Experts Crypto

Bulletin d'information mai 2024

Introduction

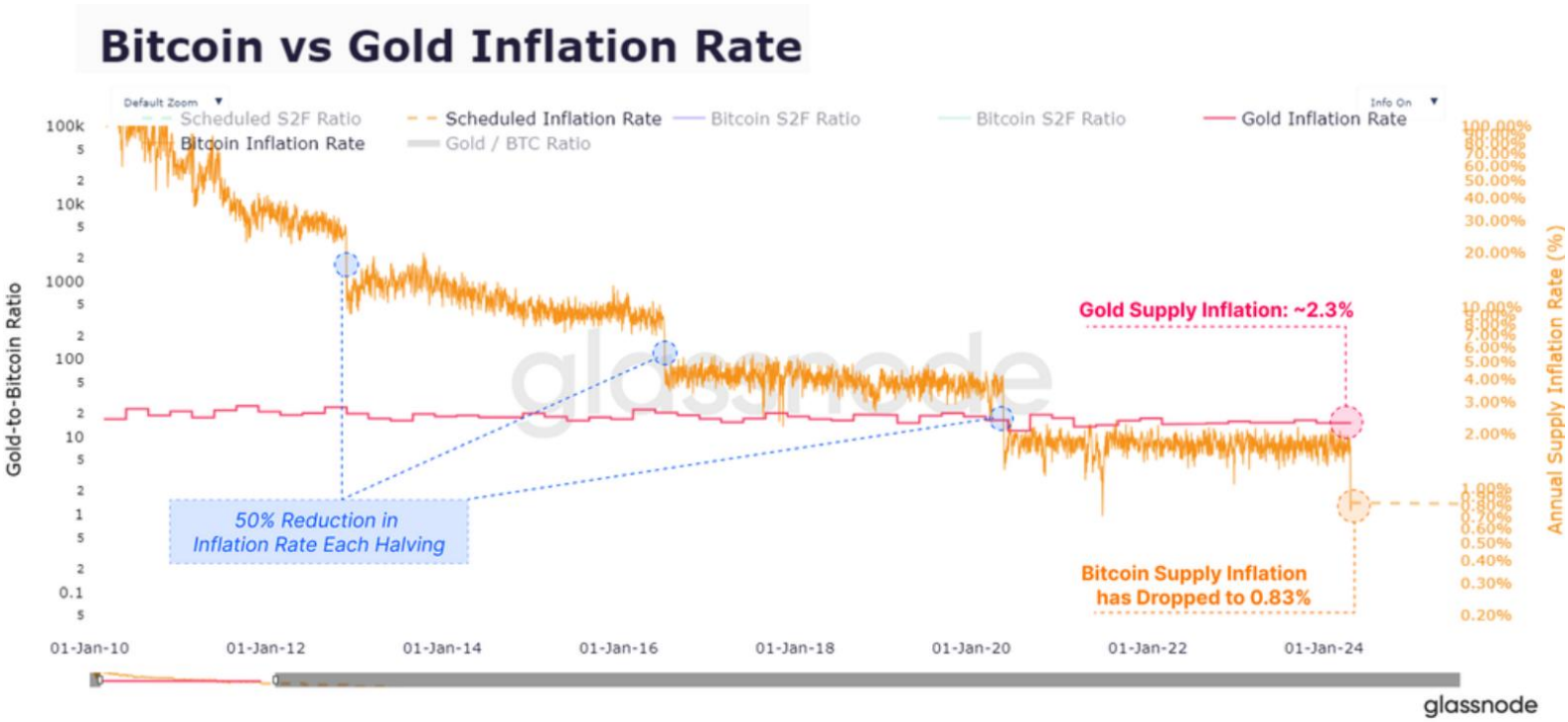
Dans cette newsletter, et selon notre coutume, nous allons nous concentrer sur l’analyse autour de Bitcoin. Nous débuterons par une présentation des principales statistiques récentes. Ensuite, nous examinerons les impacts et enjeux entourant les ETF, tant en Asie qu'aux États-Unis. Par la suite, nous aborderons les récents défis rencontrés par les développeurs dans le domaine de la confidentialité des transactions.

Cette exploration nous permettra de mieux comprendre les dynamiques actuelles et futures autour de cette technologie révolutionnaire.

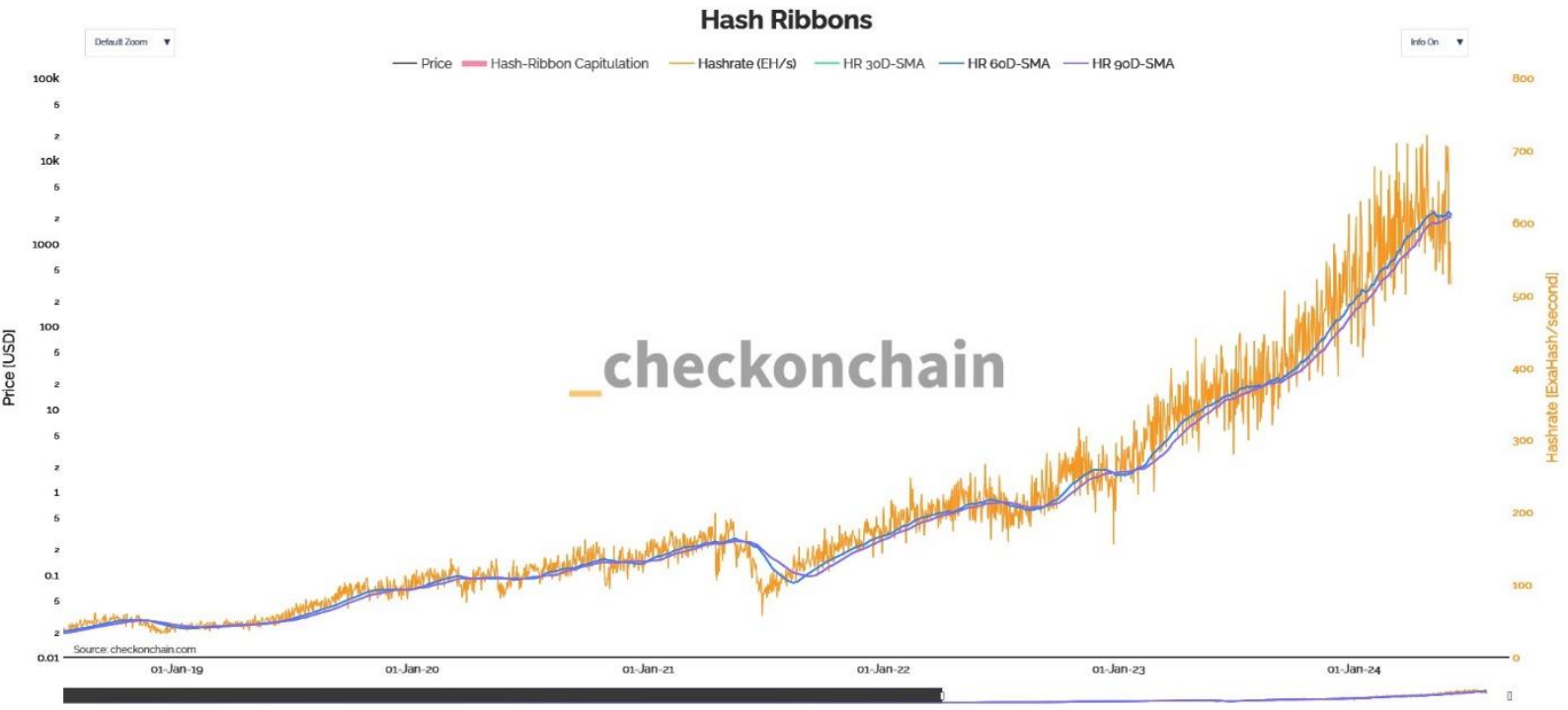
Statistiques importantes

Halving & Hashrate

À la mi-avril, le Bitcoin a connu son quatrième « halving », réduisant l'inflation de l'offre de 50 % et faisant passer le taux d'émission à 0,85 % par an. Cette réduction a renforcé le statut de monnaie dure de Bitcoin car pour la première fois, le protocole a surpassé l'or en termes de rareté d'émission.



Malgré cette diminution de la subvention de bloc (de 6,25 à 3,125 BTC créés toutes les 10 minutes), le taux de hachage du réseau a atteint de nouveaux sommets historiques. Les mineurs ont donc investi dans du matériel efficace et ont optimisé leurs coûts opérationnels afin de rester suffisamment rentable.



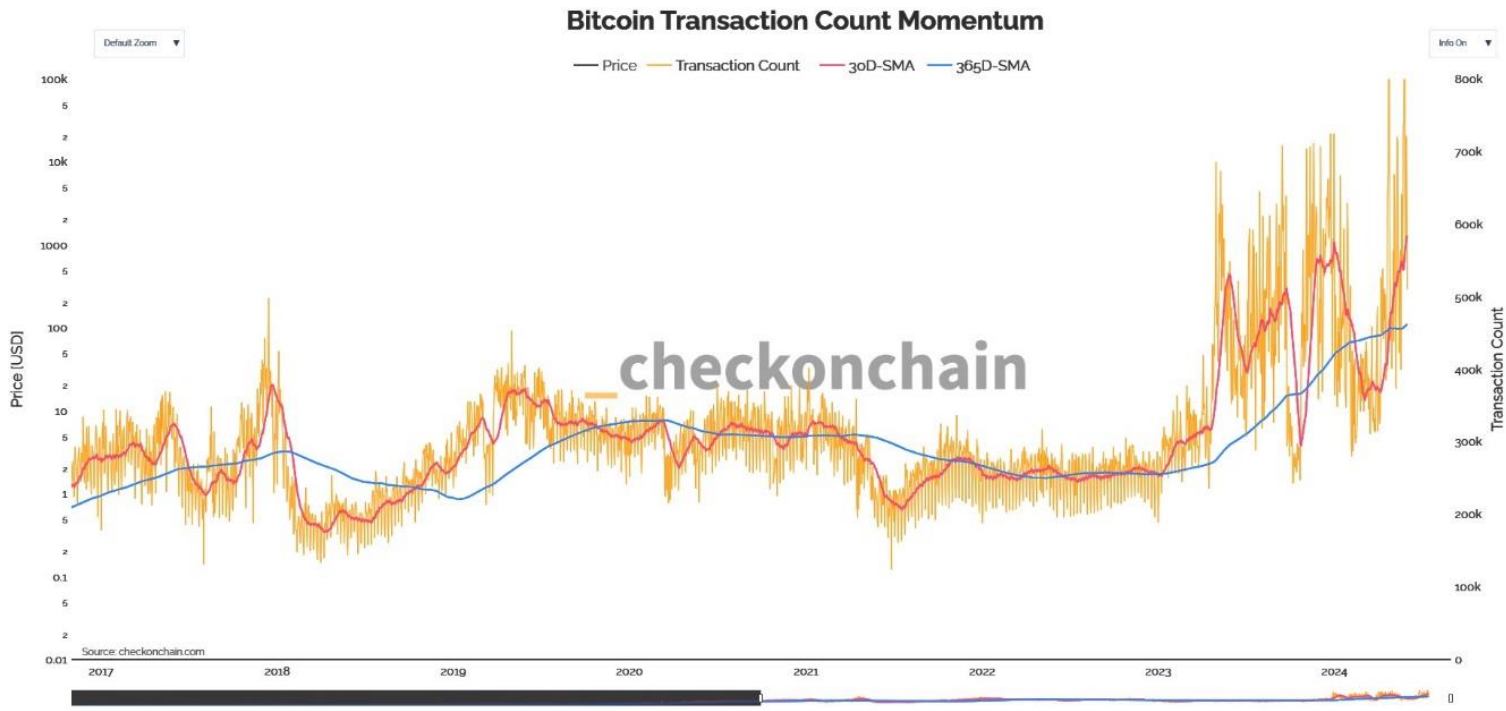
C’est une bonne nouvelle car si Bitcoin est le protocole informatique qui regroupe le plus de puissance au monde, il consomme une certaine quantité de ressources. C’est excellent pour sa sécurité, le développement des énergies renouvelables et des réseaux électriques, mais ce n’est pas réellement nécessaire pour son bon fonctionnement.

Nous pensons donc que les mineurs sont dans une course pour générer les 6% de bitcoins restants à créer dans le cadre de la subvention de bloc. Une fois que ce chiffre deviendra négligeable, seuls ceux qui peuvent fonctionner grâce aux frais de transactions resteront dans l’industrie et les autres vont petit à petit se débrancher jusqu’à ce que l’on obtienne un taux de hachage cohérent avec nos besoins (contraintes de degré de décentralisation, de ressources, de sécurité, de rentabilité).

Autres étapes importantes

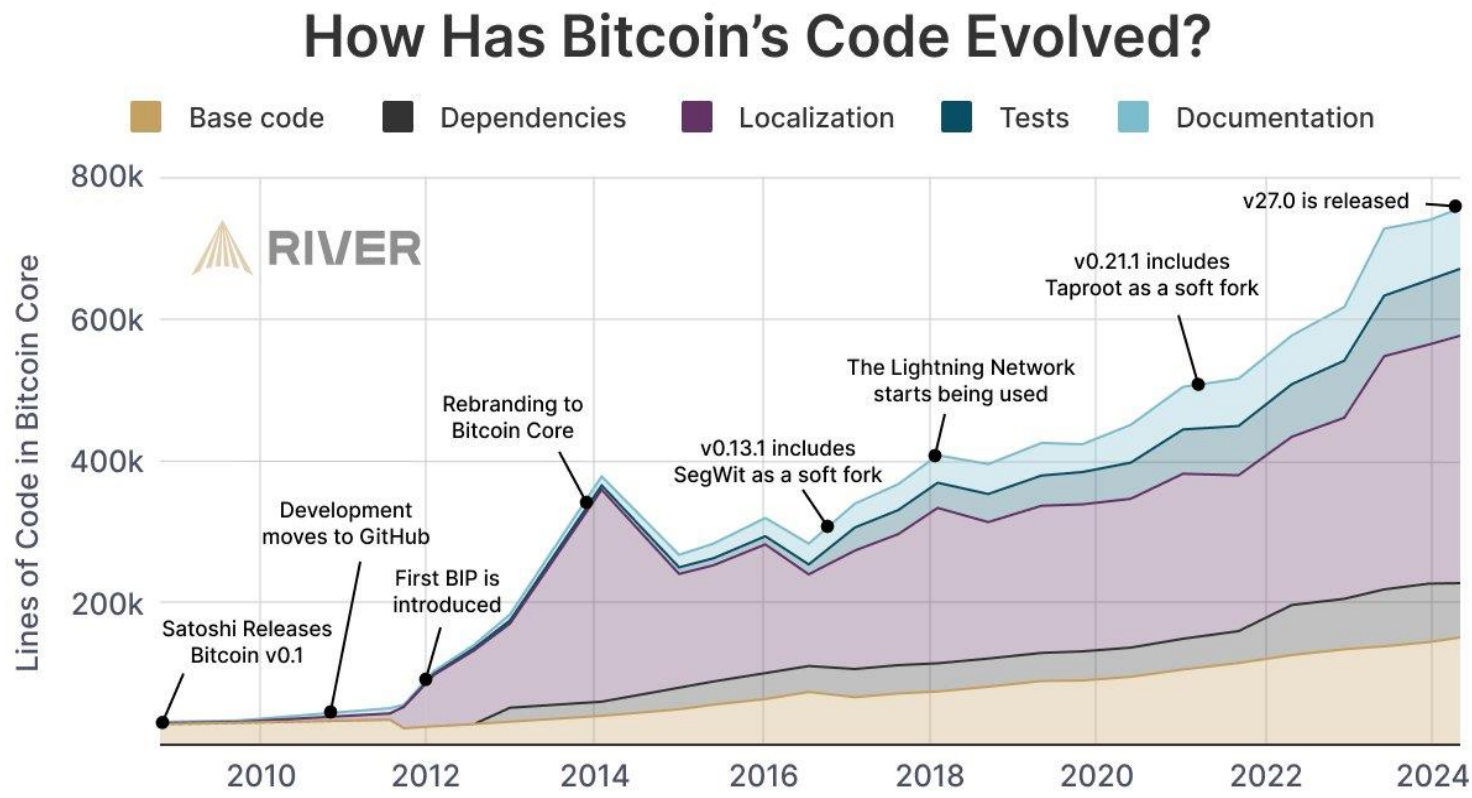
De plus, le Bitcoin a atteint de nouveaux jalons sur d’autres métriques importantes, renforçant toujours plus les fondamentaux du réseau :

- Le réseau a atteint le milliard de transactions, 15 ans après le minage du bloc de genèse le 3 janvier 2009. Cela représente une moyenne de 178 475 transactions par jour sur 5 603 jours. La moyenne quotidienne de ce mois de mai dépasse 600 000 transactions.



- Une somme stupéfiante de 106 trillions de dollars a été transférée et réglée via le réseau Bitcoin au cours des quatre dernières années. Ce chiffre impressionnant souligne la capacité du Bitcoin à maintenir sa position en tant que réseau de règlement de premier choix, malgré la volatilité et les baisses cycliques.
  A titre de comparaison, en 2023 uniquement, Visa a facilité 212 milliards de transactions pour un volume total de 12 trillions de dollars. Paypal, quant à lui, a été utilisé dans 25 milliards de transactions pour un volume total de 1,5 trillion de dollars.
  Bitcoin a encore beaucoup de progrès à faire sur le segment des petites et micro transactions, car même en prenant en compte les transactions sur les solutions de seconde couche (Lightning), leurs volumes restent encore marginaux.

- Cela dit, les dévelopements abondent sur Bitcoin. Le code informatique est passé de 26 000 lignes en 2009 à 780 000 lignes en 2024. Le code supplémentaire rend tout plus sûr, plus facile à comprendre pour les développeurs et plus accessible pour les utilisateurs.
  Si vous voulez en savoir plus sur : Quelles sont les différentes parties du code ? Qui le maintient et le développe ? Où se trouve-t-il ? Veuillez suivre ce lien.



Source: the full repository at github.com/bitcoin/bitcoin

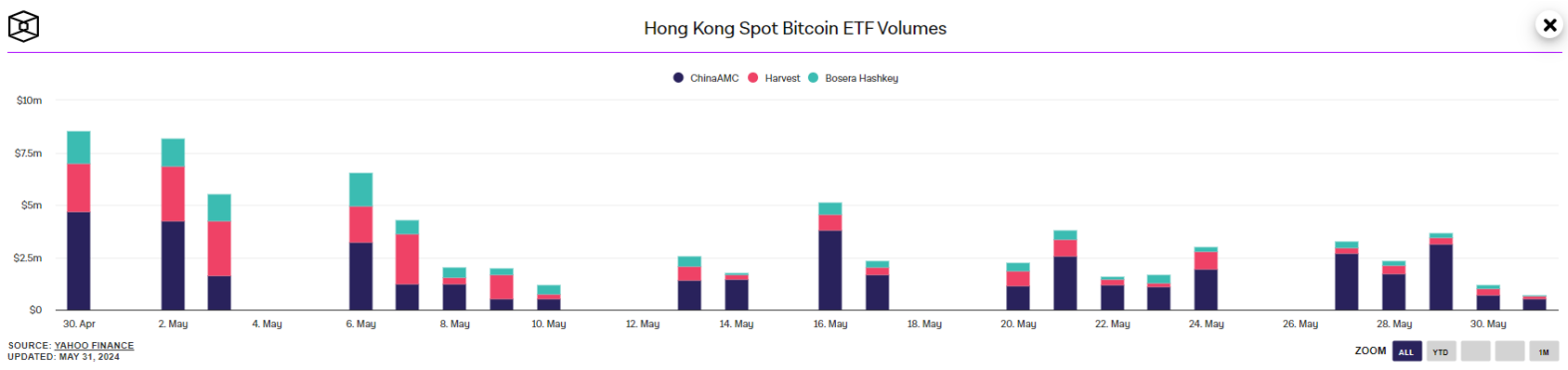
Inititalement mis en doute, Bitcoin se compare désormais avec les processeurs de paiements les plus célèbres et attire les plus gros acteurs financiers de ce monde. C'est ce que nous allons aborder maintenant.

L'engouement autour des ETF

Le continent asiatique

Le mois de mai a commencé sur les chapeaux de roue avec l'introduction des ETF spot Bitcoin sur la bourse de Hong Kong. En effet, depuis le 30 avril, il existe 6 nouveaux ETF crypto au comptant appliqués au Bitcoin et à Ethereum cotés à la bourse de Hong Kong.

Bien évidemment, le marché de Hong Kong n'a pas permis de reproduire l'euphorie déclenchée par l'approbation de la SEC en janvier dernier. Si l'on est bien loin des 4,5 milliards de dollars enregistrés par les ETF Bitcoin au comptant lors de leur première journée de cotation aux USA. Le marché de Hong Kong affiche pour sa part une participation estimée à 8,7 millions de dollars.



La position de Blackrock version Hong Kong semble pour le moment revenir au fonds ChinaAMC. Les deux fonds (BTC et ETH) de China Asset Management détiennent déjà plus de 80 % du marché récemment lancé à Hong Kong. Ce qui n'est pas surprenant car le gestionnaire d'actifs a annoncé avoir 140,5 millions de dollars américains lors de la période d'offre initiale, dont plus de 86 % sont allés vers son ETF Bitcoin au comptant.

La question demeure de savoir dans quelle mesure ce territoire peut servir de laboratoire crypto pour la Chine car, pour le moment, les investisseurs de la Chine continentale sont privés des ETF Bitcoin de Hong Kong.

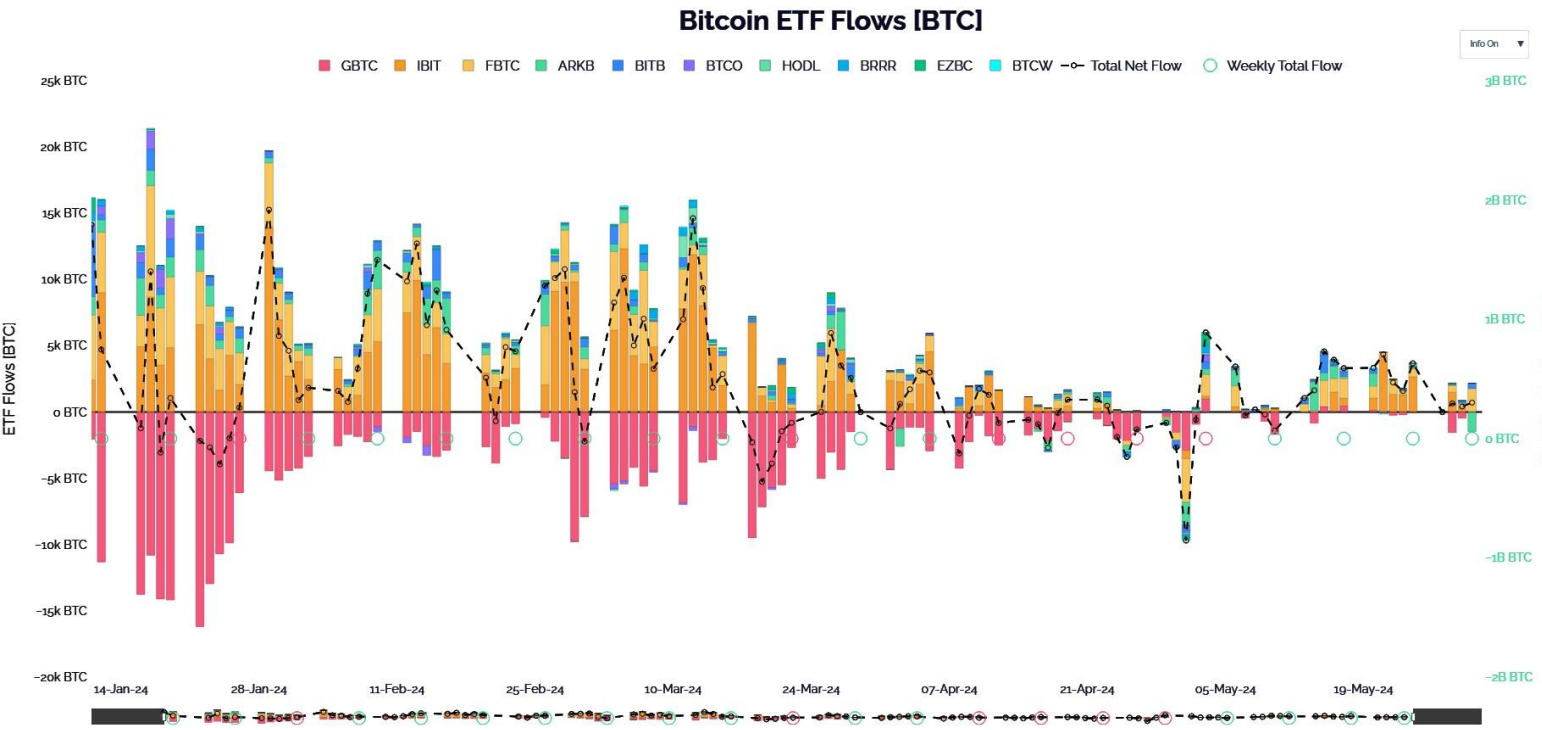
En effet, s'il existe déjà plusieurs moyens de contourner les autorités chinoises, mais ils sont peu exploités tant la position officielle du pouvoir central parait contraignante et inquiétante.

Par ailleurs, près de 70% de la richesse chinoise est placée dans l'immobilier et le secteur bat de l'aile avec plus de 100 millions de logements vides. Pour calmer les milieux économiques et éviter des troubles sociaux, il faudrait donc urgemment trouver une solution de repli pour placer de l'argent…

États-Unis d'Amérique

Du côté des États-Unis, l'ETF Bitcoin Spot de BlackRock (IBIT) a récemment surpassé le Grayscale Bitcoin Trust (GBTC) en termes d'actifs sous gestion, devenant ainsi le plus grand ETF Bitcoin au monde. Au 28 mai, IBIT détenait plus de 19,68 milliards de dollars en bitcoins, contre les 19,65 milliards de dollars du GBTC. Cette transition a été facilitée par les frais de gestion attractifs d'IBIT, à seulement 0,25 % (réduits à 0,12 % pour les 12 premiers mois ou les 5 premiers milliards de dollars d'actifs), comparés aux 1,5 % de GBTC. Depuis sa conversion

en ETF au comptant le 11 janvier, le GBTC a vu ses fonds diminuer, tandis qu'IBIT a attiré des centaines de millions de dollars d'investisseurs désireux de profiter du marché du bitcoin. (cf graphique ci-dessous)



Depuis avril, nous voyons bien que les volumes s'amenuisent, néanmoins les ETF comptant américains cumulent aujourd'hui plus de 1 millions de Bitcoin (5% de la réserve totale). Il n'y en aura jamais que 21 millions. Passé un certain point, cet appétit devra se traduire par une appréciation du prix.

D'autant plus que, des documents déposés par la Securities and Exchange Commission ont révélé que plus de 600 sociétés financières aux États-Unis ont investi dans des ETF Bitcoin au comptant (dont 421 sont exposés au IBIT de BlackRock). Des institutions telles que Morgan Stanley, JPMorgan, Wells Fargo, la Banque Royale du Canada, BNP Paribas, UBS, etc. Parmi ces sociétés, Millennium Management est devenue le plus grand accumulateur d'ETF Bitcoin au comptant, avec 1,9 milliard de dollars investis (sur les 61 qu'ils ont en gestion).

Ce qui laisse présager un changement radical dans la manière dont les fonds d'investissement traditionnels considèrent le bitcoin.

Cela étant dit, pour passer d'une note positive à une actualité plus sombre, L'affaire Samouraï Wallet rappelle qu'il est de plus en plus difficile de développer des outils favorisant la vie privée dans le monde digitalisé des crypto-actifs.

Finance & vie privée : L'équation impossible ?

Est-il encore possible de développer des business autour de la vie privée dans le monde décentralisé ? On pourrait en douter compte tenu du nombre de développeurs spécialisés qui subissent la pression des États.

Le 24 avril, c'était au tour des créateurs de Samouraï Wallet, Keonne Rodriguez et William Lonergan Hill, d'être arrêtés aux États-Unis.

Samouraï est un wallet (portefeuille) bien connu de la communauté bitcoin. Il permet d'ajouter une couche d'anonymat sur des transactions. L'application mobile s'appuie sur un "mixeur" du nom de Whirlpool. Un mixeur mélange plusieurs transactions entre elles afin de briser le lien entre l'émetteur et le bénéficiaire. À l'issue de l'opération, il devient beaucoup plus difficile de remonter les transactions sur la blockchain.

Selon le département de la Justice américain, Samouraï Wallet aurait facilité plus de 2 milliards de dollars de transactions considérées comme illégales et contribué au blanchiment de près de 100 millions de dollars liés à des activités criminelles. Les deux développeurs risquent jusqu'à 25 ans de prison.

Cette affaire n'est pas sans rappeler celle de Roman Sterlingov (Bitcoin Frog) et celle de Tornado Cash (un mixeur sur Ethereum), qui avait abouti à l'arrestation de son développeur principal Alexey Pertsev à l'été 2022. Le 14 mai 2024, un tribunal néerlandais a condamné Alexey à plus de 5 ans de prison pour complicité de blanchiment.

L'arrestation des membres de Samouraï Wallet confirme une fois de plus que les autorités ciblent clairement ce type d'outils, pourtant indispensables pour préserver un semblant de confidentialité sur la blockchain.

« On utilise un marteau au lieu d'un scalpel » (Coinbase)

« *Contrairement à l'idée régulièrement répandue par ses détracteurs, Bitcoin n'a jamais été conçu pour garantir la vie privée de ses utilisateurs* », insiste Frédéric Ocana, hacker éthique et directeur du programme cybersécurité à la Banque de France de 2017 à 2021. « *C'est principalement un outil qui permet de réaliser des transactions financières incensurables en dehors du système bancaire* », explique-t-il. (Source : interview The Big Whale)

Selon lui, les cryptomonnaies sont facilement traçables et c'est cela qui a engendré la création d'outils tels que les mixeurs pour offrir à leurs utilisateurs plus de vie privée, à commencer par Bitcoin Fog à partir de 2012, Blender en 2017 et plus récemment Tornado Cash ou Whirlpool.

Si vous subissez une fuite d'un de vos wallets sur les réseaux sociaux, un mixeur permet de retrouver un peu de discrétion. Le problème, c'est que les mixeurs de cryptomonnaies sont également utilisés par des criminels, à commencer par le groupe de hackers Lazarus (proche du gouvernement nord-coréen). Selon l'enquêteur ZachXBT, très réputé dans l'écosystème, ils auraient réussi à blanchir l'équivalent de 200 millions de dollars entre 2020 et 2023, en s'aidant notamment de mixeurs.

Faut-il pour autant les interdire et jeter leurs développeurs en prison ? Pour certaines entreprises comme Coinbase, « *on utilise un marteau au lieu d'un scalpel* », indiquait-elle dans un billet publié sur son site web en septembre 2022 :

« *Le Département de la justice est allé beaucoup plus loin en sanctionnant une technologie entière au lieu de personnes spécifiques. Le problème est double : il existe des applications légitimes pour ce type de technologie et, à la suite de ces sanctions, de nombreux utilisateurs innocents ont maintenant leurs fonds bloqués et ont perdu l'accès à un outil crucial de confidentialité* ».

Les angles d'attaque utilisés par les autorités

La plupart du temps, on reproche aux développeurs de mixeurs des cas de blanchiment, mais aussi d'opérer une entreprise de transfert de fonds (Money Services Business - MSB) illégalement.

Cette licence est délivrée par les régulateurs aux entreprises considérées comme fournissant des services de conversion ou de transmission de flux financiers.

« *Sauf que le périmètre réglementaire de cette licence n'est pas clair* », expliquait Laurent MT durant le Bitcoin Economic Forum, un développeur qui a travaillé sur Samouraï Wallet. « *Jusqu'à Tornado Cash, la règle pour ne pas être hors-la-loi stipulait que l'entité à l'origine du mixeur ne devait jamais prendre le contrôle des fonds* ».

Dans le cas de Tornado Cash et Samouraï, les autorités leur reprochent d'avoir prélevé des frais de transaction et donc d'avoir indirectement profité financièrement d'opérations de blanchiment. En outre, elles estiment également qu'en tant qu'entreprises de transfert de fonds, Samouraï Wallet et Tornado Cash auraient dû remplir leur devoir de lutte contre cette pratique.

« *Cet angle d'attaque nie le principe de neutralité de ces technologies* », ajoutait Laurent MT. « *Un développeur n'a pas à remplir le rôle de la police, cette confusion me fait penser qu'ils sont prêts à tout pour éviter la prolifération d'outils qu'ils connaissent encore mal* ».

Décentraliser sans revenu

Que faire alors pour éviter la case prison ? « *L'essentiel est de prouver sa bonne foi au régulateur tout en prenant soin de ne pas le provoquer* », rappelle Frédéric Ocana.

Dans le cas de Tornado Cash ou Samouraï, il s'agira notamment de démontrer que leur fonctionnement n'est pas optimal pour blanchir des fonds. En effet, pour être le plus efficace possible, Whirlpool recommande de laisser ses fonds le plus longtemps possible à l'intérieur du mixeur afin que les fonds soient bien mélangés. Or, c'est justement ce que souhaite éviter un criminel.

« *Lorsqu'un acteur cherche à blanchir des fonds, il doit le faire le plus rapidement possible à la manière d'un 'go fast' pour mettre les sommes volées en dehors du périmètre de toute saisie* », détaille Frédéric Ocana. « *C'est notamment pour cette raison que les schémas utilisés par Lazarus laissaient énormément de traces malgré leur utilisation de mixeurs* ».

« Au final, l'approche la plus sûre est certainement de s'inspirer de la conception de Bitcoin, c'est-à-dire éditer un protocole totalement décentralisé et ne pas percevoir de revenus à partir de celui-ci », nous partageait Laurent MT. Mais sans la promesse de revenus futurs, cela limitera les incitations des développeurs à créer de nouveaux logiciels de ce type… Heureusement que la détermination de certains ne failli pas.

Pour aller plus loin sur ce sujet, il nous paraît indispensable de lire l'article de Stachtchenko : *Les dérives de la surveillance financière menacent nos démocraties.*

Conclusion

Finalement, l'évolution de Bitcoin continue de présenter des défis et des opportunités à travers différents aspects.

Malgré la réduction significative des récompenses suite au dernier halving, l'engagement continu des mineurs est souligné par l'augmentation du hashrate.

Bien que Bitcoin ait enregistré des avancées notables, telles que le franchissement du seuil d'un milliard de transactions et des volumes de transfert colossaux, certains défis demeurent, notamment dans le domaine de la confidentialité et des microtransactions.

Cependant, grâce aux ETF, l'intérêt croissant des investisseurs institutionnels pour ce nouveau véhicule financier reflète une adoption croissante.

Les récentes arrestations des développeurs de Samouraï Wallet mettent en lumière les tensions entre l'innovation technologique et la réglementation. Bien que la protection de la vie privée demeure essentielle, les pressions réglementaires compliquent le développement de solutions dans ce domaine.

En somme, la route vers une décentralisation accrue

Pour une analyse approfondie de ces sujets et plus, nous vous recommandons :

- ETHEREUM staking & problème
- Venezuela et l'interdiction de miner Bitcoin.
- Rapport institutionnel pour 1 million de dollars sur la relation entre Bitcoin et la liberté financière.
- La célèbre newsletter macroéconomique de Lyn Alden
- Les replays de Human Action Conférence 2024 (Economie autrichienne).
- Résumé du Discours du président Milei
- La prochaine fois que votre ami « normé » étatiste vous dira que le bitcoin sera magiquement interdit, vous pourrez lui proposer de se régaler avec ceci.
- Le Forum d'Oslo pour la liberté par la fondation des droits de l'homme. Livestream 5 juin
- Documentaire BTCPAY (Must see)
- Analyse technique Bitcoin par Le Journal Du Coin
- Nouvelle ouvrage dans ma liste de lecture