Introduction à la chaîne de blocs et aux cryptomonnaies

Un message de l'Équipe conseil Portefeuilles de BMO Nesbitt Burns : Cet article vise à vous sensibiliser aux monnaies virtuelles, également appelées « cryptomonnaies ». Nous ne recommandons pas spécialement les cryptomonnaies ou les placements connexes à l'heure *actuelle* compte tenu de leur volatilité extrêmement élevée et de la très forte augmentation de leurs valeurs (avant la récente correction), ce qui les place dans la catégorie des « bulles » de placement historiques. Cela dit, nous sommes convaincus qu'il faut continuer de se tenir au courant de ce qui se passe dans ce secteur, car la dynamique du marché évolue avec les changements technologiques et les thèmes de placements technologiques émergents.

Qu'est-ce que la chaîne de blocs?

La technologie de chaîne de blocs est la base des cryptomonnaies. Une chaîne de blocs est un grand livre distribué et partagé entre un réseau de nœuds (ordinateurs). Le nom « chaîne de blocs » évoque le format de stockage des données dans la base de données. Un bloc recueille des données, comme des transactions, et le bloc est fermé une fois sa capacité limite atteinte. Le bloc est ensuite relié au bloc fermé précédemment et un nouveau bloc est formé. Les chaînes de blocs sont immuables – ce qui signifie que l'entrée des données est irréversible. Dans le cas du Bitcoin, toutes les transactions sont enregistrées de façon permanente et visibles par tous. Cette structure de base de données assure la sécurité fondamentale en raison de sa nature décentralisée et immuable. Par exemple, même s'il est possible de trafiquer un grand livre, il est impossible de réussir à trafiquer en même temps tous les grands livres distribués.

Il existe différentes variations de chaîne de blocs, comme les chaînes de blocs avec autorisation, exploitées de façon privée par un intermédiaire. Les cryptomonnaies appartiennent à la catégorie des chaînes de blocs sans autorisation (ou publiques). Il est important de noter que la technologie des chaînes de blocs est utilisée au-delà de l'univers des paiements – comme la tenue de livres, les applications décentralisées (*dApps*), les contrats intelligents et les échanges décentralisés.

Qu'est-ce qu'une monnaie virtuelle?

Les monnaies virtuelles – qui sont également des monnaies numériques ou de l'argent numérique – n'existent pas sous forme tangible, c'est-à-dire qu'elles sont accessibles et négociables par voie électronique. Une monnaie virtuelle diffère d'une monnaie numérique par la manière dont elle est émise et supportée, ainsi que par son exploitabilité. Les monnaies virtuelles décentralisées utilisent la cryptographie pour sécuriser leur registre de transactions, qui sont stockées dans une chaîne de blocs. Un exemple de chaîne de blocs est le Bitcoin (Bitcoin avec un B majuscule), qui désigne à la fois la technologie sous-jacente et l'unité de monnaie virtuelle elle-même (bitcoin avec un b minuscule). Le Bitcoin est la première chaîne de blocs au monde et existe depuis à peine un peu plus de neuf ans. Parmi d'autres exemples de chaînes de blocs décentralisées, on trouve Ethereum et Litecoin, qui partagent certaines similitudes avec le Bitcoin.

Selon les sources consultées, les monnaies virtuelles peuvent être considérées soit comme des monnaies, soit comme des actifs, soit comme des marchandises, semblables à l'or. Sans doute, les monnaies virtuelles présentent des caractéristiques semblables à celles des monnaies fiduciaires classiques (c'est-à-dire une valeur refuge, un instrument d'échange et une unité de compte). Contrairement aux monnaies classiques, les monnaies virtuelles ne sont pas contrôlées ni régies par un

organisme unique et sont, par conséquent, décentralisées. Les transactions sont effectuées dans un réseau entre pairs sans besoin d'intermédiaires comme les banques centrales ou les institutions financières.

Les monnaies virtuelles, comme le bitcoin, peuvent être utilisées pour acheter des biens et services ou détenues comme valeur refuge, et transférer de la valeur de façon fluide entre les frontières internationales. À l'heure actuelle, il existe plus d'un millier de monnaies virtuelles opérationnelles, chacune offrant quelque chose de différent.

Figure 1. Les 10 principales cryptomonnaies par capitalisation boursière ($ US)

Ticker	Cryptocurrency Name	Market Cap (Billions)	
BTC	Bitcoin	$	818.3
ETH	Ethereum	$	366.0
USDT	Tether	$	78.0
BNB	BNB	$	67.3
USDC	USD Coin	$	51.6
XRP	XRP	$	39.2
ADA	Cardano	$	38.5
SOL	Solana	$	35.0
LUNA	Terra	$	22.6
DOT	Polkadot	$	21.0

Source : CoinMarketCap (8 février 2022)

Comment fonctionne l'offre?

Il existe à l'heure actuelle deux principaux modèles de création de cryptomonnaie. Le protocole consensuel par preuve de travail (*proof of work* – PoW) a été proposé dans le livre blanc de Satoshi Nakamoto pour le Bitcoin en 2008 et constitue la méthode de prédilection des deux principales cryptomonnaies (Bitcoin et Ethereum). Le deuxième modèle est le protocole consensuel par preuve d'enjeu (*proof of stake* – PoS) introduit en 2012. Il existe d'autres protocoles consensuels comme la preuve d'historique (*proof of history*), la tolérance d'erreur associée au problème des généraux byzantins (*Byzantine Fault Tolerance* – BFT) et la preuve d'enjeu déléguée (*delegated proof of stake* – DPoS). Cependant, les algorithmes consensuels par preuve de travail et par preuve d'enjeu sont les plus couramment utilisés et sont expliqués ci-dessous :

Dans le protocole par preuve de travail, les nœuds (mineurs) qui forment le réseau se livrent concurrence pour résoudre un problème cryptographique afin de remporter l'occasion d'ajouter le prochain bloc et gagner la cryptomonnaie de la chaîne de blocs à titre de récompense. Le protocole consensuel par preuve de travail assure efficacement la sécurité et la décentralisation, mais requiert énormément de puissance informatique, de bande passante et de stockage. L'algorithme du protocole par preuve de travail incite chaque mineur à obtenir du matériel avancé pour atteindre des taux de hachage plus élevés, ce qui procure au mineur l'avantage d'être le premier à résoudre le problème cryptographique. En deux mots, le taux de hachage est une mesure de la puissance informatique totale fournie par les mineurs pour traiter des transactions. Il permet de jauger la solidité et la sécurité du réseau d'une cryptomonnaie.

Dans le protocole consensuel par preuve d'enjeu, les valideurs sont sélectionnés aléatoirement pour valider les transactions dans le bloc. Les valideurs donnent en garantie leur cryptomonnaie pour avoir la possibilité d'être sélectionnés. Le protocole par preuve d'enjeu et son potentiel de remplacer le protocole par preuve de travail sont expliqués plus en détail à la section « Évolutivité, preuve de travail, preuve d'enjeu » en page 8.

Le Bitcoin est l'une des monnaies virtuelles qui requièrent le processus de minage; toutefois, le nombre total d'unités qu'on peut créer est limité, tout comme l'offre d'or totale disponible. Dans le cas du Bitcoin, l'offre totale est plafonnée à 21 millions, chaque bitcoin étant divisible par 100 millions et sa plus petite unité divisible est appelée « Satoshi ». On prévoit que le minage des derniers bitcoins aura lieu en 2140, l'incitation se déplaçant alors uniquement vers la monétisation du processus de vérification, par opposition à la création de nouvelles unités.

Comment fonctionne la demande?

Une fois créées, les monnaies virtuelles peuvent être utilisées pour les échanges ou pour l'exécution de transactions sur le marché mondial, où de plus en plus de détaillants et entreprises acceptent les monnaies virtuelles quotidiennement. Règle générale, l'accès aux monnaies virtuelles se fait par le portefeuille de monnaie virtuelle d'un utilisateur détenu sur une application d'échange virtuel ou sur une application basée sur du matériel (*hard wallet* – semblable à une clé USB). Ces dispositifs sont accessibles par téléphone mobile ou ordinateur portable. Chaque portefeuille contient les clés publiques et privées de l'utilisateur. La clé publique est

semblable à une adresse courriel et la clé privée est en fait le mot de passe.

En utilisant la chaîne de blocs comme exemple, une transaction indiquera que « Jean donne 'un nombre X' de bitcoins à Stéphanie. » Cette transaction est signée (approuvée) par la clé privée de Jean et envoyée à la clé publique de Stéphanie (adresse de portefeuille). Après vérification par les mineurs, la transaction est effectuée et ajoutée comme partie d'un bloc à la chaîne de blocs du Bitcoin. Ce bloc renferme certaines données confirmant que la transaction a eu lieu avec d'autres transactions groupées avec elle. Toutes les données transactionnelles ne sont pas stockées dans le bloc; cependant, l'indication d'horodatage approximative du moment de la transaction et les adresses de portefeuille des personnes touchées (et non leur nom) sont incluses.

Achat et vente de bitcoins et d'autres monnaies virtuelles

Les particuliers ne peuvent acheter ou vendre des bitcoins ou d'autres monnaies virtuelles à l'heure actuelle auprès de leur succursale bancaire locale ou de leur conseiller financier. Règle générale, les monnaies virtuelles s'achètent et se vendent par l'intermédiaire d'une plateforme d'échange tierce, comme Coinbase, des firmes de courtage étrangères, des guichets automatiques Bitcoin ou un site Web d'échange entre pairs comme Local Bitcoins. Normalement, les utilisateurs créent un portefeuille relié à leur compte de banque ou à leur carte de crédit pour acheter et vendre des monnaies virtuelles. Certaines plateformes d'échange et de courtage acceptent des virements électroniques, des virements par courriel et d'autres modes de paiement, et les taux entre acheteurs et vendeurs peuvent différer grandement. Les guichets automatiques Bitcoin (« BTM ») n'acceptent généralement que des espèces et imposent des frais plus élevés pour leurs services. Cependant, les BTM limitent généralement la quantité d'unités de monnaie virtuelle qui peuvent être achetées. Bien qu'il existe de nombreux modes d'achat et de vente, l'utilisation de la technologie des chaînes de blocs assure qu'il n'y a qu'un seul grand livre, par monnaie virtuelle, qui enregistre toutes les transactions.

L'utilisation des monnaies virtuelles continue de croître, car l'économie numérique émergente se répand de plus en plus au Canada et dans le monde. Nous invitons les investisseurs à rester informés à mesure que les percées technologiques qui réunissent les monnaies et la sphère virtuelle deviennent plus accessibles.

Principales notions

D'après JPMorgan, trois importantes notions sous-tendent la compréhension de la valeur des cryptomonnaies :

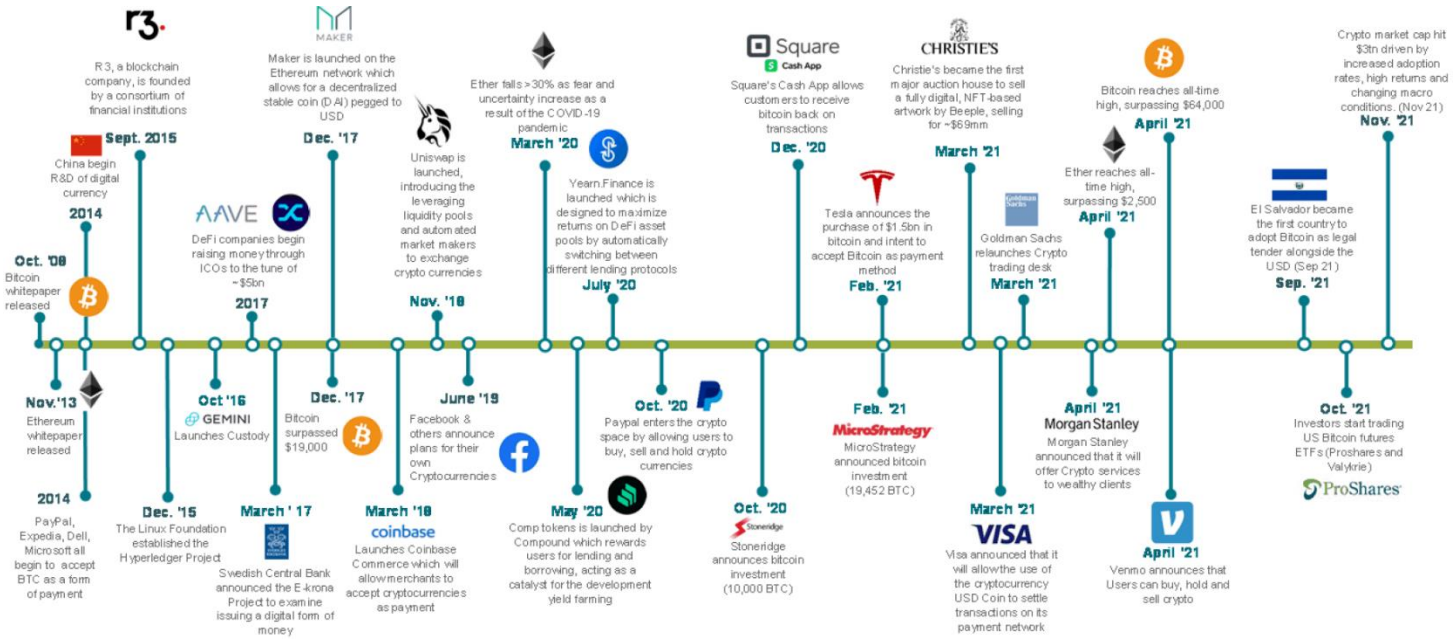
1) Les cryptomonnaies sont de la technologie. Alors que les investisseurs échangent les jetons comme des actifs, les cryptomarchés sont technologiques et leurs cas d'utilisation sous-jacents constituent d'importants facteurs de valeur. Cette technologie est également la base de communautés qui se développent autour de projets de cryptomonnaie, mais d'après JPM, la technologie prime et importe plus dans la création de valeur initiale.

2) Les jetons sont liés aux chaînes de blocs. Les investisseurs avec qui JPM s'est entretenu sont bien plus enclins à attribuer une valeur aux chaînes de blocs qu'aux cryptomonnaies. On accepte plus volontiers que la technologie des chaînes de blocs a de la valeur, tandis que les jetons numériques sont un système pyramidal tiré par le commerce de détail. Cependant, les jetons et les chaînes de blocs sont reliés. Les chaînes de blocs décentralisées ont besoin d'un jeton avec une valeur pour encourager la validation de la chaîne de blocs – il faut un jeton et ce jeton doit avoir de la valeur, tant dans le protocole par preuve d'enjeu que dans le protocole par preuve de travail. Bien que la valeur de ce jeton fluctue en fonction de l'offre et de la demande et que, par conséquent, un jeton puisse être surévalué, un jeton avec une valeur est néanmoins un composant essentiel d'une chaîne de blocs décentralisée.

3) La valeur d'un jeton est basée sur les cas d'utilisation pour la chaîne de blocs. Cette valeur est fixée par le marché, en fonction de l'offre et de la demande. Les transactions d'une chaîne de blocs sont payées en jetons natifs et il faut donc acheter le jeton sous-jacent pour pouvoir les effectuer. Par exemple, les jetons ERC-721 (également appelés « jetons non fongibles » – NFT) sont achetés en jetons Eth (Ether) et les prix de transaction sont également payés en Eth. L'acquisition de jetons Eth pour effectuer des transactions dans les projets basés sur Ethereum fait augmenter la valeur du jeton Ether.

(Source : JPM)

Figure 2 : Ligne du temps des étapes clés de l'écosystème des cryptomonnaies des dernières années



Source : Onyx by JPMorgan

Bitcoin et Ethereum

Avant de passer aux utilisations autres que de paiement de la technologie des chaînes de blocs, il est important de faire la distinction entre le Bitcoin et Ethereum. Ces deux cryptomonnaies sont les deux plus importantes du monde sur le plan de la capitalisation boursière.

Le Bitcoin se définit essentiellement comme une monnaie numérique et ses utilisations sont unidimensionnelles, comme toutes les autres monnaies, c'est-à-dire les monnaies non numériques. La rareté du Bitcoin procure à ses propriétaires une valeur qu'ils peuvent utiliser pour acheter des biens et services.

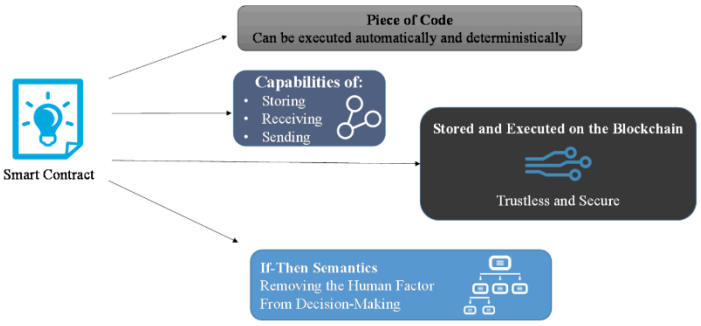
Ethereum est semblable au Bitcoin en ce qu'elle peut être utilisée comme monnaie numérique, mais une percée importante réside dans la nature de plateforme logicielle décentralisée du réseau Ethereum. Ethereum se définit essentiellement comme une chaîne de blocs programmable. Il utilise la technologie des chaînes de blocs pour permettre aux développeurs de stocker du code informatique pouvant servir à créer de nouvelles cryptomonnaies, des contrats intelligents et des applications décentralisées.

Contrats intelligents

L'expression « contrat intelligent » a été lancée par Nick Szabo, chercheur informatique, juriste et cryptographe, en 1997. L'expression initiale « contrat intelligent » inventée par Nick Szabo désignait « une série d'engagements, définis sous forme numérique, comprenant des protocoles à l'intérieur desquels les parties exécutent ces engagements ». Un exemple simple de contrat intelligent est une machine distributrice. La machine distributrice est programmée de telle sorte que vous avez la garantie d'obtenir un produit authentique si vous entrez un certain montant d'argent dans la machine. Cela élimine le besoin d'une intervention humaine (intermédiaire) pour traiter la vente du produit. Un autre exemple de contrat est le populaire site Web de financement participatif Kickstarter. Si un projet sur Kickstarter atteint le stade de financement complet, le code de Kickstarter s'auto-exécute et fournit le capital promis à l'équipe de projet. De même, le capital est renvoyé aux particuliers participants si le projet n'atteint pas le stade de financement complet à l'échéance prévue.

Les contrats intelligents (au regard des chaînes de blocs) sont écrits sur le réseau Ethereum et constituent la base des applications décentralisées. Ces contrats, comme les cryptomonnaies, sont immuables en ce qu'ils ne peuvent être modifiés après qu'ils ont été créés, distribués et publiés. Ces caractéristiques rendent l'altération des contrats intelligents presque impossible et le code est un code source ouvert, ce qui crée de la confiance dans un système sans tiers de confiance. Les contrats intelligents exécutent le code défini dans l'entente une fois les conditions préétablies satisfaites et créent ainsi de la valeur en éliminant le besoin d'un intermédiaire. Les contrats intelligents servent notamment aux emprunts et prêts, à l'assurance et aux échanges. Les contrats intelligents sont essentiels aux applications décentralisées et au Web3.0.

Figure 3. Contrats intelligents



Source : Ethereum.org, JPM

Applications décentralisées (*dApps*)

Les applications décentralisées sont des programmes qui tournent sur un réseau de chaînes de blocs et ne peuvent être construits que sur des réseaux qui supportent des contrats intelligents (p. ex. Ethereum). Les applications décentralisées n'appartiennent pas à une entité unique et tournent sur un réseau d'échange entre pairs. Chaque application décentralisée est unique de par sa fonction, tout comme nous utilisons à l'heure actuelle certains programmes pour atteindre des objectifs distincts. Les utilisateurs doivent acheter le jeton natif de l'application décentralisée pour interagir avec le programme. Par exemple, YouTube est un programme de partage de vidéos centralisé où les utilisateurs peuvent publier ou regarder du contenu. Il est facile d'imaginer le même type de programme, mais sur un réseau décentralisé où les utilisateurs peuvent publier ou regarder des vidéos sur la chaîne de blocs tout en interagissant avec l'application décentralisée à l'aide de ses jetons.

Les applications décentralisées procurent trois avantages clés en étant à code source ouvert et décentralisées.

Confiance. Contrairement aux applications centralisées auxquelles nous sommes habitués, comme Facebook, Twitter

ou Google, les applications décentralisées sont à code source ouvert et les codes des programmes sont publics. Cela crée de la confiance, car les utilisateurs sont en mesure de vérifier comment le programme fonctionne.

À l'épreuve de la censure. La nature immuable d'une chaîne de blocs et la décentralisation du programme signifie qu'il n'y a pas d'autorité centrale. Par exemple, sauf si c'est programmé dans le code, il ne serait pas possible pour un utilisateur donné d'une plateforme de médias sociaux décentralisée de supprimer une publication qui a déjà été enregistrée dans la chaîne de blocs.

Toujours en ligne. Les applications décentralisées tournent essentiellement sur des centaines d'ordinateurs en réseau et ne peuvent donc pas passer en mode hors ligne. Contrairement aux programmes centralisés qui connaissent de fréquents arrêts de maintenance ou des bogues qui font planter le site Web, les applications décentralisées restent toujours opérationnelles.

Un inconvénient notable des applications décentralisées est que les bogues (problèmes dans le code du programme) sont plus difficiles à résoudre. Les programmes, centralisés ou décentralisés, ont souvent besoin de correctifs au code pour régler des problèmes imprévus. Ce qui est beaucoup plus difficile à exécuter pour les applications décentralisées comparativement à leurs homologues centralisées.

Figure 4. Applications Web actuelles et applications décentralisées futures

	Web 2.0	Web 3.0 (powered by blockchain)
Storage	Dropbox, Google Drive, OneDrive	Storj, Filecoin, Sia, MaidSafe
Video and audio calls	Skype	Experty
Operating System	Android, IOS	Elastos, Essentia one
Social Network	Facebook, Twitter, LinkedIn	Steemit, Ono, SoMee, Mithril
Messaging	Wechat, Whatsapp, Messenger	Status, Dust, Cryptviser
Video Streaming	YouTube, Netflix	Flixxo, Dtube, Videocoin
Music	Spotify	Mycelia
Cloud Compute	AWS, Azure, GCP	Golem, SONM, Dfinity, iExec

Source : Hackermoon, enquête JPMorgan.

Tenue de dossiers

La tenue de dossiers est un autre domaine prometteur, car la technologie des chaînes de blocs peut assurer la sécurité et la transparence des données. Les bases de données centralisées sont sujettes aux défaillances localisées. Grâce au système des chaînes de blocs, les gouvernements et les entreprises peuvent utiliser des grands livres distribués privés et des contrats intelligents pour améliorer la transparence, ce qui réduit le risque de manipulation. Par exemple, les préoccupations croissantes entourant la sécurité et l'intégrité du processus électoral peuvent être apaisées au moyen des aspects décentralisés et immuables des chaînes de blocs. L'immuabilité signifie que la chaîne de blocs peut créer une piste d'audit qui ne peut être supprimée.

Jetons non fongibles (NFT)

Les jetons non fongibles sont des actifs numériques stockés dans une chaîne de blocs. « Non fongible » signifie qu'un actif numérique est unique et qu'il n'existe aucun autre jeton non fongible identique. Par exemple, les cryptomonnaies comme le bitcoin et Ethereum sont des jetons fongibles, car un jeton a une valeur égale à celle d'un autre jeton du même type.

L'Ethereum Foundation décrit les jetons non fongibles de la façon suivante : « un jeton non fongible ne compte qu'un propriétaire à la fois, géré par le code d'identification unique et par les métadonnées qu'aucun autre jeton ne peut reproduire. Les jetons non fongibles sont créés par des contrats intelligents qui en attribuent la propriété et en gèrent la transférabilité. Lorsque quelqu'un crée un jeton non fongible, il exécute le code stocké dans les contrats intelligents qui se conforment à une certaine norme, et cette information est ajoutée à la chaîne de blocs où le jeton non fongible est géré. » (Source : Ethereum). Un jeton non fongible peut être une œuvre d'art, une photo, une vidéo ou tout autre type d'actif numérique. Ce jeton est analogue aux cartes de sport de collection où la rareté crée de la valeur. Parmi la longue liste d'exemples de grandes sociétés publiques qui se sont aventurées dans l'univers des jetons non fongibles, on compte la NBA (Top Shot) et Adidas (Into the Metaverse).

L'évolution de l'Internet jusqu'à maintenant

Le premier stade de l'Internet (Web1.0) a duré de 1991 à 2004. Pendant cette période, l'Internet consistait principalement en pages d'information contenant du texte et des images. Les

utilisateurs ne pouvaient entrer leurs propres données et n'étaient strictement que des consommateurs d'information.

L'évolution vers le Web2.0 a commencé en 2004 et constitue le stade actuel de la « Toile » utilisé aujourd'hui. La principale différence offerte par le Web2.0, c'est l'interactivité entre les utilisateurs et les pages Web. Les entreprises qui possèdent des domaines spécifiques ont commencé à recueillir des données sur leurs utilisateurs et à utiliser ces données pour leur procurer du contenu auquel ils pourraient être intéressés. Les progrès de l'apprentissage machine et de l'intelligence artificielle ont permis aux entreprises centralisées de recueillir d'importantes quantités d'information sur leurs utilisateurs et de vendre cette information à des annonceurs. Ce manque de confidentialité est un enjeu clé auquel le prochain stade de l'Internet entend s'attaquer.

Web3.0

Le Web3.0 est une nouvelle conception du Web. Les tenants du Web3.0 estiment que les problèmes découlant de la centralisation monopoliste des données se résoudront par la décentralisation. La version décentralisée de l'Internet assurera de plus hauts niveaux de confidentialité, où les utilisateurs pourront contrôler l'information qu'ils échangent avec l'Internet.

Les applications Web3.0 utiliseront probablement les applications décentralisées comme forme principale d'applications grâce au réseau décentralisé inhérent à Ethereum. La progression du Web2.0 au Web3.0 se fera vraisemblablement par étapes et nous devrions voir des versions décentralisées de programmes courants. Par exemple, Storj est le double décentralisé de Google Drive. Les données du stockage infonuagique décentralisé (DCS) de Storj sont chiffrées et distribuées sur un réseau infonuagique mondial. Storj offre aux utilisateurs la confidentialité par le chiffrage et une disponibilité jour et nuit grâce à la décentralisation.

Contrairement au Web2.0, les domaines ou les applications décentralisées appartiendront aux utilisateurs. Ce sera une économie de créateurs, où les utilisateurs sont récompensés par les jetons de l'application pour la création de contenu. Plutôt qu'une seule entité reçoive tout le profit, celui-ci est partagé entre les participants qui créent du contenu et confirment le contenu sur la chaîne de blocs.

Il est important de noter que le Web3.0 en est encore à ses balbutiements et qu'aucun progrès concret n'a été réalisé sur une plateforme Web3.0. Le Web décentralisé que le Web3.0 aspire à devenir est encore au stade de recherche et développement par des organisations comme la Web3 Foundation.

Métavers

Le métavers (« méta-univers ») est devenu un mot à la mode dernièrement, depuis que Mark Zuckerberg a annoncé que Facebook changeait son image de marque pour celle de Meta Platforms Inc. le 28 octobre 2021. Alors, qu'est-ce que le métavers? Le métavers se définit comme un univers virtuel qui recouvre le monde où nous vivons et les tenants du métavers le considèrent comme la prochaine version d'Internet. C'est un monde virtuel où vous pouvez travailler, jouer et rester branché avec d'autres utilisateurs. Les utilisateurs peuvent effectuer des transactions en ligne pour acquérir des actifs numériques (jetons non fongibles) qu'ils peuvent échanger virtuellement dans le métavers. Ce ne sera pas un produit unique de Facebook (ou de Meta Platforms Inc.), mais quelque chose qui sera adopté par de nombreuses entreprises de divers secteurs en vue de rester concurrentielles.

D'après Roundhill Investments, premier émetteur de FNB du métavers (code : META), le métavers s'articule autour de sept catégories principales. Informatique, réseautage, plateformes virtuelles, normes d'échange (outils et formats du monde numérique), paiements, contenu et matériel. Des échanges sociaux aux jeux vidéo, en passant par la publicité – le métavers comporte d'énormes implications pour de nombreux secteurs. Ces catégories peuvent se définir au sens large comme des logiciels (programmes, applications, outils), du matériel (dispositifs et composants de réalité augmentée/virtuelle), de l'infrastructure (Internet et systèmes) et des plateformes virtuelles (moteurs et environnements). L'illustration ci-dessous est une liste des entreprises susceptibles de jouer un rôle important dans le métavers. (Source : Roundhill Investments)

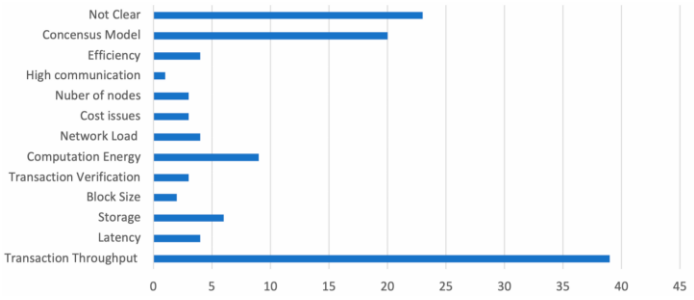
Il est important de préciser que le métavers ne doit pas nécessairement tourner sur un réseau décentralisé comme les chaînes de blocs. Les entités uniques centralisées comme Meta Inc et Roblox sont des exemples de plateformes non décentralisées où le métavers coexistera avec des plateformes décentralisées comme les chaînes de blocs.

Évolutivité, preuve de travail, preuve d'enjeu

Les trois propriétés centrales des chaînes de blocs sont la décentralisation, la sécurité et l'évolutivité. La décentralisation et la sécurité sont des propriétés centrales/essentielles qui ne peuvent être compromises, ce qui crée le problème de l'évolutivité. On parle ici du trilemme de l'évolutivité.

L'évolutivité, du point de vue de la chaîne de blocs, s'entend de la capacité du système à traiter de grandes quantités de transactions. Selon MDPI (Source : MDPI), un problème d'évolutivité se présente avec le nombre croissant de nœuds et le besoin de vérifier chaque transaction de la chaîne de blocs. La plus importante mesure de rendement dans le problème de l'évolutivité est le débit transactionnel. Le débit transactionnel est le nombre total de transactions que le protocole peut traiter en une seconde. L'évolutivité constitue à l'heure actuelle le principal obstacle des chaînes de blocs publiques populaires comme Bitcoin et Ethereum. Le problème est triple : l'évolutivité avec le format consensuel par preuve de travail, qui est le protocole consensuel le plus fréquemment utilisé, est soumise à la lenteur de la vérification et a besoin des quantités énormes d'énergie et de bande passante.

Figure 5 : Facteurs de problèmes d'évolutivité



Source : Applied Sciences MDPI

Les solutions potentielles au problème d'évolutivité peuvent se répartir en solutions de chaîne de blocs et en solutions hors chaîne de blocs. Les solutions de chaîne de blocs tentent de résoudre le problème d'évolutivité en travaillant sur le système de chaîne de blocs lui-même. Ces solutions de chaîne de blocs peuvent ensuite se subdiviser en approches associées aux blocs de données et en approches associées au protocole consensuel. Les solutions hors chaîne de blocs tentent de résoudre le problème d'évolutivité en réduisant la limitation de validation des transactions par l'exécution de transactions hors de la chaîne de blocs principale. (Source : MDPI)

Le problème d'évolutivité est étroitement lié au modèle consensuel par preuve de travail utilisé à l'heure actuelle par la plupart des cryptomonnaies. Le protocole consensuel par preuve de travail présente trois principaux problèmes :

1) Les problèmes d'évolutivité touchent l'efficacité, comme le nombre de transactions par seconde, et ce problème est abordé dans la section « Problèmes touchant la chaîne de blocs » ci-dessous.

2) L'algorithme par preuve de travail présente un avantage inhérent à ceux qui sont dotés d'un équipement perfectionné, ce qui a entraîné une concurrence déloyale et des pénuries de semiconducteurs.

3) L'algorithme par preuve de travail consomme d'énormes quantités d'énergie et cet enjeu crucial s'est amplifié dans un contexte de lutte mondiale contre les effets du réchauffement climatique.

Une solution potentielle prometteuse du problème d'évolutivité consiste en la transition d'un algorithme consensuel par preuve de travail à un protocole consensuel par preuve d'enjeu :

Dans un modèle par preuve de travail, les mineurs utilisent le matériel et l'électricité pour résoudre des problèmes cryptographiques afin de créer le prochain bloc en vue d'être récompensés par monnaie numérique. Ainsi, les mineurs de Bitcoin ont créé des fermes de cryptominage qui consomment d'énormes quantités d'électricité. De plus, les mineurs dotés de matériel perfectionné sont récompensés davantage dans un système par preuve de travail.

Dans un modèle par preuve d'enjeu (preuve de participation), un nœud est choisi de façon presque aléatoire pour valider le prochain bloc. Afin d'être un « valideur » plutôt qu'un « mineur », un nœud doit déposer de la cryptomonnaie dans

le réseau comme preuve de participation (c'est-à-dire comme garantie). Une fois que le valideur confirme les transactions dans le bloc, il reçoit les droits associés aux transactions, et le bloc est ensuite fermé et ajouté à la chaîne de blocs. La preuve d'enjeu utilise beaucoup moins d'énergie, car ce n'est pas tout le monde qui peut miner/valider la chaîne de blocs et les valideurs n'ont pas besoin de matériel perfectionné pour effectuer le processus. Cela crée un réseau plus rapide et plus décentralisé, car le réseau compte plus de nœuds.

Ethereum procède actuellement à une mise à niveau de la preuve de travail à la preuve d'enjeu. La mise à niveau est appelée « Ethereum Merge » et doit avoir lieu en 2022. Cela insufflera probablement beaucoup d'élan à Ethereum, car cela accroîtra l'évolutivité et réduira les coûts de transaction.

Manque de réglementation

Le manque de réglementation dans les réseaux de chaînes de blocs est une lame à double tranchant qui procure aux utilisateurs les avantages de la confidentialité, mais présente un risque d'escroqueries et de manipulation du marché. Le rythme de progression des possibilités de la technologie des chaînes de blocs a dépassé celui de la réglementation.

La question de la compétence territoriale est un exemple de lacune dans la réglementation des chaînes de blocs publiques. Cette question est importante, car les nœuds d'un grand livre décentralisé risquent d'être disséminés dans le monde entier. Ce qui inquiète, c'est que des lois et règlements peuvent s'appliquer différemment pour une même application selon l'endroit du monde.

Vulnérabilité des points d'extrémité

Bien que la chaîne de blocs soit « impiratable », la sécurité présente des failles pour les utilisateurs de points d'extrémité comme les portefeuilles numériques. Les cyberattaques visant à voler des cryptomonnaies sont un problème qui reste à résoudre complètement et, contrairement aux marchés financiers, il n'existe aucune assurance contre les pirates qui exploitent les portefeuilles numériques ou les erreurs des utilisateurs.

D'après JPM, la croissance, l'évolution et l'adoption généralisée du marché des cryptomonnaies ont présenté une occasion unique pour les acteurs illicites, y compris les opérateurs de logiciels rançonneurs-service (RaaS) et leurs comparses. Ces marchés sont décentralisés et échappent donc au contrôle des autorités centrales. Ils offrent également un règlement transfrontalier brut final en temps réel. Cela a permis le développement d'une foule d'outils de blanchiment comme les mixeurs, les portefeuilles confidentiels, ainsi que l'accès à toute une gamme de bourses mondiales. Une solution potentielle à ce problème est la cyberassurance qui peut être possible dans la chaîne de blocs ou hors de la chaîne de blocs. (Source : JPM)

Sélection d'actions et de FNB associés à ce thème (ce sont des exemples, et non des recommandations d'achat concrètes)

Contrats intelligents

Ticker	Company Name	Market Cap (Millions)	Revenue (Millions) FY21	Revenue (Millions) FY22E	Price / Earnings 2022E	Price / Earnings 2023E	EV / EBITDA 2022E	EV / EBITDA 2023E	EV / Sales 2022E	EV / Sales 2023E
DOCU-US	DocuSign, Inc.	$ 24,056	$ 1,453	$ 2,088	53x	41x	41x	33x	9x	7x
CSGP-US	CoStar Group, Inc.	$ 28,040	$ 1,659	$ 1,939	51x	39x	32x	25x	11x	9x
ADBE-US	Adobe Inc.	$ 251,459	$ 15,801	$ 17,938	32x	32x	28x	25x	14x	12x

Source : FactSet

Tenue de dossiers

Ticker	Company Name	Market Cap (Millions)	Revenue (Millions) FY21	Revenue (Millions) FY22E	Price / Earnings 2022E	Price / Earnings 2023E	EV / EBITDA 2022E	EV / EBITDA 2023E	EV / Sales 2022E	EV / Sales 2023E
VRSN-US	VeriSign, Inc.	$ 24,824	$ 1,265	$ 1,328	34x	29x	26x	22x	18x	16x
VEEV-US	Veeva Systems Inc Class A	$ 32,770	$ 1,465	$ 1,846	58x	50x	41x	35x	16x	14x
DSY-FR	Dassault Systemes SA	$ 57,379	$ 4,452	$ 5,351	37x	37x	28x	26x	10x	10x
INTU-US	Intuit Inc.	$ 159,226	$ 9,633	$ 12,272	40x	40x	32x	27x	12x	10x
ADBE-US	Adobe Inc.	$ 251,459	$ 15,801	$ 17,938	32x	32x	28x	25x	14x	12x

Source : FactSet

Sécurité

Ticker	Company Name	Market Cap (Millions)	Revenue (Millions) FY21	Revenue (Millions) FY22E	Price / Earnings 2022E	Price / Earnings 2023E	EV / EBITDA 2022E	EV / EBITDA 2023E	EV / Sales 2022E	EV / Sales 2023E
CYBR-US	CyberArk Software Ltd.	$ 5,389	$ 464	$ 496	N/A	383x	3645x	165x	9x	7x
AKAM-US	Akamai Technologies, Inc.	$ 18,818	$ 3,198	$ 3,456	19x	17x	12x	11x	5x	5x
NET-US	Cloudflare Inc Class A	$ 27,334	$ 431	$ 648	5019x	1018x	300x	188x	33x	25x
OKTA-US	Okta, Inc. Class A	$ 28,405	$ 835	$ 1,277	N/A	844x	N/A	204x	15x	11x
ZS-US	Zscaler, Inc.	$ 36,071	$ 673	$ 1,008	268x	268x	259x	162x	33x	25x
CRWD-US	CrowdStrike Holdings, Inc. Class A	$ 36,861	$ 874	$ 1,432	187x	121x	113x	77x	19x	14x
PANW-US	Palo Alto Networks, Inc.	$ 50,261	$ 4,256	$ 5,386	56x	56x	36x	31x	9x	7x
FTNT-US	Fortinet, Inc.	$ 50,665	$ 2,594	$ 3,340	65x	55x	43x	35x	12x	10x
CSCO-US	Cisco Systems, Inc.	$ 236,903	$ 49,818	$ 52,739	15x	15x	11x	11x	4x	4x

Source : FactSet

Métavers

Ticker	Company Name	Category	Market Cap (Millions)	Revenue (Millions) FY21	Revenue (Millions) FY22E	Price / Earnings 2022E	Price / Earnings 2023E	EV / EBITDA 2022E	EV / EBITDA 2023E	EV / Sales 2022E	EV / Sales 2023E
MTTR-US	Matterport, Inc. Class A	Software, Virtual Platform	$ 2,115	$ -	$ 109	N/A	N/A	N/A	N/A	N/A	N/A
FSLY-US	Fastly, Inc. Class A	Infrastructure	$ 3,217	$ 291	$ 349	N/A	N/A	N/A	4583x	8x	7x
U-US	Unity Software, Inc.	Software, Virtual Platform	$ 29,176	$ 772	$ 1,088	N/A	1477x	790x	148x	17x	13x
RBLX-US	Roblox Corp. Class A	Virtual Platform	$ 34,905	$ 924	$ 2,715	N/A	N/A	45x	35x	10x	8x
ADSK-US	Autodesk, Inc.	Software	$ 54,553	$ 3,791	$ 4,369	35x	28x	27x	22x	11x	9x
SHOP-US	Shopify, Inc. Class A	Payment Services	$ 100,903	$ 2,929	$ 4,575	136x	96x	120x	79x	16x	12x
NVDA-US	NVIDIA Corporation	Hardware, Infrastructure, Virtual Platform	$ 631,050	$ 16,675	$ 26,644	47x	39x	37x	33x	19x	17x
FB-US	Meta Platforms Inc. Class A	Hardware, Software, Virtual Platform	$ 764,308	$ 117,929	$ 134,860	15x	15x	10x	9x	5x	4x
MSFT-US	Microsoft Corporation	Hardware, Software, Virtual Platform	$ 2,349,968	$ 168,088	$ 198,745	28x	28x	23x	20x	11x	10x
AAPL-US	Apple Inc.	Hardware, Software, Virtual Platform	$ 2,869,611	$ 365,817	$ 394,469	27x	27x	23x	22x	8x	7x

Source : FactSet

Finance

Ticker	Company Name	Market Cap (Millions)	Revenue (Millions) FY21	Revenue (Millions) FY22E	Price / Earnings 2022E	Price / Earnings 2023E	EV / EBITDA 2022E	EV / EBITDA 2023E	EV / Sales 2022E	EV / Sales 2023E
GLXY-CA	Galaxy Digital Holdings Ltd.	$ 1,619	$ -	$ 1,588	19x	N/A	N/A	N/A	4x	N/A

Source : FactSet

Fonds ind.

Ticker	Company Name	Market Cap (Millions)
ETC-CA	Evolve Cryptocurrencies ETF CAD Unhedged	$ 25
LEGR-US	First Trust Indxx Innovative Transaction & Process ETF	$ 158
BLCN-US	Siren ETF Trust Siren Nasdaq NexGen Economy ETF	$ 223
BTCC-CA	Purpose Bitcoin ETF	$ 225
BITW-US	Bitwise 10 Crypto Index Fund Units of Benef Interest	$ 469
META-US	Roundhill Ball Metaverse ETF	$ 877
BLOK-US	Amplify Transformational Data Sharing ETF	$ 957

Source : FactSet

BMO Gestion de patrimoine
BMO Nesbitt Burns

BMO Gestion de patrimoine
BMO Nesbitt Burns