre insu. Le fait d'avoir un seul propriétaire du grand livre signifie que les banques doivent dépenser de l'énergie et des frais généraux importants pour la médiation des plaintes et la gestion des cas de fraude. Le grand livre partagé modifie ces problèmes. Étant donné qu'il existe des milliers de copies indépendantes du grand livre sur les ordinateurs individuels du réseau, une fois qu'une transaction a été ajoutée au grand livre, il est presque impossible de la modifier. (Nous discuterons des raisons techniques pour lesquelles c'est le cas dans un chapitre ultérieur).

L’anonymité Et Les Clés Privées

Étant donné que la technologie Blockchain utilise un registre distribué, tout le monde a une copie de toutes les transactions qui se déroulent dans le réseau. Le registre des transactions doit être public pour fonctionner. Cependant, sans mesures de sécurité appropriées, n'importe qui dans le monde pourrait voir ce que vous avez acheté et auprès de qui. Les mises en œuvre de la Blockchain résolvent ce problème de sécurité de différentes manières, mais la plupart s'appuient sur un système qui déconnecte vos informations personnelles de votre compte. Par exemple, les portefeuilles Bitcoin sont anonymes et vous pouvez en avoir plusieurs. La seule chose requise pour accéder à votre compte est une clé privée que vous seul connaissez. Bien que tout le monde puisse voir votre adresse de portefeuille publique, il ne saura rien à qui appartient le portefeuille. Dans le livre blanc original pour Bitcoin, il est suggéré de créer un nouveau portefeuille pour chaque transaction que vous effectuez sur le réseau Bitcoin afin de maintenir l'anonymat. Les autres crypto-monnaies, comme Monero, espèrent améliorer davantage le niveau de confidentialité des transactions Blockchain. Monero utilise des adresses furtives, dissocie les identifications d’utilisateur des montants de transaction et obscurcit les pistes de transaction afin de garantir la confidentialité (voir le chapitre sur Monero pour plus d'informations). Le résultat est une crypto-monnaie complètement introuvable qui est toujours prise en charge par un grand livre public distribué.

Imaginer Un Avenir Blockchain

Jusqu'à présent, nous avons couvert les raisons de base pour lesquelles la Blockchain a été inventée, ce qu'elle fait et un aperçu général des méthodes utilisées par la Blockchain. Nous ne faisons qu'effleurer la surface, cependant, et nous aborderons les détails techniques des solutions de Blockchain dans le chapitre suivant. Tout d'abord, examinons quelques cas d'utilisation potentiels de la technologie Blockchain. Il est important de réaliser que la technologie de la Blockchain est bien plus importante que le Bitcoin. Même si Bitcoin échoue demain, la technologie Blockchain sera toujours viable dans de nombreuses industries. Alors que de nouveaux développements se poursuivent dans les réseaux peer-to-peer, la programmation de chaînes de blocs et de nouvelles formes de cryptographie, la tendance à la confiance distribuée se poursuivra en raison des avantages évidents en termes de vitesse, de coût et de sécurité. Bien que ce ne soit pas Bitcoin ou Ethereum qui alimente l'avenir de la Blockchain, vous pouvez être sûr que les technologies derrière la Blockchain seront mises en œuvre au cours des prochaines décennies. L'effet global sera des contrats plus efficaces, des transactions plus rapides et des coûts plus bas pour les opérateurs. La Blockchain a également le potentiel de changer notre façon de faire les courses, de voyager, d'élire des dirigeants, de travailler et de vivre.

La Finance

Les applications financières de la Blockchain obtiennent la majeure partie de la couverture médiatique et sont généralement les premières plateformes basées sur la Blockchain dont les consommateurs entendent parler. Il y a de fortes chances que votre première exposition au mot "Blockchain" ait eu lieu lors d'une discussion sur Bitcoin. Cela a du sens pour deux raisons. Premièrement, la Blockchain utilise des registres et les registres sont les mieux adaptés au monde financier. La technologie est parfaite pour les applications financières. Deuxièmement, la première mise en œuvre réussie de la Blockchain, Bitcoin, a été conçue dès le départ pour être une monnaie. Un avenir financier basé sur la Blockchain semble radicalement différent du système bancaire actuel. L'utilisation de l'argent liquide est déjà en baisse, et il est probable que les pays occidentaux pourraient facilement passer à des services bancaires entièrement électroniques dans un avenir proche. Dans l'avenir de la Blockchain, toutes les transactions pourraient être payées à partir de votre portefeuille de crypto-monnaie. Grâce à une nouvelle technologie hautement évolutive, votre transaction peut être traitée et vérifiée en quelques secondes. Les fournisseurs n'auraient pas à payer pour le traitement des paiements, et acheter quelque chose serait probablement aussi simple que d'autoriser la transaction à l'aide de votre téléphone ou d'un autre appareil connecté. Bien qu'un avenir sans espèces semble probable, il n'est pas clair qui contrôlera la monnaie numérique. La question de savoir si les monnaies décentralisées comme Bitcoin ou les grandes banques l'emporteront à la fin reste à débattre. Les banques envisagent déjà des moyens d'intégrer la technologie de la Blockchain dans leurs pratiques actuelles afin de saisir les avantages de la Blockchain tout en conservant leur rôle d'intermédiaire de confiance dans les transactions financières. La réglementation des marchés financiers changera également. Les gouvernements doivent collecter des impôts et lutter contre le blanchiment d'argent, et ces deux tâches deviennent plus faciles et plus difficiles en utilisant la Blockchain. Étant donné que le grand livre est public, le suivi des transactions est beaucoup plus facile, mais avec les transactions anonymes et les comptes fantômes, il est probable que la réglementation financière du gouvernement deviendra plus difficile. C'est une des raisons pour lesquelles les grandes banques peuvent continuer à contrôler les marchés financiers, même après avoir mis en œuvre les meilleures pratiques de la Blockchain.

Les Contrats Intelligents

Les paiements sont un exemple de contrat basé sur la Blockchain, mais il existe déjà de nombreuses applications en cours de développement sur la Blockchain. Ces contrats utilisent la nature distribuée de la Blockchain pour créer la confiance sans avoir besoin d'une institution, et ils ne peuvent pas être supprimés ou perturbés par des entités extérieures.Ethereum est la Blockchain où la plupart de ces applications sont construites, et c'est la deuxième plus précieuse Blockchain dans le monde, après Bitcoin. Ethereum permet aux développeurs de s'appuyer sur sa Blockchain, et les développeurs peuvent créer des programmes sur Ethereum comme ils le feraient dans n'importe quel autre langage de programmation. Cela signifie qu'Ethereum héberge des jeux en ligne, des plateformes de médias sociaux et des fournisseurs de services, tout comme sur l'Internet. La seule différence est que ces programmes sont décentralisés. Une fois créés, ils dureront aussi longtemps que la Blockchain Ethereum. Étant donné que les utilisateurs du monde entier maintiennent la Blockchain Ethereum, un gouvernement ne peut pas faire supprimer le service, et aucun utilisateur ne peut supprimer ou modifier le contenu du service. Ce qui est marrant avec les contrats intelligents, c'est qu'ils sont illimités. Tout ce que vous pouvez coder sur un ordinateur peut être codé sur la Blockchain. À l'avenir, cela inclura probablement également l'intelligence artificielle et d'autres formes d'apprentissage automatique, rendant l'IA facilement accessible à toute personne faisant partie du réseau peer-to-peer de la Blockchain.

La Gouvernance

La technologie de la Blockchain ne se limite pas au financement. Ces dernières années, des technologies ont émergé qui permettent aux développeurs de créer des programmes supérieurs à la Blockchain. Cela signifie qu'un morceau de code est intégré dans la Blockchain et appliqué par le réseau peer-to-peer. Un bon exemple de la façon dont cela pourrait fonctionner est le vote. À l'heure actuelle, nous comptons sur les commissions électorales, les institutions centrales pour administrer les élections et compter les votes. Ces systèmes ne sont pas parfaits. Ils doivent se rendre au bureau de vote un certain jour en personne, vérifier votre identité et votre droit de vote, et remplir un bulletin de vote secret dans un isoloir. Chacune de ces étapes pose des problèmes aux électeurs. Si je ne peux pas me rendre au bureau de vote le jour en question, je ne peux pas voter. Si je n'ai pas mon identité avec moi ou si je n'ai pas reçu de pièce d'identité de l'État, je ne peux pas voter. Si je termine mon bulletin de vote de manière incorrecte, mon vote ne sera pas compté et, dans certains scénarios, des problèmes techniques ou des erreurs de calcul signifient que les votes sont exclus. À la fin du jour du scrutin, je dois faire confiance aux travailleurs électoraux de tout le pays pour ne pas tricher et comptabiliser équitablement les votes. Dans les pays où un dictateur est au pouvoir ou où les institutions ne sont pas fortes, les élections peuvent être truquées sans recours pour les électeurs. Les développeurs de Blockchain espèrent résoudre ces problèmes avec des contrats de vote intelligents via un registre distribué sur la Blockchain. L'idée est simple: créer un réseau peer-to-peer où les individus peuvent soumettre leurs votes sans avoir besoin de faire confiance à la commission électorale ou d'être là en personne. Cependant, la mise en œuvre est difficile. Comment vérifiez-vous l'identité? Comment empêchez-vous les gens de voter plus d'une fois? Si le registre est sur la Blockchain, comment gardez-vous les votes anonymes? Il faudra une cryptographie intelligente avant que nous ayons un vote basé sur la Blockchain, mais les implications sont énormes. Dès que voter devient aussi simple que de se connecter sur son téléphone ou son ordinateur et de voter, la démocratie directe et les référendums publics fréquents deviennent plus réalisables. Les décisions politiques pourraient être prises par les masses. En fait, vous pouvez voter plusieurs fois par jour sur les référendums dans votre ville.

Bien qu'il faille du travail pour s'assurer que les experts rédigent et examinent les politiques sur lesquelles le public vote, il n'est pas loin de penser que la gouvernance pourrait devenir plus agile et plus réactive grâce à la Blockchain.

Crowdfunding & ICOs

Le crowdfunding, ou financement participatif, est un exemple de service utilisant des contrats intelligents. Nous avons l'habitude de penser aux campagnes Kickstarter, et l'idée est assez simple. Les gens contribuent à une bonne idée. Lorsque l'idée atteint son objectif de financement, les créateurs de l'idée sont payés pour produire l'idée. S'ils n'atteignent pas l'objectif de financement, les bailleurs de fonds d'origine reçoivent leur argent.

Sur la Blockchain, toute la collecte de fonds, le calcul et le financement / retour d'argent sont automatisés et immuables dans un contrat intelligent. En tant qu'application décentralisée sur la Blockchain, il n'y a plus de Kickstarter en tant qu'intermédiaire. Au lieu de cela, le contrat intelligent décide du moment où une idée sera financée et les créateurs ne paient aucun frais pour le service. Récemment, le crowdfunding Blockchain a gagné en popularité pour financer de nouvelles idées de démarrage, menaçant le modèle traditionnel de financement de démarrage, de capital-risque, et les investisseurs institutionnels. Les fondateurs de start-up peuvent désormais proposer un type de véhicule d'investissement public, connu sous le nom d'offre initiale de pièces de monnaie (ICO), où chacun peut investir dans une idée en échange d'une participation à la croissance de l'entreprise. Alors que les ICO sont devenus incroyablement populaires et que beaucoup ont réussi, ils sont également largement non réglementés, ce qui en fait des investissements très risqués et soumis à des pratiques d'investissement douteuses comme la manipulation des prix à la pompe et à la décharge.

Les Assurances

L'assurance automobile est un autre exemple de contrat intelligent potentiel. Avec la croissance de minuscules capteurs et appareils dans nos voitures, nous ne sommes pas loin de pouvoir détecter quand vous avez été dans un accident et envoyer ces informations à une application décentralisée sur la Blockchain. Lorsqu'elle est intégrée à l'intelligence artificielle, à la vision par ordinateur et aux capteurs intelligents dans votre voiture, l'application Blockchain peut prendre une décision si vous êtes en faute et payer la réclamation en quelques secondes, tant que vous payez vos primes chaque mois. Maintenant, il n'y a plus de compagnie d'assurance pour les frais généraux, et l'application d'assurance Blockchain n'essaie pas de gagner de l'argent, donc vos primes mensuelles ne sont que ce qu'elles doivent être.

L’identité Et L’identité Des Choses

Le registre distribué de Blockchain peut également héberger des informations sur l'identité.

Au lieu de compter sur des institutions centralisées pour délivrer des pièces d'identité nationales, des permis de conduire, des passeports, des certificats, des diplômes et des comptes, la Blockchain peut faciliter une identité transparente tout-en-un. La sécurité de la Blockchain signifierait que vos transactions restent anonymes par défaut. Cependant, vous pouvez choisir de partager des informations d'identité dans le cadre de l'exécution d'un contrat intelligent. Au fil du temps, nous pourrions normaliser l'identité et la citoyenneté mondiales sur la Blockchain pour chaque personne vivante.

Конец ознакомительного фрагмента.