

La montée en puissance des crypto-actifs

Ce qu'ils sont, comment ils peuvent être utiles aux entreprises de services financiers et comment les concevoir



En 2009, le bitcoin était le seul crypto-actif sur le marché. Depuis, le bitcoin et la technologie de blockchain sur laquelle il repose ont conduit à l'émergence de nombreuses autres blockchains, chacune avec ses propres crypto-actifs. On estime qu'il existe aujourd'hui plus de 2 000¹ crypto-actifs. Chaque mois, de nombreux autres sont créés. Ces crypto-actifs - de nouveaux actifs numériques natifs tels que les crypto-monnaies ou des actifs traditionnels tokenisés comme l'immobilier et l'or - sont devenus une nouvelle classe d'actifs dont la valeur économique est détenue ou contrôlée par des particuliers, des entreprises ou des pays.

Alors, que sont exactement les crypto-actifs et d'où vient leur valeur ? Quelles sont les opportunités induites pour notre économie et nos entreprises ? Et comment bien les concevoir ? Dans ce livre blanc, nous démystifions la complexité de la conception des crypto-actifs et indiquons comment les entreprises de services financiers peuvent les exploiter à leur avantage.

En tant que classe d'actifs, les crypto-actifs sont équipés pour jouer un rôle important dans les économies d'aujourd'hui en révolutionnant notre façon de commercer. Ils permettent de développer de nouveaux modèles économiques et d'améliorer la gestion des actifs par la réduction des tensions et des frais généraux, par l'augmentation des liquidités, par la codification des règles et réglementations, et par l'augmentation de la transparence tout au long du cycle de vie des actifs.

Techniquement, un crypto-actif est la représentation numérique d'une valeur ou de droits garantis par contrat - généralement appelée « token » ou jeton - qui est sécurisée de manière cryptographique par des algorithmes. Le crypto-actif repose sur l'utilisation d'une blockchain (ou chaîne de blocs) ou d'une autre technologie de registre distribué (ou DLT pour Distributed Ledger Technology), et peut être transféré, stocké ou échangé de manière électronique².

Le crypto-actif hérite de toutes les bonnes fonctionnalités de la blockchain : programmable, ouvert, immuable, ne connaît pas les frontières, décentralisé, n'a pas besoin d'autorisation, disponible 24h/24. Il peut être utilisé par des humains ainsi que par des logiciels et des machines comme les appareils de l'Internet des objets (IoT), ce qui permet de transformer n'importe quel actif physique classique en un actif numérique.

Les tokens utilisant la blockchain peuvent représenter des actifs natifs nouveaux tels que le bitcoin ou des actifs non natifs qui sont adossés sur des actifs classiques comme ce qui suit (Voir **Figure 1**) :

- Les stablecoins représentant des monnaies fiduciaires, comme les tokens Tether adossés sur le dollar américain avec parité égale, et la Libra, la future pièce de Facebook adossée sur un panier de devises.
- Des métaux, comme le DGX de Digix qui représente un gramme d'or placé dans une chambre forte.
- L'immobilier - Les propriétaires émettent des tokens sur des plates-formes reposant sur une blockchain ; ceux-ci représentent un nombre de parts d'actifs immobiliers tels que ceux émis via les startups Harbour, Galaxy Digital Holdings, Propellr, Fluidity et Blockchain App Factory.

¹ <https://coinmarketcap.com/>

² Taskforce, C. (2018). Cryptoassets Taskforce: final report. HM Treasury, Financial Conduct Authority et Bank of England.

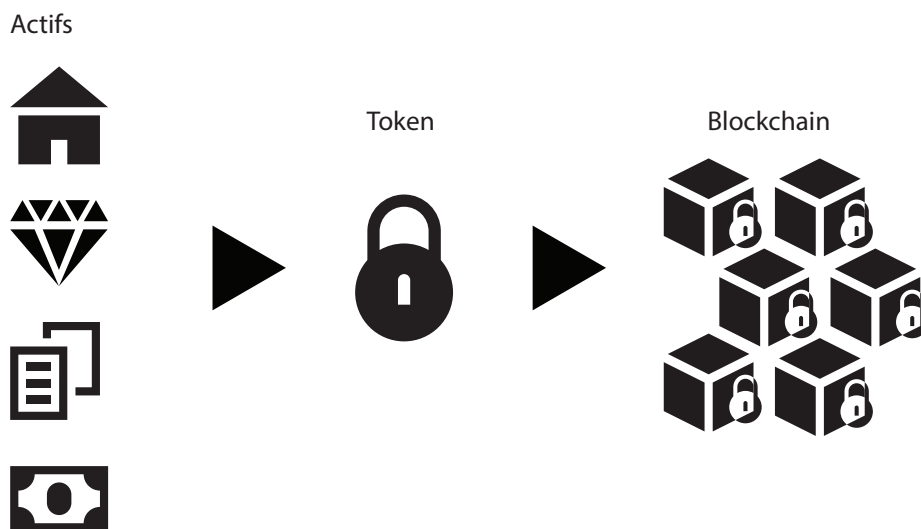


Figure 1. Tokenisation d'actifs

Bouleverser les échanges avec les tokens

Les transactions sur les marchés de capitaux impliquent des processus de négociation, de compensation et de règlement, et de nombreux tiers - courtiers, plates-formes de négociation, chambres de compensation, agents de règlement, dépositaires et émetteurs, comme le montre la **Figure 2**. Il est coûteux et complexe de mettre en place et de diriger ces organes tiers. Il est nécessaire également d'avoir des processus longs et complexes pour garantir l'intégrité et la protection des parties prenantes. Le coût d'un premier appel public à l'épargne (ou IPO pour Initial Public Offering), par exemple, peut atteindre plus d'un million de dollars³, avec un coût annuel récurrent pouvant atteindre 1,9 million de dollars.

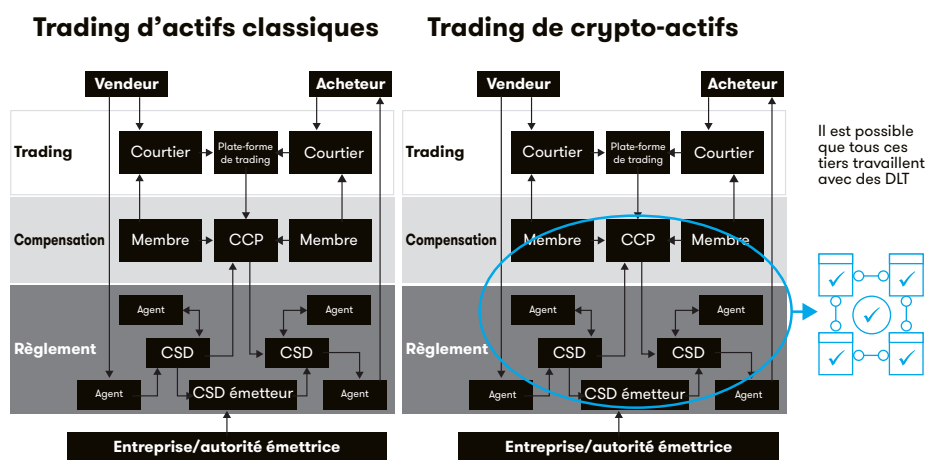


Figure 2. Trading d'actifs classiques contre crypto-actifs⁴

³ PWC. (6 août 2017). Considering an IPO to fuel your company's future? Disponible à l'adresse <https://www.pwc.com/us/en/services/deals/library/cost-of-an-ipo.html>

⁴ Pinna A. et Ruttenberg W. (Avril 2016). Distributed ledger technologies in securities post-trading. Revolution or evolution? Banque centrale européenne. Collection Occasional Paper. No.172.

La blockchain permet de réduire les coûts et de rationaliser les processus de compensation et de règlement en remplaçant les tiers et en éliminant le besoin de les avoir, ou en réduisant leurs fonctions, tout en maintenant l'intégrité et les protections. Elle favorise également le trading décentralisé, soit en peer-to-peer ou par le biais d'échanges décentralisés.

Il est possible, grâce à cette technologie, de facilement établir, confirmer ou transférer la propriété d'un actif dans la blockchain. Le règlement réel peut être effectué immédiatement ou presque en temps réel si les actifs sont natifs. Pour les actifs non natifs, il peut être nécessaire d'avoir recours à un dépositaire ou un agent de règlement pour prendre en compte/appliquer le règlement final.

Le tableau qui suit propose un comparatif entre actifs classiques et crypto-actifs, et présente les principaux intervenants dans la chaîne de valeur des échanges :

Activité	Trading d'actifs classiques (actions par ex.)	Trading de crypto-actifs non natifs (actifs hors blockchain tels que tokens STO)	Trading de crypto-actifs natifs (dans blockchain comme le bitcoin ⁵)
Trading	Échanges centralisés	<ul style="list-style-type: none"> • Trading en peer-to-peer • Échanges de STO centralisés • Échanges de STO décentralisés 	<ul style="list-style-type: none"> • Trading en peer-to-peer • Échanges centralisés • Échanges décentralisés
Compensation	Organes de compensation	Organes de compensation et protocole	Protocole logiciel
Règlement	Dépositaires/ Organes de règlement	Dépositaire hors blockchain et protocole	Protocole logiciel

Comment les crypto-actifs permettent d'améliorer les services financiers

La tokenisation des actifs dans les services financiers au moyen de blockchains peut révolutionner et résoudre les problèmes en matière de paiement, d'investissement, de trading et de mobilisation de capitaux. La tokenisation des actifs favorise les entreprises de services financiers :

- **Diminution de la tension et des frais généraux** associés à la création, au transfert et à la gestion d'actifs classiques tels que titres, matières premières et actifs immobiliers. La tokenisation permet d'éliminer de nombreux autres processus, de réduire les dépenses, et de faciliter le commerce et le règlement des actifs en temps réel.

⁵ Pinna A. et Ruttenberg W. (Avril 2016). Distributed ledger technologies in securities post-trading. Revolution or evolution? Banque centrale européenne. Collection Occasional Paper. No.172.

- **Augmentation des liquidités** par le biais de la conception de crypto-actifs divisibles pour l'immobilier ou d'autres actifs classiques, et de leur ample mise à disposition sur les plates-formes de trading. Les crypto-actifs divisibles impliquent qu'un grand nombre de personnes peuvent chacune posséder une fraction d'une propriété ou d'un autre actif. De plus, les actifs tokenisés disponibles sur un marché sont facilement disponibles pour être échangés sur d'autres marchés. En fait, les lieux d'échanges partagent généralement leurs carnets de commandes avec les fournisseurs de liquidités, lesquels ensuite permettent la mise à disposition des actifs sur les marchés mondiaux. Les informations sur le prix des actifs circulent dans les lieux d'échanges plus rapidement et plus efficacement. De meilleurs prix en résultent parce que les écarts entre offres de vente et offres d'achat se réduisent et parce que la recherche des prix est améliorée.
- **Simplification des procédures visant le respect de la réglementation** par l'automatisation des règles et par leur application via le biais d'un code dans les contrats intelligents dans la blockchain. Le respect des règles, complexe et coûteux à imposer dans le monde physique - par exemple, limiter le nombre de propriétaires et le nombre de parts qu'ils peuvent posséder, faire respecter leurs droits en conséquence - est facile à imposer dans un contrat intelligent dans une blockchain.
- **Augmentation de la transparence** tout au long du cycle de vie de l'actif par la mise en avant de la confiance et de la transparence inhérentes à la blockchain. Les transactions en blockchain sont disponibles, vérifiables et auditable. Dans les blockchains publiques sans autorisations, le registre des transactions est accessible à n'importe quel utilisateur. Dans les blockchains privées avec autorisations, il n'est accessible qu'aux participants dans le réseau.
- **Création de modèles économiques et d'incitations** par la virtualisation de n'importe quelle valeur ou activité intéressante et par la facilitation des transferts entre les participants, ce qui les encourage à créer plus de valeur. De plus, créer des tokens en plus d'un réseau décentralisé permet d'éliminer les tiers traditionnels et de perturber leurs modèles. Le BAT (ou Basic Attention Token), par exemple, vise à troubler le monde de la publicité numérique traditionnelle⁶ en faisant de la valeur - ici, l'attention des utilisateurs - un élément à échanger entre pairs - les publicateurs, les annonceurs et les utilisateurs.

Prendre en compte le contexte

Concevoir un nouveau crypto-actif ou tokeniser des actifs classiques est complexe et nécessite de prendre en compte les problématiques commerciales, juridiques et technologiques.

Les problématiques commerciales

Comprendre les problèmes que permet de régler la tokenisation est essentiel pour concevoir le rôle du nouveau crypto-actif et ses usages. D'importantes entreprises évoluant dans le secteur des services financiers ont classé les crypto-actifs dans trois catégories⁷ conformément aux rôles qu'ils jouent (Voir **Figure 3**) :

⁶ Logiciel Brave. (13 mars 2018). Basic Attention Token (BAT) Blockchain Based Digital Advertising. Disponible sur le site Basic Attention Token : <https://basicattentiontoken.org/>

⁷ Taskforce, C. (2018). Cryptoassets Taskforce: final report. HM Treasury, Financial Conduct Authority et Bank of England.

- **Crypto-actifs d'échange** tels que le bitcoin et le litecoin, également appelés crypto-monnaies. Ils sont principalement utilisés comme moyen de paiement, pour acheter et vendre des biens et des services, pour faciliter les règlements décentralisés entre pairs, ou comme investissement.
- **Crypto-actifs de sécurité** sont principalement utilisés comme des placements faits et échangés en vue de gains en capital. Ils représentent une propriété, des actions ou d'autres droits liés à un investissement. On les utilise comme outils pour lever des capitaux pour acheter des actions.
- **Crypto-actifs utilitaires** sont principalement utilisés pour accéder à des services spécifiques fournis ou hébergés sur une plate-forme de blockchains. Considérez-les comme une clé API payante (mais pas comme une API). Vous pouvez acheter une clé API auprès d'Amazon Web Services, puis échanger cette clé API contre du temps sur le cloud d'Amazon. De même, sur une blockchain comme Ethereum, vous pouvez utiliser un crypto-actif utilitaire pour accéder à une plate-forme informatique décentralisée.

Certains crypto-actifs peuvent être classés dans plusieurs catégories, ce conformément aux utilisations qui en sont faites. Par exemple, certains crypto-actifs couramment utilisés pour les paiements sont également utilisés pour les investissements. Le réseau public ouvert de blockchains d'Ethereum, qui donne accès à une plate-forme informatique décentralisée pour avoir des contrats intelligents comme un utilitaire pour émettre des offres, est également utilisé pour les paiements et, dans certains cas, pour les investissements.

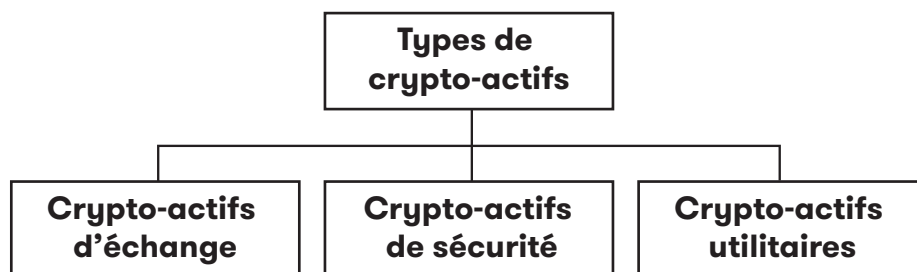


Figure 3. Classifications des crypto-actifs

Les problématiques juridiques

Concevoir des crypto-actifs nécessite de s'interroger sur les cadres réglementaires en place, sur la propriété des actifs, et sur le lieu où les actifs seront émis et échangés. Certaines réglementations ont une portée mondiale, la loi relative à la lutte contre le blanchiment d'argent et le financement du terrorisme par exemple, et concernent tous les types de services financiers. Certaines autres réglementations varient en fonction du type de token, de son utilisation et de l'endroit où se trouve son propriétaire ou l'entité gérant l'actif.

Les problématiques technologiques

Prendre en compte les problématiques technologiques est crucial pour la réussite du nouveau crypto-actif. Il est nécessaire de prendre d'importantes décisions en matière technique : évaluation et sélection des technologies/fournisseurs, conception et mise en œuvre de la solution, etc. Concevoir des crypto-actifs nécessite de faire des compromis sur trois plans, celui de la performance, celui de la résilience et celui de la confidentialité. Ces décisions peuvent imposer de privilégier⁸ l'une des dimensions plutôt que les deux autres :

- **La résilience plutôt que la performance.** Un réseau de blockchains augmente sa résilience contre les pannes et les attaques en ajoutant plus de nœuds à son réseau. Ceci permet de bénéficier d'une redondance parce que les données sont disponibles dans plusieurs nœuds, mais cela se fait au détriment de la performance.
- **La confidentialité plutôt que la performance.** La confidentialité dans les blockchains s'opère en limitant la distribution des données dans le réseau : (1) par la création de différents sous-registres disponibles pour un nombre limité de participants ou (2) par la mise en œuvre d'algorithmes de chiffrement gourmands en calcul. Dans les deux cas de figure, la performance du réseau est impactée négativement.
- **La confidentialité plutôt que la résilience.** La résilience dans les blockchains est mieux assurée lorsque toutes les données sont disponibles dans un grand registre commun accessible à tous les participants par le biais d'un grand nombre de nœuds. Limiter l'accès pour favoriser un cadre permettant de satisfaire aux exigences en matière de confidentialité nécessite d'avoir différents sous-registres et/ou des algorithmes de chiffrement complexes qui impactent négativement la résilience du réseau dans sa capacité à faire face aux pannes et aux attaques.

Plusieurs étapes mènent à la réussite

Dans le cadre du développement des crypto-actifs, une approche par étapes permet de répondre méthodiquement et de manière approfondie aux objectifs et exigences en matière commerciale et technique. Il y a cinq phases principales (Voir **Figure 4**).



Figure 4. Les cinq phases de l'élaboration d'un crypto-actif

Étape 1 : Déterminer la vision et les objectifs stratégiques

Élaborer une vision et comprendre les objectifs stratégiques implique d'identifier les objectifs des crypto-actifs et les fonctionnalités nécessaires à leur mise en œuvre.

1. Déterminer le type de crypto-actif et ses objectifs. S'il s'agit d'un crypto-actif d'**échange** pour faciliter un paiement, posez les questions :
 - Est-ce pour un paiement pour du gros ou du détail ?
 - Est-ce que cela fonctionnera avec les systèmes de paiement classiques, tels que les règlements bruts en temps réel, les systèmes d'alimentation améliorés et les systèmes de compensation automatisés, ou avec les systèmes et réseaux cryptographiques publics tels que le bitcoin et Ethereum ?

⁸ Taskforce, C. (2018). Cryptoassets Taskforce: Final Report. HM Treasury, Financial Conduct Authority et Bank of England.

La plupart des banques centrales envisagent les technologies de blockchain pour leurs projets de conception et d'implémentation de monnaies numériques pour les paiements. Et nombre de grandes sociétés de services financiers ont mis au point des stablecoins (une version numérique des monnaies fiduciaires).

S'il s'agit d'un crypto-actif de **sécurité** pour un investissement, posez les questions :

- Quel actif représente-t-il ?
- Est-il natif ou non natif ?
- Quel type de droits de propriété ou de parts représente-t-il ?

Nombre d'entreprises de services financiers sont en train de mettre au point des tokens de sécurité pour des applications diverses.

S'il s'agit d'un crypto-actif **utilitaire** posez les questions :

- Sera-t-il utilisé pour accéder à des produits ou services simples et spécifiques, tels que des ressources informatiques de base - processeur, mémoire ou bande passante ?
- Ou sera-t-il utilisé pour accéder à un produit ou service complexe tel que ce qui relève de l'intelligence artificielle (IA), de la publicité, de la messagerie ou de la prévision sur les marchés ?

2. Établir quelles sont les principales utilisations - L'ensemble des séquences d'interaction possibles entre les crypto-actifs et les utilisateurs pour atteindre un objectif particulier : paiement, investissement, accès ou collecte de fonds. Ces cas sont à la base de ce qui permet de déterminer toutes les actions ou événements qui définissent les interactions.

3. Examiner les principales fonctions.

- **Confidentialité.** Quelles sont les exigences en matière de confidentialité pour le nouveau crypto-actif ? Les transactions sont-elles publiques ou privées ? Si elles sont privées, sont-elles privées pour toutes les parties prenantes, ou y a-t-il des exigences en matière de confidentialité spécifiques pour chaque groupe de parties prenantes ? Par exemple, dans certains actifs numériques tels que les monnaies numériques des banques centrales, les régulateurs doivent pouvoir accéder à toutes les informations, tandis que d'autres parties prenantes ont un accès limité en rapport avec leurs transactions.
- **Processus d'émission d'actif.** Ce nouvel actif fera-t-il l'objet d'une émission publique ou privée ? L'émission publique de crypto-actifs s'effectue de deux manières :
 - » Par le biais d'un processus d'offre appelé soit offre initiale de pièces (ou ICO pour Initial Coin Offering), soit offre d'échange initiale (ou IEO pour Initial Exchange Offering), soit offre de jetons de sécurité (ou STO pour Security Token Offering), selon le type de crypto-actif et ses utilisations. Il existe de nombreuses différences entre ces processus d'offre, mais la plus importante relève de l'entité chargée de la gestion du processus : S'agit-il de l'entité qui crée l'actif (pour une ICO), d'une bourse où les actifs seront listés et échangés (pour un IEO) ou de l'autorité de régulation du marché des capitaux (pour une STO) ?

- » Par le biais du *minage*, un processus qui récompense les participants qui trouvent la réponse à un problème de calcul permettant de sécuriser le réseau avec des crypto-actifs nouvellement émis. Toutes les blockchains publiques de preuves de travail, le bitcoin entre autres, reposent sur le minage.

Les offres privées ou non publiques sont possibles et généralement effectuées avec des stablecoins et des monnaies numériques émises par une banque centrale. Certains crypto-actifs, tels que le Zcash, sont, au moment de leur émission, partiellement ouverts et partiellement privés.

- **Niveau de décentralisation.** Les crypto-actifs varient dans leur niveau de décentralisation. Il faut savoir dans quelle mesure les principales fonctions et fonctionnalités de l'actif sont distribuées ou déléguées et soustraites au participant central officiel dans le réseau de blockchains. Certains crypto-actifs, tels que le bitcoin, sont très décentralisés ; certains, comme les stablecoins, sont très faiblement décentralisés ; et d'autres, comme Ethereum, EOS et Ripple, sont entre les deux.

- **Offre d'actifs.** L'or et les autres actifs classiques utilisés pour garantir les crypto-actifs doivent être fixes et correspondre au montant des réserves sur lesquelles ils reposent. De plus, les émetteurs peuvent appliquer des frais d'émission ou des règles spécifiques.

Certains crypto-actifs publics financent leur développement ou leur communauté en prenant une partie des frais d'émission. Zcash, par exemple, collecte la « récompense du fondateur »⁹. Ainsi, depuis 4 ans, 10 % du total des 21 millions de tokens Zcash proposés vont aux fondateurs, le reste aux mineurs du réseau.

- **Autres fonctions.** En matière de crypto-actifs, les décisions concernent également :
 - » Le caractère fongible ou non fongible : La fongibilité implique que chacune des unités d'un crypto-actif est interchangeable et ses parties indiscernables.
 - » Le caractère divisible ou indivisible : Les actifs divisibles peuvent être divisés en unités plus petites. Certains actifs sont indivisibles, ceux utilisés dans les jeux notamment (CryptoKitties par exemple).
- **Échange d'actifs.** Si l'actif est échangeable, où va-t-il être vendu ? Où seront réalisées les procédures de compensation et de règlement ? Un tiers dépositaire peut-il être impliqué ?

⁹ Hopwood D., Bowe S., Hornby T. et Wilcox N. (19 mars 2018). Autorité de certification de Hyperledger Fabric. (2017). Disponible dans la documentation de Hyperledger Fabric : <https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/>

Étape 2 : Déterminer les exigences.

Après avoir défini la vision et les objectifs, il convient de clarifier les exigences. Les exigences fonctionnelles indiquent exactement comment exécuter chaque procédure dans le cycle de vie du crypto-actif :

- **Émission** : Comment l'actif va-t-il être émis ? De manière publique (ICO, IEO ou STO) ou de manière privée ? S'il est adossé à d'autres actifs, comment le processus de mise en gage garantira-t-il que la quantité émise correspond à la quantité nantie ou réservée ?
- **Transfert** : Quelle est la procédure de transfert entre participants ? Le transfert peut-il être lancé à partir de n'importe quel nœud participant ou uniquement à partir de nœuds spécifiques ? Y a-t-il des règles régissant les transferts ? Les transferts doivent-ils être approuvés ?
- **Échange** : Si les actifs sont échangeables, comment s'opérera le cycle de vente (échange, compensation et règlement) ?
- **Destruction** : Qu'arrive-t-il à l'actif lorsqu'il doit être détruit ? Les actifs adossés devront-ils être rachetés ?

Les considérations sans rapport avec les fonctions concernent la sécurité, la disponibilité, l'évolutivité et la performance.

La sécurisation des systèmes de crypto-actifs et du réseau de blockchains est particulièrement cruciale. Elle implique le contrôle de l'accès aux nœuds, la sécurité des contrats intelligents, la performance et l'évolutivité.

Étape 3 : Évaluer et choisir la technologie

Après avoir clarifié les objectifs et les exigences, il faut déterminer quelles technologies de blockchain correspondent le mieux aux exigences fonctionnelles et non fonctionnelles. Il est possible de construire de zéro une blockchain, mais ceci nécessite beaucoup d'efforts et de temps.

Les crypto-actifs qui nécessitent un niveau élevé de décentralisation peuvent être construits à partir des nombreuses blockchains publiques. Ces blockchains permettent d'atteindre une large palette d'objectifs et de spécifications.

Les systèmes de blockchains publiques sont soit sans autorisation, ce qui implique que n'importe qui peut participer (Bitcoin et Ethereum par exemple) ; soit avec autorisation (Ripple et EOS par exemple), ce qui implique qu'une autorisation doit être donnée par une ou plusieurs des entités qui dirigent le réseau.

Les blockchains privées et avec autorisation fonctionnent bien pour les crypto-actifs détenus par un petit groupe de participants qui ont besoin de confidentialité (les monnaies numériques d'une banque centrale par exemple). À l'heure actuelle, Quorum, Hyperledger Fabric et Corda dominent le marché des blockchains privées avec autorisation.

Étape 4 : Concevoir la solution

Développer une architecture pour les solutions de crypto-actifs nécessite de prendre des décisions concernant les composants sur plusieurs plans :

- **Respect de la vie privée et confidentialité.** De nombreuses technologies permettent de bénéficier de confidentialité dans les blockchains : Channels and Private Data Collections dans Hyperledger Fabric (HLF), Zero Knowledge Proof protocols (ZKP) dans Quorum ou Flows and Settler dans Corda.
- **Rôle des protocoles de consensus et des nœuds.** De nombreux protocoles de consensus existent et sont largement utilisés : Proof-of-Work (PoW), Proof-of-Stake (PoS) et Practical Byzantine Fault Tolerance (PBFT) par exemple. Chacun de ces protocoles convient à un ensemble spécifique de scénarios et de fonctions.
- **Protocoles de transfert d'actifs.** Le transfert de propriété des actifs peut être effectué de manière native dans la chaîne ou entre chaînes. Les transferts entre chaînes (appelés échanges atomiques) peuvent être conçus et mis en œuvre au moyen des protocoles HTLC (Hash Time Locked Contracts).
- **Garde et stockage d'actifs.** Il s'agit ici de savoir comment stocker et sécuriser les crypto-actifs. Les crypto-actifs adossés sur des actifs classiques peuvent nécessiter le recours à des prestataires de services de garde tiers.
- **Token ou compte.** Les blockchains utilisent le token ou le compte pour suivre le solde du crypto-actif et en prouver la propriété. La méthode reposant sur le token est plus évolutive et offre un niveau de confidentialité plus élevé, tandis que la méthode reposant sur le compte est plus adaptée dans les contextes où l'on a besoin de moins de confidentialité et de plus d'efficacité.
- **Contrats intelligents.** Les programmes de contrat intelligent contiennent le code qui exécute les fonctions et applique les règles régissant le crypto-actif. Pour ce qui est de la conception, ils sont donc l'élément le plus important.
- **Interface et portefeuille.** L'interface de l'application interagit avec la blockchain à l'endroit où les utilisateurs exécutent des fonctionnalités sur les crypto-actifs.
- **Sécurité.** En matière de sécurité, les principaux problèmes de conception relèvent, d'une part, des modalités d'autorisation des nouveaux nœuds dans le réseau. Le réseau peut reposer sur une infrastructure à clés publiques pour laquelle une autorité émet des certificats numériques pour les nœuds autorisés ; ou sur une liste blanche d'adresses de nœuds associée à un contrat intelligent. L'autre problème est en rapport avec les modalités de sécurisation des clés privées dans les nœuds participant au réseau. Il est courant dans le secteur d'imposer la mise en place de modules matériels de sécurité.
- **Intégration et API.** Il peut être nécessaire d'exposer les données des crypto-actifs au moyen d'API. Concevoir un crypto-actif comme un écosystème nécessite de rendre accessibles les spécifications du système aux autres utilisateurs, tels que développeurs, prestataires de services, agents de paiement et d'échange, pour qu'ils puissent créer d'autres produits et services en plus des nouveaux crypto-actifs.

Étape 5 : Mettre en œuvre la solution

La phase de mise en œuvre implique le développement et le déploiement des composants conçus, en s'assurant qu'ils sont testés et qu'ils répondent aux exigences fonctionnelles et non fonctionnelles de l'entreprise.

Les crypto-actifs ont le potentiel d'offrir des avantages significatifs aux entreprises de services financiers : nouveaux modèles économiques, rationalisation des processus, simplification des procédures visant le respect réglementaire, diminution du nombre de tiers impliqués, réduction des coûts et augmentation de la transparence.

Cependant, concevoir ces nouveaux actifs est complexe et nécessite de traiter nombre de problématiques commerciales, techniques et juridiques. Il faut également prendre des décisions difficiles, des décisions qui impliquent de possibles compromis en matière de performance, de résilience et de confidentialité.

Pour les entreprises, adopter une approche progressive pour la conception et la mise en œuvre de crypto-actifs permet de voir clairement la démarche et d'agir sur tous les nombreux aspects du projet.

Un monde de possibilités

Les possibilités liées à la tokenisation des actifs classiques, ou même celles liées au développement de nouveaux crypto-actifs, sont immenses. Quand les avantages et les utilisations potentielles sont conformes aux objectifs de l'entreprise, il est judicieux pour les sociétés de services financiers d'entrer dans le monde passionnant et nouveau des blockchains et des crypto-actifs.

L'auteur



Alsayyed Haiyan, spécialiste des FinTech et des blockchains chez DXC Technology, offre des services de conseil en matière de conception et de mise en œuvre des crypto-monnaies et des crypto-actifs, de monnaies numériques des banques centrales, de crowdfunding, de trading sur le marché de la crypto, d'investissement, de paiement et de réglementation du secteur des FinTech.

 **Pour recevoir une information vraiment intéressante :**
www.dxc.technology/optin

À propos de DXC Technology

DXC Technology, le leader mondial des services informatiques, gère, modernise les systèmes essentiels et y intègre les nouvelles solutions numériques pour favoriser la réussite de ses clients. Grâce à une présence mondiale, des collaborateurs partout sur la planète, des plates-formes innovantes, une indépendance technologique et un vaste réseau de partenaires, DXC donne à plus de 6 000 clients, des entreprises évoluant dans les secteurs privé et public dans 70 pays, les moyens de prospérer en se transformant. Rendez-vous sur www.dxc.technology pour de plus amples informations.