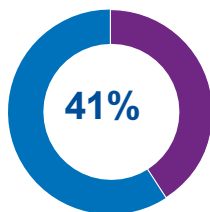


# Blockchain

## KPMG technology risk insights

### Qu'est-ce que la blockchain ?

La blockchain est un système dans lequel un enregistrement des transactions est conservé sur plusieurs ordinateurs (nœuds) qui sont reliés dans un réseau peer-to-peer. Elle supprime le besoin d'intermédiaires tels que les banques ou les courtiers pour servir de tierce partie.



41 % des chefs d'entreprise estiment que leur société aurait dû investir davantage dans la blockchain au cours des cinq dernières années.<sup>1</sup>

\$19b

Les dépenses mondiales en solutions blockchain ont été prévues à 19 milliards de dollars d'ici 2024.<sup>2</sup>

### Comment fonctionne la blockchain ?

#### Cryptographie



Une blockchain est une chaîne de blocs contenant des informations sur les transactions :

- Chaque bloc de données contient une clé de hachage unique, qui est comme une empreinte digitale, utilisée pour identifier un bloc et son contenu.
- Chaque bloc contient des transactions, un hachage et une copie du hachage du bloc précédent (à l'exception de le bloc de genèse, qui n'a pas de hash de bloc précédent). Ce concept rend la blockchain immuable. Si les données d'un bloc précédent sont modifiées, son hachage change, ce qui le déconnecte de la chaîne en cours de blocs.

#### Grand livre distribué



Au lieu de s'appuyer sur une autorité centrale pour gérer le grand livre, les blockchains utilisent un système d'échange de données.

réseau distribué d'égal à égal :

- Lorsqu'une personne rejoint le réseau, elle télécharge une copie complète de la blockchain. Chaque nouvel utilisateur, ou ordinateur, du réseau est appelé un nœud.
- L'architecture distribuée pair-à-pair offre une plus grande disponibilité que les réseaux traditionnels basés sur le client-serveur, car il n'y a pas de point de défaillance unique.

#### Consensus



Les nouvelles transactions sont envoyées à tous les nœuds, qui reçoivent alors des validées et regroupées en blocs :

- Le consensus garantit que les pairs du réseau s'accordent sur un état cohérent des enregistrements.
- Une fois le consensus atteint, le nouveau bloc est publié sur la blockchain de chaque nœud.
- Les nœuds rejettent les blocs dont les données violent les règles du protocole ou semblent avoir été altérées.
- Les mécanismes de consensus les plus courants sont la preuve de travail (PoW) et la preuve d'enjeu (PoS).

#### Contrats intelligents



La principale différence entre un contrat traditionnel et un contrat intelligent est que les contrats intelligents sont automatisés :

- Un contrat est créé entre les parties.
- Les parties peuvent choisir de rester anonymes.
- Des déclencheurs prédéfinis sont activés.
- Le contrat s'exécute tel qu'il est défini dans le code source.
- Un participant peut analyser toutes les activités et prendre des décisions en connaissance de cause.
- Les données saisies peuvent être utilisées à des fins d'analyse et d'établissement de rapports.
- Les données sont introduites dans les blockchains et utilisées pour l'exécution des contrats intelligents à partir de sources externes, en particulier les flux de données et les API ; une blockchain ne peut pas directement "récupérer" des données. Ces flux en temps réel sont appelés "oracles" et fonctionnent comme un logiciel intermédiaire entre les données et les contrats intelligents.

Sources d'information

<sup>1</sup> AP News, "CFOs Are Ready for Digital Transformation in 2021, New Survey Shows," février 2021

<sup>2</sup> Yahoo ! Finance, "Global Spending on Blockchain Solutions Forecast to be Nearly \$19 Billion in 2024, According to New IDC Spending Guide", avril 2021.

# Principaux risques liés à la blockchain

L'adoption de la technologie blockchain illustre l'investissement d'une entreprise dans l'innovation, mais l'innovation s'accompagne de nouveaux risques.

Pour exploiter pleinement le potentiel des technologies des grands livres distribués, les organisations doivent identifier et atténuer de manière proactive tous les risques liés à l'adoption de ces technologies.

KPMG est là pour vous aider à maximiser l'investissement de votre entreprise tout en vous aidant à gérer les risques potentiels.

## Gouvernance



- Conception et normes de la blockchain
- Politiques et procédures
- Gestion des fournisseurs
- Gestion de l'identité et de l'accès
- Réglementation et conformité
- Provenance des actifs
- Lutte contre le blanchiment d'argent
- Sanctions

## Infrastructure



- Risques liés au réseau Blockchain
- Vulnérabilités des logiciels
- Gestion du protocole
- Intégration
- Interopérabilité
- Gestion des nœuds
- Mécanisme de consensus

## Données



- Gestion des données
- Gestion de la vie privée
- Reprise après sinistre
- Gestion de l'information hors chaîne
- Bloom de la blockchain
- Intégrité des données
- Connaître son client

## Gestion des clés



- Gestion des clés publiques et privées
- Entropie
- Sécurité des clés/protocoles
- Le sharding
- Multi-sig
- Gestion du portefeuille
- Accès au module de sécurité matériel (HSM)

## Contrats intelligents

- Développement de contrats intelligents
- Conception de contrats intelligents
- Examen et maintenance du code
- Risques de déni de service
- Risque lié aux sources externes
- Risques juridiques



## Développement



- Normes insuffisamment développées :
  - Actuellement, la blockchain ne dispose pas de normes appropriées en raison de sa croissance rapide. Différentes organisations travaillant sur leur "propre" blockchain, il est difficile de les normaliser.
- La normalisation entre les industries et les blockchains :
  - La grande variété de cadres signifie qu'il y a un manque de normalisation. C'est potentiellement l'un des plus grands risques que les projets de blockchain actuels. Ces normes s'appliquent à l'ensemble de l'écosystème de la blockchain, y compris les Initial Coin Offerings, les crypto-monnaies, les cadres de travail et les systèmes d'information, et ainsi de suite.
- Intégration et interopérabilité dans les systèmes existants et entre les blockchains
- Code non testé :
  - La qualité du code reste une préoccupation majeure à la plupart des solutions de blockchain. Les organisations décentralisées doivent faire preuve d'une grande prudence lorsqu'elles déploient leurs solutions. L'organisation autonome décentralisée (DAO) en est un exemple. Il s'agit d'un système autonome qui automatise l'ensemble de l'organisation.
  - Le piratage de la DAO est l'un des plus tristement célèbres des piratages concernant la technologie blockchain. Créé en 2016 et connu sous le nom de "The DAO", l'incident a entraîné la perte d'environ 50 millions de dollars d'Ether à la suite d'une exploitation du code source ouvert.\*

\*A \$50 million hack just shown that DAO was all too human, Wired, June 18, 2016.

Les cas d'utilisation de la blockchain s'étendent à tous les secteurs d'activité et à toutes les fonctions

## Vente au détail



### La loyauté à coup de jetons

Permettre un écosystème de fidélisation entre partenaires piloté par un portefeuille unique basé sur la blockchain qui permet aux clients d'accumuler, d'échanger ou de convertir des points de fidélité de manière transparente dans les unités commerciales et les offres de services de l'entreprise.

## Soins de santé et sciences de la vie



### Chaîne d'approvisionnement en médicaments

L'infrastructure de confiance numérique, soutenue par la blockchain, permet aux participants d'authentifier les vaccins, de valider la capacité à honorer les commandes, de prédire la demande et de prendre des mesures préventives contre les pénuries.

## Monnaie numérique de la banque centrale



### Monnaie virtuelle

Exploiter le grand livre distribué pour mettre en œuvre une stratégie de monnaie virtuelle afin de soutenir le développement de l'économie nationale et de diversifier les sources de revenus des banques centrales.

## Marchés publics



### Suivi des immobilisations

Suivi de l'expédition, de l'élimination, de la distribution et du cycle de vie des biens matériels, tels que les ordinateurs portables, les imprimantes, les photocopieuses, etc., afin de réduire les coûts administratifs et d'automatiser les processus manuels inefficaces.

### Provenance des pièces et suivi douanier



Exploiter le grand livre numérique pour suivre les pièces lors de leur expédition, de leur importation, de leur usinage et de leur exportation à travers des sites internationaux afin d'optimiser le paiement des taxes et la gestion des stocks.

### Gestion des subventions



Transparence et traçabilité dans la distribution des fonds avec un registre des transactions vérifiable et des moyens simplifiés d'identifier et de vérifier les bénéficiaires admissibles.

# Comment KPMG peut vous aider

KPMG offre une perspective expérimentée pour comprendre, développer et maintenir la sécurité et la conformité des technologies de registres distribués.

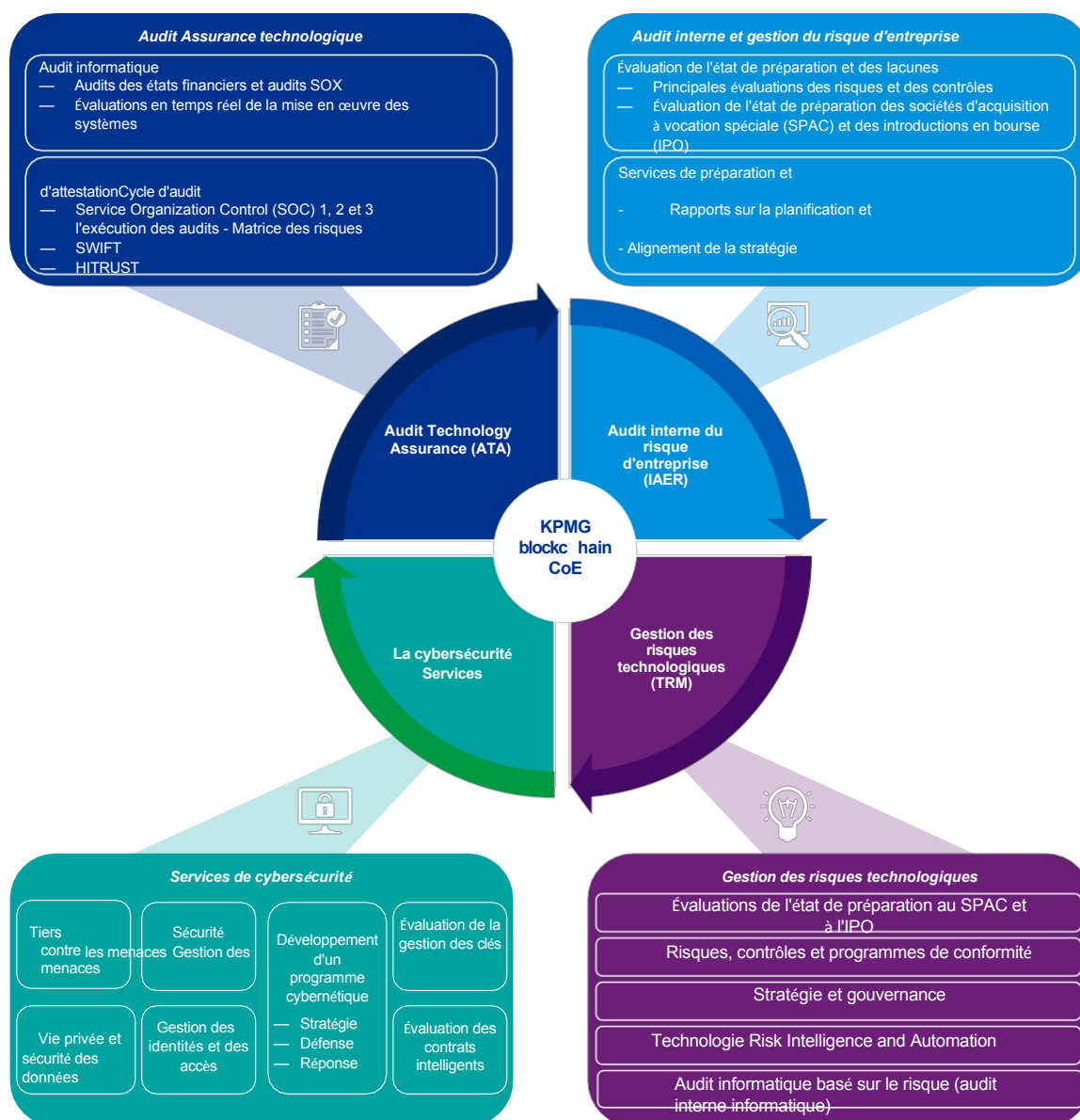
Notre approche est fondée sur des processus rigoureux basés sur l'assurance, combinés à une connaissance approfondie des technologies de l'information (TI) et des applications spécifiques à l'industrie par une équipe de professionnels en la matière qui vous offrent des perspectives pour élever le niveau d'exigence.

Notre vaste expérience, notre méthodologie et nos outils permettent aux clients d'adopter et de maintenir en toute confiance la technologie des grands livres distribués.

Nos services englobent le cycle de vie complet des solutions blockchain et des entreprises de crypto-monnaies. Ces services comprennent la réalisation stratégique, l'orientation réglementaire, l'évaluation des risques, la conception et l'évaluation des contrôles, l'audit informatique et le soutien à l'attestation, ainsi que l'information et la cybersécurité. En outre, nous travaillons en étroite collaboration avec les lignes de services d'audit, de fiscalité et de conseil plus large de KPMG pour aider à fournir une offre complète de services à nos clients.

## KPMG Blockchain Solutions

**Nos services robustes permettent à nos clients d'identifier, de gérer et d'atténuer les risques posés par l'adoption des technologies de registres distribués.**



Pour plus d'informations, visitez [read.kpmg.us/TRM](http://read.kpmg.us/TRM)

## Contactez nous

### **Bryan McGowan**

**Principal**

**Gestion du risque technologique T :**

816-802-5856

**E :** [bmcgowan@kpmg.com](mailto:bmcgowan@kpmg.com)

### **Brian Consolvo**

**Directeur général**

**Gestion des risques**

**technologiques T :** 757-646-6378

**E :** [bconsolvo@kpmg.com](mailto:bconsolvo@kpmg.com)

### **Ahmed Saleh** Directeur

**Gestion des risques**

**technologiques T :** 402-661-8713

**E :** [amsaleh@kpmg.com](mailto:amsaleh@kpmg.com)

Tout ou partie des services décrits dans le présent document peuvent ne pas être autorisés pour les clients d'audit de KPMG et leurs sociétés affiliées ou entités apparentées.

[kpmg.com/socialmedia](http://kpmg.com/socialmedia)



Les informations contenues dans le présent document sont de nature générale et ne sont pas destinées à traiter de la situation d'une personne ou d'une entité en particulier. Bien que nous nous efforcions de fournir des informations exactes et opportunes, nous ne pouvons garantir que ces informations sont exactes à la date de leur réception ou qu'elles continueront à l'être à l'avenir. Nul ne devrait agir sur la base de ces informations sans un avis professionnel approprié après un examen approfondi de la situation particulière.

2021 KPMG LLP, société à responsabilité limitée du Delaware et membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société privée anglaise à responsabilité limitée par garantie. Tous droits réservés. Le nom et le logo de KPMG sont des marques commerciales utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale de KPMG. NDP250066-1A