Blockchain et Distributed Ledger Technology - Transformer le Monde Financier

Souvent dans l'actualité, Blockchain est appelé à transformer le fonctionnement des marchés financiers, en révolutionnant l'industrie dans tous les secteurs.

Elementum Metals: 25/02/2021

25/02/2021

Pour accompagner notre conférence en ligne sur le secteur émergent des chaînes de production, nous avons répondu à quelques questions que notre public nous a posées, englobant les questions techniques, la comparaison et les contrastes, et même l'influence des mèmes sur Internet. Vous avez une autre question pour notre équipe ? Utilisez notre page de contact pour nous contacter.

Quelles sont les différences entre les Blockchains publics, privés et autorisés ?

Blockchain public : Il s'agit d'un Blockchain où tout le monde peut rejoindre et participer aux activités du réseau Blockchain. Ces chaînes sont décentralisées, ce qui signifie qu'aucune entité ne peut contrôler le réseau. Les exemples les plus connus sont ceux de Bitcoin et Ethereum.
Blockchain privé : Une chaîne de blocage qui permet uniquement aux membres autorisés de rejoindre le réseau. L'opérateur a le droit d'outrepasser, de modifier ou de supprimer les entrées nécessaires sur la chaîne de blocage. Il s'agit d'une centralisation. Les exemples comprennent Ripple et Hyperledger.
Chaîne de blocage autorisée/hybride : possède les propriétés des chaînes de blocage privées et publiques. Ils deviennent de plus en plus populaires en raison de leur capacité à attribuer des autorisations spécifiques à de divers utilisateurs sur le réseau. Cela varie d'une plate-forme à l'autre, et plusieurs sont beaucoup plus petites que les noms plus établis.

La thèse de l'investissement qui sous-tend la finance décentralisée est très solide : l'impression de monnaie sans précédent par les banques centrales conduira probablement à une

dépréciation, et une réserve de valeur non négligeable est un excellent moyen de s'en prémunir. Ma question est la suivante : pourquoi Blockchain ? Quels sont ses avantages par rapport aux autres réseaux de paiement sécurisés ? Dans le cas de Bitcoin, il semble maladroit - c'est une entreprise à forte intensité énergétique, à l'histoire tenace (marché noir), et le fait que chaque transaction doit être vérifiée par tout le monde semble inefficace ?

Une excellente question, avec quelques éléments de réponse. Premièrement, pourquoi utiliser Blockchain pour les paiements ? La Blockchain est immuable, démocratique, décentralisée et écrite dans un code qui ne peut être modifié. Cela lui confère un avantage inattaquable par rapport aux autres réseaux de paiement sécurisés (Stripe, Apple Pay, etc.), qui sont fondamentalement centralisés. Si j'effectue un paiement en utilisant une de ces sociétés, cette transaction est vérifiée, approuvée et gérée par cette seule société centralisée. Cela peut être associé à des risques de sécurité (une seule cible centralisée pour les pirates), à des coûts plus élevés (un seul organisme centralisé peut facturer des frais sur les transactions) et à des conditions non démocratiques (une seule société centralisée peut fixer ses propres conditions).
La chaîne de blocage, en revanche, permet de construire l'infrastructure à partir de la base. Cela signifie que vous concevez et définissez l'économie et l'offre monétaire une fois au début, et que personne ne peut "imprimer" de l'argent supplémentaire à un stade ultérieur - cela contribue à l'avantage de "réserve de valeur" que vous mentionnez. Bitcoin a essayé de le faire (son offre est limitée à 21 millions de bitcoins qui peuvent être extraits), mais comme vous le dites, cela est associé à de nombreuses inefficacités, notamment l'utilisation intensive d'énergie nécessaire pour extraire les pièces (voir la question 4 ci-dessous pour en savoir plus). Le fait que chaque transaction doit être vérifiée par d'autres utilisateurs ne doit cependant pas être considérée comme l'une de ces inefficacités, mais plutôt comme une force du système - elle permet d'éviter la nécessité d'une plateforme centralisée (et donc vulnérable et potentiellement coûteuse) inhérente aux autres systèmes de paiement sécurisé.
Bien que vous avez raison de signaler l'histoire du marché noir de Bitcoin, il s'agit davantage d'un reflet des activités des premiers utilisateurs que d'un signe de faiblesse - peu de gens pourraient soutenir que la monnaie physique devrait être totalement écartée parce qu'elle a été utilisée pour des raisons malveillantes dans le passé.
Alors, qu'est-ce qui pourrait exister d'autre ? De nouveaux concepts de paiement basés sur la chaîne de paiement apparaissent, tant pour les paiements de gros que de détail, certains étant décentralisés, d'autres plus centralisés. En voici quelques exemples :

- Ripple : utilisé pour les paiements interbancaires et transfrontaliers décentralisés, il permet de régler des transactions en 3 à 5 secondes dans le monde entier et de traiter 1 500 transactions par seconde grâce au XRP.
- Diem (ex-Libra pour le commerce de détail) : Un système de paiement Blockchain autorisé, proposé par Facebook.
- CBDCs (Central Bank Digital Currencies) : Elles apparaissent dans le monde entier, la Chine ayant lancé la première monnaie numérique de banque centrale au monde, connue sous le nom de DCEP, qui est une version numérique du yuan, garantie par des dépôts en yuan à la Banque centrale de Chine.

En conclusion, vous avez donc raison de dire que Bitcoin est un système maladroit qui présente des inconvénients évidents et de plus en plus médiatisés (il reste à voir s'ils peuvent être corrigés). Toutefois, la technologie qui sous-tend Bitcoin, c'est-à-dire la chaîne de blocs, permet une efficacité bien plus grande que d'autres systèmes de paiement plus familiers qui ont été développés au cours des deux dernières décennies.

Quelle est la distinction entre la "preuve du consensus des enjeux" utilisée apparemment dans les nouvelles chaînes de blocs / crypto-monnaies et celle utilisée pour les bitcoins ("preuve de travail") ?

Le mécanisme de preuve de travail (PoW) est utilisé pour sécuriser la chaîne de blocage des bitcoins et pour créer un consensus. Il fonctionne en faisant en sorte que tous les nœuds (participants/dispositifs) du réseau résolvent des algorithmes mathématiques (afin de vérifier la légitimité de la transaction), le premier nœud trouvant une solution étant récompensé (la récompense du mineur est un certain nombre de Bitcoins). Le PoW offre des avantages supplémentaires en matière de sécurité à Blockchain, car il ralentit la création d'un nouveau bloc à environ 10 minutes, ce qui signifie que si un pirate veut falsifier un bloc, il doit refaire le PoW de chaque bloc du système, ce qui est presque impossible à faire en raison des échelles impliquées.
Les points négatifs associés au PoW sont cependant les suivants :
i. En raison des récompenses minières, des sociétés minières de plus en plus grandes sont créées, consommant de grandes quantités d'électricité (il a été récemment largement rapporté que l'exploitation minière de Bitcoin consomme autant d'énergie que l'ensemble de l'Argentine).
ii. Pour augmenter les chances de réussite de l'exploitation minière, les mineurs se regroupent en "pools miniers", ce qui rend en fait la chaîne du bloc plus centralisée, sapant

regroupent en "pools miniers") ce qui rend en fait la chaîne de bloc plus centralisée, sapant ainsi l'esprit de décentralisation de l'entreprise.
Dans les forums en ligne en 2011, un nouvel algorithme a été proposé, appelé "Preuve de l'enjeu" (Proof of Stake - PoS), où l'on utilise plutôt un processus d'élection dans lequel un nœud est choisi au hasard pour valider le bloc suivant. Au lieu de mineurs, il utilise des validateurs qui frappent et forgent de nouveaux blocs. Pour devenir un validateur, le nœud doit déposer un certain nombre de pièces comme enjeu (pensez à cela comme un dépôt de garantie). Plus vous "déposez", plus vous avez de chances de devenir un validateur. C'est plus juste que PoW, car PoW favorise ceux qui ont des économies d'échelle en termes de capital minier/énergie, alors que les barrières à l'entrée avec PoS sont comparativement plus faibles. Pour garantir des validations correctes, les validateurs perdront une partie de leur mise s'ils approuvent des transactions frauduleuses. Tant que cette perte est supérieure à leur récompense, le consensus se maintient grâce à la motivation par les prix. Enfin, le système de points de vente est plus décentralisé car il permet d'arrêter les gisements miniers et il est moins coûteux de créer un nœud dans la chaîne de points de vente.
Les inconvénients associés aux points de vente sont cependant les suivants :
i. 51% d'attaques : Contrairement aux PoW où vous devez acquérir 51% du réseau, pour les PoS vous devez acquérir 51% de la capitalisation boursière de la monnaie, ce qui pour les cryptocurrences à faible capitalisation boursière pourrait être relativement facile.
ii. Les algorithmes de PoS ne sont pas complètement aléatoires car ils dépendent de l'enjeu des validateurs (ce qui peut favoriser les individus les plus riches).
Pour l'instant, les PoS ne sont pas courants, bien qu'il soit prévu que le système soit utilisé dans Ethereum 2.0, qui sera publié en 2021.

Un commentaire sur Tesla et la décision d'acheter Bitcoin plutôt qu'une autre forme de bien numérique ? S'agit-il de pure spéculation ?

Du point de vue de l'entreprise Tesla, cela pourrait être une conséquence des taux d'intérêt négatifs et de la gestion de trésorerie qui cherche des moyens de diversifier la répartition des actifs. Du point de vue de Musk, il est difficile de dire quelle était sa motivation la plus profonde. Il a investi à la fois dans des Bitcoin et des Dogecoin, ce qui a provoqué une hausse des prix des deux cryptocurrences après l'annonce de ces achats sur Twitter.
Musk est assis dans un siège spécial, il peut essayer des technologies et des concepts qui suscitent une réaction positive du marché, indépendamment de toute raison économique ou commerciale. Les analystes de Wedbush Securities ont estimé que Tesla a déjà réalisé 1 milliard de dollars de bénéfices grâce à son investissement dans Bitcoin. L'entreprise est en passe de réaliser plus de bénéfices grâce à ses investissements dans Bitcoin que de vendre des VE en 2020.
Quant au choix de Bitcoin et Dogecoin par rapport aux autres cryptocurrences, les choses sont moins claires. Bitcoin est de loin le choix le plus important et le plus évident, peut-être donc perçu comme étant moins risqué, alors que Musk lui-même a souvent cultivé l'image d'être branché sur la culture en ligne - Dogecoin, ayant été initialement issu de mèmes internet (ainsi que d'une capitalisation boursière de plusieurs milliards) pourrait être interprété comme en faisant partie. Il convient de noter, cependant, qu'il n'est pas le seul personnage de premier plan à soutenir publiquement la crypto-monnaie : les entrées revendiquées des musiciens Gene Simmons et Snoop Dogg ont également contribué à susciter de l'intérêt.

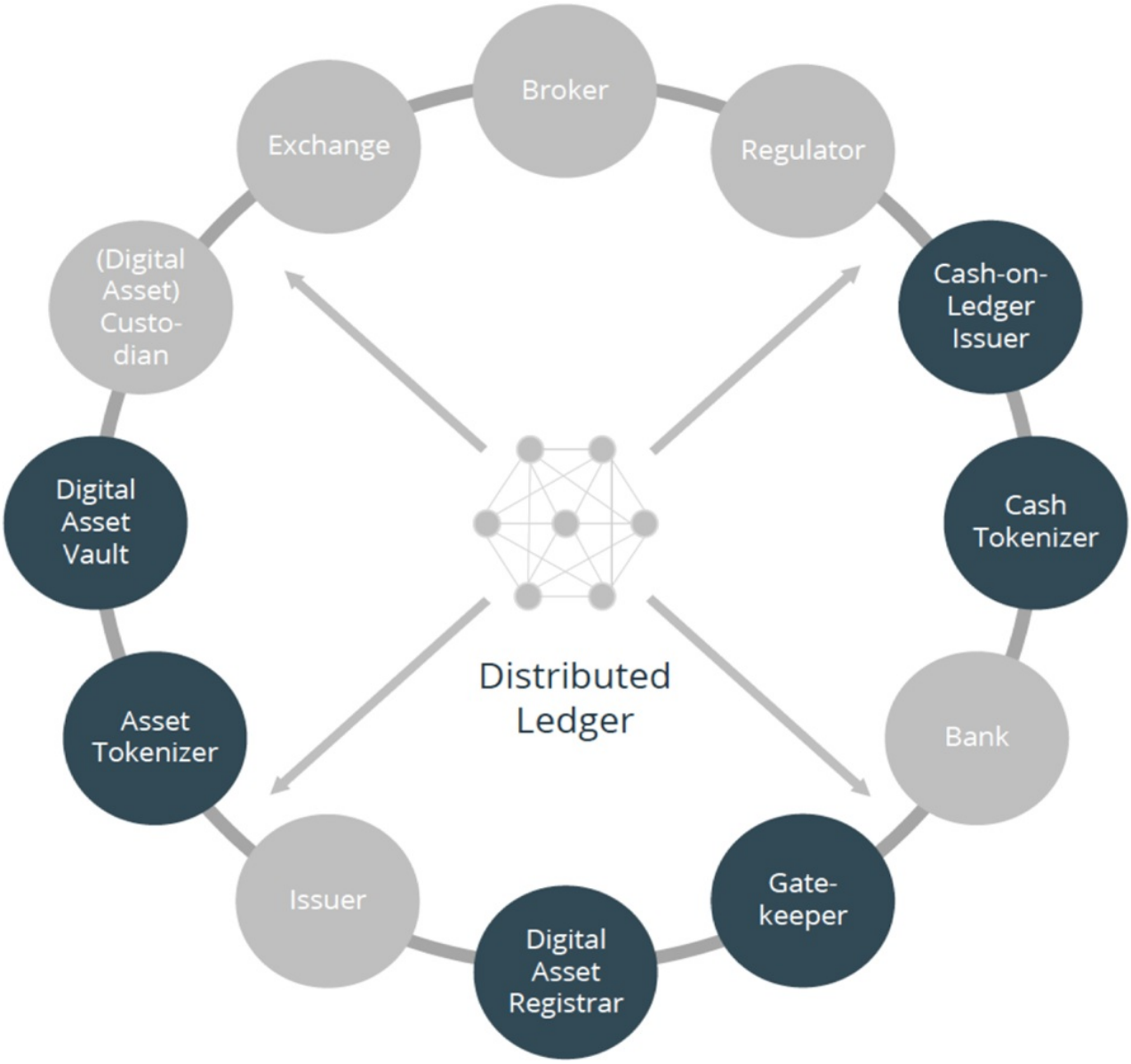
Quelle est la capitalisation boursière des protocoles de

financement décentralisé ?

En février 2021, la capitalisation boursière est de 45 milliards USD.

En quoi le rôle du "Distributed Ledger Technology" (DLT) sur les marchés des capitaux diffère-t-il de celui des bourses traditionnelles ?

Les bourses traditionnelles présentent un mode de communication et d'échange d'informations bilatéral et séquentiel. DLT a déjà commencé à restructurer les chaînes de valeur des marchés des capitaux en modifiant les hypothèses traditionnelles et en créant la confiance sans opérations humaines.
DLT peut apporter une valeur ajoutée aux marchés des capitaux grâce à :
i) Au partage de l'information entre tous les participants - en réduisant les coûts de rapprochement
ii) Aux contrats intelligents - Élimination du risque de contrepartie
iii) À la piste d'audit immobile - amélioration de la réglementation
iv) Aux processus numérisés - Permettant une automatisation pure
La plupart des rôles traditionnels sur les marchés de capitaux, tels que les courtiers, les bourses et les dépositaires, continueront d'exister sur un marché de capitaux DLT. Toutefois, de nouveaux rôles seront nécessaires en plus des rôles traditionnels. Le diagramme ci-dessous illustre ce point :



Source: Tokentrust AG

Les caractéristiques, propriétés et entités modifiées comprennent :

- Les gardiens ont des coffres-forts pour les biens numériques où ils protègent les clés privées nécessaires pour accéder aux portefeuilles cryptés et donc aux biens.
- **Digital Asset Vault,** le logiciel acheté par les gardiens pour assurer le stockage des clés privées.
- **Asset Tokenizer**, qui permet des processus conformes à la loi en fournissant des contrats intelligents afin d'authentifier les instruments financiers au nom de l'émetteur.
- **Digital Asset Registrar**, qui facilite le consensus entre les différentes parties prenantes et régit le Digital Asset Registry en validant toutes les transactions sur la plateforme.
- **Gatekeeper**, qui accorde/restreint l'accès à la plateforme via des contrôles KYC/AML.
- **Cash on Ledger Issuer**, qui gère les contrats intelligents et initie les transactions fiat par la banque et valide les transactions cash on ledger.
- **Cash Tokenizer,** qui fournit l'infrastructure permettant d'émettre des espèces de grand livre garanties à 100% pour le règlement en chaîne (livraison contre règlement de paiement).
  Un exemple concret est celui de la Bourse de Thaïlande qui crée une plate-forme de tokenisation et d'échange d'actifs gérée par DLT. Informations adaptées d'ici.

Quel rôle jouent les monnaies numériques émises par les banques centrales (CBDC) pour la symbolisation des marchés de capitaux ?

La symbolisation répond au besoin d'un nouveau format dominant pour représenter les actifs et les droits, apportant plus de flexibilité et de liquidité. Comme la monnaie de banque centrale reste préférée pour les grandes transactions, les CBDC restent un moyen d'échange prometteur basé sur des jetons. Elles fonctionnent comme les monnaies fortes, mais avec des possibilités numériques. Les CBDC peuvent compléter la monnaie en circulation et servir d'alternative aux paiements par carte. En outre, elles peuvent faciliter la diversification des formats de paiement et permettre l'échange de jetons en monnaie de banque centrale, ce qui renforce la confiance dans la tokenisation. Enfin, les CBDC facilitent les relations de paiement direct, réduisant ainsi le besoin d'intermédiaires et donc les coûts de transaction élevés que nous observons traditionnellement sur les marchés de capitaux.

Compilé par Jay Kumar, NTree International, for Metal.Digital.