Experts Crypto

Bulletin d'information février 2023

> “It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning.”
>
> — Henry Ford

INTRODUCTION

La nouvelle année a apporté un regain d'optimisme sur le marché des cryptoactifs, le prix du **Bitcoin** (BTC) ayant augmenté de **39 %** en janvier, le marché dans son ensemble reprend des couleurs et comme d'habitude il y a des projets qui ont su tirer leur épingle du jeu. Que ce soient des anciens mastodontes comme **Solana** (+140%), **Fantom** (+150%) et **AVAX** (+83%), ou bien des nouveaux arrivants tels que **Aptos** (+420%), **CANTO** (+500%) et **RNDR** (+260%). L'euphorie s'est réinstallée aussi vite qu'elle a disparu nous rappelant que le sentiment dans l'écosystème est tout aussi volatile que les cours. Quelques bougies vertes et tout le monde abandonne l'idée d'un retracement plus conséquent pour remettre sur la table des scénarios saugrenus.

Cette newsletter sera consacrée aux deux projets qui tirent l'adoption vers le haut depuis leurs balbutiements, à savoir **Bitcoin** et **Ethereum**. Avec, pour commencer, une considération particulière aux **secondes couches** d'Ethereum (couche d'exécution des transactions) car selon nous Ethereum domine largement le combat des couches primaires (l'endroit où les transactions sont vérifiées et validées). Pour ensuite se concentrer sur Bitcoin et la couche primaire d'Ethereum. Pour finir, nous reviendrons sur les évènements d'adoptions des cryptoactifs dans le monde et sur certaines actualités qui ont attiré notre attention. Sans oublier le passage obligatoire par l'analyse technique.

Bonne lecture chers collaborateurs.

ANALYSE TECHNIQUE

BTC/USD en hebdomadaire avec une nouvelle résistance en noir par rapport au mois précédent.
https://www.tradingview.com/x/CW45GOPh/

BTC/USD en mensuel pour avoir une vision globale du cours.

https://www.tradingview.com/x/kTzf6sOn/

Ce qu'on constate c'est que la résistance mensuelle à 23300$ se retrouve également au sommet de la zone hebdomadaire des 24300$. En d'autres termes, le marché est à la résistance. Comme précédemment, nous restons prudemment ouverts à l'idée d'une hausse supplémentaire, étant donné la reconquête de la fourchette estivale de 19 000$ à 20 000$.

Il y a deux façons de mener ce combat contre la résistance de manière positive :

- D'abord, un simple franchissement et une confirmation mensuelle et hebdomadaire au-dessus du sommet de la fourchette 23300-24300 servirait de preuve tangible d'une poursuite vers la cible des 30000$.

- Deuxièmement, un repli formant un plancher plus haut. En effet, le marché peut être positif tant qu'un plus bas supérieur est formé à ou au-dessus de la zone des 19000$ - 20000$

Tout repli qui perdrait la fourchette estivale serait très baissier.

BTC/USD en journalier n'apporte pas beaucoup plus d'information mise à part une zone tracée à la main en jaune qui nous suggère une accélération à la baisse alimentée par beaucoup de stoploss qui pourraient être déclenchés si toutefois nous revisitons la zone. Nous vous invitons à [revoir la conférence du 23/01/23]() pour comprendre quelles sont les raisons derrière la propulsion du marché au-dessus de la résistance des 22600$. La nouvelle résistance en vert correspond au niveau hebdomadaire.

https://www.tradingview.com/x/5cBLxYsf/

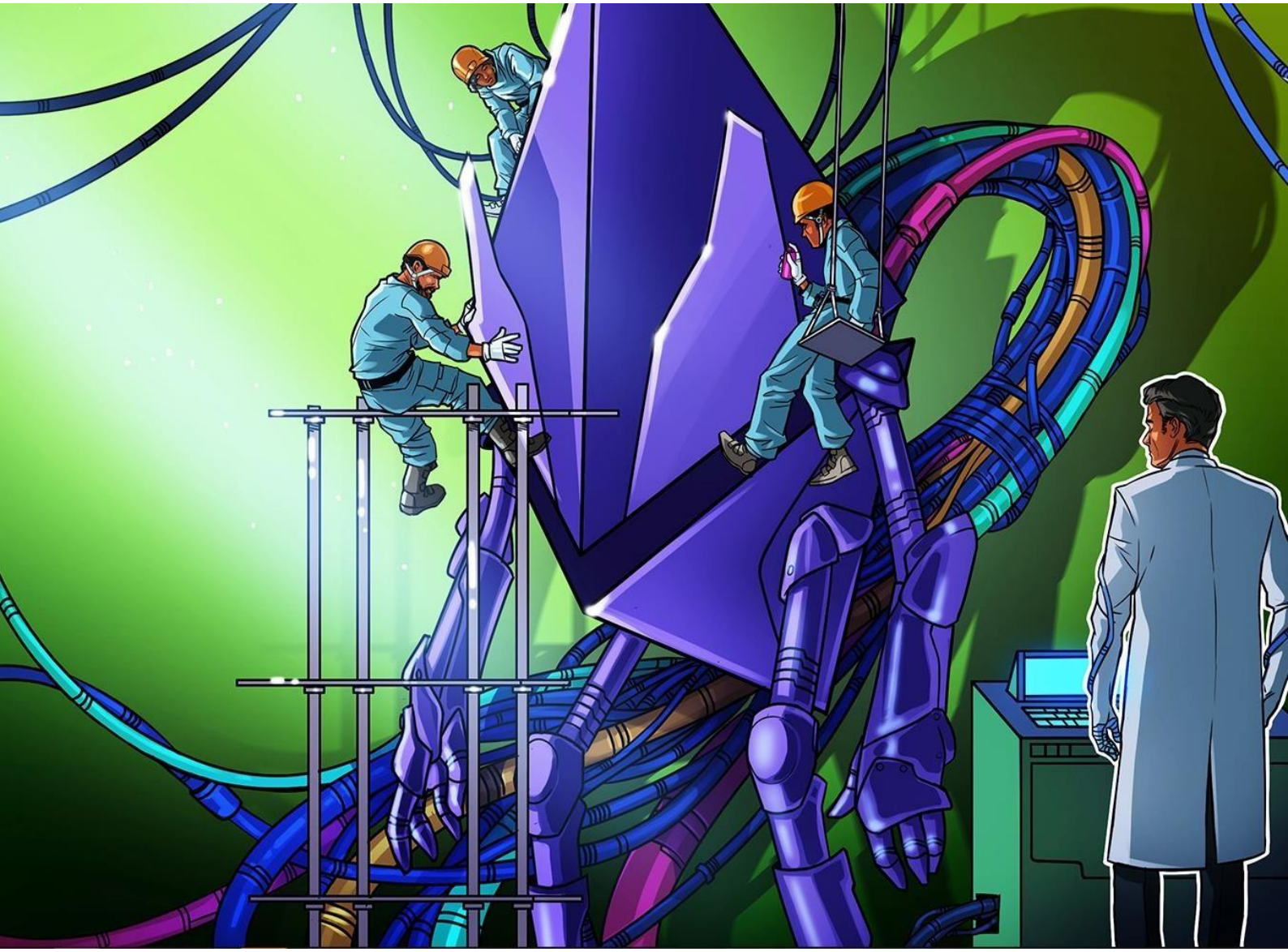
https://www.tradingview.com/x/vIPKHQKL/

Aptos a été la vedette de cette rotation à la hausse du marché. La mère des shorts squeeze qui a laissé sur son chemin des tombes remplies de cadavres de vendeurs à découvert. Sur cette belle note, le graphique journalier montre une tentative de rupture de la structure à la suite d'une clôture en-dessous des 18$.
La prochaine structure quotidienne viable est la consolidation entre 12$ et 13$.
Ce jeton a été très fort donc notre première idée n'est pas de chercher des raisons de le vendre. Au contraire, tant que la structure n'est pas rompue, nous serons à l'affût des signes d'un nouveau rebond haussier.

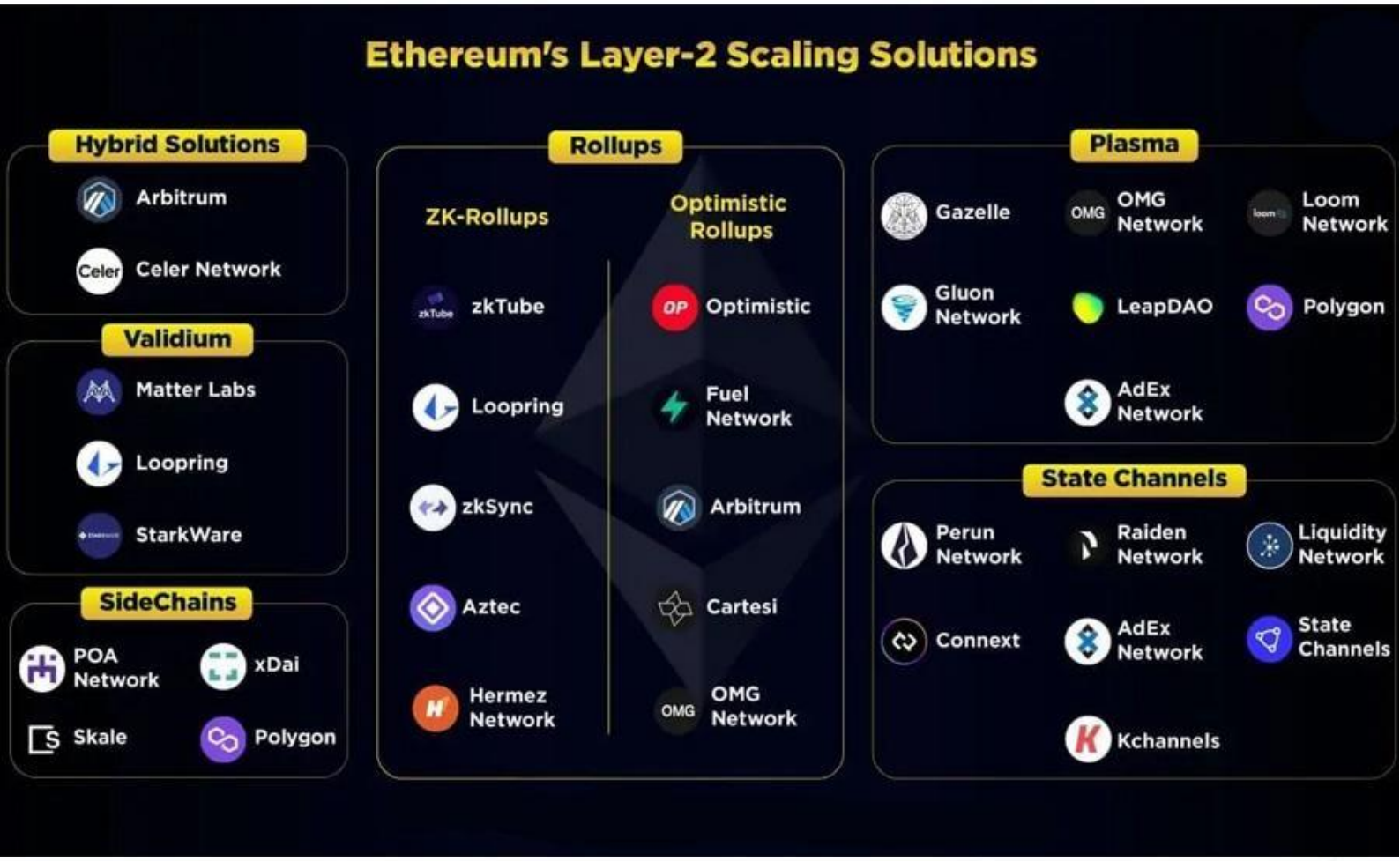
En résumé, si la rupture journalière ne se maintient pas, c'est-à-dire si le niveau des 18$ est repris, nous nous attendons à un autre resserrement à la hausse. Si la rupture se maintient, nous sommes ouverts à des rebonds intérimaires sur la zone de support toute neuve des 12$/13$. Dans tous les cas, il s'agit de garder un œil sur l'un des projets les plus en vogue.

ANALYSE FONDAMENTALE

1/ Les solutions de secondes couches (Layer 2)



Nous avions déjà mentionné les **layer 2** dans les newsletters, que ce soit le **Lightning Network** sur Bitcoin ou bien les multiples solutions sur Ethereum. Dernièrement les besoins de **mise à l'échelle** de la blockchain Ethereum se font de plus en plus sentir et les projets essayant de corriger ce problème sont nombreux. Vous trouverez ci-dessous une vue (incomplète) des différentes réponses :



Si vous souhaitez plonger dans les fondamentaux des solutions de passage à l'échelle sur Ethereum, cliquez sur ce lien. Nous allons essayer de définir de manière succincte ces appellations :

- **Les solutions Plasma** utilisent des arbres de Merkle pour créer une chaîne supplémentaire à la blockchain principale.

- **Les chaînes latérales** (sidechains) sont des blockchains latérales qui exécutent les transactions séparément de la blockchain principale et fonctionnent indépendamment en utilisant leur propre algorithme de consensus. Elles se connectent à Ethereum via un pont bidirectionnel.

- **Les canaux d'états** (State Channels) permettent aux participants d'effectuer des transactions hors chaîne tout en ne soumettant que deux transactions au réseau Ethereum. Les participants doivent verrouiller une partie de l'état d'Ethereum, comme un dépôt d'ETH, dans un contrat multisignature (« multisig »). Verrouiller l'état de cette façon constitue la première transaction et ouvre le canal. Les participants peuvent alors effectuer des transactions

rapidement et librement hors chaîne. Une fois l'interaction terminée, une transaction finale est soumise sur la blockchain, déverrouillant l'état.

- **Les roll-up** fonctionnent en exécutant des transactions sur la surcouche (Layer 2), tout en soumettant des données à la blockchain mère.

Il existe deux types de roll-up : **Les roll-up ZK** (Zero Knowledge), qui regroupent plusieurs transferts en une seule transaction, **et les roll-up optimistes**, qui fonctionnent en parallèle d'Ethereum.

Les roll-up ZK regroupent les transactions en créant ce que l'on appelle un SNARK (Succinct Non-interactive Argument of Knowledge) – Il s'agit d'une **preuve cryptographique** qui est soumise à la couche primaire, de sorte qu'une seule transaction est envoyée à Ethereum. Les roll-up ZK permettent des **transactions rapides**, mais la portée de ces transactions est limitée car ils ne sont **pas totalement compatibles** avec Ethereum.

Les roll-up optimistes s'installent en parallèle de la chaîne principale d'Ethereum et **supposent** que les transactions sont **valides par défaut** (d'où le terme optimiste). Les transactions sont mises en attente pendant 7 jours, après quoi elles sont considérées comme valides et ajoutées à la chaîne Ethereum. Ils peuvent offrir des améliorations en matière d'évolutivité car ils n'exécutent des calculs que dans le cas où l'intégrité d'une transaction est remise en cause. Les roll-up optimistes **assurent la compatibilité et la composabilité**, une exigence de la DeFi, mais ils sont soumis à des temps d'attente plus longs et à des attaques potentielles.

Propriétés	Optimistic rollups	ZK rollups
Coût fixe du gas par lot	Environ 40 000	Environ 500 000
Coût du gas par transaction	Plus important	Plus faible
Coûts de calcul hors chaîne	Plus faible	Plus important
Délai de retrait	Environ 1 semaine	Très rapide (il suffit d'attendre le prochain lot)
Complexité de la technologie	Accessible	Très complexe
Capacité de généralisation	Plus facile, car proche du réseau principal	Plus difficile

source : cryptoast

- **Validium** n'est pas différent de la technologie ZK roll-up dans la mesure où il utilise des preuves à divulgation nulle de connaissance (ZK proofs), mais **les données sont stockées hors chaîne**.
Cela peut permettre jusqu'à **10 000 transactions par seconde** sur chaque chaîne Validium et **un risque d'attaque plus faible.**
Cependant, il n'y est pas possible d'exécuter tous les types de contrats intelligents, la génération de preuves ZK nécessite une puissance de calcul élevée et les temps de finalisation peuvent être plus lents.

Les solutions les plus abouties sont **Arbitrum, Polygon et Optimism** (respectivement 1.4, 1.2 et 0.8 milliards de dollars en TVL)(les TVL sont totalement différentes sur le site L2beat ??). D'après Vitalik Buterin les solutions les plus prometteuses sont les ZK roll-up et Validium et elles deviendront **la norme** dans les années à venir, cependant les développeurs s'acharnent à améliorer leur **compatibilité** avec Ethereum et leur **composabilité** pour qu'elles puissent répondre à un maximum de cas d'usage.
La communauté française est largement engagée sur le protocole **StarkWare** qui utilise les validium, des STARKs (Scalable Transparent Argument of Knowledge) à la place des SNARKs et son propre langage informatique **le Cairo**. D'ailleurs les STARKs sont de plus en plus utilisés par les autres protocoles également mais c'est le fondateur de Starkware (et Zcash) qui les a inventés. (Eli-BenSasson).

Depuis le **Merge d'Ethereum** les roll-up optimistes ont pu se développer à grande vitesse. Et nous voyons pléthore de projets se déployer sur **Arbitrum et Optimism**. Mais nous allons nous concentrer sur le couteau suisse des solutions de scaling Ethereum : **Polygon Network**. On peut voir dans le premier tableau que Polygon utilise les solutions Plasma et Sidechains mais le projet a également racheté le projet Hermez qui travaille sur les ZK roll-up depuis 3 ans. Puis a également racheté le Mir Protocol, une autre solution basée sur les ZK Roll-up.

Ils sont parmi les premiers à avoir mis l'accent sur leur **faible dépense énergétique**. Cette stratégie leur a permis de surfer sur la vague « **responsable** » et « **écologique** » avant le Merge d'Ethereum. De plus, Polygon a recruté beaucoup de personnes venant de grands groupes Web2 et a utilisé leurs compétences et contacts pour attirer ces grands groupes. Cela a entraîné un cercle vertueux qui, associé à des frais de transactions peu onéreux, font de Polygon une rampe de lancement idéale pour les entreprises.

C'est pourquoi le protocole est devenu l'un des **partenaires privilégiés** des entreprises. Polygon a été choisi par **Meta** comme protocole pour créer des NFTs directement dans Instagram. « Une plateforme de cette taille nous aidera à faire basculer plus **d'un milliard d'utilisateurs** dans le Web3 », a déclaré début novembre Sandeep Nailwal, le cofondateur indien du protocole.

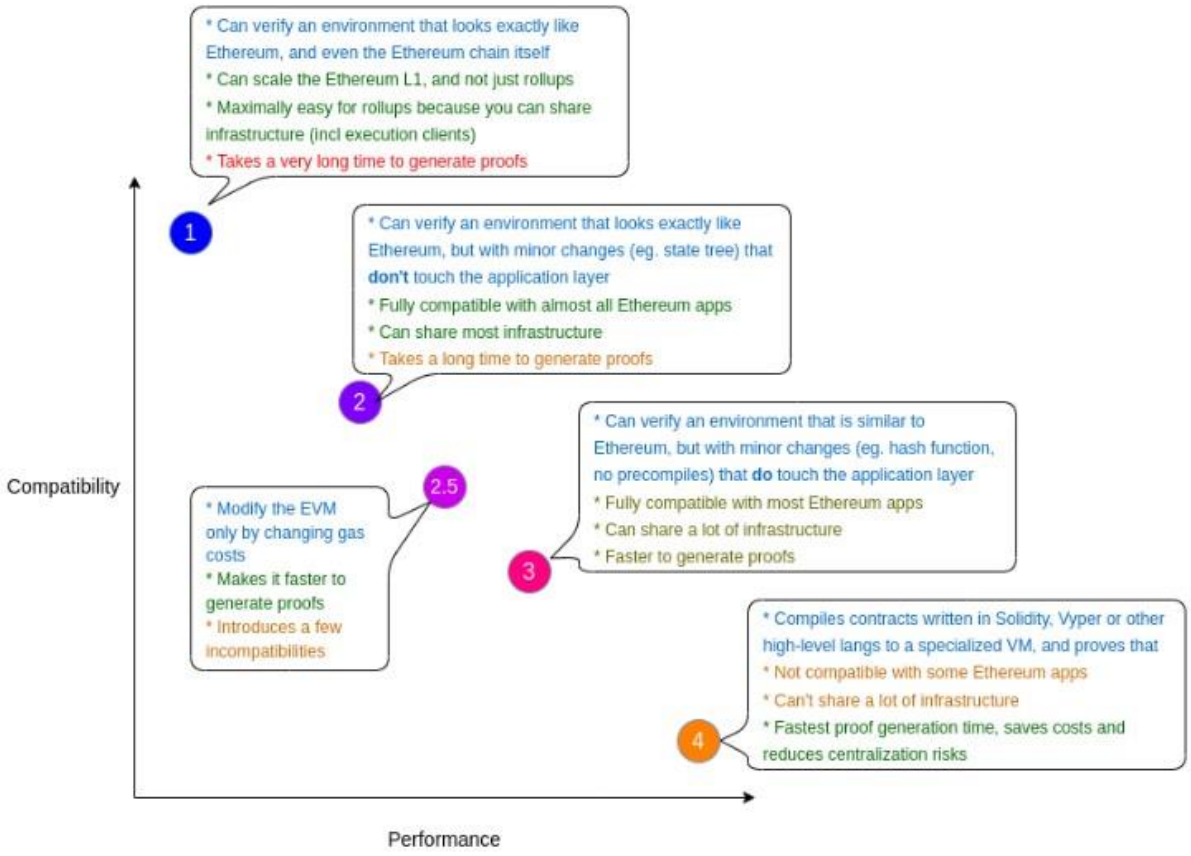
Le groupe américain, **Starbucks**, a développé son nouveau programme de fidélité avec Polygon. Actuellement en bêta test, « Starbucks Odyssey » permettra aux clients de collectionner des NFTs de la marque et d'accéder à des expériences exclusives. **Nike** lancera en 2023 une plateforme de vêtements virtuels (Swoosh) basée sur Polygon. Même le géant américain de la grande distribution **Walmart** travaille avec eux ! Sans oublier leur dernier partenariat avec **Mastercard** visant l'industrie musicale. (Et il y en a d'autres)

Le 17 janvier 2023 Polygon a confirmé son **dynamisme** et son souhait de constamment améliorer la qualité de ses solutions de mise à l'échelle. En effet, la chaîne a subi un hardfork avec un double objectif :
- Diminuer les frais de transaction en période de forte activité
- Diminuer les réorganisations de la chaîne

Un hardfork présente des risques mais s'avère nécessaire afin d'améliorer les fondations d'un protocole blockchain au fil des innovations et des rétrospectives. Celui-ci devrait permettre d'améliorer à la fois **la sécurité** et **la scalabilité** de la chaîne Polygon.

Beaucoup d'experts estiment que les layer 2 d'Ethereum seront le moteur de la prochaine bulle spéculative, comme celle observée sur les layer 1 en 2020-2021 (Solana, Avalanche, Cardano, Polkadot etc.).
À ce petit jeu, les projets les plus récents pourraient attirer les investisseurs. D'ailleurs, les lancements des futurs jetons du réseau **StarkNet** et de **ZkSync** sont déjà considérés comme des **événements majeurs** en 2023. A notre avis, **Polygon** profitera moins de ce moment spéculatif et l'enjeu pour ses équipes sera de valoriser les volumes et le nombre de projets qui sont développés dessus. Mais ce n'est pas l'avis de tous, Route2FI partage son avis sur twitter et nous devons lui concéder, il est plutôt convaincant.

Une dernière chose qu'il faut garder en tête c'est que pour remplir leurs missions, les solutions de seconde couche doivent proposer des environnements dits « EVM équivalents » (compatible avec la machine virtuelle Ethereum). Si certaines solutions n'ont pas de problème à ce niveau, ce n'est pas le cas des ZK roll-up. Comme nous venons de le voir, les ZK roll-up ne sont pas totalement compatibles EVM car ils ne peuvent pas implémenter une simple copie de l'EVM d'Ethereum.
Par conséquent, les protocoles de ZK roll-up doivent développer des **versions alternatives** à l'EVM, compatibles avec le traitement des preuves ZK.
Ces versions de l'EVM compatibles avec les zero-knowledge proofs sont **appelées zeroknowledge EVM** ou **zkEVM**.
Vitalik a écrit un article sur le sujet pour essayer d'apporter un peu de lumière sur ces complexités techniques, bien détaillé dans son graphique ci-dessous :



Heureusement, le Journal du Coin nous aide à comprendre ces intrications. Le résumé est donné par leur tableau ci-dessous :

Type de zkEVM	Avantages	Inconvénients
Type 1	Compatibilité parfaite	Temps de génération des preuves
Type 2	Équivalence parfaite à l'EVM	Temps de génération des preuves
Type 3	Facilité de développement Temps de génération des preuves réduit	Nombreuses incompatibilités
Type 4	Temps de génération des preuves réduit	Nombreuses incompatibilités

Pour information, les ZK roll-up de Starknet sont des Zkevm de **type 4** et ceux de Polygon sont de **type 2**.

2/ Améliorations Bitcoin et Ethereum

A/ bitcoin and lightning

ORDINALS

Le lancement d'Ordinals (21 janvier), un protocole permettant de créer des NFTs sur la blockchain Bitcoin, a fait resurgir un **débat** existant depuis les débuts de Bitcoin, à savoir :

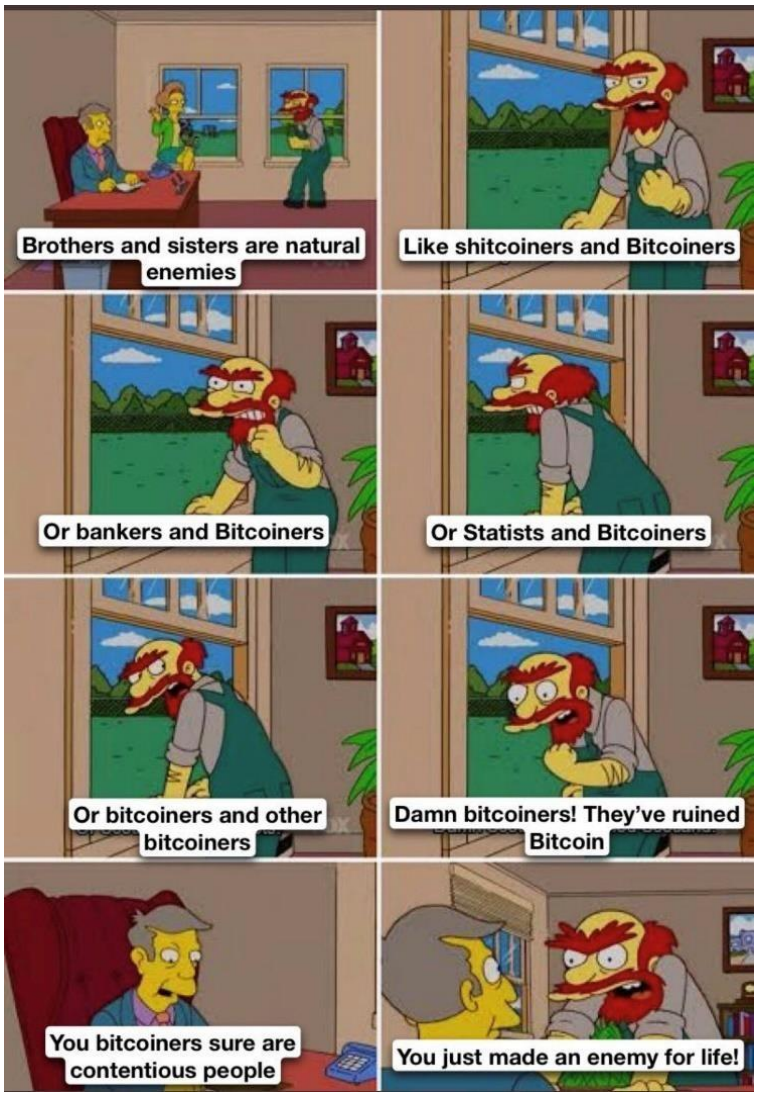
Bitcoin est-il voué à rester seulement un réseau de paiement décentralisé ou peut-il aussi devenir un écosystème d'applications décentralisés ?

Selon **Casey Rodarmor**, le développeur à l'initiative d'**Ordinals**, le protocole permet d'ajouter du texte ou des images à des **satoshis**, la plus petite unité sur Bitcoin, pour créer des **« artefacts numériques ».**

Ordinals est le dernier projet visant à introduire les NFT dans l'écosystème Bitcoin. Le premier projet, **Counterparty**, a d'abord introduit les jetons non fongibles dans Bitcoin en 2014 et avec la collection Rare Pepes en 2016 la pratique s'est largement popularisée. Puis **Stacks** a suivi en 2017. Cependant, le projet **Ordinals** est différent car les actifs, y compris les JPEG et même

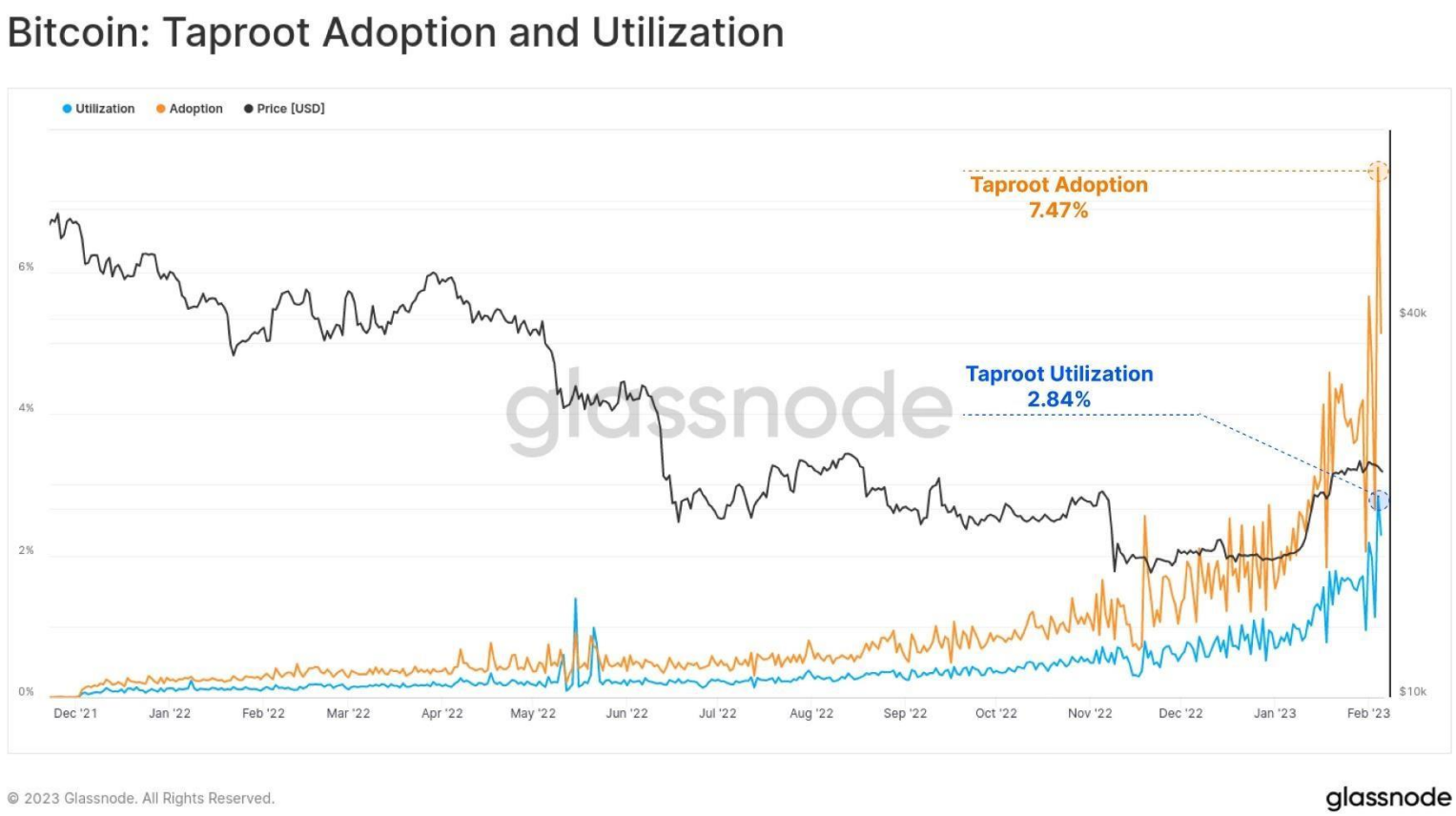
les jeux vidéo, sont inscrits directement sur des satoshis sur la blockchain Bitcoin sans avoir besoin d'une sidechain ou d'un jeton supplémentaire.

Pour approfondir le sujet, le chirurgien Pourteaux a écrit un article très détaillé.
Nous vous avons traduit sa conclusion :
« Le débat entre les transactions financières et le stockage de données de la communauté bitcoin existe depuis presque aussi longtemps que le bitcoin lui-même. Alors que ce débat semblait avoir été réglé en 2014 avec le compromis OP_RETURN, il est sur le point d'être rouvert avec l'abandon involontaire par Tapscript de la quasi-totalité des limitations relatives aux stockages de données. Malgré l'insistance des bitcoiners les plus acharnés, il existe de nombreuses **applications intéressantes** pour les crypto-monnaies en dehors des **transactions financières**, et les NFT en sont un exemple. Bien sûr, **l'intégrité du réseau bitcoin** pour les transactions financières est **primordiale**, et toute utilisation non financière devrait idéalement soutenir cet objectif principal plutôt que de lui nuire. »



TAPROOT

L'adoption de Taproot atteint des sommets (cf graphique ci-dessous). Taproot vise à accroître **la scalabilité et la confidentialité** de la blockchain sans compromettre **la sécurité ou la décentralisation**. Cette mise à jour permettrait aussi d'envisager un avenir de modularité pour l'évolution du code informatique de Bitcoin. (Une plus grande flexibilité sur les contrats intelligents sur Bitcoin).



Source : Glassnode

Pour suivre tous les développements du code informatique de Bitcoin, nous vous conseillons Bitcoin Optech (disponible également en français !)

Lightning Network

Minecraft s'associe à The Bitcoin Company. Vous pouvez construire votre citadelle et miner de vrais satoshis, seul ou avec vos amis, sur le serveur Minecraft Satlantis. Ceci ouvre la voie vers la création d'une **véritable économie** dans le jeu grâce à Bitcoin et Lightning.

Nous avons évoqué **NOSTR** (Notes and Stuff transmitted by Relays) dans la conférence du lundi 06/02/2023. C'est un protocole ouvert qui vise à créer un réseau mondial de partage de données résistant à la censure, principalement axé sur l'amélioration des réseaux sociaux. Forcément les Bitcoiners en sont déjà des grands fans. De plus, **Edward Snowden** semble être d'accord, puisqu'il a déclaré sur Nostr qu'il n'avait jamais vu Bitcoin « se sentir aussi puissant que sur Nostr ». Et il ajoute :
« Les transactions instantanées et effectivement libres qui découlent du fait d'avoir autant de personnes sur les adresses Lightning, c'est comme arriver sur une autre planète. »

Emeralize. Il s'agit d'une **nouvelle plateforme d'apprentissage** en ligne, qui utilise Bitcoin et Lightning comme rail de paiement pour rendre les cours plus **largement accessibles** et plus faciles à **monétiser**. Nous sommes bien sûr encore aux prémices du projet, mais il y a déjà deux cours disponibles (l'un gratuit par Zebedee, l'autre partiellement payant, par Pleblab). Pour chaque cours, il est possible de donner un pourboire au créateur (ou même à plusieurs créateurs grâce au fractionnement des paiements) pour soutenir son/leur travail.

Ce qui nous amène au projet suivant ZEBEDEE ! Une application disponible sur Android et IOS regroupant plusieurs jeux qui permettent de **gagner des satoshis**. Les derniers jeux ajoutés, avec la participation de VIKER, sont **ChessBitcoin** et **BitcoinScratchMatch**. Les deux nouveaux jeux marquent une nouvelle étape dans un partenariat qui a produit **10 jeux** jusqu'à présent et qui a été le premier à introduire le concept de **« play-and-earn** » durable dans les jeux mobiles occasionnels, alimenté par les transactions Bitcoin.

Le lancement de Wavlake, l'idée générale de cette application est de permettre aux artistes de publier de la musique originale et de gagner directement des pourboires en bitcoins en retour. Ça reste encore très expérimental mais les créateurs sont des vrais passionnés de musique et de bitcoin donc il est possible que leur passion porte leur projet et attire les foules.

Le célèbre intermédiaire financier suisse, **Mt Pèlerin**, intègre la seconde couche de Bitcoin. Il est dès aujourd'hui possible d'acheter et vendre des satoshis directement sur le réseau Lightning, via le **Bridge Wallet** proposé par **Mt Pelerin** (un portefeuille auto-hébergé) De plus, les utilisateurs pourront désormais facilement régler des achats aux boutiques acceptant Bitcoin. Et inversement, ils pourront **recevoir et convertir** leur satoshis vers leur compte bancaire dans **14 devises fiduciaires**, dont le franc suisse, l'euro et le dollar.

La totalité de l'expérience Lightning network est désormais disponible sur **CashApp**. Leurs utilisateurs pourront désormais envoyer et recevoir des bitcoins vers d'autres portefeuilles compatibles avec Lightning, **instantanément et gratuitement**. Nous rappelons que **CashApp** est l'une des applications de **Square** (2009 Jack Dorsey), l'un des plus gros processeurs de paiement au monde derrière **Paypal** et **Stripe**. En 2022, **Square** a traité des paiements d'une valeur de **64 milliards** de dollars.

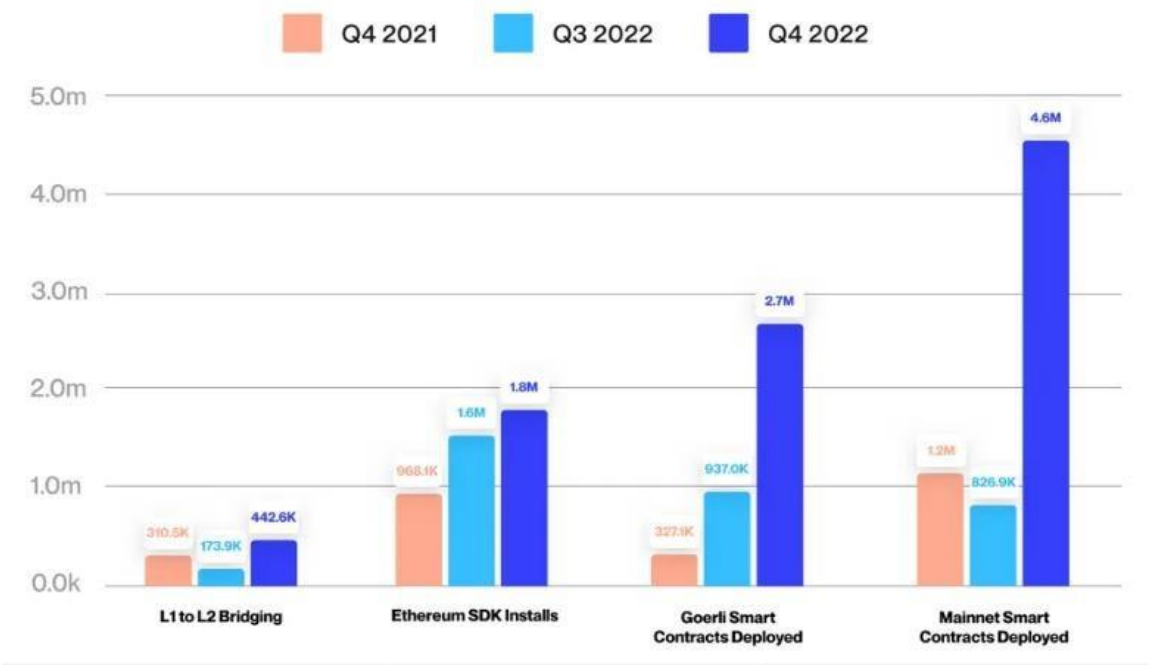
Dans la même lignée, **Jack Mallers** a annoncé un partenariat avec **Fiserv** en lançant un projet pilote sur **CloverCommerce**, une association de moins grande envergure mais notre cher Jack insiste qu'il est temps **de montrer au monde** que le réseau Lightning est le **processeur de paiement supérieur**. Et il est vrai qu'un réseau de paiement ouvert, instantané, bon marché, inclusif et innovant semble trop beau pour être vrai.

Pour finir, l'un des défis les plus importants pour le réseau Lightning est de recevoir des paiements **tout en étant hors ligne**. Aujourd'hui, il est pratiquement impossible de le faire dans une configuration sans tiers de confiance, car votre nœud doit être en ligne pour signer la transaction d'engagement lorsque vous recevez des fonds. **Le but** du réseau Lightning est de réussir à offrir la meilleure expérience utilisateur possible sans compromis en matière de **souveraineté et de confidentialité** (ou, de manière plus réaliste, avec le moins de compromis possible). Et les avancées sont prometteuses mais nous ne sommes pas assez maîtres en la matière pour prétendre pouvoir expliquer les progressions.

Pour essayer de comprendre par vous-même voici quelques liens utiles :
https://nitter.lacontrevoie.fr/moneyball/status/1613277882029346819
https://lists.linuxfoundation.org/pipermail/lightning-dev/2023-January/003820.html
https://fanismichalakis.fr/posts/latest-strikes-4/#asynchronous--offline-payments-in-eclair
https://blog.lnmarkets.com/

B/ Ethereum, le fork Shangaï et les adresses furtives

Il ne se passe pas un instant sans que quelque chose bouge sur Ethereum. **L'innovation incessante** a été extrêmement soutenu durant le marché baissier de 2022 (cf graphique cidessous) et 2023 nous réserve également son lot de surprises.

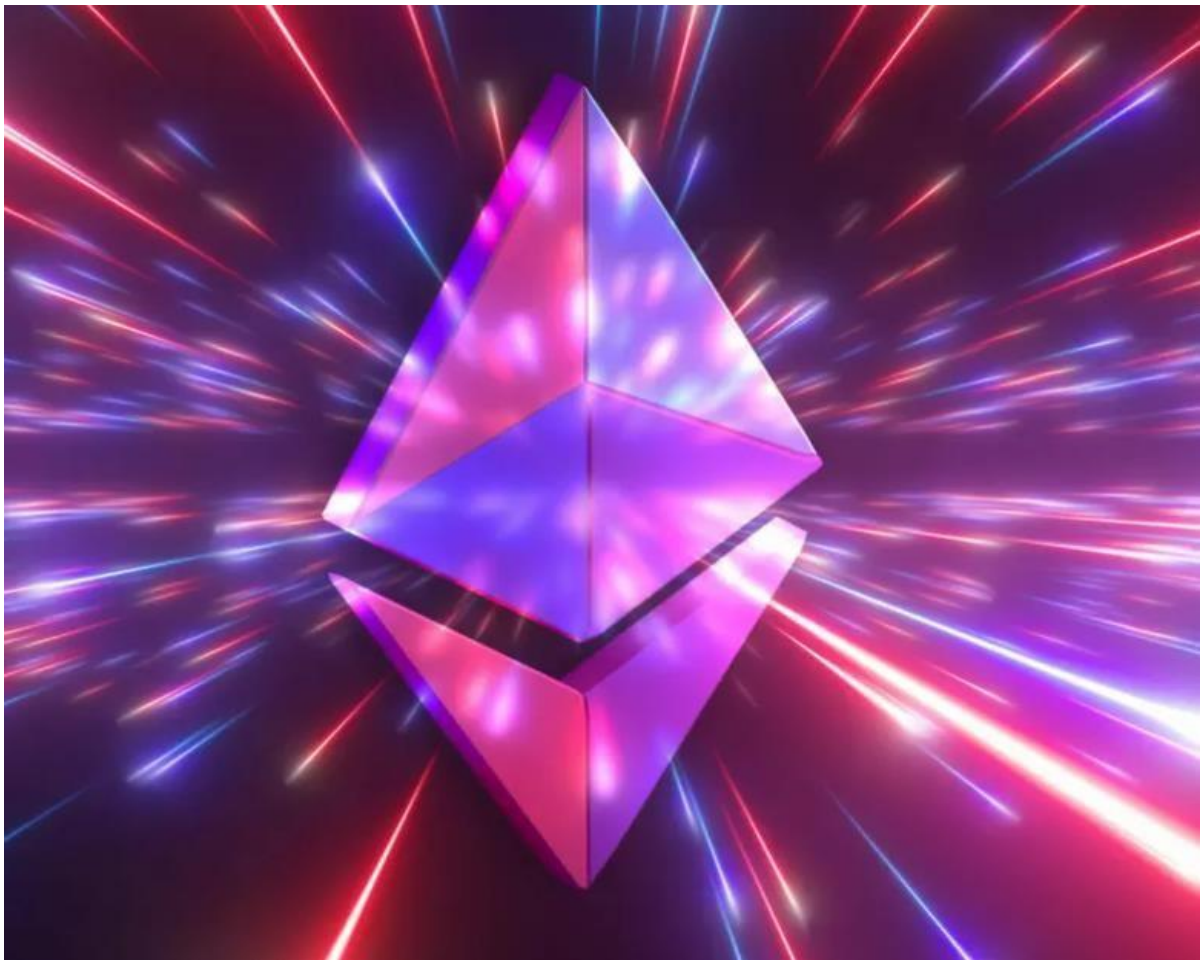


Le Hard fork Shanghaï

Le 15 septembre dernier **Ethereum** a marqué l'histoire en finalisant sa transition du **Proof of Work au Proof of Stake** (Nous vous invitons à relire les détails dans la newsletter d'août). Toutefois, les ETH déposés en staking (immobiliser des jetons ETH dans le but de valider les transactions) sur la **beacon chain** sont encore bloqués sur celle-ci. Mais la situation devrait changer en mars avec le lancement du hard fork. Une mise à jour qui permettrait aux validateurs de **retirés** leurs Ethers du contrat. Introduire la possibilité de retirer ses fonds de la chaine validatrice est naturellement **une priorité** pour la communauté et les développeurs du réseau. Nous pensons que c'est une **avancée positive** pour la chaîne Ethereum car les individus seront plus enclins à devenir validateurs s'ils ont la **possibilité de récupérer** leurs fonds selon leur bon vouloir. Ce qui devrait encourager plus de staking donc plus de **sécurité et de décentralisation**. Et les chiffres parlent d'eux-mêmes car ils sont en constante croissance. En effet, un total de 25.5 milliards de dollars en Ether sont verrouillés sur le contrat validateur de staking. Le nombre de validateurs (lot de 32 Ethers stakés) est en constante augmentation depuis le lancement de la beacon chain et a dépassé le nombre symbolique des 500 000 le 12 janvier 2023.

Cela dit, les développeurs Ethereum ont pris leur **précaution** car ils ont plafonné les retraits à 43 200 ETH par jour (16.5 millions actuellement). Cette limite devrait permettre d'éviter un **exode massif** et soudain des validateurs une fois la mise à jour terminée. Il y aura évidemment des « stakers », ayant bloqué leur ETH il y a longtemps, qui vont débloquer rapidement en raison des **vents macroéconomiques contraires** de ces deux derniers trimestres mais nous devons regarder la situation dans son ensemble : Actuellement, **moins de 15%** des ETH sont bloqués. Ce chiffre est très faible car les chaînes en POS à grande capitalisation ont généralement **40 à 75%** de leur réserve en circulation verrouillé. De plus, ETH ne sera pas considéré comme plus risqué que les autres jetons en POS dont l'écosystème est largement

moins développé. Ainsi, nous pensons que beaucoup plus de détenteurs d'ETH décideront de « mettre en jeu » leur jetons après la **mise à jour Shangaï**. Cela ne signifie pas que le pourcentage d'ETH mis en gage atteindra 70% du jour au lendemain, mais en prenant tous les éléments en considération, il serait surprenant que le plus grand réseau POS, doté d'un écosystème L1 et L2 florissant, reste longtemps parmi les réseaux ayant le plus faible pourcentage de jetons stakés.



Pour **nuancer** un peu notre enthousiasme, le passage en POS et l'introduction de la mise à jour EIP 1559 **renforcent la centralisation du réseau** dans le sens où Ethereum est devenu **déflationniste** (de moins en moins de jetons disponibles) et les validateurs (ceux qui possèdent déjà des gros montants d'ETH) reçoivent des récompenses en ETH. Par conséquent, les gros portefeuilles accumulent de plus en plus de jetons alors que ces derniers sont de plus en plus rares. Par conséquent**, la concentration de la possession** de jeton ETH s'accentue, ce qui nuit à la décentralisation du projet. C'est-à-dire que les propriétaires de nœuds validateurs peuvent **accroitre leur influence** sur le réseau au fil du temps **sans déployer de ressources supplémentaires**. (Il leur suffit de staker leurs récompenses).

S'ajoute à cela, deux autres phénomènes :

- Premièrement, les détenteurs d'ETH peuvent participer au **staking liquide**, ce qui leur permet d'emprunter des ETH avec leur ETH et d'augmenter leur récompense. Donc **ils cumulent** toujours plus de jetons.
- Deuxièmement, la **raréfaction** du jeton ETH provoque son **appréciation** qui, à son tour, va **accroître** le coût d'un nœud validateur. Finalement, ce phénomène va **restreindre** la possibilité de posséder un nœud validateur et **exacerber** la centralisation du réseau.

Notre chère Lyn Alden explique ceci avec un exemple très éloquent : « Ce serait comme un système politique dans lequel vous obtenez un vote pour chaque centaine de dollars que vous possédez, et où le gouvernement vous verse également un dollar pour chaque vote. Mary, professeur de sciences au lycée, avec 20 000 dollars de patrimoine, obtient 200 voix et reçoit 200 dollars du gouvernement pour avoir voté. Jeff Bezos, dont la valeur nette est de 200 milliards de dollars, obtient 2 milliards de voix et reçoit 2 milliards de dollars du gouvernement pour avoir voté. Il est un citoyen plus précieux que Mary, par un facteur d'un million, et il est également mieux payé par le gouvernement parce qu'il est déjà riche. »

Vers un réseau Ethereum plus confidentiel

Malgré une évolution fulgurante, le réseau fait encore face à de nombreux défis. Nous avons beaucoup parlé de la scalabilité mais un autre des principaux challenges pour les années à venir est la **confidentialité.** C'est pourquoi Vitalik a publié le résultat de ses recherches sur le sujet. Il y met en lumière un nouveau type d'outil : **les adresses furtives** (stealth addresses). D'après le co-fondateur, ce type d'adresse pourrait être implémenté rapidement et représenterait une avancée significative pour la vie privée des utilisateurs d'Ethereum.

C/ Faits divers

Le gouvernement américain

Commençons par cette annonce de la justice américaine du 18 janvier 2023 promettant une action **d'application de la loi à l'échelle internationale.** Des mots qui nous ont fait peur et pourtant rien de sensationnel car il s'agit de la saisie d'une plateforme d'échange jusqu'alors inconnue au bataillon **« Bitzlato »**. Certes, c'est une entité utilisée de manière intensive par **Hydra Market** (première marketplace dédiée aux échanges illégaux sur le darknet). Mais les volumes étaient si faibles que la saisie ne s'éleva qu'a **543 BTC**. Plus de peur que de mal à la suite de cette annonce, c'est une plateforme douteuse sanctionnée pour un écosystème plus sain.

Par la suite, la **Maison Blanche** a publié (27 janvier) une nouvelle feuille de route concernant la réglementation des cryptoactifs sur le territoire.
Ses recommandations portent notamment sur l'élargissement des pouvoirs des régulateurs, le renforcement des exigences en matière de communication d'informations, le renforcement des sanctions en cas de faute, l'augmentation des fonds alloués à l'application de la loi et le suivi des conseils formulés dans le rapport du Conseil de surveillance de la stabilité financière mandaté par le décret.

Au-delà de ce projet de loi, Bitcoin fait de plus en plus parler de lui chez les politiciens américains. Entre ceux qui ont officiellement déclaré en avoir acheté et ceux qui essayent de faire passer des lois pro-cryptos, la tendance est clairement à la démocratisation. La dernière initiative nous vient de l'Arizona, où une sénatrice a carrément demandé de rendre Bitcoin cours légal dans l'Etat. Elle nage en plein rêve car elle a également demandé que les cryptoactifs soient exonérés d'impôt.

Malgré l'hiver crypto et les nombreux opposants, **la question de l'adoption** continue de faire son bout de chemin.

Le Brésil et l'Argentine envisage une monnaie unique

Le président argentin **Alberto Fernandez** salue le président **brésilien Luiz Inacio Lula da Silva** au palais Itamaraty à Brasilia, le 2 janvier 2023.

Les deux chefs d'État ont prévu des discussions et une annonce officielle auprès des médias dans les semaines à venir. Le ministre argentin de l'économie, **Sergio Massa**, se montre toutefois prudent et mesure bien la complexité de ce projet commun :

« Il y aura une décision pour commencer à étudier les paramètres nécessaires pour une monnaie commune, ce qui inclut des questions allant des enjeux budgétaires au poids de l'économie (de chaque pays), en passant par le rôle des banques centrales. »

Cette **nouvelle couche monétaire** deviendrait peut-être le remède pour ces pays en crise et pourrait façonner la croissance du continent pour les prochaines décennies.

Le Salvador continue de nous épater

Ce petit pays d'Amérique Centrale n'arrête pas de surprendre ! Cette fois-ci, c'est en remboursant l'intégralité des 800 millions de dollars de dette qui arrivait à maturité le 24 janvier 2023. Surprenant, c'est le moins que l'on puisse dire sachant que le FMI et l'ensemble des médias les plus influents avaient parié contre la solvabilité du pays suite à la décision du président **Nayib Bukele** de rendre le Bitcoin cours légal.

Ce dernier a pris plaisir à prouver qu'ils ont eu tord dans un communiqué via twitter, dans lequel il s'exprime impudemment : « Ils mentent et mentent et mentent, et quand leurs mensonges sont exposés, ils passent en mode silence radio ».
Par ailleurs, ce remboursement s'inscrit dans le programme de rachat de la totalité de la dette Salvadorienne engagé par le pays en juillet 2022. Une dette qui s'élève à 26 milliards de dollars. Soit 81% de leur PIB.

En contraste total, il est curieux de voir que les institutions internationales ne s'inquiètent pas plus du fait que :

- Du côté de la France, la dette a explosé de 2 000 milliards d'euros (accumulée en 40 ans) à plus de 3 000 milliards d'euros durant les seules 6 petites dernières années. Environ 113% du PIB.
- Du côté des Etats-Unis, la dette s'élève à 31 458 milliards de dollars. Près de 120% de leur PIB. Nous ne rentrerons pas dans les détails sur les problèmes liés au plafond de leur dette.

A titre de comparaison, l'endettement par habitant au Salvador est de 5300 dollars, pour la France il est de 43000 euros et aux USA, il est de 94000 dollars.
Le combat de ne s'arrête pas sur le terrain économique, il s'est poursuivi durant le concours de Miss univers.
Si la victoire a été décernée aux USA, la miss du Salvador a arboré une belle médaille Bitcoin qui lui a valu d'être remarqué par la communauté crypto.

Nous souhaitons réussite et prospérité à ce courageux pays, et ce même si l'adoption de bitcoin sur leur territoire n'est pas encore au rendez-vous. En effet, le journaliste de **Cointelegraph**, **Joseph Hall**, s'est rendu sur place à plusieurs reprises et témoigne d'une adoption difficile car, selon lui, si la population adore son nouveau dirigeant, elle ne comprend pas encore les tenants et aboutissants de cette nouvelle technologie.

L’Iran et la Russie

Un nouveau jeton stable adossé sur l’or devrait voir le jour pour permettre de contourner les sanctions économiques imposées par le leader mondial. En effet, en utilisant une monnaie virtuelle appuyée sur l’or, l’Iran et la Russie pourront échanger des biens et des services sans avoir à utiliser le dollar américain, qui est la monnaie dominante dans les transactions internationales.

ETF Bitcoin à Hong Kong

Ce genre de véhicule financier existe déjà sur la bourse de Hong Kong depuis 2021. Néanmoins le responsable de Samsung Asset Management Hong Kong, Park Seong-jin explique à cointelegraph que l’expérience de la branche d’investissement de Samsung en matière de gestion du risque pourrait attirer encore plus d’investisseurs institutionnels. Il s’agirait d’un ETF (Exchange Traded Fund) de contrat à termes basé sur bitcoin et marquerait une preuve supplémentaire de l’intérêt que les acteurs économiques ont pour Bitcoin.

ETH continue d’attirer les innovations financières

Index Coop est une entreprise qui facilite l’accès à l’investissement dans l’écosystème crypto. Le 24 janvier 2023, ils ont annoncé la création d’un nouvel index composé des principaux jetons des projets de staking liquide sur Ethereum. Un produit qui saura trouver des intéressés quand bien même le staking liquide pourrait être moins prisé dès que la mise à jour **Shangai** aura eu lieu.

D’autre part, la NAB, **National Australia Bank**, sera la deuxième des quatre grandes banques australiennes à lancer une monnaie stable. Après que la banque rivale **Australia and New Zealand Bank** (ANZ) ait créé la sienne, baptisée **A$DC**, l'année dernière. La pièce, baptisée **AUDN**, sera lancée sur les blockchains Ethereum et Algorand dans le courant de l'année et pourrait jouer un rôle dans les plans de transition énergétique de l'Australie.

AAVE déploie sa troisième version sur le réseau principal d’Ethereum après 10 mois de test sur d’autres réseaux. Cette mise à jour était très attendue car elle permettra de déployer le fameux jeton stable **GHO**. Un évènement majeur dans l’écosystème de la finance décentralisée.

L'Intelligence Artificielle : la nouvelle tendance

Enormément de choses à dire encore sur ce sujet, nous vous invitons à lire les articles suivants : ChatGPT : une brève introdutcion

Microsoft investit des milliards de dollars dans open AI, l'entreprise derrière le phénomène ChatGPT

Le phénomène se déverse sur l'écosystème crypto.

Canto et Aptos

Le grand gagnant de ce début 2023 est le jeton APT de **Aptos**. Cette blockchain de type layer 1 a été inventé par une partie de l'équipe du projet **Diem** (ou Libra) de **Meta**. Celle-ci se veut révolutionnaire sur plusieurs aspects. D'abord en utilisant un **nouveau langage de programmation**, ensuite en exploitant une **nouvelle méthode de consensus**. Pour une revue exhaustive du projet, **Cryptoast** rentre ici vraiment dans les détails.

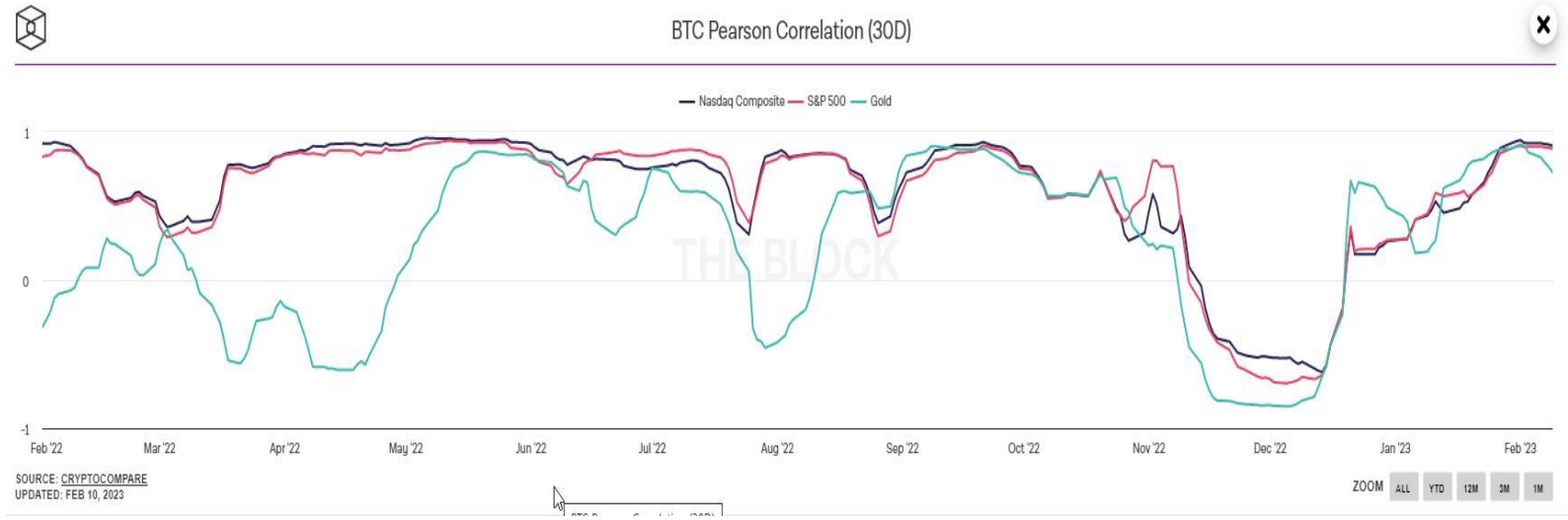
Lancée en aout 2022, **Canto** est une blockchain **permissionless** **(sans permission)**, de type Layer 1, qui fonctionne avec la machine virtuelle Ethereum. Elle fait partie du réseau **Cosmos** et propose une monnaie stable native appelée **NOTE**. Les développeurs de **Canto** affirment que l'écosystème a été "construit pour tenir les promesses de DeFi"

Les **principaux objectifs** formulés par **Canto** sont les suivants :

- Offrir des frais nuls pour les fournisseurs de liquidité et permettre une liquidité gratuite pour les traders, les protocoles et les autres participants.
- Développer une infrastructure publique gratuite sans l'utilisation de jetons de gouvernance souveraine ou de loyer.
- Contourner l'appropriation des utilisateurs par l'interface afin d'encourager les utilisateurs à s'engager dans de nouveaux protocoles.

CONCLUSION

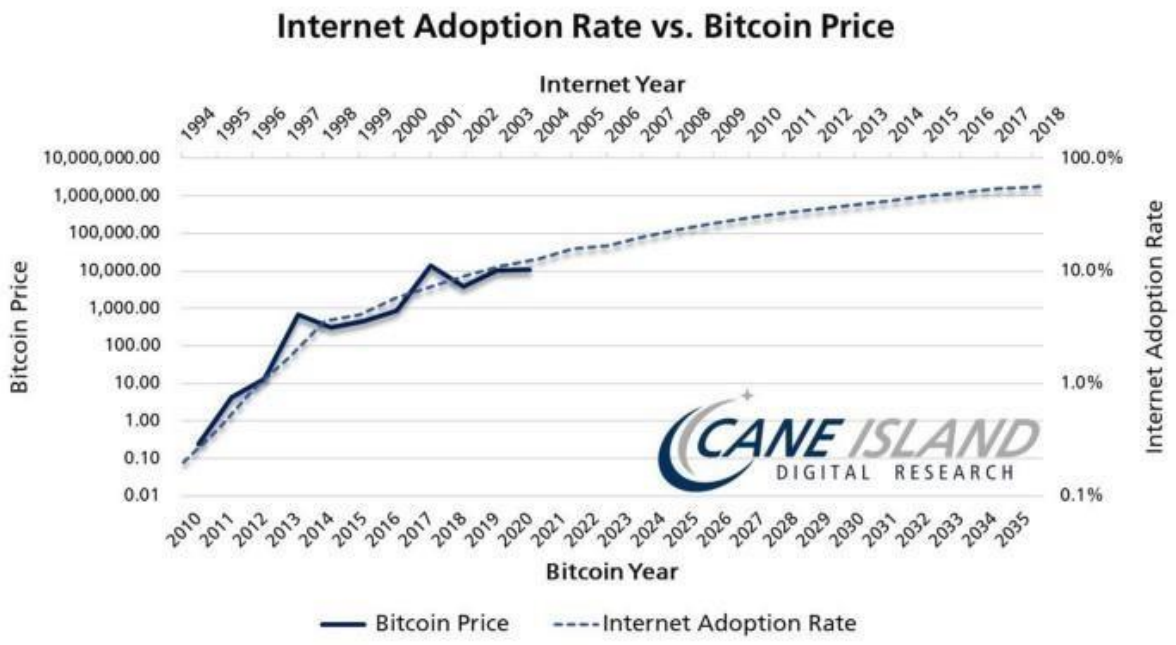
Le mois de janvier était dynamique autant sur les cours qu'au niveau du nombre d'évènements marquants. Les marchés traditionnels et les cryptoactifs continuent de montrer une **corrélation positive** (cf graphique ci-dessous).



Mais nous prévoyons que cela pourrait changer en 2023. Les valorisations des actions technologiques ont produit des rendements surdimensionnés depuis 2020. Avec le retour progressif à la normale, ces actifs ne bénéficieront potentiellement plus des faibles taux d'intérêt, de l'augmentation de la masse monétaire et des cas d'utilisation spéculative de la pandémie. Cependant, nous pensons que la proposition de valeur des réseaux décentralisés et immuables reste inchangée, ce qui fait des actifs numériques une alternative intéressante pour les investisseurs à la recherche de rendements irréguliers.

Note plus personnelle :

Quand je suis devenu investisseur crypto, j'étais naïf. En quelques mois, je pensais avoir compris Bitcoin. Après 6 années, je commence seulement à réaliser que l'absence de permission et la décentralisation entraînent des conséquences subtiles, qui font du Bitcoin son plus grand adversaire.
En cherchant les limites d'une technologie qui repousse les frontières du possible, on voit constamment de nombreux pièges.
Je pense qu'il n'est pas surprenant et plutôt humain de paraître "moins optimiste" au cours d'un tel processus. Je vous invite à regarder ce Masterclass de Thaddeus Dryja (l'un des cocréateurs du Lightning Network).



Ce n'est pas parce que je partage mon pessimisme avec vous que je ne suis pas enthousiaste sur notre futur et le graphique ci-dessus témoigne bien qu'il y a de quoi rester optimiste. Cet article du journal du coin, parlant des gens qui œuvrent dans l'ombre pour le bien commun, transpire d'espoir. Je pense aussi à deux projets qui aspirent à rendre ce monde plus équitable et plus transparent :

Le futur de la charité – Giveth
Une initiative française dans le domaine de l'investissement responsable – Goodvest

Merci beaucoup d'être un lecteur fidèle de notre bulletin d'information, cela signifie beaucoup pour nous et nous espérons vraiment que vous appréciez le contenu publié !

Pour aller plus loin :

https://medium.com/coinmonks/the-crypto-secret-you-dont-know-about-dbffbfd0720c

https://www.ft.com/content/ef6ed550-422a-4540-a8af-41ff2ac30e67

https://decrypt.co/120234/dungeons-dragons-reverses-course-nft-ban-amid-backlash

https://blogs.scientificamerican.com/voices/the-tragedy-of-the-tragedy-of-the-commons/