

THE BITCOIN

BTC

Comme vous le savez, nos lectures se concentrent essentiellement sur « l'étude » de sociétés cotées en bourse, en se basant sur les principes de l'analyse fondamentale. Cependant, bien qu'il y ait déjà beaucoup à faire dans le milieu des actions, nous voulions parler du Bitcoin, qui devient un sujet de plus en plus difficile à éviter au fur et à mesure que le temps passe, et pour cause, aujourd'hui, la valeur totale de tous les bitcoins minés serait de 2.24 trillions de dollars. Étant un sujet vaste mais surtout très complexe, nous nous efforcerons de rendre ce document accessible et synthétique sur le sujet. Le but de la lecture suivante sera de comprendre qu'est-ce que le Bitcoin et ses enjeux financiers afin de répondre à la question suivante : « Devrions-nous acheter du Bitcoin ? »

Histoire : Rubrique incontournable de nos écrits, la partie historique se révèle importante ici, car bien que l'année officielle au cours de laquelle le Bitcoin a été introduit au monde est 2008, des dizaines d'années ont été nécessaires pour jeter les bases essentielles en matière de cryptographie. Et pour cause, le concept de cryptographie remonte aux années 1970 avant la publication de « Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups » en 1982 par David Chaum, proposant un protocole ressemblant à celui de la Blockchain. Suite à cela, c'est Stefan Brands qui développe des protocoles similaires mais leur adoption a été limitée car ils nécessitaient un contrôle centralisé. Les systèmes plus « révolutionnaires » apparaîtront à la fin des années 90 avec Hashcash, un système de preuve conçu par Adam Back, pour le contrôle du spam, qui deviendra fondamental pour le processus de minage du Bitcoin. Au même moment, des propositions de « bit gold » et « b-money » se font par Wei Dai et Nick Szabo. La dernière avancée précédant l'arrivée de cette technologie restera l'invention du premier système de preuve de travail réutilisable utilisant Hashcash, par Hal Finney en 2004.

Avant de poursuivre avec l'arrivée du Bitcoin, une observation intéressante s'offre à nous. Comme mentionné plus haut, la technologie sur laquelle se base la « cryptomonnaie » n'est pas récente et date au contraire des débuts d'internet. C'est important, car cela nous apprend que ce n'est pas une simple tendance « née » d'une période post-crise économique (2008). Ce qui nous amène à penser que si le Bitcoin était apparu en même temps (que les ordinateurs), cela aurait sûrement été moins perturbant et difficile à assimiler qu'aujourd'hui et donc, moins controversé. À l'époque, il est possible que les affaires étaient principalement orientées sur le développement des ordinateurs et des téléphones mobiles.

C'est en 2008, dans un contexte de crise financière, que le Bitcoin émergera finalement, avec deux dates importantes. Le point de départ se trouve être l'enregistrement du domaine bitcoin.org, le 18 août 2008. Puis, le 31 octobre de la même année, sera publié le document suivant : « Bitcoin: A Peer-to-Peer Electronic Cash System » par Satoshi Nakamoto. Ce



document de 9 pages introduit les aspects généraux et techniques qui fondent ce « système de paiement ». https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf La lecture de ce document est fortement recommandée, car elle vous permet de « comprendre » ce qu'est le Bitcoin et comment fonctionne son système en 12 chapitres (1. Introduction – 2. Transactions – 3. Serveur d'horodatage – 4. Preuve-de-travail – 5. Réseau – 6. Prime de résultat – 7. Demande d'espace disque – 8. Vérification de paiement simplifiée – 9. Combinaison et séparation des valeurs – 10. Vie privée – 11. Calculs – 12. Conclusion). Cette lecture sera donc le meilleur moyen de vous affranchir de l'asymétrie d'informations qui existe entre les personnes spécialisées dans la cryptographie et le commun des mortels, en approfondissant chaque notion (bien évidemment). Nous parlerons davantage de Satoshi Nakamoto et ses mystères dans une autre section de ce document. En revenant sur la première publication, il semblerait que la plupart des éléments provenaient de publications académiques antérieures, selon Arvind Narayanan. Ce qui signifie que la grande innovation de Satoshi concernerait la combinaison de différents éléments afin de parvenir à créer un système de monnaie numérique décentralisé (et non une création particulière). C'est 5 mois après la publication de ce « livre blanc » sur la structure du réseau du Bitcoin, que l'on assiste au minage du premier bloc de genèse par Nakamoto, avec l'inscription « The Times 03/Jan/2009 Chancellor on brink of second bailout for banks. » (Le chancelier est sur le point de lancer un deuxième plan de sauvetage pour les banques) intégré dans ce bloc en guise de marque temporelle mais aussi de message sur l'instabilité du système bancaire. Très peu de temps après cet événement historique, le 12 janvier 2009, la première transaction Bitcoin est enregistrée avec l'envoi de 10 bitcoins de Nakamoto à Hal Finney. La première cotation du bitcoin est faite en calculant l'électricité nécessaire pour le produire. Celle-ci s'élève en 2009 à 1309 bitcoins pour 1 \$. Malgré la mise en pratique de ce qui était auparavant plutôt théorique, le réseau est resté petit pendant un certain moment, avec seulement quelques enthousiastes de la cryptographie. Pour avoir une idée de sa taille, en mars 2010, l'utilisateur « SmokeTooMuch » avait mis aux enchères 10.000 BTC pour \$50 sans trouver aucun acheteur. Ces mêmes 10.000 Bitcoins vaudraient aujourd'hui 1.2 Milliards de dollars. Cette anecdote annonce parfaitement bien la suivante, qui reste le plus grand événement de l'histoire de cette « monnaie », la première transaction (en échange d'un bien ou d'un service). En effet, même si certains ignorent une partie de l'histoire du Bitcoin, tout le monde connaît le « Jour de la pizza Bitcoin », qui se tient chaque année, le 22 mai. Ce jour symbolique remonte en 2010, lorsque Laszlo Hanyecz, un programmeur vivant en Floride, dépose l'annonce suivante sur un Bitcoin Talk forum : *“I'll pay 10.000 bitcoins for a couple of pizzas... like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a “breakfast platter” at a hotel or something, they just bring you something to eat and you're happy! I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc... just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire. If you're interested please let me know and we out a deal. Thanks, Laszlo”*. C'est Jeremy Sturdivant, un anglais, qui accepte l'offre, en commandant deux pizzas chez Papa John's à Jacksonville FL, en échange des 10.000 bitcoins. Ce jour a officiellement démontré le potentiel du Bitcoin en tant que moyen d'échange. Malgré cette transaction symbolique et amusante, Monsieur Sturdivant avait tout de même fait une affaire en payant deux pizzas aux



alentours de 25\$ en échange de bitcoins valant environ 41\$ à cette époque. Ce n'est que seulement 9 mois plus tard, que le bitcoin atteint la parité avec le dollar (une très courte période). Cependant, entre temps, la première crise de cette technologie a vu le jour. En effet, le 15 août 2010, une personne dont on ignore encore l'identité est parvenue à exploiter une faille dans le code source (originel) afin de créer 92 milliards de bitcoins. Seulement 1 an et demi après son lancement, c'est le développeur Jeff Garzik qui signale sur le forum Bitcointalk une anomalie à la hauteur du bloc 76 438, tout en essayant de comprendre une étrange transaction. Il découvre que son initiateur réussit à créer 92 233 720 368 BTC. Cette faille restera connue sous le nom de « overflow bug » et a nécessité la création d'un patch correctif. C'est apparemment Satoshi en personne qui publiera 5 heures après l'événement, la version corrective 0.3.10 de Bitcoin. Pour rentrer dans la partie technique de cette correction, il fallut effectuer un soft fork du réseau pour revenir au bloc 76 438. Les blocs produits entre temps, et donc les transactions qui les composent, ont dû être abandonnés, pour repartir depuis la nouvelle blockchain « saine » (comprenant le correctif et sans l'anomalie). En conclusion, pendant un court instant, il existait plus de 93 milliards de Bitcoins et le réseau a été interrompu pendant 5 heures. C'est le 12 décembre 2010 que Satoshi Nakamoto disparaît publiquement, il déclare passer le relais au développeur américain Gavin Andresen en lui confiant la clé d'alerte du protocole. Celle-ci permet d'adresser instantanément un message à tous les ordinateurs qui constituent les nœuds du système (en cas d'attaque informatique par exemple). L'année suivante (2011), de nombreuses cryptomonnaies émergent à partir du code source ouvert du Bitcoin. En 2012, on assiste à la création de la Bitcoin Foundation, une société à but non lucratif, afin de restaurer la réputation du bitcoin, salie par la criminalité et la fraude, mais également pour promouvoir son développement et son adoption. Cette importante association est basée à Washington et ses fondateurs sont : le célèbre développeur impliqué dans le développement du Bitcoin ; Gavin Andresen, l'entrepreneur Charlie Shrem, l'ancien dirigeant de Mt. Gox. Le français Mark Karpelès et Peter Vessenes, l'ancien dirigeant de Bitcoin.com ; Roger Ver et Patrick Murck. L'ensemble de ces efforts déployés, à travers des associations et des blogs internet, le Bitcoin devient de plus en plus apprécié, au point que WordPress accepte tous les paiements en bitcoins à partir de Novembre 2012 et que BitPay dénombre 1000 commerçants ayant adopté cette nouvelle monnaie également. Mars 2013, remet en lumière les défis techniques du Bitcoin, puisque la blockchain s'est temporairement scindée suite à la création d'un bloc de la version 0.8 que la version 0.7 a considéré invalide. C'est donc pendant 6 heures que deux réseaux Bitcoin ont fonctionné simultanément. Cet événement prouve que des changements technologiques pourront toujours représenter une menace pour le fonctionnement du Bitcoin. Malgré cet incident, la monnaie virtuelle a franchi la barre symbolique des \$1.000 en Novembre de la même année. L'année 2013 ouvre également le chapitre de l'attention réglementaire avec la classification officielle des mineurs de bitcoins en tant qu'entreprises de services monétaires. Cette volonté de contrôle se poursuit avec la saisie d'environ 26.000 bitcoin par le FBI sur le marché (illégal) Silk Road en Octobre, à la suite de l'arrestation de son opérateur, Ross Ulbricht. Bien que son prix continue de croître, c'est à la fin de l'année (en décembre 2013) lorsque la banque populaire de Chine annonce l'interdiction d'utilisation de Bitcoin aux institutions financières, que son prix chute, avant de se rétablir. C'est seulement quelques mois après, en 2014, qu'une crise majeure va venir perturber le Bitcoin. Cette crise est l'effondrement brutal



de la plateforme Mt. Gox, suite à un piratage informatique débouchant sur le détournement de 744 408 Bitcoins. Initialement spécialisé dans l'échange de cartes « Magic : The Gathering Online », l'entreprise se reconvertit en lieu d'échange de cryptomonnaies et c'est son acheteur Mark Karpelès, qui en a été le principal responsable de 2011 à sa chute en 2014. Suite à cette crise, le cours du Bitcoin est subitement tombé de \$1.000 à \$200, ce qui est compréhensible puisque qu'au début de l'année 2014, on estime que la plateforme émettait environ 70% des transactions en monnaie Bitcoin dans le monde. Bien évidemment, la communauté spécialisée dans le Bitcoin a pris conscience de l'importance de construire une infrastructure solide, ce qui a marqué l'année 2015. Et malgré la crise récente, c'est dorénavant plus de 100 000 commerçants qui accepteront les paiements en Bitcoins au cours de cette année (2015). Une grande avancée technologique survient en août 2017 avec la mise en place de Segregated Witness (SegWit). Cette mise en place fait suite au débat sur la scalabilité du Bitcoin, qui atteint son point culminant en 2017. Segwit est donc une modification du protocole Bitcoin qui a été introduite lors d'un « soft fork » du réseau original de Bitcoin et qui permet d'améliorer le débit de transactions sur un réseau blockchain, et donc d'améliorer la scalabilité et les frais de transactions. Cette technologie est introduite pour la première fois, non pas sur le Bitcoin mais sur le Litecoin. Segwit va donc réduire le poids des transactions en les séparant en deux. Avec une première partie comprenant les wallet-adresses (de l'expéditeur et destinataire) et la deuxième partie comprenant les données témoins (witness data), à savoir, les signatures de la transaction. Les données témoins sont donc détachées du bloc principal, ce qui réduit considérablement la taille de la transaction. Les transactions SegWit ont fini par représenter plus de 65% du total des transactions début 2020. Malgré l'activation de cette innovation, les désaccords sur l'avenir du Bitcoin ont conduit à la création du Bitcoin Cash par le premier hard fork majeur de Bitcoin ayant eu lieu le 1er août 2017. L'année 2017 ne se solde pas uniquement par des progrès technologiques. La valeur d'un Bitcoin dépasse les \$20.000 en décembre, créant un engouement mondial massif pendant que le Japon reconnaît cette cryptomonnaie comme un moyen de paiement légal en 2017. Dès 2020, le profil d'adoption du Bitcoin s'élargit fortement avec de grandes entreprises qui décident d'investir d'importants montants : MicroStrategy avec 250 millions de dollars – Square avec 50 millions de dollars – MassMutual avec 100 millions de dollars – puis Tesla en 2021 avec 1.5 milliards de dollars et des politiques d'acceptation de paiements de voitures en Bitcoin. Toujours en 2020, Paypal permet à ses utilisateurs d'acheter, de vendre et de détenir du Bitcoin, touchant directement 340 millions de personnes (des clients). Plus connu encore, en Septembre 2021 le président du Salvador, Nayib Bukele, introduit le Bitcoin comme monnaie légale dans le pays, au côté du dollar américain. Peu de temps après, un nouveau record historique est atteint avec \$69.000 pour un bitcoin, avant d'expérimenter une volatilité significative. Apparition des « Ordinals » sur Bitcoin et « Non-Fungible token ».

Satoshi Nakamoto : Pour cette deuxième rubrique nous décidons d'accorder de l'importance au(x) fondateur(s) de cette technologie. Bien que « Satoshi Nakamoto » soit un nom qui évoque quelque chose pour tout le monde, il cache encore beaucoup de secrets. Ce pseudonyme est apparu pour la première fois en 2008 lors de la publication du livre blanc « Bitcoin : A Peer-to-Peer Electronic Cash System ». Sous ce même pseudonyme, les premiers blocs ont commencé



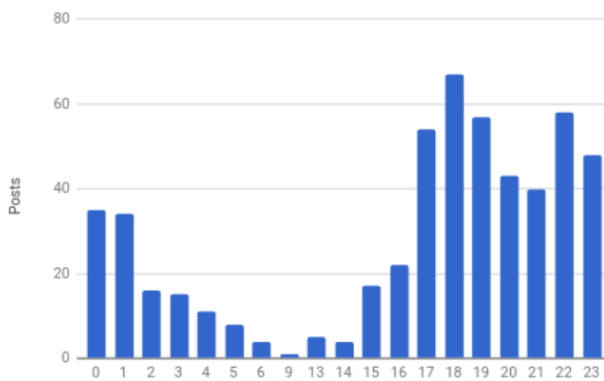
à être minés en 2009 tout en participant activement dans la communauté Bitcoin en répondant aux questions et en proposant des améliorations. Ce n'est qu'en 2011 qu'il disparaît de la scène publique. Il s'agit donc d'un (si ce n'est le plus) grand mystère de la finance moderne. Le propos au sujet de ce pseudonyme est très loin d'être simplement anecdotique puisqu'il peut constituer un des risques majeurs envers cette technologie (ou bien être un des aspects les plus positifs). Pour ne pas passer à la rubrique suivante sans éléments de réponse, nous allons nous plonger dans les indices et les faits qui permettraient de mieux cerner les nuances de ce sujet.

Commençons par la raison de son anonymat. Il est probable que ce soit tout simplement par choix afin de préserver l'intégrité du système qu'il a mis en place. En restant inconnu, le créateur ne peut influencer le développement de sa technologie, pour le meilleur (certainement). Par opposition, on retrouve Vitalik Buterin qui joue un rôle important dans le développement de l'Ethereum. Sa contribution pour sa cryptomonnaie est nécessaire mais représente un risque concentré sur sa personne. Du côté du Bitcoin, révéler l'identité de son fondateur serait dans de nombreux cas assez compromettant, que ce soit pour la confiance des détenteurs de la monnaie numérique comme pour des risques de pressions politiques. En étant ainsi, cette technologie peut se développer de façon organique en limitant le nombre de facteurs extérieurs influençant son développement. Cet anonymat persistant et le retrait de son fondateur pourraient donc être des raisons renforçant le caractère décentralisé du Bitcoin. Il s'agit d'une décentralisation fondée sur le contrôle et la gouvernance de la monnaie à la communauté.

En ce qui concerne à présent l'identité de Satoshi Nakamoto, certains dévoués du sujet penchent davantage pour la croyance qu'il s'agit plutôt d'un groupe de personnes derrière cette invention (dont certains seraient sûrement morts d'ailleurs). Ce que l'on sait c'est que le livre blanc sur le Bitcoin a été publié le 31 octobre 2008 sur le forum de P2P Foundation sous le pseudo Satoshi, sous un profil affirmant être un Japonais né le 5 avril 1975. Cependant, l'absence de publication en japonais et la qualité de son anglais laissent la communauté dans le doute. Avant la publication du white paper, Satoshi avait contacté Adam Back (le concepteur de Hashcash), puis Wei Dai (concepteur de b-money). C'est Ray Dillinger et Hal Finney qui reçoivent de façon privée le code du Bitcoin afin de l'examiner. Ces noms sont donc les premiers à avoir communiqué avec la personne anonyme, ils proposent donc différentes pistes. Aujourd'hui la liste des potentiels « satoshi » est plutôt longue. Il existe un membre du forum « Bitcointalk.org » nommé Stéphane Thomas, qui a représenté graphiquement les horodatages des « traces » de Satoshi. Résultat, aucune publication entre 14h et 20h, heure japonaise. Le plus probable est donc l'horaire américain.



Satoshi Posts to bitcointalk.org by Hour of Day BST



Une coïncidence pousse tout de même au questionnement. Lors de la publication du white paper, Satoshi reçoit 2 réponses négatives et une seule positive de la part d'Hal Finney qui reçoit et se connecte à la première version du logiciel le 10 janvier 2009. Ce sont ces deux mêmes hommes qui inaugurent la première transaction du réseau 2 jours plus tard.

- 31/10/2008 : Satoshi Nakamoto publie le livre blanc de Bitcoin
- 03/01/2009 : Lancement du réseau Bitcoin (bloc Genesis)
- 12/01/2009 : Première transaction BTC vers Hal Finney
- 23/04/2011 : Nakamoto envoie son dernier email à la communauté des développeurs

Blockchain : Pouvant être facilement traduit par « chaîne de blocs » ce terme est très souvent employé et il est indispensable de visualiser ce qu'est la technologie de la blockchain pour comprendre comment Bitcoin. La blockchain est aujourd'hui la fondation sur laquelle reposent de nombreuses cryptomonnaies mais est en réalité rien d'autre qu'un registre comptable numérique et horodaté. Attention cependant, Bitcoin est un cas de blockchain, ces deux choses fonctionnent ensemble pour cette cryptomonnaie mais la technologie de la blockchain est plus vaste et possède de nombreuses applications dans d'autres domaines sous différentes formes.

L'illustration la plus courante pour comprendre la blockchain est celle d'un livre (grand livre comptable) où l'on pourrait assimiler les pages à des blocs stockant différentes transactions, qui elles-mêmes seraient reliées entre elles grâce à la cryptographie et formant ainsi une « chaîne de blocs ». Dans le cas du Bitcoin, ces nouveaux blocs vont être créés par les membres (constitués de milliers d'ordinateurs puissants connectés en peer-to-peer, que l'on appelle des mineurs) qui cherchent à extraire du Bitcoin en résolvant des équations cryptographiques. C'est le système qui va diffuser publiquement chaque nouvelle transaction sur le réseau et le partager de nœud en nœud (tous les ordinateurs). Puis, les mineurs vont pouvoir rassembler ces transactions dans un nouveau bloc (toutes les 10 minutes environ) et les ajouter définitivement à la blockchain constituant donc le livre définitif du Bitcoin. Ces nœuds actifs en permanence vont être appelés des mineurs, utilisant des ressources informatiques importantes, en échange desquelles ils vont gagner une petite quantité de cryptomonnaie (avec le bitcoin limité à 21 millions). Donc, la puissance de calcul qui sert à produire des confirmations de transactions afin de les afficher dans la blockchain est rémunérée par la mise sur le marché de nouveaux bitcoins (dans la limite de 21 millions) et à plus long terme par les frais de transaction consentis par les utilisateurs pour accélérer le processus de validation. Les mineurs sont soumis à la concurrence, ainsi, plus il y aura de mineurs disposés à accomplir une tâche, plus la difficulté

pour confirmer des transactions devient élevée. De manière technique, pour réussir à confirmer un bloc de transactions, un mineur doit passer par un processus appelé « Proof Of Work » (preuve de travail) qui consiste à décrypter des données, d'où l'appellation de cryptomonnaies.

Au niveau du fonctionnement de ce type de blockchain pour le Bitcoin, aucun nœud du réseau ne peut avoir le contrôle exclusif, ce qui explique pourquoi la blockchain est un registre décentralisé. En plus d'être décentralisé, ce registre est autonome car chaque nœud possède un exemplaire du registre et ne nécessite donc pas l'intervention d'un tiers de confiance ou de quelque autorité. On dit alors que le registre de la blockchain du Bitcoin est décentralisé et autonome. De cette façon on peut distinguer plusieurs types de registres, selon la structure du réseau. Il peut s'agir de grand livre distribué, grand livre privé et grand livre public où tout le monde peut voir chaque transaction (bien que les portefeuilles soient anonymes), ce dernier système est celui utilisé par le Bitcoin et l'Ethereum.

Pour synthétiser la technologie de blockchain (en dehors de son application pour Bitcoin), on peut dire que c'est un mécanisme de base de données (registre) qui permet un partage transparent des informations au sein d'un réseau. La particularité est que les données sont stockées dans des blocs reliés entre eux dans une chaîne. Ces données sont chronologiquement cohérentes car personne ne peut supprimer ou modifier la chaîne sans le consensus du réseau. Ainsi, la blockchain peut créer un grand livre (registre) inaltérable ou immuable pour le suivi de tout processus lié à des paiements avec des mécanismes intégrés empêchant des entrées de transactions non autorisées, créant ainsi une cohérence dans la visibilité de ces transactions.

Utilisation : Maintenant que nous connaissons les événements qui ont accompagné l'ascension du Bitcoin et les principes de la technologie sur laquelle il s'appuie, nous allons nous positionner du point de vue du détenteur. Tout d'abord, comment détient-on du Bitcoin ? Dans un premier temps, il est nécessaire de passer par une plateforme d'échange (un courtier). Le but ici n'est pas de recommander une plateforme en particulier mais voici une liste des courtiers les plus fréquentés dans ce marché : Binance – Bybit – OKX – Coinbase – Bitget – MEXC – Gate.io – HTX – Kraken – Crypto.com – KuCoin – Upbit – Bitfinex – Gemini – Bitstamp. Il en existe naturellement bien d'autres encore mais pour faire ressortir le leader en termes de volume, il s'agit de Binance, qui gère un volume quotidien qui dépasse régulièrement les dizaines de milliards de dollars (45 Milliards de dollars). Binance est donc la plateforme où se concentre la majorité des transactions BTC mondiales, assurant la meilleure découverte de prix et de liquidité. Pour les Français, l'achat de Bitcoin via une plateforme PSAN est recommandé. PSAN signifie « Prestataires de Services sur Actifs Numériques », il s'agit d'un statut délivré par l'AMF (Autorité des Marchés Financiers), le régulateur français. Une fois la plateforme choisie, il suffit de se créer un compte (vérification d'identité probable) et alimenter celui-ci, de préférence par virement bancaire. Au préalable, il faut ajouter la plateforme en bénéficiaire et apporter des informations de virements pour que le courtier puisse l'associer à votre compte. Votre achat peut se découper en deux temps : vous déposez des/une monnaie(s) « fiat » (en général sans frais mais 1 à 2 jours) puis vous achetez vos Bitcoins. Autrement, vous pouvez directement acheter du Bitcoin par carte bancaire mais au risque d'être exposé à des



frais de transaction allant de 0.27 % à 5 %. Il existe bien évidemment d'autres options pour certaines plateformes qui autorisent les comptes Paypal etc... Une fois que vous avez votre plateforme et de l'argent déposé dessus, vous pouvez acheter du Bitcoin de deux façons. La première façon, étant la plus simple, consiste à accéder à l'interface simplifiée de votre courtier et de simplement renseigner votre devise d'achat, votre montant d'achat et puis de confirmer la transaction. La seconde façon d'acheter du Bitcoin se rapproche beaucoup plus d'un ordre en Bourse, où vous pourrez donc définir certains types d'ordres (prix limite d'achat, etc.) avec différentes durées de validité.

Ces étapes vous serviront pour acheter du Bitcoin, mais pas forcément pour le sécuriser. Il faut savoir que lorsque vous achetez un ou plusieurs Bitcoin sur une plateforme, vous pourrez les retrouver dans votre « wallet custodial » qui est votre portefeuille administré par votre courtier. De manière générale, un portefeuille, parfois aussi appelé porte-monnaie, est un appareil ou programme dont la fonction est de gérer des cryptomonnaies (d'en recevoir, d'en envoyer et de les conserver). Par ailleurs, un wallet Bitcoin génère une paire de clés (asymétrique), dont une clé privée et une clé publique. La clé privée est le mot de passe secret ultime qui prouve que vous êtes propriétaire d'un Bitcoin et vous permet donc de le dépenser en signant les transactions. Cette clé privée est souvent représentée en 64 caractères hexadécimaux ou dérivée d'une « seed phrase » de 12 à 24 mots. Cette fameuse seed phrase ne doit jamais être partagée, on recommande souvent de la conserver sur un matériel physique (papier, métal, etc...) en lieu sûr ou auprès d'un tiers. Une grande attention est apportée à cette clé car comme vous l'aurez compris, elle vous permet de déplacer les BTC de façon irréversible, de ne pas perdre vos BTC et d'éviter de vous faire voler (vos BTC). La seconde clé, publique, est, elle, dérivée mathématiquement de la première (de façon irréversible) et sert à générer des adresses Bitcoin (publiques) afin de pouvoir être partagée et recevoir des fonds. Cette clé publique peut donc être partagée librement et sert à générer des adresses Bitcoin. Cependant, un wallet peut générer plusieurs paires de clés (et adresses) à partir d'une seule seed phrase pour plus de sécurité mais nous en reparlerons plus tard. Pour en revenir aux plateformes, votre « wallet custody » possède donc une clé publique et une clé privée. Seulement, c'est votre courtier qui détient les clés privées de ces Bitcoins. D'où la phrase « Not your keys, not your coins ! ». Cela signifie que si la plateforme est piratée, fait faillite (comme FTX en 2022 ou Mt. Gox en 2014), gèle les retraits, ou subit une réglementation, vous risquez de perdre l'accès à vos fonds. Sachant cela, on comprend mieux l'intérêt de vouloir sécuriser ses Bitcoins une fois achetés.

Une fois acheté, il est fortement recommandé de transférer ses Bitcoins vers un portefeuille personnel sécurisé « Self-Custody Wallet ». Pour commencer, il existe deux grands types de portefeuilles : les « hot wallets » et les « cold wallets ». Un hot wallet sera directement connecté à Internet lors de son utilisation, tandis qu'un cold wallet ne le sera pas. De ce fait, on comprend rapidement pourquoi les cold wallets sont considérés comme plus sécurisés, car ils réduisent la surface d'attaque pour un piratage informatique. Dans un premier temps, les hot wallets sont des solutions de stockage à chaud des clés privées, des solutions qui utilisent des appareils connectés à internet et concerneront donc tout ce qui est portefeuille logiciel (software wallet). Il est évidemment déconseillé de stocker de grosses sommes de bitcoins sur ce type de portefeuille car il offre une plus grande surface d'attaque pour les piratages. Dans cette catégorie



de portefeuille, on retrouve les nœuds complets, les portefeuilles légers, les extensions de navigateur et les portefeuilles web. Nous allons détailler les spécificités de chaque portefeuille ci-dessous.

Hot Wallets

- Les nœuds complets (full nodes) : Aussi appelé client complet, il s'agit du premier type de portefeuille ayant jamais existé. Un nœud complet réalise toutes les tâches nécessaires au réseau, à savoir le téléchargement de la blockchain, la validation des transactions non confirmées ainsi que la validité des blocs. Cette difficulté d'usage rend ce genre de portefeuille peu adapté aux gens ordinaires et plutôt conçu pour les acteurs impliqués et les utilisateurs avancés. Le logiciel de nœud complet le plus connu est Bitcoin Core, utilisé par 95 % des nœuds du réseau.
- Portefeuilles dits « légers » (lightweight wallets) : ce sont encore des nœuds mais qui ne téléchargent pas la blockchain mais qui procèdent à des vérifications simplifiées des transactions qui nécessitent que peu de ressources informatiques. Ces wallets sont disponibles sur ordinateur, tablette, mobile. Pour les ordinateurs on peut utiliser Electrum. Les lightweight wallets sont souvent appelés portefeuilles SPV pour Simplified Payment Verification. Ils peuvent interagir avec les nœuds complets du réseau pair-à-pair de la cryptomonnaie ou bien avec une infrastructure de serveurs dédiés qui rendent l'utilisation plus facile (comme Electrum). Dans les deux cas, cela fonctionne au détriment de la confidentialité de l'utilisateur (certaines méthodes de brouillage peuvent tout de même être utilisées).
- Les extensions de navigateur web : Il s'agit bien de Chrome, Firefox ou Brave... En fonction de l'extension, le portefeuille ne procède pas à la vérification de transactions. Les extensions, étant présentes depuis le navigateur, elles se retrouvent de fait très utiles pour interagir avec les applications décentralisées. On a, entre autres, Badger pour Bitcoin Cash.
- Les portefeuilles web (web wallets) : Interfaces en ligne permettant de gérer des fonds. Vous gérez vos clés privées grâce au navigateur et elles ne sont jamais révélées à autrui. Les quelques vulnérabilités de ce type de portefeuille résident dans le fait qu'ils ne procèdent généralement pas à la vérification des transactions et se contentent des informations fournies par les serveurs du site utilisé. De plus, ces portefeuilles sont sensibles à l'hameçonnage de la page web utilisée. On trouve Blockchain.com et coin.space, qui gèrent tous les deux le bitcoin et le bitcoin cash.

À la différence des hot wallets, les cold wallets sont des solutions de stockage à froid des clés privées, c'est-à-dire hors de tout accès direct à Internet. Ce type de stockage est souvent recommandé pour les détenteurs à grande échelle de Bitcoins car il est réputé pour être le plus sécurisé. D'ailleurs il est courant pour les plateformes d'échange d'avoir recours à cette méthode pour conserver les fonds de leurs clients. N'importe quel objet hors-ligne peut servir de cold wallet mais les deux types de portefeuille les plus populaires sont les portefeuilles matériels et papier.



Cold wallets

- Les portefeuilles matériels « Hard Wallets » : ce sont des appareils qui permettent de générer et de conserver des clés privées de manière isolée et de permettre de signer des transactions hors ligne. Il est encore aujourd'hui considéré comme la solution la plus sûre de détenir ses bitcoins. On retrouve le français Ledger ou encore Trezor, BitBox, Coldcard, Jade, Passport, etc. comme marques les plus connues dans ce type de solution.
- Les portefeuilles papiers « paper wallets » : Ce sont les portefeuilles les plus simples de tous ceux que nous avons présentés. Cette solution consiste à imprimer sa clé privée directement sur une feuille de papier, cela devient donc un portefeuille papier. On peut effectuer plusieurs transactions vers ce portefeuille sans en compromettre la sécurité, mais il est recommandé d'effectuer une seule transaction suite au retrait de bitcoins de ce portefeuille. Pour créer un portefeuille papier, il suffit tout simplement de se rendre sur le site bitcoinpaperwallet.com. Attention cependant, ces portefeuilles ne permettent pas de signer des transactions et sont donc à usage unique.

Après avoir répondu à la question « comment acheter du bitcoin ? », nous allons répondre à la question « comment gagner de l'argent avec ses bitcoins ? » et apporter des arguments contredisant les remarques décrivant le bitcoin comme un actif qui ne « produit rien ». En effet, il existe différentes façons de percevoir une rémunération passive grâce à ses cryptomonnaies. Pour commencer, il est possible de « staker » ses Bitcoins sur une plateforme tout en conservant leur garde. Le « staking » consiste en une immobilisation de ses cryptomonnaies (en tant qu'investisseur) sur un réseau blockchain (pour une durée déterminée) en vue de le sécuriser, en échange d'une rémunération. Ces bitcoins bloqués soutiendront donc l'infrastructure de la blockchain en permettant aux validateurs de vérifier les transactions et d'ajouter de nouveaux blocs à la blockchain. En échange de ce soutien, les investisseurs reçoivent des récompenses de staking qui leur seront payées dans la cryptomonnaie concernée. Le montant de ces rémunérations est exprimé en taux de rendement annuel et payé annuellement. Toutefois, le bitcoin fonctionnant sur des systèmes de PoW (Proof of Work – « Preuve de travail ») ne peut être staké que sur des systèmes/protocoles PoS (« Proof of Stake ») comme l'Ethereum par exemple. Par exemple, la plateforme Kraken propose un staking de Bitcoins via Babylon afin de contribuer à la sécurité des réseaux Bitcoin Supercharged Networks basés sur la preuve d'enjeu (PoS). Un second moyen de percevoir une rémunération en échange de ses cryptomonnaies est de pratiquer le Yield Farming en devenant un « Liquidity Provider », un fournisseur de liquidité. Cette deuxième méthode consiste à déposer ses cryptos dans un « pool » de liquidité, qui est une réserve de crypto, et reçoit une preuve d'apport en échange. En déposant ses cryptos dans ce pool, il perçoit donc un rendement en tant que fournisseur de liquidité. Cette liquidité est vitale pour le bon fonctionnement de l'écosystème des cryptomonnaies, à savoir, emprunter ou échanger des cryptos (effectuer un swap). Ces transactions nécessitent souvent des collatéraux et des réserves de nombreuses cryptomonnaies, d'où la création de pools. Lorsque les swaps sont effectués ou les emprunts sont contractés, certains frais s'appliquent et permettent donc de rémunérer les investisseurs ayant mis des liquidités à disposition. L'avantage de cette seconde méthode est que l'investisseur peut récupérer sa mise à tout moment, c'est donc un placement assez liquide. En prolongeant les



deux premières méthodes, on peut facilement comprendre le principe du « Lending ». Comme son nom l'indique, il permet à un détenteur de cryptomonnaies de les prêter, en échange d'intérêts. Pour ce faire, il suffit de déposer ses valeurs sur un protocole lending-borrowing. Ces mécanismes doivent donc se dérouler sur des applications décentralisées, les DApps (decentralized applications), fonctionnant en pair-à-pair et permettant à n'importe quel individu de prêter et d'emprunter des cryptomonnaies. Ici, comme dans le deuxième cas, l'investisseur deviendra un « Liquidity Provider » et les procédures de respect des règles d'emprunts et leurs bons fonctionnements seront assurés par des smart contracts. À cela s'ajouteront des règles de collatéral afin d'offrir le maximum de sécurité en dépit de l'absence d'intermédiaire. À ce sujet, la plupart des emprunts en finance décentralisée sont sur-collatéralisés, ce qui signifie que l'emprunteur doit fournir un collatéral supérieur à la somme empruntée.

Pourquoi acheter du Bitcoin :

Maintenant que nous connaissons l'histoire derrière cette technologie et les moyens d'acheter du Bitcoin et d'en générer des revenus passifs, nous devons chercher à comprendre ce qui pousse les gens à en acheter et pourquoi sa valeur est aussi importante aujourd'hui.

En général, l'on achète un bien ou un service afin de satisfaire un ou plusieurs besoins. Comprendre pourquoi certaines personnes achètent du bitcoin revient à se poser la question : quel(s) besoin(s) cherchent-ils à satisfaire ? Pour répondre à cette question de façon plus facile et intuitive, on propose de commencer par identifier la valeur de Bitcoin. Pour ce faire, il serait logique de comprendre dans un premier temps ce qu'est la valeur et dans un second temps, ce qu'est le bitcoin (ce qui est déjà le cas en grande partie). Pour rester synthétique, la valeur s'approche traditionnellement par deux concepts/courants : la théorie de la valeur-travail, élaborée principalement par Adam Smith, David Ricardo et Karl Marx – ainsi que la théorie de la valeur-utilité, élaborée principalement par Jean-Baptiste Say, William Stanley Jevons, Carl Menger et Léon Walras. La première théorie part du principe qu'il existe un prix « normal » et qu'il est déterminé par les moyens de production (approche objective), à savoir, la terre, le capital et le travail. La deuxième théorie développée à partir des années 1870, adopte une approche dite subjective, se basant sur le prix de marché. Dans cette deuxième théorie, celle de la valeur-utilité, sont introduits de nouveaux paramètres, tels que la conscience, les désirs (de l'homme) ainsi que les notions de rareté, d'utilité marginale et totale (permettant de résoudre le paradoxe de l'eau et diamant). Aujourd'hui, la majorité des économistes adhèrent à la théorie de la valeur-utilité, c'est donc celle sur laquelle nous allons essayer de baser notre raisonnement. Cependant, le débat n'étant toujours pas terminé, construire des critères/indicateurs pour expliquer la valeur de tout bien et particulièrement du bitcoin, reste difficile et nécessite de s'inspirer des deux théories ainsi que de se servir de bon sens. Ci-dessous un tableau plus ou moins objectif, essayant de représenter les différentes sources de valeurs/explications derrière le prix du bitcoin.

Critère	Explication	Application sur le Bitcoin
Coût de production	Ce que ça a coûté (MP – Machines – Ouvriers etc..)	Coût de minage.



Valeur d'usage/utilité	À quoi cela sert te à quel point c'est utile pour une personne.	Système paiement décentralisé – Réserve de valeur.
Rareté	S'il y en a peu, ça devient précieux.	Offre limitée à 21millions de BTC.
Prix de marché	Ce que les gens sont prêts à payer aujourd'hui (le prix affiché ou négocié).	\$73 000
Valeur subjective/Préférence personnelle	Ce que ça vaut pour une personne à titre personnelle.	Révolution libertarienne.
Valeur d'échange	Prix de marché, valeur de revente.	Immobilier – Voitures.
Valeur symbolique/statut	Une idée, un souhait, un sentiment (Luxe – appartenance à un groupe).	Appartenance à un mouvement – Conviction.

Suite à la lecture de ce tableau, on peut rapidement comprendre que Bitcoin répond à de nombreuses caractéristiques et n'est donc pas « sans valeur » comme de nombreuses vieilles pensées souhaitaient nous faire croire. Maintenant que nous avons des points de repère sur la valeur de cette technologie, nous pouvons chercher à comprendre pourquoi ce nouvel actif/monnaie connaît un succès aussi important. Et pour ce faire, il faut commencer par se poser une question propre à l'investissement, qui est : « Pourquoi un actif coûte-t-il tant ? » plutôt que de chercher à estimer sa valeur. Cette méthode s'avère être pertinente puisque le marché intègre très souvent plus de données que nous puissions le faire et qu'après tout, il vaut mieux naviguer dans le courant plutôt qu'être contre celui-ci mais dans la bonne direction. À présent, si l'on souhaite trouver des réponses sur pourquoi le Bitcoin connaît autant de succès et son prix est aussi important, je pense que les réponses sont présentées au début de son histoire et dans le message laissé par son fondateur dans le bloc de genèse. Le papier blanc est apparu le 31 octobre 2008 soit juste après la faillite de Lehman Brothers, ce qui nous aide fortement à comprendre sa signification. Pour résumer la situation et l'interprétation des acteurs du Bitcoin aujourd'hui. La crise financière de 2008 a laissé beaucoup de séquelles sur l'économie américaine et par conséquences mondiales. Mais elle a surtout montré quelles étaient les nouvelles mentalités de l'industrie financière. Richard Fuld a reçu des compensations de \$480M – Angelo Mozilo (Countrywide Financials), \$471M – Stanley O'Neal (Merrill Lynch), \$161M – James Cayne (Bear Stearns), \$163M – Henry Paulson (Goldman Sachs), \$500M – etc. Le principe ici n'est pas de critiquer ou de chercher à comprendre pourquoi les rémunérations et bonus se présentaient dans de telles proportions mais plutôt de montrer pourquoi l'opinion des épargnants et d'autres investisseurs s'est mise à changer suite à un sentiment d'insécurité et de perte de confiance. La période suivante comptait 15 millions de chômeurs aux États-Unis avec 170 mille familles sans-abri alors que seulement 9 banques distribuaient un bonus total de 32.6 milliards de dollars avant de recevoir un renflouement massif de 700 milliards de dollars, faisant augmenter la dette nationale, créant de l'inflation tout en créant un sentiment d'injustice. Par ailleurs, cette dette nationale est passée de 10 trillions de dollars pour un PIB de 15 trillions de dollars en 2008 à une dette de 38.40 trillions de dollars pour un PIB de 29.2 trillions de dollars en 2025. Ces éléments renforcent la perte de confiance envers le système économique américain



et affaiblissent le pouvoir d'achat de ses citoyens. Plus actuellement, la situation politique ne s'améliore pas non plus puisque pendant que le budget prévoyait 130 milliards de dollars d'aide à l'Ukraine avec 1 autre trillion de dépenses militaires annuel, les journaux publient le titre suivant : « Why Do US Congressional Leaders Keep Beating the Stock Market ? ». Après ce tableau relativement sombre de la direction économique des États-Unis après la dernière grande crise, on comprend plus facilement pourquoi autant d'acteurs se sont intéressés au système bitcoin. En premier lieu le dollar se dévalue, en second lieu il est de plus en plus difficile de faire confiance au système et aux gouvernements et cette instabilité fait naître une crainte de nouvelle crise majeure imminente. C'est aujourd'hui, près de 17 ans après que l'on se rend réellement compte de l'utilité et de l'importance de cette innovation, faisant de Satoshi un visionnaire ou plutôt un acteur économique très réaliste. Le bitcoin n'a de cesse gagnée en valeur à mesure que le temps passe (donc que la situation économique s'aggrave) et que le dollar se dévalue (rendant la croissance des prix du Bitcoin assez mécanique). Cette observation nous conduit donc à affiner notre vision de la valeur. En se détachant quelques instants de la valeur de marché d'un Bitcoin, on se rend compte qu'il s'agit en réalité d'une véritable innovation libertarienne du début à la fin. C'est un système qui permet de détruire l'acteur intermédiaire de l'économie, les banques. Le créateur reste inconnu et après des années de recherches et d'indices, même les autorités fédérales, tel que le FBI, ne parviennent pas à trouver le responsable. Cette histoire est très marquante et remarquable, surtout quand le but de cette invention est de créer de l'anonymat et lutter contre un système qui ne satisfait plus beaucoup de personnes sur terre. Bien que Satoshi Nakamoto ne soit pas tangible, d'autres le sont, c'est le cas de Pavel et Nikolaï Durov, les frères fondateurs de la messagerie Telegram. Le cas de Nikolaï (en particulier) nous permet de comprendre en définitif qui sont les véritables créateurs de valeurs. Les grands progrès scientifiques parviennent en effet à transformer nos modes de vies et repenser nos systèmes sociaux. Ces progrès ont été, la découverte de la lumière (artificielle) de l'électricité etc... Nikolaï était avant tout un mathématicien de rang mondial et un informaticien. Avec son frère, ils ont en quelque sorte mis leurs savoir scientifique et compétences informatiques au service du monde entier en créant une messagerie cryptée pour laquelle ils sont prêts à faire des sacrifices. Bien que l'exemple de Telegram soit plus parlant, Bitcoin peut être un phénomène d'autant plus important que la création d'une messagerie qui compte tout de même environ 1 milliard d'utilisateurs aujourd'hui. Cette dernière réflexion de ce paragraphe nous permet de répondre de façon simple à la question qu'est-ce qu'est Bitcoin dans un cadre intellectuel. Bitcoin est l'application principale d'une innovation technologique majeure qui représente une révolution financière pour les acteurs économiques du monde entier. À présent, pour répondre aux questions initiales ; le monde s'intéresse de plus en plus à Bitcoin, car la confiance envers le système financier s'effrite à mesure que les années passent et que les indicateurs économiques se dégradent, car le dollar continue de se dévaluer, car cette technologie est un refuge accessible à de très nombreux pays dont les devises s'écroulent continuellement, car il devient même un actif alternatif et permet de répondre à encore plus de critères (caractéristiques d'un produit/actif) d'investissement pour d'autres. Les personnes achetant du Bitcoin peuvent englober différents profils, certains cherchent une nouvelle sécurité, une forme d'or plus perfectionné, d'autres adhèrent à une nouvelle idéologie. Même si le terme idéologie peut inquiéter certains investisseurs, il faut garder à l'esprit que



nombreuses sont les sociétés immobilières, les concessions automobiles et autres commerces en tout genre qui acceptent d'être payés en Bitcoin. Ce qui montre que la qualification devise n'est pas inappropriée et qu'il n'y a pas besoin d'autorités gouvernementales pour que le Bitcoin s'impose dans l'industrie financière. Pour répondre à la dernière question, pourquoi un Bitcoin vaut \$ X (le nombre de dollars actuellement), il est préférable d'offrir un tableau (ci-dessous) indiquant environ la valeur d'un Bitcoin en fonction de la masse monétaire qu'il représente. La masse monétaire totale de chaque catégorie est tirée de la présentation de Michael Saylor au Bitcoin 2024. Cette représentation est plus intuitive et accessible que bien d'autres notions abstraites.

Classes d'actifs	Valeur totale	Prix d'un Bitcoin
Or	\$ 16 T	\$ 762 000
Art	\$ 18 T	\$ 857 000
Actions	\$ 116 T	\$ 5 523 809
Obligations	\$ 300 T	\$ 14 286 000
Immobilier	\$ 330 T	\$ 15 714 000

Vecteur de l'investissement, Michael Saylor : Bien que la plupart des informations importantes au sujet de Bitcoin aient été dites précédemment, il est intéressant de se pencher sur le cas de Michael Saylor. Il est le multimilliardaire cofondateur de la société (ex MicroStrategy) Strategy qui est l'une des premières sociétés à avoir acheté du Bitcoin dans le cadre de sa stratégie financière. La société posséderait aujourd'hui environ 700 000 Bitcoins selon différentes sources. Cet engagement aussi massif dans cette cryptomonnaie nous amène donc à écouter le narratif derrière la conviction de Michael Saylor envers ce nouvel actif. Il s'impose incontestablement comme un des plus grands défenseurs et croyants de Bitcoin. Pour ce faire nous allons reprendre sa présentation au Bitcoin 2024.

Transcription de Michael Saylor : Je veux parler de la Révolution Bitcoin et je veux aussi parler de la reconstruction de notre économie mondiale avec le capital numérique. Le monde tel que nous le connaissons repose sur des idées du XXe siècle et sur des technologies du XXe siècle. Les actions se négocient de 9 h 30 à 16 h, sauf en cas de jour férié bancaire ; on ne peut rien faire le week-end. Tout est lent, tout est coûteux.

Si nous voulons prospérer au XXIe siècle, nous avons besoin de nouvelles idées et elles doivent reposer sur de nouvelles technologies. Ce graphique, vous l'avez déjà vu. Je l'ai affiché : 900 000 milliards de dollars de richesse mondiale. Ces 900 000 milliards sont répartis entre des actifs physiques et des actifs financiers fondés sur des idées et des technologies du XXe siècle. Dans le coin supérieur gauche, il y a une petite tache orange, le petit actif orange qui pourrait changer la donne, ce que nous appelons Bitcoin. Il représente un billion de dollars. Cela semble énorme quand on part de zéro, mais quand on le regarde dans l'ensemble du schéma mondial, cela représente 0,1 %.

Voici une autre façon de voir ce même graphique : ce ne sont pas 900 000 milliards d'actifs, mais un ensemble d'actifs détenus pour leur valeur d'usage et un ensemble d'actifs détenus comme réserve de valeur à long terme, le capital à long terme. Quand j'achète une maison, je



veux y vivre. Mais quand j'achète des obligations, je place simplement mon argent là parce que je ne sais pas quoi en faire d'autre. Quand on commence à voir le monde comme contenant une énorme quantité de capital à long terme – 450 000 milliards de dollars ou plus – et qu'on réfléchit à la manière dont nous stockons ce capital, on voit apparaître le moteur de la révolution. L'économie mondiale souffre parce que nous nous appuyons sur des actifs imparfaits et des systèmes imparfaits pour stocker ce capital. Cela paralyse notre capacité à préserver le capital. Alors, comment concevoir un meilleur système ?

Voici ce que disait Tesla : « Si vous voulez comprendre l'univers, pensez en termes d'énergie, de fréquence et de vibration. » Je vais traduire cela. Je vais parler de la physique de l'argent.

L'énergie, c'est l'argent, le capital ou la richesse – on peut les utiliser de manière interchangeable ici. La fréquence, c'est la durée, la durée de vie : combien de temps cela va-t-il durer ? Une minute, une heure, un an, un siècle ? Et nous faisons vibrer l'argent chaque fois que nous échangeons entre nous, que nous transférons d'un lieu à un autre ou que nous transformons un bien en un autre type d'actif.

Voici une équation importante : la durée de vie utile d'un actif = la valeur de l'actif ÷ le coût pour le maintenir en bon état. Si vous cherchez la durée de vie utile de votre argent dans un actif, posez-vous la question : combien cela coûte-t-il chaque année de maintenir cet actif en parfait état ? Combien dois-je dépenser pour éviter la dépréciation ou la détérioration ? Il s'avère que cette durée de vie utile est très proche de ce que nous appelons dans la communauté Bitcoin le ratio stock-to-flow. Les deux concepts sont très liés quand on les mesure en années.

La plupart des individus et la majorité des entreprises utilisent des actifs financiers pour préserver leur capital. C'est là que réside notre principal défi. Prenons les actifs financiers. Je veux conserver mon argent sur une longue période. Je commence avec un milliard de dollars. Je le mets en pesos : l'argent se dégrade en deux ans. Un taux d'inflation de 98 % vous dépouille de votre énergie économique, de votre capital. Ce n'est pas un bon actif à longue durée. La lire turque ? Votre capital dure trois ans. Le dollar américain, avec l'inflation monétaire traditionnelle du siècle dernier, pourrait durer environ 14 ans. Mais ce n'est pas comme si vous l'aviez pendant 14 ans : sa valeur est aspirée linéairement tout au long de ces 14 années.

Vous placez votre argent dans un Hedge fund ? Le coût annuel est de 2 % de frais de gestion plus 20 % de la performance, environ 4 % par an sur des actifs classiques. Cela fait de cet actif un actif de 25 ans. Les bons du Trésor ? Vous obtenez un rendement, mais après impôt, disons 3,5 %, contre une inflation monétaire de 7 % : votre argent dure peut-être 30 ans. Un fonds commun de placement avec 1 % de frais par an ? C'est à peu près le meilleur scénario. Si vous arrivez à obtenir un portefeuille diversifié à 10 points de base, le risque de contrepartie vous ramènera quand même à environ 1 % de coût. Voilà pour les actifs financiers. Nous faisons fonctionner le monde avec un ensemble d'idées du XXe siècle et, en moyenne, un actif financier dure 30 ans.

Nous savons tous que l'inflation dilue la valeur des actifs financiers, mais l'inflation n'est que la partie visible de l'iceberg. Vous subissez aussi des dilutions par les tarifs douaniers, les péages, les litiges, les taxes de transfert, les impôts sur le revenu, les plus-values... À chaque



fois que vous faites vibrer et bouger votre argent, on vous taxe. Et si les taxes ne vous détruisent pas, il reste encore la météo, la concurrence, l'obsolescence, la politique, les catastrophes...

Si vous voulez préserver votre énergie économique, vous devez lutter en permanence contre toutes ces frictions. La plupart des gens trouvent cela frustrant et sans issue, alors ils abandonnent les actifs financiers et se tournent vers les actifs physiques pour préserver leur capital. Une Ferrari ? Pas une bonne façon de conserver son argent pour toujours. Au bout de 5 ans, vous avez dépensé autant en assurance, entretien et dépréciation que ce que vaut la voiture. Un yacht ? Pas mieux. Si vous dépensez 10 % de sa valeur par an pour l'entretenir, la dépréciation vous frappe aussi. Une maison à Miami Beach ? Si vous achetez une maison à 10 millions de dollars, il vous faudra 10 millions supplémentaires pour l'entretenir sur 17 ans. Il ne vous reste plus rien. L'argent métal ? 22 ans. Un entrepôt ? 40 à 50 ans. Un lingot d'or ? 62 ans. Un tableau ? 72 ans. La terre ? La taxe foncière moyenne aux États-Unis est de 1,1 %. Votre argent dure donc 91 ans... sauf si le gouvernement réévalue la propriété, et alors c'est moins. Le plus ancien ranch familial aux États-Unis, le King Ranch, a tenu 173 ans. Toutes les autres familles du pays ont échoué. La plus longue détention de propriété ? Le Crown Estate au Royaume-Uni. On pourrait dire que la famille royale le détient depuis 1066, mais en réalité il est passé des Plantagenêts aux Stuarts, aux Lancastre, aux York, puis aux Hanovre... Peut-être sept familles différentes. Aucune ne l'a emporté avec elle. On pourrait penser que les actifs physiques durent mille ans. En réalité, 50 à 75 ans est probablement le maximum que vous obtiendrez. L'entropie dilue la valeur de vos actifs physiques. Elle aspire l'énergie, le capital hors d'eux. Il y a une raison pour laquelle on appelle ça la Terre et non le Paradis.

Les politiciens sont très créatifs : taxe municipale, taxe de comté, taxe d'État, taxe fédérale, taxe de transfert, taxe d'usage... Et si cela ne suffit pas, il y a le contrôle des loyers, le contrôle des prix, le choc culturel, la discrimination, la récession, l'effondrement de la monnaie, les locataires qui ne paient pas, quelqu'un qui glisse sur le trottoir et vous poursuit en justice, la météo, la guerre, le crime, les catastrophes...

Et si les prix de l'énergie explosent, c'est fini. Le capital physique n'est pas une solution simple. J'ai appris à MIT les trois lois de la thermodynamique :

- On ne peut pas gagner - On ne peut même pas faire match nul - Mais on ne peut pas quitter la partie

On pourrait s'arrêter là et être un peu déprimé. Mais nous ne voulons pas perdre. Alors on commence à penser : et si on trouvait un moyen de sortir du jeu ? Alors on pourrait au moins faire match nul... et peut-être gagner. Satoshi a trouvé un moyen. Il l'a donné et il est parti. C'est Bitcoin. Bitcoin est du capital numérique. C'est ce qu'il a créé. Bitcoin est un capital immortel, immuable et immatériel. Il a une durée de vie infinie. Il n'est pas attaqué par les forces du climat, de l'entropie, de l'inflation. Il est immatériel, il n'existe pas dans le monde physique, il ne subit pas toutes ces horreurs qui frappent les actifs financiers et physiques. C'est la solution à notre dilemme économique : transformer notre capital des actifs financiers et physiques vers des actifs numériques. Cela résout le problème auquel nous sommes tous confrontés.



Quelle est la durée de vie de Bitcoin ? Si vous placez votre Bitcoin chez un dépositaire institutionnel de qualité, vous payez 10 points de base par an. Selon la première loi de l'argent, cela signifie que votre capital dure mille ans. Le dépositaire ne durera peut-être pas mille ans, mais cela n'a pas d'importance : vous pouvez déplacer votre Bitcoin chaque année ou chaque décennie et rester toujours un pas devant la faillite des dépositaires. Vous ne pouvez pas téléporter un immeuble. Vous ne pouvez pas téléporter le King Ranch. Mais Bitcoin, oui. Si vous le conservez vous-même (self-custody), cela coûte environ 1 point de base par an avec de bons portefeuilles hardware et dispositifs de signature, et une journée par an pour vérifier. Vous avez alors un actif de 10 000 ans. Et si vous le confiez à une IA ? Un programme informatique peut maintenir les clés privées pour le prix de l'électricité. Vous obtenez un actif de 100 000 ans. Les IA voudront du Bitcoin. Si elles doivent choisir entre posséder du Bitcoin, un ranch au Texas, un lingot d'or ou des pesos argentins, le choix est évident. Les actifs numériques sont dans une catégorie à part. Quand on les compare à tous les autres actifs de préservation de capital, ils sont hors échelle. Tout le reste vit dans le domaine des 30, 40, 50 ans. Bitcoin est dans le domaine des 1 000 à 100 000 ans. C'est une percée dans la préservation du capital... et donc une révolution économique. Si vous voulez devenir riche, échangez intelligemment. Voici un principe très simple : échangez le temporaire contre le permanent. Échangez votre glace qui fond contre des pesos, les pesos contre des dollars, les dollars contre de la terre, la terre contre du Bitcoin. Échangez la monnaie contre du capital. Échangez le fragile contre le résilient. Échangez le local contre le global. Échangez le physique contre le numérique. Échangez la sécurité contre la rareté. Vous ne pouvez pas vous tromper en allant dans cette direction. Échangez la monnaie contre du capital. Échangez quelque chose de fragile contre quelque chose de résilient. Échangez la sécurité contre la marchandise. Échangez la marchandise contre la rareté. Vous ne pouvez pas vous tromper en allant dans cette direction.

Parlons maintenant de quelques grands échanges de l'histoire, certains valant des milliers de milliards de dollars. Les Hollandais comprenaient la puissance navale. Ils comprenaient les navires, ils en avaient des milliers. Ils ont acheté le meilleur port du Nouveau Monde pour quelques centaines de dollars en babioles en plastique et en textiles. Aujourd'hui, cela vaut deux mille cinq cents milliards de dollars. C'était un investissement qui a rapporté 6 % par an pendant 398 années consécutives, soit un rendement de 10,5 milliards de fois. Et quand on y pense, on se dit : pourquoi diable auraient-ils abandonné le meilleur port d'Amérique contre un tas de tissus, de plastique et de verre ? Mais les gens qui le leur ont vendu ne comprenaient pas ce qu'était la puissance navale. Si vous ne comprenez pas pourquoi vous allez vouloir cette propriété à l'avenir, vous ne la valoriserez pas correctement. Napoléon voulait conquérir l'Ancien Monde, Jefferson voulait étendre le Nouveau. La France vend donc la Louisiane aux États-Unis pour 15 millions de dollars en 1803. Ces 15 millions ont probablement duré quelques mois pour alimenter l'armée française, puis c'était fini. Jefferson, lui, a obtenu 27 % du territoire des États-Unis actuels. Cela représente un rendement de 800 000 fois, soit plus de 12 000 milliards de dollars aujourd'hui, et ça vaudra encore plus demain. Jefferson avait de la vision, tout comme cet homme : Seward. Seward achète l'Alaska pour 7 millions de dollars, deux ans après que le pays ait été dévasté par la guerre de Sécession. John D. Rockefeller essayait à peine de lancer une compagnie pétrolière. Aujourd'hui, il y a un trillion de dollars de pétrole sous l'Alaska. Un retour colossal pour un simple bout de papier. Quelle est la valeur du capital



numérique ? Prenons les 450 000 milliards de dollars, multipliez par 3 % : c'est votre coût d'entropie, votre coût d'inflation. Cela coûte au monde 13,5 billions de dollars par an pour essayer de préserver sa richesse face à toutes ces horreurs. Si on applique un multiple de 20, comme on le fait pour valoriser une entreprise ou une obligation à très longue durée, cela donne 270 000 milliards de dollars.

Le capital numérique vaut donc entre 10 000 et 20 000 milliards de dollars par an, et des centaines de milliers de milliards en valeur totale. Suis-je complètement à côté de la plaque ? Vérifions la réalité : le capital numérique a rapporté 55 % par an ces quatre dernières années. Le meilleur actif financier au monde, les obligations, a fait -5 %. Imaginez capitaliser votre entreprise ou votre pays sur du -5 % au lieu de +55 %. Ça fonctionne, c'est évident. Revenons à mon graphique de la richesse mondiale. On voit toujours ce petit carré Bitcoin dans le coin gauche. Mais que se passe-t-il vraiment ? Voici ma prévision macro Bitcoin sur 21 ans, jusqu'en 2045. Je pense que le rendement annuel composé va passer progressivement de 55 % à 50 %, 45 %, 40 %, 35 %, 30 %, 25 %, puis 20 %. Il va ralentir graduellement jusqu'à croître environ deux fois plus vite que l'indice S&P. À ce rythme, Bitcoin atteindrait 13 millions de dollars par pièce en 2045. Cela pourrait être 3 millions dans le scénario pessimiste, 49 millions dans le scénario haussier. Mais même à 13 millions, Bitcoin représenterait environ 7 % de tous les actifs mondiaux.

Et le reste des actifs ? Je pense que l'IA et la technologie vont révolutionner le secteur technologique. Nous n'avons aucune entreprise à mille milliards, puis nous en avons eu plusieurs. Nous allons en voir beaucoup plus : des entreprises avec 100 000 IA et zéro employé, qui feront le travail d'anciennes entreprises de 100 000 salariés. Nous verrons apparaître des méga-corporations : robots de livraison, voitures autonomes, une entreprise qui fournit un médecin personnel à un milliard de personnes sans aucun docteur sur la paie. Les actions vont donc croître très vite. L'or va être démonétisé. La terre sera moins monétisée. Mais regardez : en 2045, le futur ne paraîtra pas si révolutionnaire. Il ressemblera beaucoup à aujourd'hui... sauf que Bitcoin sera visible sur le graphique. Quand Bitcoin sera visible, ce sera le scénario de base. Quelles sont les implications ? Comment gagner de l'argent avec ça ? Stratégie Bitcoin individuelle : que faire ?

Faites de Bitcoin votre actif de trésorerie principal. Convertissez vos revenus excédentaires en Bitcoin. Utilisez du crédit subventionné : si l'État vous prête de l'argent à bas taux, empruntez et achetez du Bitcoin. Trouvez une façon fiscalement efficace d'investir dans Bitcoin. Que ne pas faire : ne quittez pas votre emploi, ne perdez pas votre concentration sur Bitcoin, n'utilisez pas de prêts sur marge ni de trading avec effet de levier. Vous vous faites liquider pendant votre sommeil un samedi soir, c'est catastrophique. Un prêt immobilier à 30 ans à 3 % garanti par l'État ? Très bien. Un levier 10x overnight ? Très mal. Prenons une personne typique : 750 000 \$ de patrimoine net, 200 000 \$ de revenus annuels (+5 % par an), taux d'épargne de 25 %, donc 50 000 \$ investis par an.

Plusieurs stratégies possibles :

- Normie : portefeuille diversifié classique → 8 millions en 21 ans



- 10center : 10 % en Bitcoin → plus du double
- BTC Maxi : 80 % des actifs + 80 % des revenus en Bitcoin → 100 millions
- Double Maxi : Maxi + emprunt supplémentaire de 250 000 \$ contre la maison → 150 millions
- Triple Maxi : financez la maison pour acheter du Bitcoin, vendez tout pour du Bitcoin, déménagez dans une juridiction à faible fiscalité (Singapour, Émirats...) et investissez 50 000 \$ de plus → 214 millions

On voit la puissance de l'effet de levier. Le choix vous appartient. Il faut environ 15,9 BTC pour être Triple Maxi. 6,25 BTC suffisent déjà pour devenir très riche. Pour les entreprises : Faites de Bitcoin votre trésorerie. Convertissez vos flux de trésorerie en Bitcoin. Émettez des actions pour acheter du Bitcoin quand c'est accrétif. Émettez de la dette pour acheter du Bitcoin quand c'est accrétif. Ne saignez pas votre capital avec des dividendes imposables. Ne cédez pas votre capital avec des rachats d'actions. Ne diluez pas vos actionnaires avec des acquisitions risquées et surévaluées.

Vérification de réalité : c'est exactement la stratégie Triple Maxi appliquée par MicroStrategy depuis 48 mois (au 10 août de cette année). Si vous pensez pouvoir copier Microsoft, Apple ou Google, très bien, vous ferez 20-25 % de rendement annuel. Si vous voulez copier Nvidia, vous battez tout le monde. Mais aujourd'hui, dans les conseils d'administration de Microsoft, Apple, Google et Tesla, ils sont stressés à l'idée de copier Nvidia... alors que copier MicroStrategy est très simple. Je viens de vous donner le playbook. Quatre années de cette stratégie donnent +1 300 %. Conclusion : construisez une structure de capital solide, évitez les pratiques financières dilutives. Pour une institution (église, association, endowment universitaire, fondation) : Modifiez vos statuts pour pouvoir investir en Bitcoin. Réallouez des actifs à courte durée vers des actifs à très longue durée. Vous n'investiriez pas dans des glaces qui fondent, ni dans des pesos. Alors pourquoi détenir des instruments financiers à 20 ans ou des terrains physiques à 50 ans ? Achetez un instrument à mille ans : Bitcoin. Le coût du capital n'est plus le S&P à 13 %, c'est Bitcoin à 55 %. Utilisez ensuite un levier intelligent. Modèle : portefeuille d'un milliard de dollars

- Normie → 5 milliards en 21 ans
- Maxi (100 % Bitcoin) → beaucoup plus
- Double / Triple Maxi (avec levier) → 100x, 300 milliards possibles.

Le coût du capital n'est plus celui du S&P à 13 %, c'est celui de Bitcoin à 55 %. Pensez à 55 % comme étant votre nouveau coût du capital, puis utilisez un levier intelligent.

Passons maintenant à la richesse des nations – c'est la partie la plus intéressante. Quelle est la stratégie Bitcoin nationale ? Ce qu'il faut faire et ne pas faire. Réallouez votre trésor public : sortez de l'or et des obligations (actifs à courte durée) pour aller vers un actif à 10 000 ans. Émettez de la monnaie pour acheter du Bitcoin. Émettez de la dette pour acheter du Bitcoin. Encouragez la détention de Bitcoin par des lois favorables. Protégez l'autoconservation (self-custody) pour les individus et les entreprises. Soutenez l'intégration de Bitcoin avec le système



bancaire de votre pays. Ce qu'il ne faut PAS faire : ne menez pas de politiques hostiles envers Bitcoin et ses détenteurs. Maintenant, imaginons que vous êtes un pays endetté, avec un gros déficit. Je pourrais nommer des pays, mais je ne le ferai pas. Disons simplement que vous devez beaucoup d'argent, vos taux d'intérêt sont élevés et vous êtes en difficulté. Quelles sont vos options ? Normie, 10center, Maxi, Double Maxi ou Triple Maxi ?

- Maxi : vous mettez un tiers de votre trésor en Bitcoin.

- Double Maxi : 65 % du trésor.

- Triple Maxi : vous mettez tout votre trésor en Bitcoin et commencez à émettre de la dette pour en acheter davantage.

Pour ceux qui savent lire entre les lignes : le premier pays qui achète du Bitcoin en émettant sa propre monnaie gagne la partie. C'est simple : vous imprimez du papier. Souvenez-vous du chèque de Seward. Il a émis un chèque. On pourrait se plaindre en disant « on ne pouvait pas se le permettre », mais c'était deux ans après la guerre de Sécession : le pays était en faillite, des millions de morts, le Sud en ruines, le Nord en colère. Et pourtant Seward a eu l'idée d'acheter une immense toundra gelée à des Russes qui voulaient du papier. Les gens ont déjà fait des choses dans des situations bien pires. Regardez les résultats :

- Normie : vous devez 3 000 milliards, vous n'allez nulle part.

- Maxi : vous remboursez votre dette.

- Double Maxi : vous devenez riche.

- Triple Maxi : vous devenez très riche.

Pourquoi ? Parce que vous achetez maintenant la propriété vers laquelle tout le monde se précipitera dans cent ans. C'était pareil avec Standard Oil : en 1867 il n'y avait pas d'essence, pas d'automobiles, pas de locomotives diesel. Tout cela a été inventé après. Mais le bon sens dit : « Je peux acheter quelque chose qui vaut à peu près 1 % de la taille d'une nation pour quelques millions, pourquoi ne pas le prendre ? » Stratégie Bitcoin pour les pays riches étrangers (ceux qui ont beaucoup d'argent, comme l'Arabie saoudite ou la Norvège) :

- Normie : vous restez comme d'habitude.

- Maxi : 25 % de vos réserves en Bitcoin.

- Triple Maxi : 75 % + conversion de tous vos excédents en Bitcoin.

Résultat : vous devenez incroyablement riches – 58 000 milliards de dollars riches. Mais surtout, cela renforce énormément votre sécurité nationale : vous finissez avec 50 000 milliards ou plus de capital numérique. Personne ne peut le voler. Ils bombardent votre pays, envahissent vos frontières... ils n'auront pas le Bitcoin. C'est excellent pour votre sécurité financière ET votre sécurité nationale.

Mais attention : si l'Arabie saoudite ou la Norvège appliquent la stratégie Triple Maxi, cela représente environ 4,2 millions de Bitcoin à la fin de la période. Il n'y a pas beaucoup de place

pour des Triple Maxi au niveau des États-nations. Il y en aura peut-être un, deux maximums. C'est une opportunité pour le premier acteur agressif. Il y aura beaucoup de familles Triple Maxi, beaucoup d'entreprises Triple Maxi... mais très peu de nations Triple Maxi. Et les États-Unis ? C'est un cas particulier, mais les règles restent les mêmes : Achetez du Bitcoin, vendez le papier, débarrassez-vous de votre or, allez sur du long terme. Et les interdits restent les mêmes : n'importunez pas les bitcoiners, n'envoyez pas l'industrie à l'étranger, n'envoyez pas le capital à l'étranger.

Notre scénario de base : nous pensons que l'IA et les nouvelles technologies vont générer une forte croissance. Nous supposons que les États-Unis seront dirigés par des dirigeants compétents qui sauront exploiter la technologie, créer des voitures autonomes, des robots, des sites à un milliard d'utilisateurs offrant gratuitement comptabilité, conseils juridiques et médicaux... Cela fera croître les recettes plus vite que les dépenses, et les taux d'intérêt finiront par baisser. Mais quelle est la stratégie Bitcoin des États-Unis ?

- Normie : vous achetez un peu (disons 500 000 BTC).
- 10center : 1 million de BTC.
- Double Maxi : 2 millions de BTC.
- Triple Maxi : 4 millions de BTC + conversion systématique de tous les excédents nationaux en Bitcoin.

Conséquences :

- Normie : même avec une forte croissance de productivité et une technologie brillante, vous restez endetté – ça n'empire pas trop, c'est déjà ça.
- Maxi : vous remboursez la moitié de la dette.
- Double Maxi : vous passez en excédent.
- Triple Maxi : au lieu de devoir 30 000 milliards, la nation possède 30 000 milliards.

Bitcoin ne résout pas tous nos problèmes. Il résout la moitié des problèmes – et c'est la moitié simple. L'autre moitié est très compliquée, elle demandera beaucoup d'énergie et beaucoup de gens. Mais cette moitié-là est très simple à régler.

Bitcoin, c'est Cyber Manhattan : des centaines de milliers de milliards de dollars de capital vont converger là. Nous allons démonétiser la toundra russe, l'immobilier chinois, tout en Afrique, tous les bâtiments moches et inutiles que les gens ont achetés sans en avoir besoin. Tout cela va être démonétisé. Vous achetez du Bitcoin → vous démonétisez un immeuble, un boulevard, un quartier entier. 276 à la puissance 3, c'est ce que vous voyez aujourd'hui. Je vais terminer avec une citation. Satoshi Nakamoto a lancé le réseau Bitcoin le 3 janvier 2009. Le 17 janvier 2009, 14 jours plus tard – 16 mois avant le Pizza Day, quand Bitcoin ne valait rien et n'allait rien valoir pendant encore un an –, Satoshi a écrit :

« Il pourrait être judicieux d'en acquérir quelques-uns au cas où cela prendrait. Si assez de gens pensent de la même façon, cela deviendra une prophétie auto-réalisatrice. »



Jamais paroles plus sages n'ont été prononcées. Vous avez sous les yeux une preuve d'un billion de dollars... et il reste encore mille fois à venir. Vous avez beaucoup plus d'informations à portée de main. L'écriture est sur le mur. Bitcoin est le futur du capital. Bitcoin est le futur de l'argent. Il pourrait être judicieux d'en acquérir, parce que ça a déjà pris. Merci.

Engrenage politique puissant, Donald Trump : Comprendre les évolutions du prix d'un Bitcoin n'est pas facile. Certes, il existe des paramètres tels que le Halving, mais ils ne sont pas aussi nombreux que dans d'autres classes d'actifs. C'est pourquoi il devient pertinent de s'intéresser à Donald Trump qui semble lourdement contribuer à la direction du prix de cette cryptomonnaie. En effet, à l'aube de son second mandat, le marché semblait très optimiste quant à l'avenir du Bitcoin. Suite à sa réélection, le prix du coin atteignait même plus de 124 000 dollars américains. En quoi les projets de Trump constituent-ils un aussi grand signe d'optimisme pour le Bitcoin et le reste du marché des cryptomonnaies ?

Dans un premier temps, Trump ainsi que son administration ont mis en place une série de mesures et de décisions favorables à leur adoption, notamment en abandonnant des enquêtes visant les entreprises et la criminalité liées aux cryptomonnaies. Par ailleurs, le président a également lancé et créé sa propre cryptomonnaie, le \$Trump et a conservé d'importants investissements dans ce domaine. C'est donc en janvier 2025, par décret présidentiel, que Trump crée un groupe de travail sur les actifs numériques et s'engage à faire des États-Unis la « capitale mondiale des cryptomonnaies ». Puis, c'est en mars, lors de la chute de 20 % du Bitcoin qu'il exécute une réserve américaine composée de Bitcoin, Ethereum, Solana, Cardano et Ripple, à hauteur de 300 milliards de dollars américains.

Il faut aussi prendre en compte qu'en mai 2025, la famille Trump possédait quatre entreprises de cryptomonnaies. Ses fils aînés Eric et Donald Jr. ont fondé une société de minage de Bitcoin, American Bitcoin, une fusion avec American Data Centers en 2025. Même si les actifs de Donald Trump sont détenus en fiducie et gérés par ses enfants pendant qu'il est président des États-Unis, on peut affirmer que son engagement envers les cryptomonnaies est profond et que tant qu'il sera président, un nuage d'optimisme et de sécurité continuera de couvrir le marché du Bitcoin.

C'est également la société mère de Truth Social qui est optimiste sur le Bitcoin en exploitant des ETF Crypto Blue Chip mais également en levant de l'argent par le biais d'émissions d'actions et d'obligations afin de se constituer une réserve de Bitcoins.

Objections fréquentes :

Beaucoup de personnes projettent un avenir sombre pour le Bitcoin et les cryptomonnaies, ce qui peut créer beaucoup de confusion. Dans cette rubrique nous allons essayer de fournir plus d'informations à deux objections courantes concernant le Bitcoin. La première étant : « Le Bitcoin est la nouvelle bulle des tulipes » et la seconde fait référence aux déclarations de Warren Buffett.

- La bulle des tulipes : Également appelé « Tulipomanie », il s'agit d'un grand engouement pour les tulipes ayant eu lieu dans le nord des Provinces-Unies (Pays-Bas) au milieu du XVII^e siècle. Cet engouement apparut suite à l'importation d'une centaine



de nouvelles espèces de plantes entre la fin du XVI^e siècle et le début du XVII^e. La tulipe venue d'Istanbul présente de très nombreuses variétés (autour de 50) et suscite plus d'attention que les autres espèces. À cette époque seuls les botanistes et certains amateurs s'en préoccupent sérieusement à des fins d'études. Jusqu'à ce que certains bourgeois fortunés en achètent afin de les planter dans leurs jardins privés à l'arrière de leurs maisons longeant les canaux d'Amsterdam. De là naît un intérêt certain pour cette plante dont les variétés sont importantes et méconnues à l'époque et parvient à devenir un objet de luxe. Les tulipes ne sont pas faciles à cultiver et l'apparition de virus transforme les couleurs et motifs des plantes pour les rendre plus jolies et uniques. Le récit historique du crash tient spécifiquement lieu en 1636 et 1637. Les tulipes ne pouvant se déplanter et planter qu'entre juin et septembre aux Pays-Bas, le reste de l'année les ventes se faisaient à terme. Enfin, ce marché se transforme de façon importante et avec l'arrivée de clients étrangers (comme des Français), les spéculateurs décident d'entrer sur les échanges. Un système analogue à celui d'une bourse de commerce se met en place entre quelques acteurs fortunés, de l'ordre d'une centaine environ, afin d'échanger des contrats à terme de tulipes. À ce stade, ce marché est qualifié de Windhandel, littéralement « commerce du vent », parce que les transactions ne portent pas sur des bulbes réels. En février 1637, le prix des contrats à terme de bulbes de tulipe s'effondre alors qu'une épidémie de peste bubonique s'empare de la ville centrale de ces échanges, Haarlem. Aujourd'hui encore, nous n'avons que très peu de données fiables sur les prix exacts des bulbes mais la proportion serait de l'ordre d'une dizaine de fois le salaire d'un artisan. Selon certaines recherches menées par Goldgar, seulement quelques dizaines de personnes auraient payé plus de 3000 florins pour un bulbe de tulipe soit l'équivalent d'un salaire annuel d'un artisan qualifié. Selon cette même recherche, la chute des prix n'a pas eu un grand impact sur la société étant donné que ces échanges étaient réservés à de riches personnes.

À mesure que l'histoire de la bulle des tulipes est racontée, les raisons pour lesquelles le Bitcoin n'est en rien comparable à cet événement deviennent évidentes. Dans un premier temps l'arrivée du sujet n'a rien à voir. Les tulipes ont été importées depuis l'actuelle Turquie et personne ne comprenait comment certaines d'entre elles devenaient différentes. Le Bitcoin n'est pas une découverte mais le fruit de recherches en partie scientifique et technologique. Le code est connu et est compris par beaucoup. Dans un second temps, les tulipes s'inscrivent dans un petit cadre, les acheteurs et vendeurs étaient relativement fortunés et leurs valeurs provenaient du fait qu'elles soient considérées comme des éléments de luxe et de décoration. Ce qui fait que c'est également un bien qui peut s'inscrire dans un phénomène de mode et donc doit connaître un cycle. Aujourd'hui même les éléments naturels considérés à forte valeur sont menacés par les produits de synthèse, tels que le diamant ou l'ivoire. D'autant plus que les tulipes n'existent pas en nombre fini. À la différence, Bitcoin est rare (21 millions de coins) et répond à des besoins en matière financière. Sa technologie est sérieusement utilisée dans de nombreux autres domaines également. Les tailles de marché ne sont également en rien comparables, le marché des tulipes était plutôt local alors que le Bitcoin est échangé en temps continu sur toute la planète. La tulipe est également un

bien qui ne se modifie pas en fonction de son nombre d'utilisateurs à l'inverse de Bitcoin qui ne cesse de se renforcer au niveau de sa sécurité et de sa liquidité à mesure que son marché s'élargit (loi de Metcalfe).

- Warren Buffett déclarant : « If you told me, you owned all the Bitcoin in the world and you offered it to me for \$25, I wouldn't take it because what would I do with it. I have to sell it back to you one way or another I mean maybe it will be the same people but it isn't gonna do anything... ». « Si vous me disiez posséder tous les Bitcoins du monde et que vous me les proposiez pour 25 dollars, je refuserais. Qu'en ferais-je ? Je serais obligé de vous les revendre d'une manière ou d'une autre. Peut-être même aux mêmes personnes, mais cela ne me servirait à rien... ». Cette déclaration rejoint plutôt bien celle de son associé de longue date Charlie Munger qui qualifiait le Bitcoin de « rat poison ». En ce qui concerne la déclaration de Warren Buffett, il est intéressant d'écouter la « réponse/commentaire » de Michael Saylor qui semble avoir un avis assez dessiné sur ces différentes remarques. C'est pour cette raison que je vous propose de lire la transcription de sa réaction. Mais avant cela, revenons sur la phrase de W.B. Après réflexion je ne pense pas qu'elle doit être prise très au sérieux. Je pense cela car il est surprenant de voir que le début de la phrase commence avec une hypothèse aussi étrange, et comme l'expression française le dit : « avec des si, on refait le monde ». Il n'est pas utile de tenter d'analyser davantage cette phrase à partir de ce moment... D'un côté, cela veut dire que personne n'en voudrait et donc que cette technologie ne sert à rien. Ce qui veut dire que le sujet n'est pas totalement abordé, d'autant plus que le principe d'une devise n'est pas de produire mais dans la réalité un très grand nombre de services financiers vous offrent de l'argent pour le dépôt de vos devises dans certains endroits. Cependant, Buffett réfléchit souvent à la valeur d'un actif ou d'une entreprise en partant du principe qu'il le possède en totalité. Or ici, il s'agit d'une toute nouvelle technologie dont le fonctionnement est contre-intuitif sur certains points, et le célèbre investisseur se vante lui-même d'être en retard sur la technologie.

Transcription du commentaire de Michael Saylor :

Ce que vous voyez est une disruption culturelle massive. Ce que vous observez, c'est une onde de choc qui traverse la culture. Vous voyez la force la plus disruptive au monde en ce moment, et elle percute les gens et les institutions plus vite qu'ils ne peuvent l'absorber, l'apprécier et la comprendre.

C'est comme des ondes de choc dans le monde réel. Si je déplace un profil d'ail aérodynamique dans l'air plus vite que le son, la vitesse du son est la vitesse à laquelle l'air communique avec lui-même. L'air ne peut pas s'écarter de mon passage, je le percute, je crée une turbulence massive et du bruit. La façon de résoudre cela, c'est d'aller plus lentement, mais vous n'êtes plus supersonique.

Charlie Munger n'était pas un partisan d'Apple Computer, n'est-ce pas ? Et Amazon ? Et Microsoft ? Warren Buffett est ami avec Bill Gates depuis combien d'années et il n'a toujours pas acheté d'actions Microsoft ? Et Microsoft était une idée assez bien comprise il y a 40 ans, 30 ans.

Ce que vous avez, c'est quelque chose de si puissant que tout le monde est invité à avoir une opinion. Les présidents, le président de la Russie, le président de la plupart des



États-nations, on leur demande d'avoir une opinion. Chaque investisseur est invité à avoir une opinion. Mais si je vous disais que vous ne pouvez pas vraiment le comprendre sans investir 100 heures de temps ? Combien de personnes après 40 ans passent 100 heures à étudier quoi que ce soit ? Vous savez, une fois que vous atteignez l'âge de 65 ans... Vous ne pensez pas que Munger, Buffett, Gates, ces gens ont passé 100 heures à étudier Bitcoin ? (Présentateur) N'êtes-vous pas sûr qu'ils ne l'ont pas fait ? Il est presque certain qu'il n'a pas passé 10 heures.

Je dirais la même chose pour la plupart des investisseurs macro en ce moment. Je dirais la même chose pour beaucoup d'investisseurs crypto. La plupart des gens dans l'espace crypto n'ont pas passé 100 heures à étudier cela. Combien de personnes ont passé 100 heures à étudier l'action qu'ils détiennent dans leur portefeuille ? Vraiment ? Combien de personnes passent 100 heures à étudier Facebook ?

Ce que je dis, c'est que les gens devraient faire la recherche jusqu'à ce qu'ils obtiennent la conviction nécessaire pour prendre leur propre décision. À la fin de la journée, c'est de la propriété. Je ne promeus pas mon propre actif. Je ne promeus pas un échange. Je suggère essentiellement : allez vers l'ouest, jeunes gens, prenez de la terre. C'est comme allez en Amérique, prenez de la propriété et faites votre vie pour vous-mêmes. Mais c'est à vous de décider si vous voulez faire cela ou non.

Le point plus important, cependant, c'est que chaque personne influente au monde se voit demander d'avoir une opinion, mais ils ne passent pas 100 heures sur cette opinion. Si je remontais l'horloge de 100 ans et que j'allais voir chaque politicien et chaque personne riche du monde en 1900 et que je leur demandais ce qu'ils pensaient de l'électricité, que diraient-ils ? Et les avions en 1904, quelle était l'opinion à l'époque ? Donc ce n'est pas déraisonnable.

Et je ne pense pas que nous devrions passer beaucoup de temps à nous fixer sur les opinions de personnes célèbres, puissantes et riches à propos d'une technologie qu'elles n'ont pas choisi de faire un point focal de leur intérêt. Surtout quand elles ont 98 ans, je pense que cela doit être un facteur.

Le point le plus important, c'est que tout le monde pense par soi-même. Donc vous n'iriez pas voir Charlie Munger et lui demander de choisir des actions pour votre portefeuille. Chaque action gagnante de la dernière décennie — Netflix, Google, Apple, Facebook, Amazon — combien d'entre elles vous ont été recommandées par l'une de ces personnes dont vous demandez l'opinion ? Aucune. Aucun des antagonistes ou critiques de Bitcoin n'aurait recommandé ou n'a recommandé aucune de ces actions.

Donc c'est en quelque sorte un point. C'est vraiment juste du marketing ou des étincelles qui sont envoyées parce que ce qui se passe, c'est que ces gens dans les médias les interviewent et ils veulent les faire réagir, donc ils lancent cela. Personne ne demande l'opinion de Warren Buffett sur l'argent ou l'or en ce moment parce que personne n'est intéressé à entendre la réponse.



Il est difficile de résumer en quelques lignes l'ensemble des notions abordées dans ce document mais bien que la plupart des thèmes seront repris sur Substack je vais m'efforcer de donner mon opinion de façon synthétique.

En se concentrant seulement sur l'histoire de la première cryptomonnaie il est certains qu'elle dépasse complètement le cadre classique de la gestion de portefeuille. Le terme approprié serait une spéculation extraordinaire transformatrice de vie. *(Nombreux sont les experts financiers et académiques aux sujets des théories financières et d'investissements mais lorsqu'il s'agit de réaliser l'impensable, nos esprits doivent s'affranchir de nombreuses contraintes intellectuelles)*. En ce qui concerne l'avenir de Bitcoin, l'enjeu tourne surtout autour de l'éducation et de la connaissance, pour reprendre les mots de Satoshi (« *Il pourrait être judicieux d'en acquérir quelques-uns au cas où cela prendrait. Si assez de gens pensent de la même façon, cela deviendra une prophétie auto-réalisatrice.* »). Sur le plan du marché, Bitcoin semble légèrement se corréliser au marché ces derniers temps. Un bon test sera lors de la prochaine grande crise financière... Si Bitcoin parvient à survivre alors il faudra sérieusement envisager son existence comme un actif aussi important que l'immobilier. Le vent reste toutefois en faveur des croyants de cette technologie puisque les grands adeptes comme Michael Saylor possède un grand capital à disposition. Ce qui pourrait expliquer pourquoi sur le court terme la volatilité est importante mais sur le long terme la hausse du prix reste « systématique ». On pourrait se demander si les hausses suivies des vagues de baisse, causées par des spéculateurs et des ventes de foules, sont à l'origine des sérieux partisans du Bitcoin qui ne cessent d'en racheter et donc de consolider son prix (sur un horizon temporel plus long).

Sources :

MEXC.Blog – Bitcoin.org – Bitcoin Wiki - Bitwiseinvestments – Finance-heros – Cryptoast – Wikipedia -

