Experts Crypto

Bulletin d'information mars 2025

« L'analyse des séries temporelles (Stern, 1993, 2000) montre que l'énergie est nécessaire en plus du capital et du travail pour expliquer la croissance du PIB. Cependant, la recherche économique dominante a tendance à minimiser l'importance de l'énergie. Les principaux modèles utilisés pour expliquer le processus de croissance n'incluent pas l'énergie comme facteur de production. »

Cette citation provient de l'article The Role of Energy in the Industrial Revolution and Modern Economic Growth de David I. Stern et Astrid Kander, publié en 2012 dans *The Energy Journal*.

Table des matières

Introduction

En 1964, l'astrophysicien soviétique Nikolaï Kardachev proposait une échelle pour classer les civilisations en fonction de leur capacité à exploiter l'énergie. Cette échelle, désormais célèbre, définit trois types de civilisations : une civilisation de **type I**, capable d'utiliser toute l'énergie disponible sur sa planète ; de **type II**, capable d'exploiter l'énergie de son étoile ; et de **type III**, maîtrisant l'énergie de sa galaxie tout entière.

Aujourd'hui, notre civilisation ne serait qu'au stade 0.7 de cette échelle. Pourtant, un certain nombre de transitions clés nous rapprochent, lentement mais sûrement, de ce premier palier. Parmi elles, une révolution silencieuse, souvent mal comprise, pourrait jouer un rôle déterminant : **Bitcoin**.

Bitcoin est souvent perçu comme une innovation monétaire. Pourtant, il pourrait bien jouer un rôle inattendu dans notre progression vers le type I. Par sa nature décentralisée, son incitation économique à optimiser l'usage énergétique et sa capacité à capter l'énergie excédentaire ou perdue, le minage de Bitcoin devient un catalyseur de l'innovation énergétique.

Et si, en apprenant à produire, utiliser et répartir notre énergie de manière plus efficace, Bitcoin nous aidait à franchir une étape décisive dans notre évolution ?

Dans ce contexte, le minage de Bitcoin, qui est le pilier soutenant le système Bitcoin fonctionnel, apparaît comme une révolution technologique qui favorise l'innovation dans l'industrie énergétique. Le « mining » correspond au processus de validation des transactions Bitcoin et leur ajout au registre de toutes les transactions qui constitue la chaîne temporelle Bitcoin (aussi appelée blockchain). Il repose sur un algorithme appelé preuve de travail distribuée (PoW), conçu pour inciter à la participation et favoriser la sécurité et la décentralisation du réseau Bitcoin.

Ce processus est également à l'origine de l'émission de bitcoin. Il est donc appelé minage car il rappelle l'extraction de l'or et d'autres minéraux. Bien qu'il n'y ait aucune activité physique humaine dans des carrières ou dans des grottes, il y a une dépense d'énergie (matériel et électricité) nécessaire à l'extraction de bitcoin.

En bref, on peut le décrire comme le processus qui met de nouveaux bitcoins en circulation et ajoute de nouvelles transactions à la blockchain. Ces deux fonctions apparemment simples sont rendues possibles grâce à un système informatique robuste fonctionnant en conformité avec le protocole Bitcoin et son modèle de gouvernance, créant ainsi le système monétaire décentralisé et innovant que nous connaissons aujourd'hui.

Cet article explique comment une structure technologique et économique telle qu'une blockchain s'articule autour de cette nouvelle industrie qu'est le mining de cryptoactifs. Dans une seconde partie, nous tenterons de déboulonner les idées reçues sur sa consommation énergétique à l'aide d'un raisonnement simple et de données précises et concrètes.

Le minage de Bitcoin

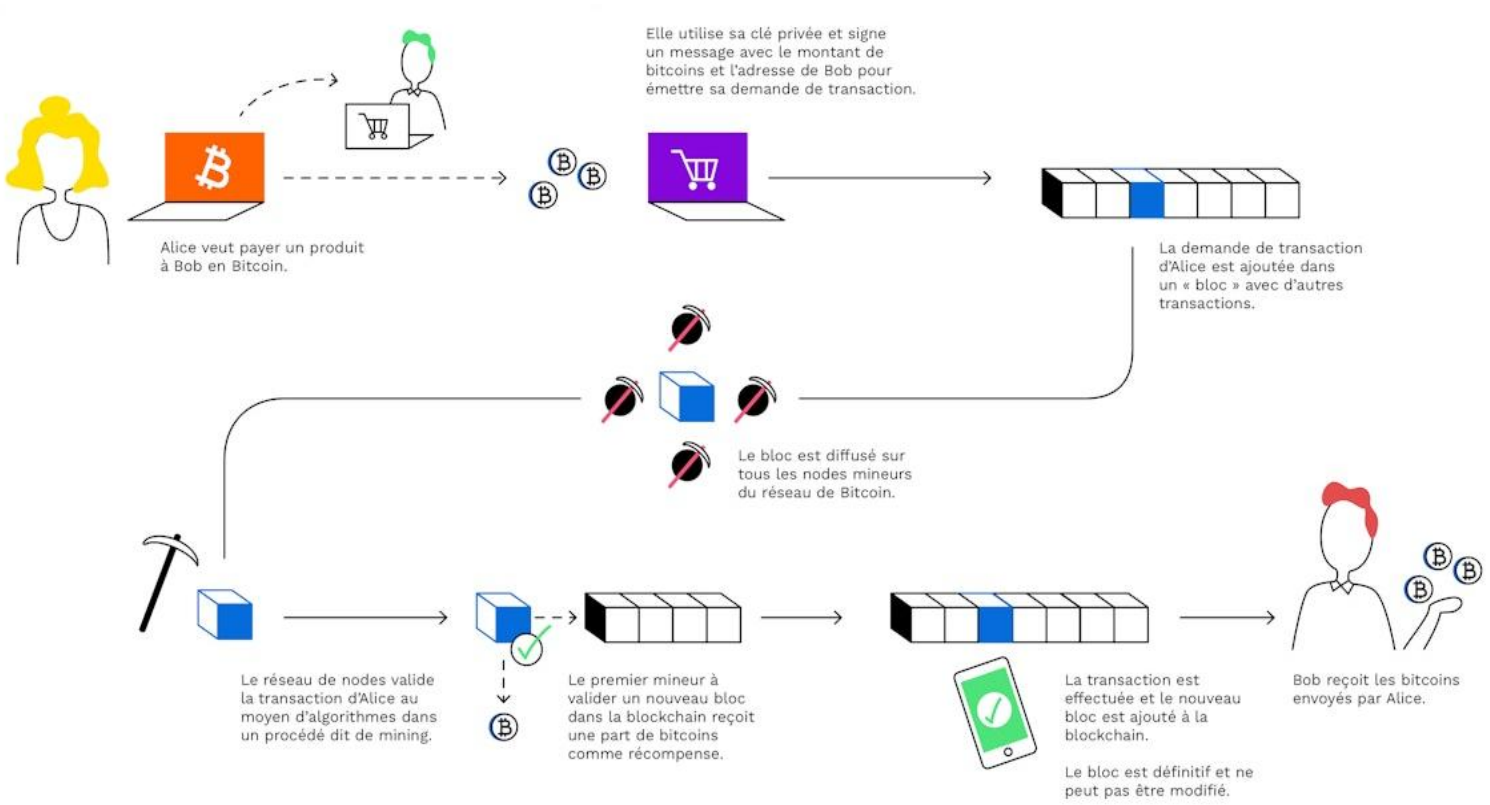
Simplement, le minage est le procédé par lequel les transactions non confirmées sont validées et ajoutées à la blockchain. Lorsqu'une transaction est envoyée, elle est d'abord diffusée au réseau et stockée dans une sorte de salle d'attente appelée un mempool (memory pool ou piscine de mémoire). C'est là que toutes les transactions en attente patientent avant d'être traitées.

Les mineurs parcourent ce mempool pour sélectionner les transactions qu'ils souhaitent inclure dans le prochain bloc. Un bloc peut être vu comme une **page du registre** : il regroupe un ensemble de transactions validées, ainsi que d'autres informations techniques. Les mineurs organisent les transactions de manière à optimiser l'espace dans un bloc. Enfin, ils doivent résoudre un problème mathématique fastidieux, la fameuse preuve de travail. Ce processus demande une grande puissance de calcul.

Le premier mineur à trouver une solution valide à ce problème voit son bloc accepté par le réseau. Il est alors récompensé par l'ensemble des frais de transaction contenus dans ce bloc, ainsi que par une récompense en bitcoins nouvellement créés. C'est pourquoi les mineurs ont tendance à privilégier les transactions avec des frais plus élevés, car elles leur assurent une meilleure rentabilité.

Les mineurs du monde entier, connectés au réseau pair-à-pair de Bitcoin, collaborent pour garantir l'intégrité du registre en validant uniquement les transactions légitimes, empêchant ainsi toute tentative de double dépense. Cette activité, énergivore et intensive en calcul, s'apparente au fonctionnement de centres de données et joue un rôle essentiel dans la sécurisation et le bon fonctionnement du réseau Bitcoin.

Voici un schéma simple d'une transaction sur le réseau Bitcoin :



L’importance du minage

La solution à la fraude transactionnelle

Le minage de Bitcoin crée de nouveaux blocs et les ajoute au registre en respectant des règles prédéfinies. Les nœuds participant au réseau doivent convenir que les utilisateurs, identifiés publiquement par des adresses cryptographiques, sont bien les propriétaires légitimes des soldes en bitcoins.

Les mineurs et plus largement tous les nœuds jouent un rôle de coordination pour le réseau Bitcoin, fonction qui, dans les systèmes de paiement traditionnels, est assurée par un intermédiaire de confiance comme une banque ou toute autre institution financière.

Pour éliminer la dépendance à un tiers de confiance, Bitcoin doit empêcher que des fonds soient dépensés deux fois ou utilisés par une personne autre que leur propriétaire.

L'utilisation des signatures numériques, une invention cryptographique des années 1970, empêche les utilisateurs non autorisés de dépenser l'argent des autres. Une paire de clés privée-publique constitue une preuve solide de propriété qui permet uniquement au détenteur de la clé privée de dépenser ou de déplacer des bitcoins.

Cependant, les signatures numériques à elles seules ne garantissent pas que les bitcoins reçus en paiement n'ont pas été dépensés ailleurs (le problème de la double dépense).

Pour résoudre ce problème, Satoshi a utilisé la preuve de travail basée sur le hachage d'Adam Back pour permettre l'organisation chronologique des transactions en blocs et permettre au réseau d'atteindre un consensus sur l'état actuel du registre en suivant la chaîne de blocs la plus longue.

Ce mécanisme protège la blockchain contre les attaques, car les transactions ne deviennent réversibles que si un acteur malveillant refait le travail de preuve de tous les blocs précédents. Étant donné que de nouveaux blocs sont constamment ajoutés à la chaîne, il est pratiquement impossible pour ces acteurs de rattraper leur retard.

L'important travail de calcul requis pour miner du Bitcoin est si coûteux en ressources que les acteurs malveillants sont plus incités à les dépenser pour miner plutôt que de tenter de le compromettre.

Une brève histoire du minage de Bitcoin

Bitcoin repose sur un réseau pair-à-pair composé de dizaines de milliers de nœuds pour fonctionner : les nœuds mineurs et les nœuds utilisateurs. Ces nœuds sont la base d'un réseau de paiement qui déplace des milliards de dollars chaque année sans intervention d'une entité centrale.

Lorsque Satoshi Nakamoto a lancé Bitcoin en 2009, la distinction entre l'exploitation d'un nœud Bitcoin et le minage était mince. Les opérateurs de nœuds et les mineurs étaient souvent les mêmes, car de nombreux utilisateurs, exécutant

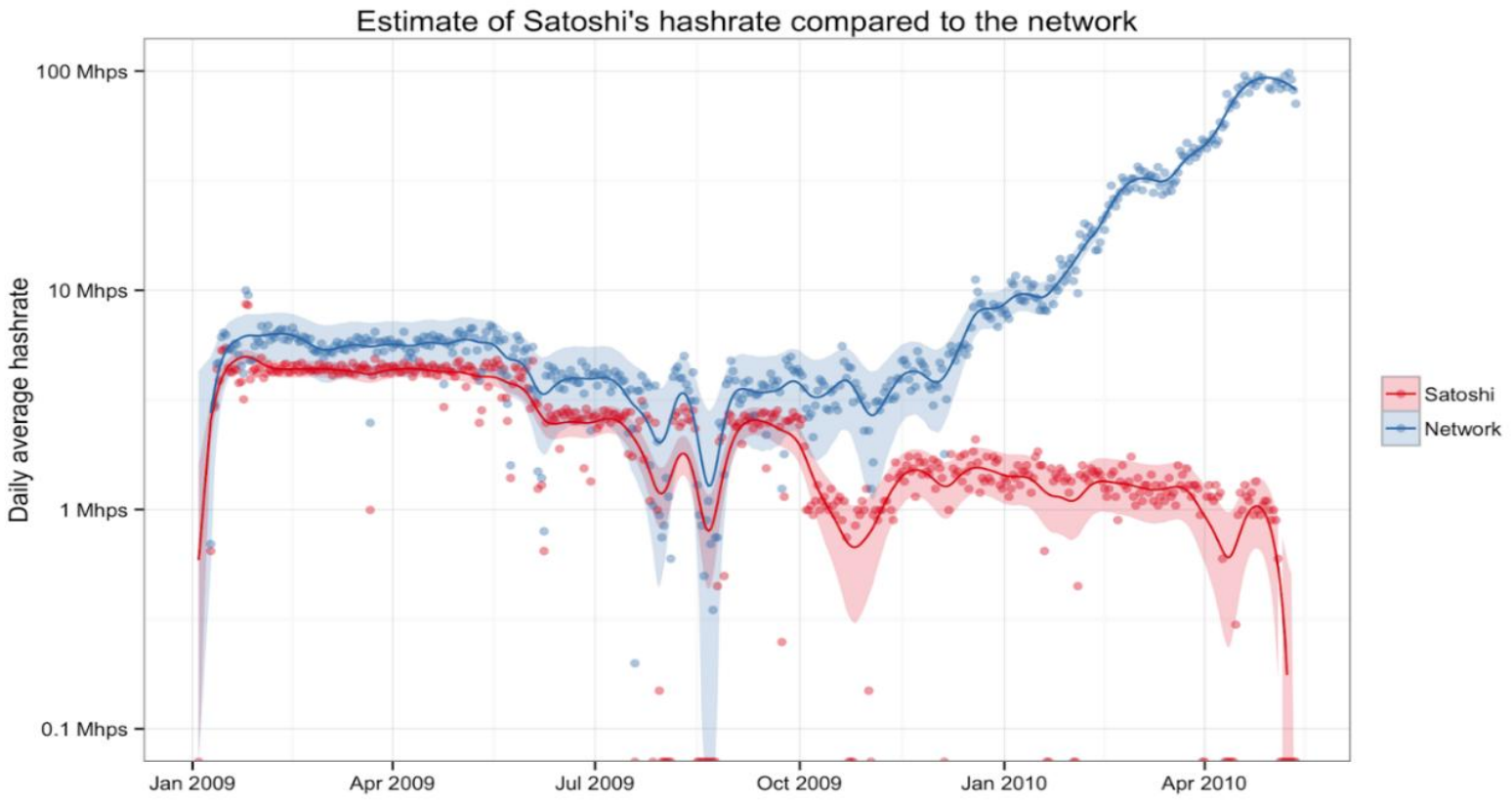
des nœuds sur leurs ordinateurs, pouvaient aussi miner du Bitcoin de manière rentable avec leurs processeurs.

Vous trouverez ici une analyse technique du comportement minier d'une entité qui serait plausiblement Satoshi

Depuis, le minage est passé d'une activité artisanale à une industrie prospère, évoluant parallèlement au prix du Bitcoin et aux incitations à miner.

L'une des différences les plus significatives entre Bitcoin et la plupart des autres cryptoactifs est l'absence de bitcoins pré-minés (des coins émis avant le lancement du projet). En effet, Satoshi a lancé le réseau avant de miner du bitcoin afin de ne pas avoir un avantage sur quiconque souhaitait participer au système. Pour comparer, la fondation Ethereum a pré-miné 10% de la réserve totale de ETH avant de lancer la blockchain. L'entreprise Ripple a forgé l'entièreté des jetons XRP et n'a mis en circulation pour le moment que 60% des réserves en circulation. Ce qui représente déjà une capitalisation boursière de 128 milliards de dollars et une réserve dormante de 80 milliards.

Une fois le réseau Bitcoin lancé, le 3 janvier 2009, Satoshi a miné le premier bloc, connu sous le nom de **bloc Genesis** ou **bloc 0**, contenant 50 bitcoins. En tant que seul mineur sur le réseau Bitcoin à cet instant, Satoshi créait des blocs en utilisant un ordinateur personnel standard. Voici un article qui donne une approximation précise de la fortune de Satoshi.(environ 1 million de bitcoins). Il a très rapidement été rejoint par d'autres enthousiastes et personnellement je considère ce lancement comme le plus neutre possible donc juste et équitable. Ci-dessous, une comparaison de la puissance de calcul de Satoshi par rapport au réseau.



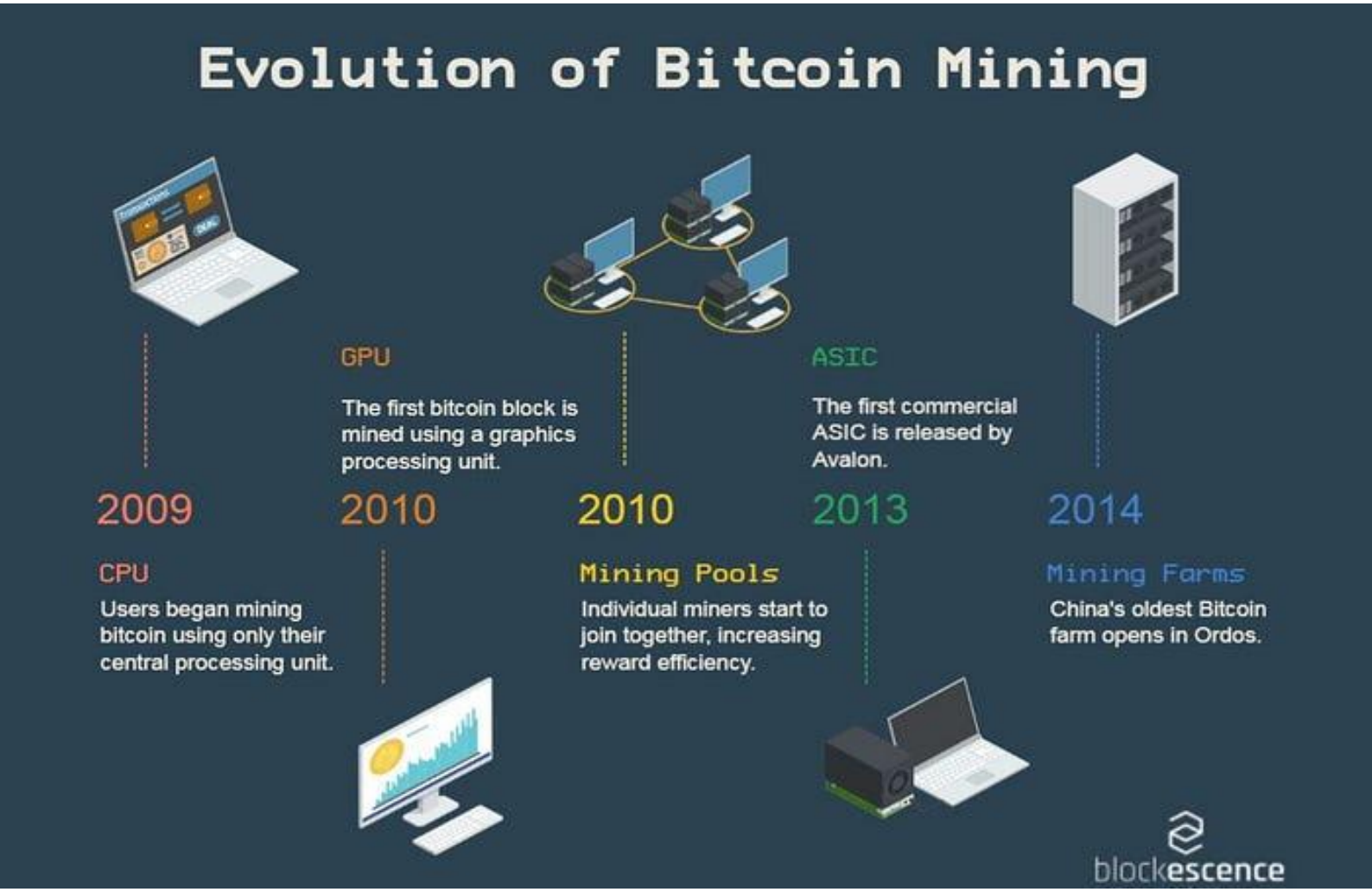
Des processeurs (CPU) aux cartes graphiques (GPU)

En seulement dix ans, le matériel utilisé sur le réseau Bitcoin a connu une évolution technologique rapide. L'équipement de minage joue un rôle fondamental dans le succès du réseau, car il détermine si l'activité est rentable pour les mineurs.

Dans les premières années de Bitcoin, les opérateurs de nœuds et les mineurs effectuaient des opérations très similaires en utilisant le même type de matériel : **les processeurs centraux (CPU)**.

Les CPU contrôlent le traitement et l'exécution des commandes d'un ordinateur. En raison de la faible concurrence entre les mineurs aux débuts de Bitcoin, la puissance de calcul nécessaire pour créer de nouveaux blocs et obtenir des récompenses de minage était très faible et pouvait être facilement fournie par des dispositifs équipés de CPU.

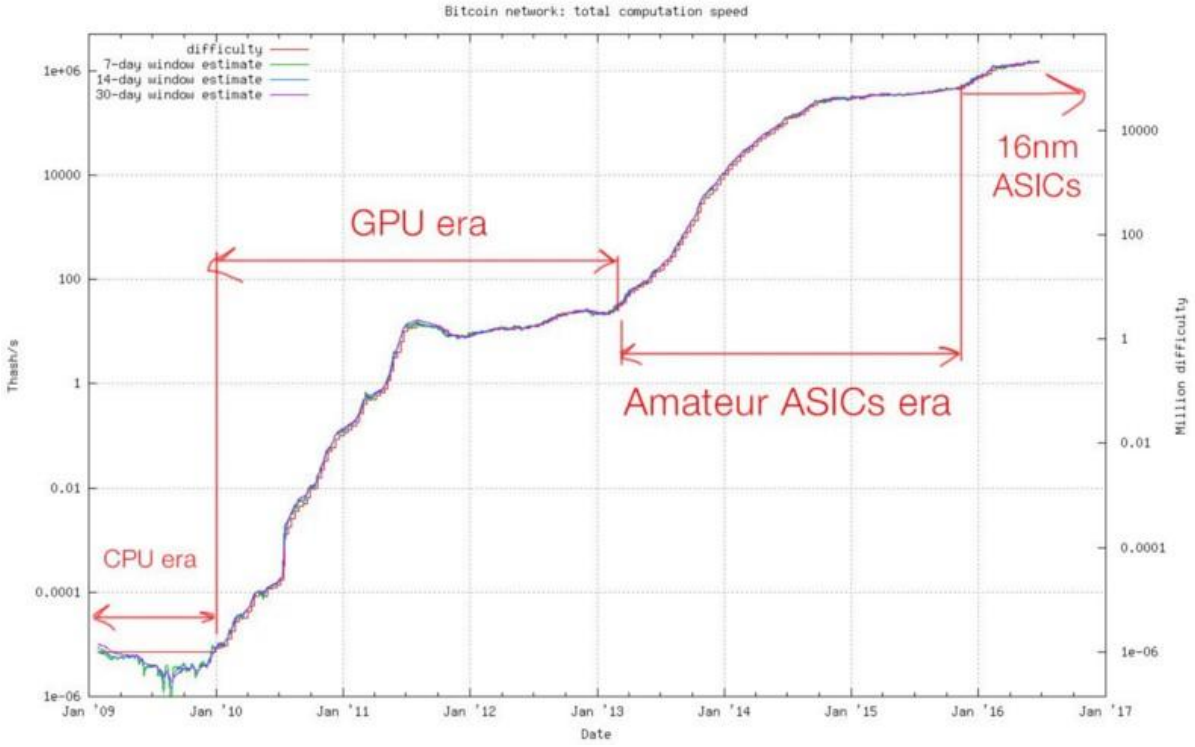
Une fois que Bitcoin a commencé à prendre de la valeur en 2011, atteignant d'abord 1 $ puis 30 $ par pièce, la concurrence pour miner du bitcoin est devenue plus intense et le minage par **unité de traitement graphique (GPU)** a été adopté. Initialement conçus pour les applications de jeux vidéo, les GPU sont capables d'effectuer de nombreux calculs mathématiques simultanément et sont beaucoup plus rapides que les processeurs centraux (CPU).



Des GPU aux ASIC

En 2012, les circuits logiques programmables (FPGA), une étape intermédiaire entre un processeur programmable rapide et un ASIC dédié, ont été utilisés jusqu'à ce que les circuits intégrés spécifiques à une application (ASIC) émergent et dominent le minage de bitcoin jusqu'à aujourd'hui.

Les ASIC ont commencé à être utilisés pour le minage de bitcoin en 2013. Ils sont conçus sur mesure pour une application spécifique, et dans le cas de Bitcoin, ces puces sont optimisées uniquement pour effectuer le hachage SHA-256. Elles sont bien plus rapides que les GPU. Aujourd'hui, l'utilisation des ASIC est la seule méthode économiquement viable pour miner du bitcoin. Pour information, en 2016 les puces ASIC faisaient 16 nanomètres alors que maintenant la même puissance est déployée sur 3 nanomètres. Sur le graphique ci-dessous vous retrouverez les moments exacts où les évolutions ont eu lieu.



La preuve de travail (PoW)

La preuve de travail est au cœur du réseau Bitcoin. Sans elle, chaque participant pourrait modifier la blockchain à son avantage. En l'absence d'une autorité centrale pour résoudre les conflits, la PoW garantit le bon fonctionnement du réseau.

Le mécanisme de preuve de travail remplit deux fonctions :

- Il s'assure que tous les participants partagent la même copie de la blockchain.

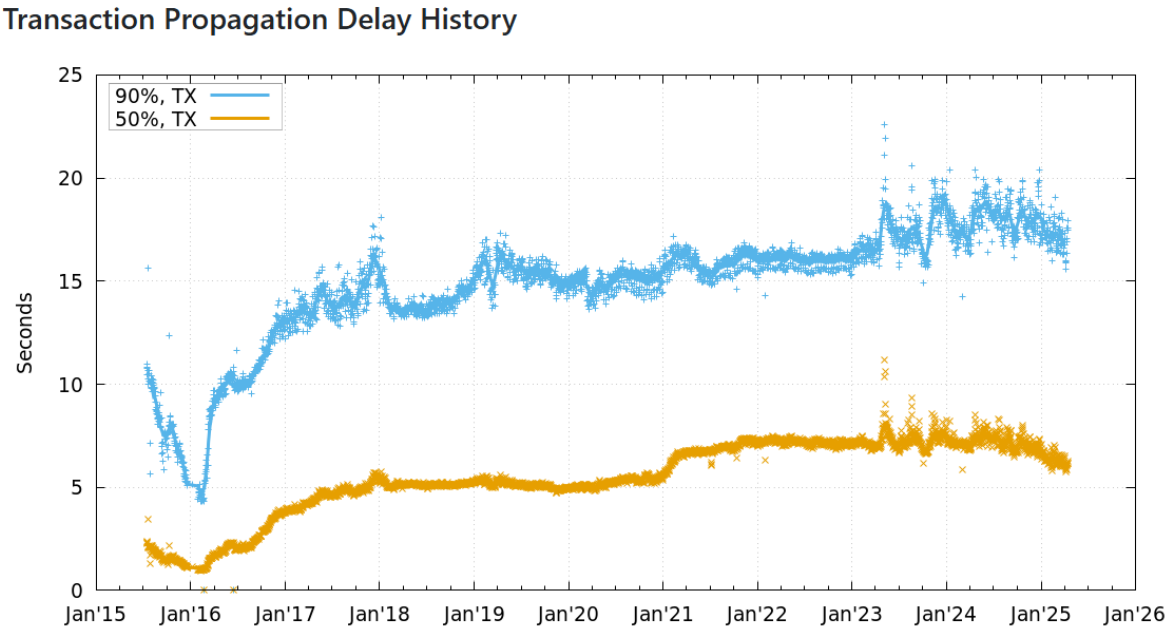
- Il empêche les fonds d'être dépensés plus d'une fois en se basant toujours sur la chaîne de données la plus longue. (Celle avec le plus de preuve de travail).

Le processus de minage

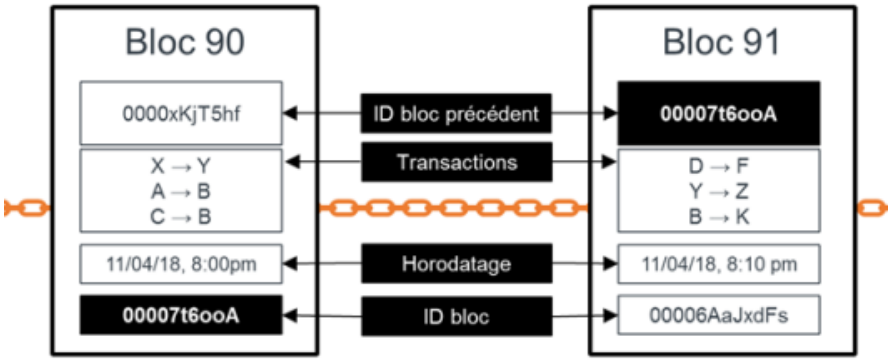
Le minage suit les étapes suivantes, réalisées en boucle continue :

1. Sélectionner et regrouper les transactions diffusées sur le réseau dans un bloc. Les transactions en attente de confirmation peuvent être visualisées dans un mempool. Il n'y a pas de piscine global, chaque nœud maintient sa propre salle d'attente et tente de remplir un bloc avec des transactions, indépendamment des autres.

Pour information, il faut environ 20 secondes pour qu'une transaction soit présente sur tous les mempools :



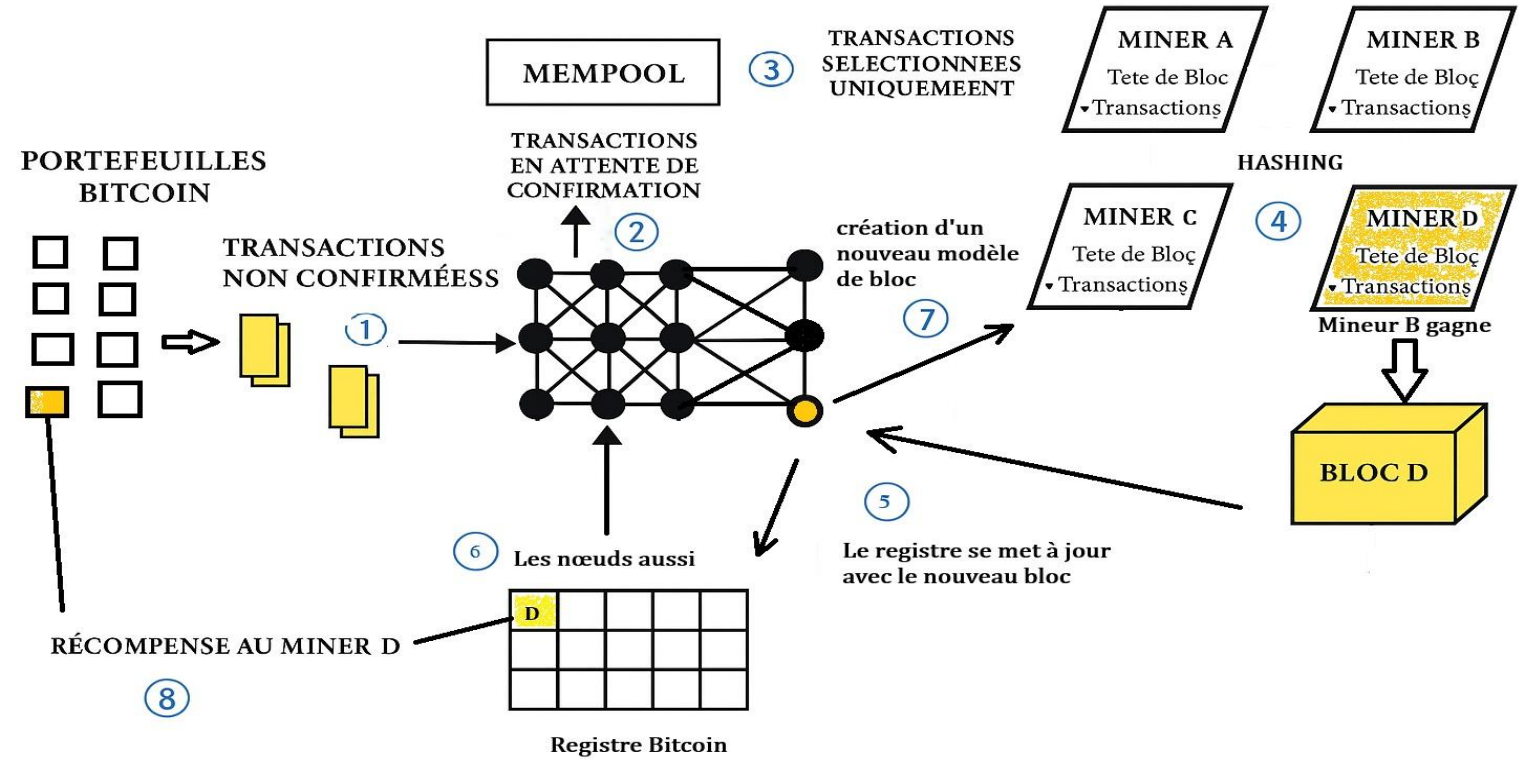
2. Sélectionner le bloc le plus récent sur le chemin le plus long de la blockchain et insérer l'empreinte de son en-tête dans le nouveau bloc (ce qui forme les maillons de la chaîne).



3. Essayer de résoudre le problème de preuve de travail (PoW) du nouveau bloc tout en surveillant les nouveaux blocs provenant des autres nœuds.

   Pour valider un bloc, un mineur doit trouver un hachage qui respecte un critère de difficulté fixé. Pour cela, il modifie sans cesse une équation mathématique avec une valeur spécifique appelée "nonce" pour tomber par hasard sur un résultat qui correspond.
   Le nonce est un champ dans l'en-tête du bloc qui, lorsqu'il est modifié, change totalement le résultat du hachage. Les machines spécialisées essayent ainsi des milliards de nonce chaque seconde jusqu'à en trouver un conforme aux exigences, ce qui permet de valider le bloc.

4. Si une solution est trouvée, le nouveau bloc est ajouté à la blockchain locale et diffusé au réseau pair-à-pair. (Quelques secondes suffisent pour que le nouveau bloc se propage sur tout le réseau). En voici un schéma condensé.



Création de Bloc

5. Ensuite une nouvelle boucle démarre. « Tick Tock Next Block »

L’algorithme de hachage SHA 256

Dans le réseau Bitcoin, la preuve de travail (Proof of Work ou PoW) repose sur l'utilisation d'une fonction cryptographique appelée **hachage**, qui permet de transformer un ensemble de données (comme l’en-tête d’un bloc) en une **empreinte numérique unique** de longueur fixe représentée sous forme d’une longue séquence binaire (256 bits). En pratique, elle est souvent affichée en hexadécimal (64 caractères, car chaque octet est codé par deux caractères hexadécimaux). Par exemple :

000000000000000057e25a0b9e6d7c4f6b0b8c8e8c7a0b7e4f9a1c2d3e4f5a6

Le réseau Bitcoin utilise spécifiquement l’algorithme **SHA-256**, conçu par la NSA, réputé pour sa robustesse cryptographique.

L’équation à résoudre est construite de telle sorte que le mineur doit générer une empreinte numérique (le hachage) à partir des données de l’en-tête d’un bloc, en utilisant la fonction SHA-256, et que cette empreinte doit répondre à un critère précis : être inférieure à une cible de difficulté fixée par le réseau Bitcoin.

Concrètement :

- L’en-tête du bloc contient des informations comme les transactions, le hachage du bloc précédent et une valeur appelée nonce.
- Le mineur passe ces données dans la fonction SHA-256, qui produit un hachage (une chaîne de 256 bits).

- Pour que le hachage soit valide, il doit commencer par un certain nombre de zéros, ce qui dépend du niveau de difficulté (par exemple, plus la difficulté est élevée, plus il faut de zéros au début).
- Si le hachage obtenu ne respecte pas ce critère, le mineur modifie le nonce et recommence le calcul, répétant ce processus des milliards de fois jusqu'à trouver un hachage conforme.

Propriétés de la fonction SHA-256

SHA-256 (Secure Hash Algorithm 256 bits) est une fonction de hachage appartenant à la famille SHA-2. Elle présente plusieurs caractéristiques essentielles pour la sécurité de Bitcoin :

- Sens unique : À partir d'un ensemble de données, il est facile de calculer un hachage (une empreinte numérique de 256 bits), mais il est pratiquement impossible de retrouver les données d'origine à partir du hachage.
- Résistance aux collisions : Il est extrêmement difficile de trouver deux ensembles de données différents produisant le même hachage. Cette propriété garantit qu'un attaquant ne peut pas falsifier un bloc sans que cela soit détecté.
- Sensibilité aux modifications : Une infime modification dans les données d'entrée (par exemple, changer un seul caractère) produit un hachage totalement différent, rendant toute tentative de manipulation évidente.
- Déterminisme : Pour un même ensemble de données, SHA-256 produit toujours le même hachage, ce qui permet une vérification cohérente par tous les nœuds du réseau.

Notes sur les mesures de hashrate

La puissance de calcul d'un réseau suivant un protocole de preuve de travail se mesure au nombre d'empreintes numériques (hash en Anglais) calculées par seconde avec les unités suivantes :

GH/s (gigahash) 1 000 000 000

TH/s (terahash) 1 000 000 000 000

PH/s (petahash) 1 000 000 000 000 000

EH/s (exahash) 1 000 000 000 000 000 000

ZH/s (zettahash) 1 000 000 000 000 000 000000

YH/s (yottahash) 1 000 000 000 000 000 000 000 000

Chaque hash calculé correspond à une tentative de trouver une collision entre la fonction cryptographique de hachage et la cible de difficulté fixée par le protocole.

La puissance de calcul informatique mise à la disposition du réseau Bitcoin vient de franchir un nouveau seuil historique en ce début de mois d'avril. En effet, le

hashrate du Bitcoin a bien dépassé – pour le moment furtivement – la barre des 1 Zetahash par seconde (ZH/s).

Un hashrate élevé indique une plus grande sécurité du réseau. Car il devient plus difficile et coûteux pour un attaquant de prendre le contrôle de plus de 50 % de la puissance de calcul. Une opération nécessaire pour réaliser la fameuse attaque dite de 51 %.

Pour approfondir votre compréhension sur ce mécanisme de hachage, une **excellente vidéo explicative** est disponible ici.

Et pour les plus curieux : voici une explication mathématique des fonctions de hachage.

L'ajustement de la difficulté

L'ajustement de la difficulté et la réduction des récompenses sont les bases du système d'émission programmatique de Bitcoin. En moyenne, le réseau est conçu pour créer un bloc toutes les dix minutes.

Cet équilibre est maintenu grâce à un ajustement périodique de la difficulté, qui ajuste la valeur cible du hachage des blocs. Lorsque plus de mineurs rejoignent le réseau, le taux de création des blocs augmente. En conséquence, la difficulté de minage est augmentée pour ramener ce taux à la moyenne de dix minutes.

Tous les 2 016 blocs (environ toutes les deux semaines), les nœuds Bitcoin recalculent la difficulté en fonction du temps qu'il a fallu pour miner les 2 016 blocs précédents.

Le premier bloc de Bitcoin (le bloc Genesis) rencontrait une difficulté de 1, ce qui signifie qu'il a probablement été miné instantanément. À titre de comparaison, la difficulté actuelle du minage est de plus de 30 000 milliards. Cela signifie qu'un matériel de minage spécialisé (ASIC) doit exécuter en moyenne plus de 30 000 milliards de hachages avant de trouver un bloc valide.

Ce mécanisme est une des pierres angulaires de l'édifice Bitcoin :

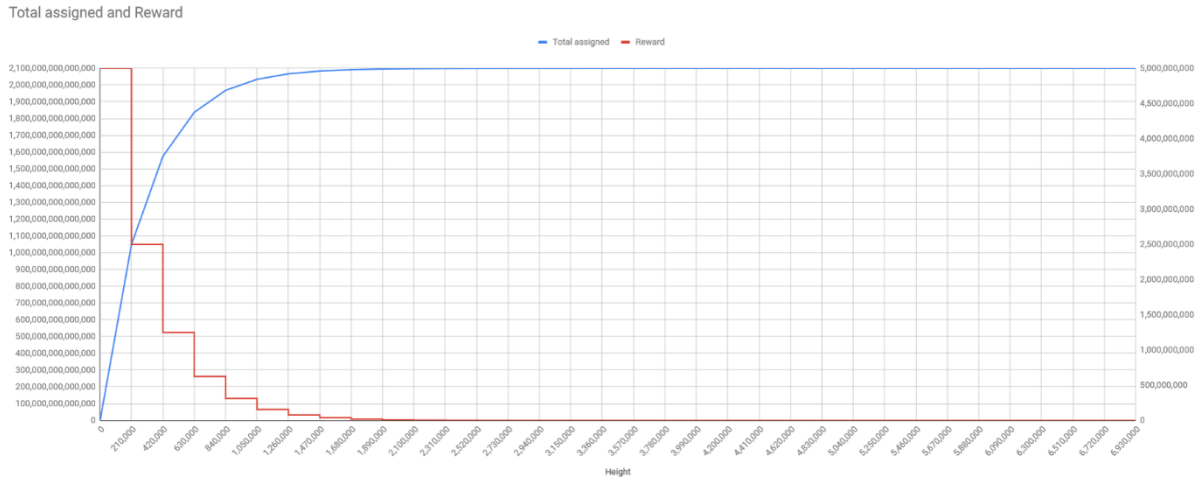
- Il agit contre le progrès technologique dont dispose les mineurs.
- Il assure une progression régulière de la blockchain.
- Il offre un cadre mathématique théorique satisfaisant pour modéliser les processus de comptage de blocs comme des processus de Poisson.

La récompense de bloc

Le minage nécessite une puissance de calcul considérable, qui a un coût élevé. Pour inciter les participants à investir leurs ressources, Bitcoin attribue deux types de récompenses pour chaque bloc miné avec succès :

- Une récompense de bloc (subvention de bloc).
- Les frais de transaction.

Conformément à l'algorithme de Bitcoin, la récompense de bloc est divisée par deux tous les 210 000 blocs (environ tous les quatre ans). Elle est actuellement fixée à 3,125 bitcoins par bloc et nous venons de dépasser le seuil de 20 millions de bitcoin créés.



Cette diminution progressive garantit que la quantité totale de bitcoins émise est limitée à 21 millions d'unités d'ici l'année 2140. Une fois cette limite atteinte, les mineurs seront rémunérés uniquement par les frais de transaction payés par les utilisateurs du réseau et d'autres incitations exogènes.

Comment commencer à miner

Deux options existent pour se lancer dans le minage de Bitcoin : miner chez soi ou déléguer le minage à une entreprise. Chaque option a ses avantages et ses inconvénients.

Bien que le minage de Bitcoin soit dominé par des entreprises fortement financées possédant de vastes entrepôts remplis d'équipements, il est toujours possible pour des particuliers de miner de manière indépendante. Cependant, c'est une activité spécialisée qui nécessite :

- Une connaissance approfondie du sujet.
- Un ASIC performant.
- Un système de refroidissement efficace.
- Une source d'électricité stable et abordable.
- Une connexion Internet fiable.

Avant de s'engager dans le minage domestique, il est crucial d'en peser les avantages et les inconvénients pour éviter les erreurs coûteuses.

Minage en solo vs minage en pool

- **Minage en solo** : Les mineurs travaillent seuls et gardent l'intégralité de la récompense s'ils trouvent un bloc. Cependant, avec l'augmentation de la difficulté, il devient extrêmement rare de miner un bloc en solo et la rentabilité n'est plus suffisante pour être profitable uniquement avec la récompense de bloc. C'est pourquoi, certains particuliers utilisent la chaleur produite par les machines qui calculent pour baisser leur facture de chauffage.
- **Minage en pool** : Les mineurs regroupent leur puissance de calcul et partagent les récompenses en fonction de leur contribution. Cela permet d'obtenir des revenus plus réguliers. Si le problème de centralisation de la gouvernance a déjà été posé en 2017 et résumé dans le livre « La Guerre de la taille de bloc » (Block Size War).

La centralisation du mining en une poignée de pool reste une source d'inquiétude.

Investir dans l'industrie du mining

Une alternative au minage direct consiste à investir dans des entreprises spécialisées. Cela peut se faire de plusieurs manières :

1. Acheter du matériel et le faire héberger par une société de minage.
2. Acheter une part de la puissance de calcul d'une entreprise.
3. Investir directement dans une société de minage.

Cependant, ces options impliquent généralement de fournir des informations personnelles (KYC) et de payer des frais de service. De plus, les investisseurs n'ont aucun contrôle sur la gestion de l'entreprise, ce qui représente un risque supplémentaire.

Quelques entreprises de minage connues :

- **Iris Energy** (Canada, minage alimenté par des énergies renouvelables).
- **Core Scientific** (USA, plus grand mineur de Bitcoin en termes de puissance de calcul).
- RIOT **Blockchain** (USA, acteur majeur coté en bourse). Propriétaire de la plus grande ferme de mining au Texas (photo ci-dessous)
- **Blockstream** (Entreprise cofondée par Adam Back, pionnier du hachage).
- **Hut 8 Mining** (Canada, l'un des plus grands inventaires de bitcoins auto-minés).

- **XMW Morphware** (entreprise utilisant l'énergie d'Itaipu, le plus grand barrage d'Amérique latine au Paraguay).

Est-ce qu’il y aura un futur pour le mining de bitcoin ?

L’économie de l’espace de bloc

L'article « A Treatise on Bitcoin Block Space Economics » de Jameson Lopp explore en profondeur les dynamiques économiques liées à l'espace de bloc dans le réseau Bitcoin. Plus spécifiquement les implications des limites de taille de bloc sur la sécurité, la décentralisation et l'accessibilité du réseau.

Le dilemme fondamental est le suivant : faut-il privilégier un coût faible de validation complète du système (favorisant la décentralisation) ou un coût faible des transactions (favorisant l'accessibilité) ? Historiquement, Bitcoin a opté pour la première approche, limitant la taille des blocs pour maintenir la possibilité pour les utilisateurs de faire fonctionner des nœuds complets.

L'espace de bloc est une ressource limitée, et sa rareté crée un marché des frais de transaction. Une augmentation de la taille des blocs pourrait réduire cette rareté, diminuant les incitations économiques pour les mineurs et la sécurité du réseau. Par ailleurs, des frais de transaction élevés encouragent l'utilisation efficace de l'espace de bloc et le développement de solutions de second niveau comme le Lightning Network.

Propositions d'ajustement de la taille des blocs

Il existe plusieurs propositions historiques visant à ajuster dynamiquement la taille des blocs, telles que les BIP100 à BIP109. Ces propositions sont critiquées pour diverses raisons, notamment à cause de leur complexité, leur vulnérabilité à la manipulation par les mineurs et leur manque de prise en compte des coûts opérationnels des nœuds.

Jameson Lopp explique que des blocs trop petits peuvent exclure les utilisateurs et favoriser la centralisation, tandis que des blocs trop grands peuvent compromettre la décentralisation et la sécurité. Il propose l'idée d'un mécanisme d'ajustement dynamique de la taille des blocs, basé sur l'utilisation de l'espace de bloc et les frais de transaction, tout en tenant compte des avancées technologiques et des coûts opérationnels des nœuds.

Lopp conclut que, bien qu'il n'y ait pas d'urgence à modifier la taille des blocs, il est crucial d'engager une réflexion à long terme sur l'économie de l'espace de bloc. Il appelle à une approche prudente et équilibrée, visant à préserver la sécurité, la décentralisation et l'accessibilité de Bitcoin pour les générations futures.

Une voie pour électrifier l'avenir

Dans de nombreuses régions, comme l'Afrique subsaharienne (ASS), où plus de 600 millions de personnes n'ont pas accès à l'électricité, le manque d'énergie entraîne stagnation économique, baisse de la production alimentaire, pauvreté et troubles civils. L'accès à l'électricité est étroitement lié à la croissance économique, les régions avec moins de 80 % d'électrification ont un PIB par habitant réduit.

Développer les infrastructures électriques dans ces zones est coûteux et souvent hors de portée pour les gouvernements à ressources limitées. Le minage de Bitcoin offre une solution potentielle en utilisant l'énergie inutilisée dans des lieux reculés pour générer des revenus, finançant ainsi la construction de réseaux électriques.

Malgré les critiques sur son impact environnemental, le minage de Bitcoin révèle des avantages humanitaires et énergétiques. Le documentaire primé Stranded : A Dirty Coin Short d'Alana Mediavialla Diaz illustre comment, en ASS, les mineurs de Bitcoin exploitent l'énergie inutilisée pour revitaliser des infrastructures électriques abandonnées, contribuant à électrifier des régions défavorisées.

L'intersection entre le minage de Bitcoin et la production d'énergie offre des opportunités pour une transition énergétique durable :

- Gestion efficace des réseaux électriques.
- Réduction des émissions de méthane.
- Accélération de l'adoption des énergies éolienne, géothermique, hydroélectrique et solaire.
- Amélioration de l'économie du nucléaire.
- Exploitation de l'énergie océanique : Le minage de Bitcoin peut réduire les coûts de l'énergie thermique des mers (OTEC), rendant cette technologie viable pour les nations côtières.

- Récupération de chaleur : La chaleur générée par le minage peut être réutilisée pour chauffer des bâtiments, des serres ou des piscines, améliorant l'efficacité énergétique et la durabilité.

L'intégration croissante entre le minage de Bitcoin et les infrastructures énergétiques favorise une convergence vers une énergie durable et abondante, répondant à la demande énergétique mondiale croissante tout en soutenant le développement et la lutte contre la pauvreté.

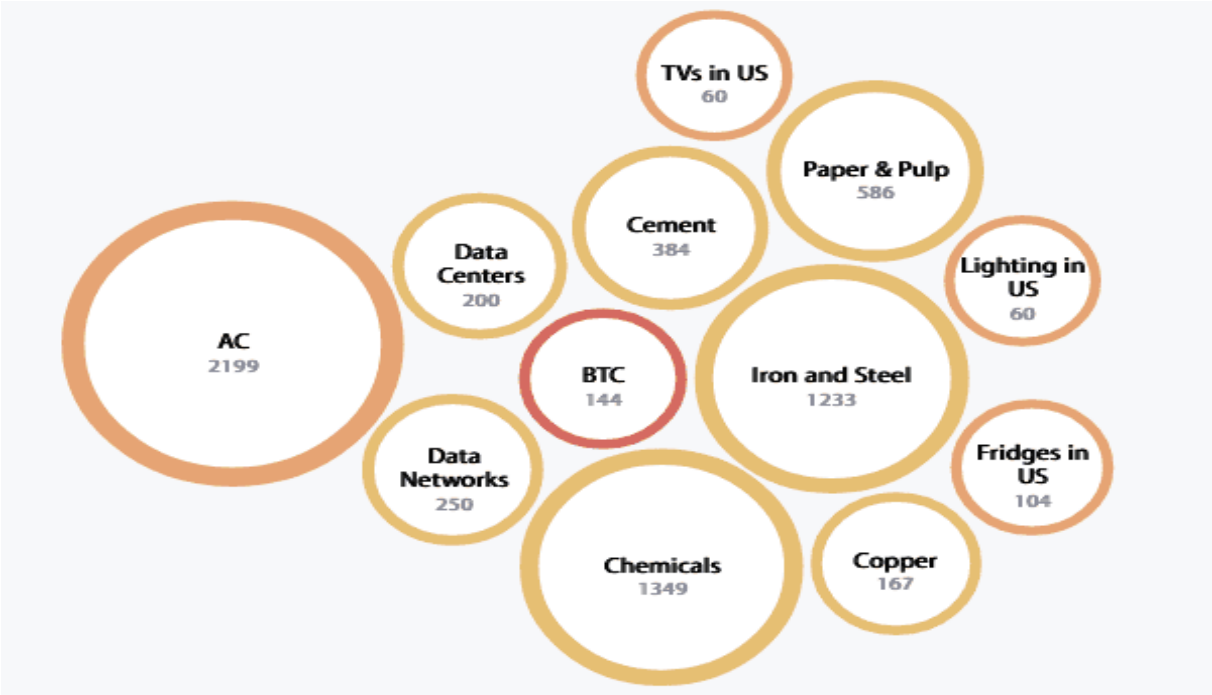
Monétiser les surplus énergétiques

Le protocole Bitcoin incite les mineurs à réaliser un arbitrage géographique permanent pour obtenir l'électricité la moins chère. En raison des imperfections du marché de l'électricité, même s'il peut y avoir des exceptions, dans la plupart des cas, l'électricité la moins chère provient d'excédents de production.

Contrairement aux énergies renouvelables, les énergies à base de stock, uranium ou fossiles, sont dites pilotables en ce qu'elles ne génèrent pas de surplus. Quand la demande baisse, il est toujours possible de diminuer la production en conservant le stock plutôt que de le brûler à perte ou avec un manque à gagner.

Les énergies renouvelables, quant à elles, sont intermittentes et ne peuvent pas s'ajuster en permanence à une demande elle aussi fluctuante. L'électricité étant difficile à stocker ou à transporter sur de grandes distances, il existe donc des surplus spécifiques aux renouvelables.

Comparé à une production électrique mondiale de plus de 27 000 TWh par en en 2021, Bitcoin utilise environ 144 TWh. Autrement dit, si la production d'électricité ne générait que 1% de surplus, ce qui est une hypothèse très basse, Bitcoin n'en monétiserait aujourd'hui que la moitié. Voici la consommation électrique mondiale par catégorie (AC = climatisation) :



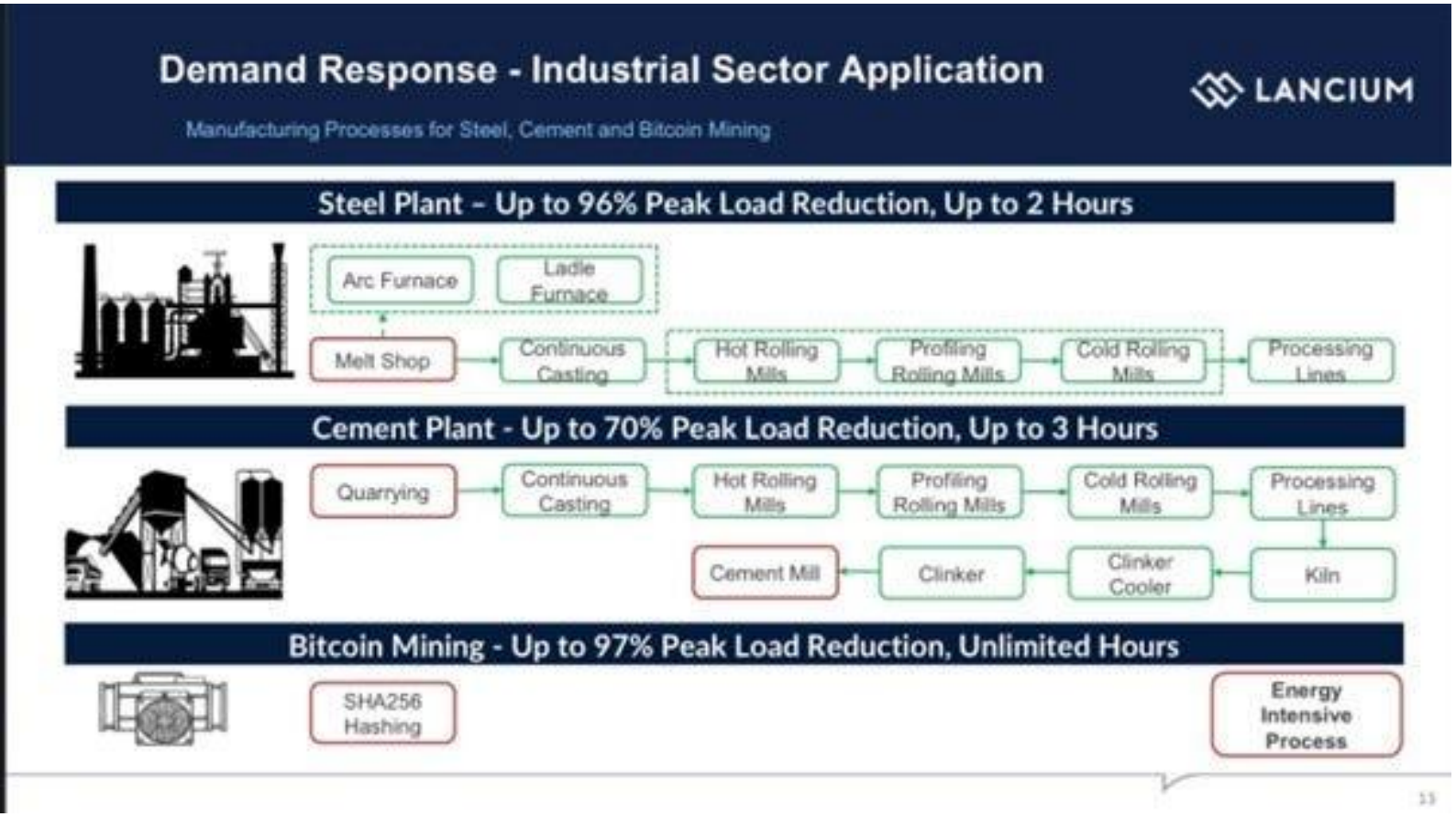
Et je dirais même que le marché « informatique Bitcoin » est le prédécesseur de l'économie moderne des centres de données. Le boom de l'IA n'aurait pas atteint cette ampleur sans Bitcoin et ses débouchés :

1. Des centaines de milliards de dollars de construction de centres de données ;
2. Alimenté par l'électrification à moindre coût ;
3. Stimuler une demande persistante de matériel ;
4. Pionnier de la colocalisation derrière le compteur.

La symbiose entre le Mining et les réseaux électriques

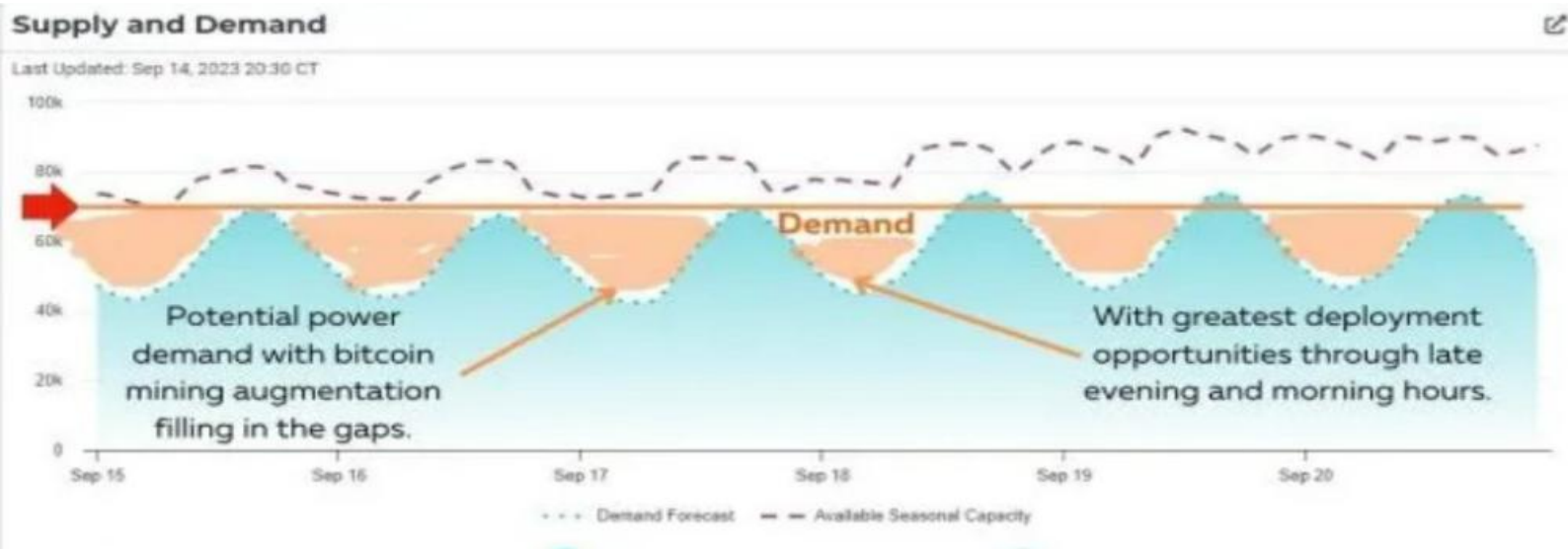
Le mining de Bitcoin, constitue un processus fortement énergivore, tout en offrant des opportunités économiques et technologiques notables. Les centres de données dédiés au minage d'actifs numériques s'apparentent aux infrastructures d'informatique de stockage de données exploitées par de grandes entreprises telles que Google ou Amazon. Dans les deux cas, l'électricité est transformée en produit numérique au moyen d'ordinateurs, d'infrastructures spécialisées et d'une main-d'œuvre hautement qualifiée.

Toutefois, une différence majeure réside dans la flexibilité opérationnelle : les centres informatiques traditionnels présentent une capacité d'adaptation limitée, tandis que les centres de minage peuvent ajuster rapidement leur niveau de production en fonction de la demande en électricité du réseau. Ainsi, les installations dédiées au Bitcoin, peuvent agir en tant que charges flexibles, participant à des programmes de réponse à la demande destinés à maintenir l'équilibre des réseaux électriques. Ces opérations peuvent, en effet, réduire leur consommation énergétique en temps réel, permettant ainsi de libérer de la capacité au profit du réseau lorsque la demande excède l'offre disponible. Voici un exemple de l'agilité de Bitcoin par rapport à d'autres industries.



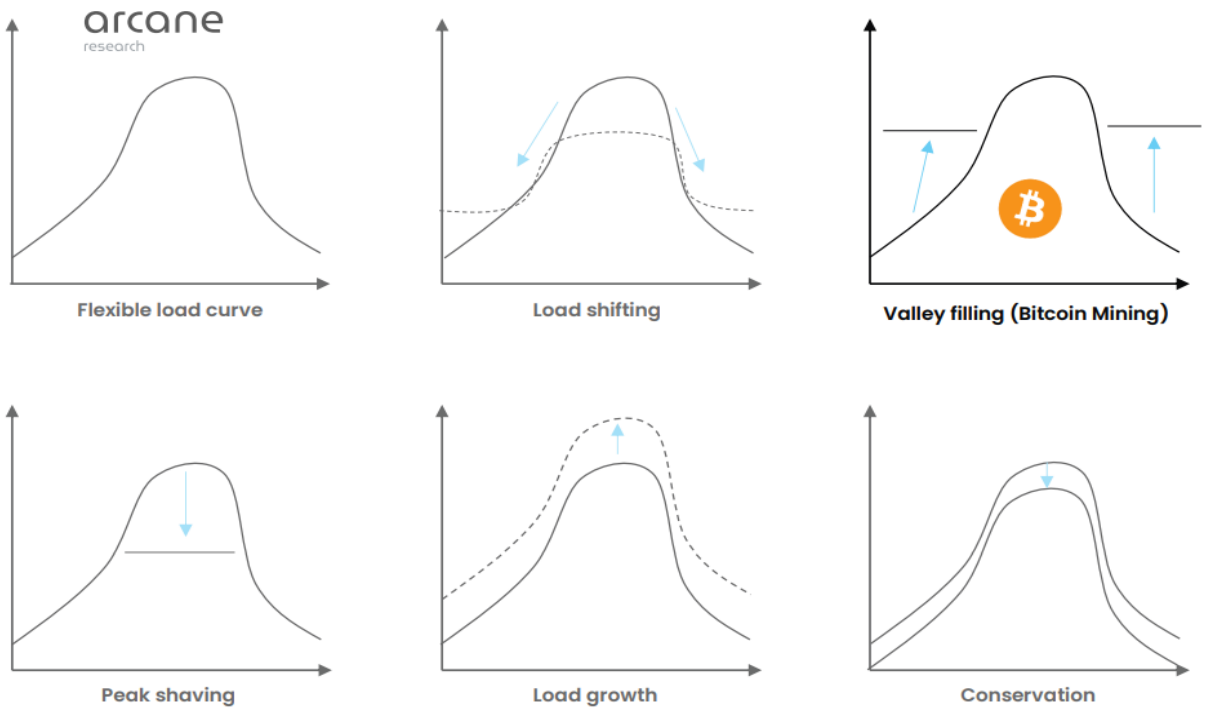
Des stratégies hybrides commencent à se déployer, combinant au sein d'une même infrastructure les activités de minage de Bitcoin et les charges de calcul intensif liées à l'IA, dans ce qu'on appelle les "mullet data centers". Dans ces centres, l'arrière-plan flexible du minage ("la partie mullet") équilibre la charge énergétique fluctuante du front-end de calcul IA. Lorsque la demande de puissance de calcul IA diminue, par exemple la nuit ou lors de périodes creuses, les opérations de minage prennent le relais pour absorber l'énergie excédentaire, évitant ainsi tout gaspillage et maximisant l'efficacité énergétique.

Cette capacité d'ajustement est précieuse : elle permet aux exploitants de centres de données d'optimiser l'utilisation de leurs infrastructures 24 heures sur 24, tout en augmentant leurs revenus. De plus, le minage de Bitcoin peut aussi servir de solution temporaire pendant la construction de data centers IA : en déployant des conteneurs de minage mobiles sur un site en cours de développement, il devient possible de rentabiliser immédiatement l'électricité disponible avant que les installations IA principales ne soient opérationnelles. Ce modèle hybride représente ainsi une passerelle stratégique pour accompagner l'expansion rapide des besoins en calcul IA, tout en valorisant pleinement les ressources énergétiques locales.



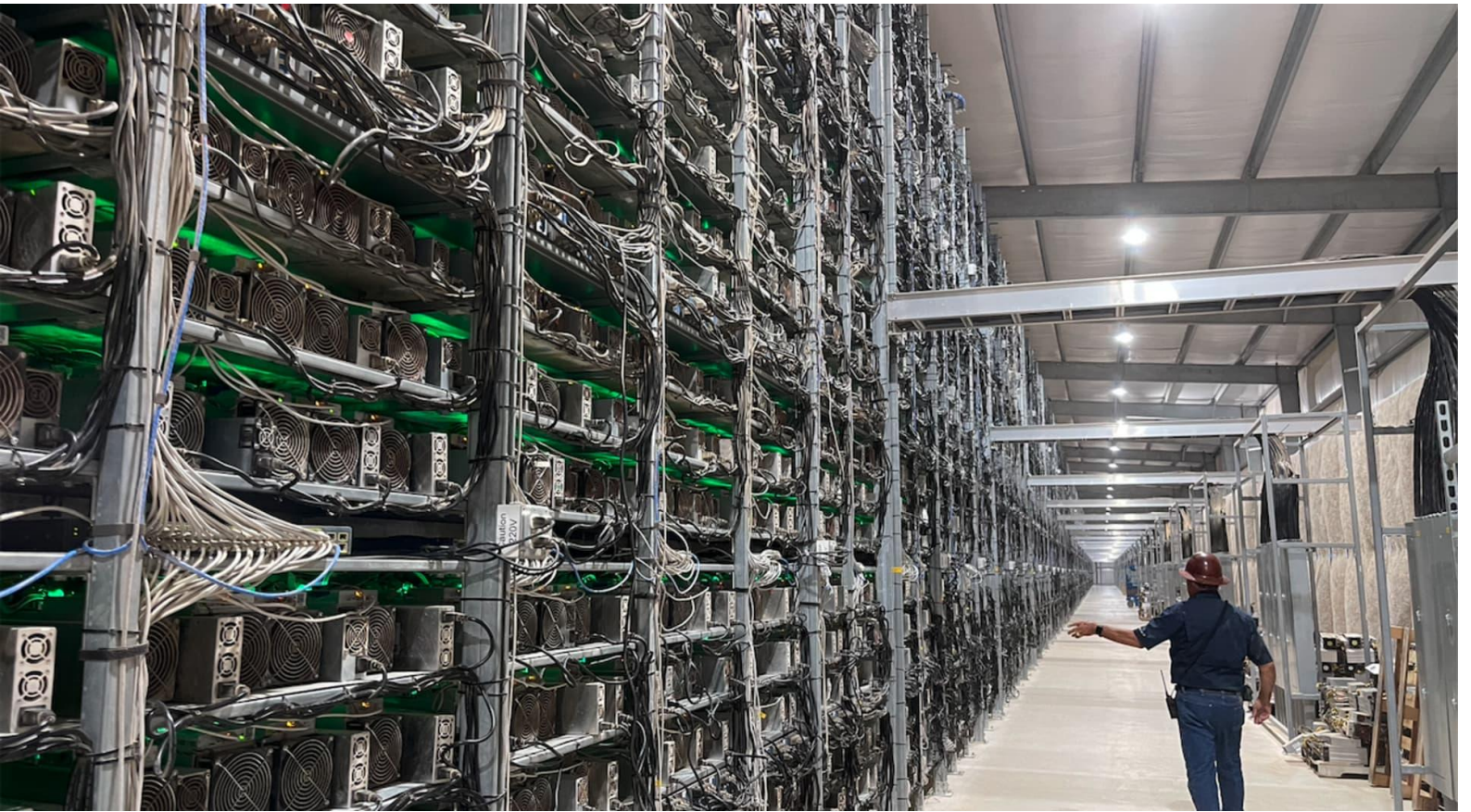
Cette synergie permet de stabiliser les prix de l'électricité. En achetant de l'électricité lorsque l'énergie renouvelable est abondante et que les prix sont bas, les mineurs de bitcoins exercent une pression sur la demande qui peut faire monter les prix de l'électricité les plus bas, améliorant ainsi la rentabilité des centrales d'énergie renouvelable.

Cette relation est vraie pour toutes les industries car Bitcoin ne discrimine pas. Il peut être miné par n'importe qui, n'importe où. Ainsi, il peut venir compléter toute demande en électricité.

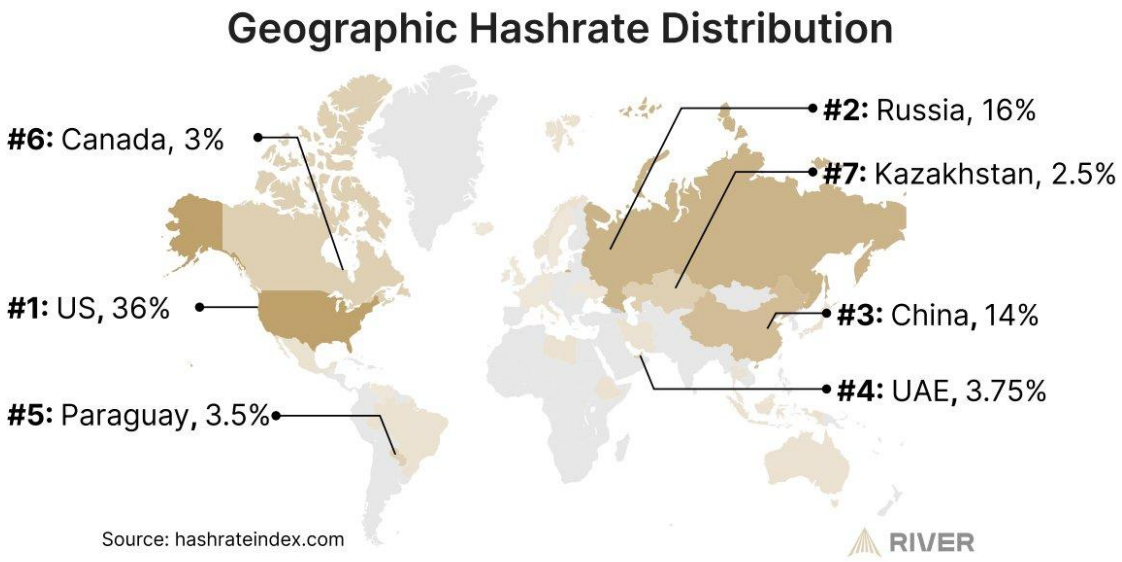


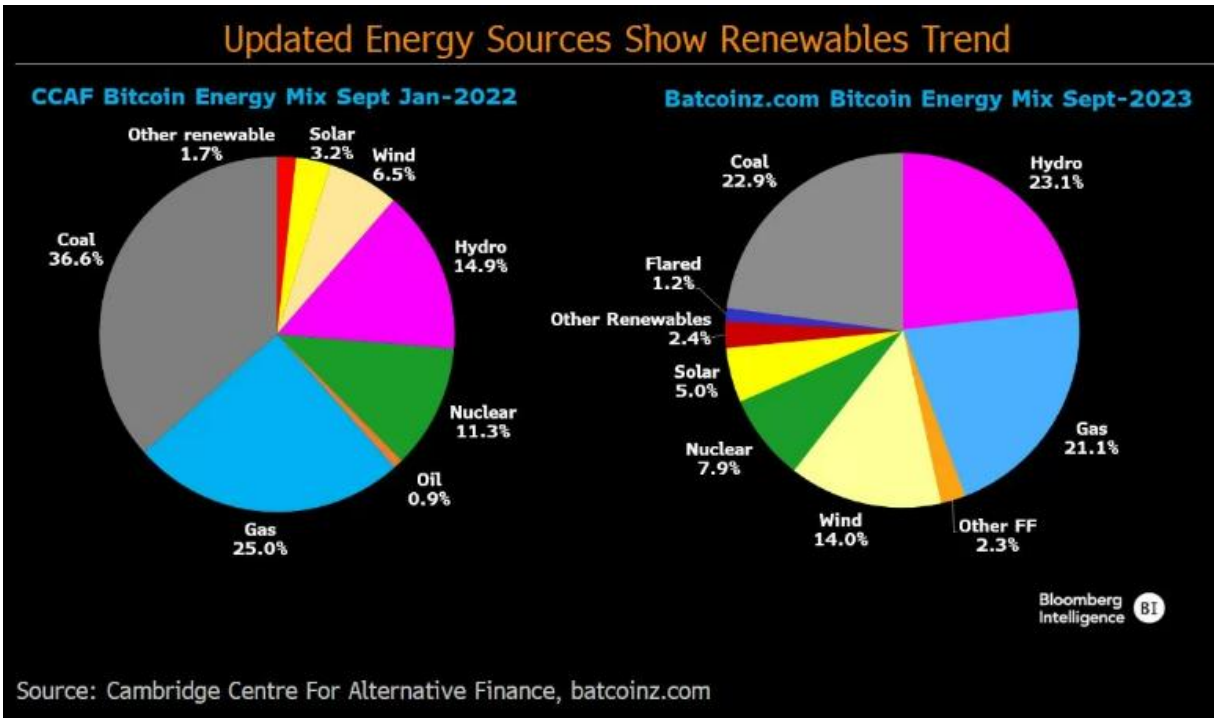
Source: Shaun Connell (Lancium)

La figure ci-dessus illustre la répartition de la charge d'un système électrique et les six différentes façons dont nous pouvons la manipuler. Les mineurs de bitcoins ont un impact sur le système grâce à un mécanisme appelé "valley filling, peak shaping", qui augmente la charge de base sans augmenter la charge de pointe, car les mineurs de bitcoins sont fortement incités à éteindre leurs machines lorsque l'électricité est rare et les prix élevés. Une charge de base plus élevée améliore la rentabilité des énergies renouvelables et incite à la construction de capacités supplémentaires.



La géographie du minage et les dernières initiatives





BBC News rapporte que dans une communauté isolée de 15 000 personnes à l'extrême nord-ouest de la Zambie, qui dépend de l'énergie hydroélectrique, « la mine de bitcoins représente désormais environ 30 % des revenus de l'usine, ce qui leur permet de maintenir les prix bas pour la ville locale ».

L'exploitation minière de Bitcoin a permis au Texas d'éviter 18 milliards de dollars de dépenses énergétiques Selon un rapport du DARI, le minage de bitcoins a permis au Texas d'économiser jusqu'à 18 milliards de dollars en éliminant le

recours à des centrales de pointe au gaz coûteuses. Grâce aux programmes de réponse à la demande d'ERCOT, les mineurs de bitcoins réduisent leur consommation d'énergie pendant les pics de demande, stabilisant ainsi le réseau et évitant des pannes comme celles de la tempête hivernale de 2021. Cette stratégie a également favorisé l'intégration de sources d'énergie renouvelables, offrant une alternative économique et écologique aux solutions de réseau traditionnelles. (Plus à ce sujet par Sébastien Gouspillou)

Reportage de 60 minutes expliquant comment l'exploitation minière bitcoin aide l'environnement en réduisant les émissions de méthane dans le Wyoming.

Le royaume du Bhoutan, niché dans l'Himalaya, a récemment été révélé comme l'un des plus grands détenteurs gouvernementaux de Bitcoin, avec 13 011 BTC évalués à environ 780 millions de dollars, soit près d'un tiers de son PIB estimé à 3 milliards de dollars. Contrairement à d'autres nations qui acquièrent des cryptoactifs par des saisies judiciaires, le Bhoutan a accumulé ses avoirs en Bitcoin principalement grâce à ses propres opérations de minage, menées par Druk Holdings & Investments, le bras d'investissement de l'État. Ces activités de minage, en expansion depuis 2023, s'appuient sur l'abondante énergie hydroélectrique du pays, offrant une solution de minage respectueuse de l'environnement. En partenariat avec la société Bitdeer, le Bhoutan prévoit d'augmenter sa capacité de minage de 100 à 600 mégawatts, consolidant ainsi sa position stratégique dans le domaine des cryptoactifs tout en diversifiant ses sources de revenus au-delà de l'hydroélectricité, du tourisme et de l'agriculture.

Le parc national des Virunga, en République démocratique du Congo, premier parc au monde à exploiter un centre de minage de Bitcoin, utilise l'énergie excédentaire de ses centrales hydroélectriques pour alimenter une installation qui a évité sa faillite. Initié par Sébastien Gouspillou, ce projet, opérationnel depuis 2020, a généré jusqu'à 150 000 dollars mensuels en 2021, compensant la chute des revenus touristiques due à la pandémie et aux conflits, tout en soutenant la conservation de la biodiversité et l'accès local à l'électricité.

Enfin, ceci est une photo de l'installation géothermique construite dans un volcan au Salvador, qui abrite désormais du matériel de minage de bitcoins grâce au président du pays et à son nouvel intérêt pour le bitcoin. De plus, l'équipe de Blockstream était récemment sur place au Salvador et a pu connecter cette installation de minage de bitcoins à son infrastructure satellite, ce qui est également assez cool. (Les 10 installations les plus épiques)

Tous les producteurs d’énergie ont intérêt à déployer des centres de données remplis de mineurs ASIC afin de tirer parti de la demande perpétuelle offerte par le réseau de minage de Bitcoin. De plus, l’extrême compétitivité de ce secteur stimule une demande intense pour l'amélioration de l'efficacité des puces ainsi que pour la recherche non seulement de l’énergie la moins chère, mais aussi de la capacité la plus abondante qui reste sous-utilisée. C’est pourquoi les producteurs d’énergie et les compagnies d’électricité adoptent cette approche : ils utilisent le minage de Bitcoin pour maximiser leur efficacité, améliorer leurs opérations et générer une source de revenus supplémentaire.

Les fondements mêmes du secteur énergétique sont en train d’être repensés. Le tribalisme historique au sein du secteur de l’énergie disparaîtra à mesure que tous les producteurs concentreront leurs efforts vers le grand avenir orangé qui se profile à l’horizon. Et ils sont tous en bonne position pour en tirer des profits considérables.


Bitcoin mining and energy
Technological innovations and profitability
Technological innovations for sustainability
Sustainability and long-term viability
Policy and economic implications
Energy consumption and efficiency
Profitability challenges
Renewable energy and sustainability
Regulatory and policy framework
Sustainability and long-term viability
Social and governance implications
Technological and operational innovations
Economic and market dynamics
Environmental and energy impact
Economic and environmental implications
Market dynamics
Risk and information spillover
Energy consumption and environmental impact
Economic and investment implications
Sustainability and policy implications
Technological and methodological innovations
Carbon footprint and energy consumption
Carbon footprint and greenhouse gas emissions
Energy consumption and sources
Economic and environmental interactions
Policy and regulatory implications
Technological innovations and alternatives

Conclusion

Notre civilisation s’appuie sur une organisation économique où l'énergie, le capital, le travail, la matière et les produits interagissent de façon numérique dans un cycle interdépendant d'informations. L'énergie joue un rôle central en alimentant les infrastructures sous forme d'électricité. Cette énergie sécurise le capital investi, lequel est alors mobilisé par le travail, permettant des échanges de rémunération et de connaissances. Le travail génère des informations qui stimulent l'efficacité et la croissance du capital. Ce dernier, en retour, finance les efforts de recherche et développement pour de nouvelles sources d'énergie.

Le capital est également investi dans la transformation de la matière en produits, générant des biens consommables. Ces produits sont ensuite utilisés ou consommés par les ressources humaines et matérielles, complétant le cycle économique. Cette interdépendance repose sur une logique thermodynamique où chaque élément soutient les autres dans un équilibre systémique.

Techniquement, Bitcoin est une monnaie d’Internet, basée sur des infrastructures électroniques alimentées par de l'énergie et de l'électronique, cette dernière dissipant l'énergie sous forme de chaleur (effet Joule). L'innovation de Bitcoin ne réside pas dans la blockchain elle-même, mais dans l'utilisation de la preuve de travail pour sécuriser des unités de la valeur des informations numériques et donc de ce qu'elles représentent ; donc de toute l'économie moderne.

Le nombre d’unités est fini, et leur mise en circulation est proportionnelle aux capacités des réseaux électroniques, ajustée périodiquement. Parce qu'Internet

est un réseau universel, cette unité ne peut être confiée à une banque centrale. Le registre des transactions est donc distribué et accessible à tous.

Bitcoin est ainsi à la fois une unité d'échange monétaire et un système de paiement dans son "territoire" : Internet et les zones qui l'acceptent. Avec une puissance de calcul cumulée surpassant celle de tous les supercalculateurs combinés, Bitcoin est aujourd'hui le réseau numérique le plus sécurisé au monde.

Contrairement à toute technologie précédente, le minage de Bitcoin incite à explorer des moyens rentables de capter l'énergie, sans se soucier des limitations géographiques ou des contraintes énergétiques conventionnelles. Cet élan financier pourrait déclencher une révolution énergétique d'une ampleur comparable à celle de la Révolution industrielle, et potentiellement propulser l'humanité vers une civilisation de type I. Une vision également partagée par Alana, qui, interrogée sur son prochain projet de film, a déclaré : « Le prochain portera sur ce qu'il faudrait pour atteindre une civilisation de type I en utilisant Porto Rico comme modèle d'outsider, alors que l'île traverse une importante transformation de ses infrastructures. C'est un moment crucial dans l'histoire de Porto Rico, et cela peut servir d'exemple pour les réseaux électriques défaillants à travers le monde. »

À mesure que les incitations économiques poussent le minage de Bitcoin à saturer le secteur énergétique, une convergence est en cours. Les producteurs d'énergie monétisent leur surplus et leur énergie isolée grâce au minage de Bitcoin, tandis que les mineurs s'intègrent verticalement pour améliorer leur compétitivité. Dans un avenir proche, les mineurs les plus efficaces pourraient devenir eux-mêmes producteurs d'énergie, inversant potentiellement le modèle traditionnel du réseau électrique.

Ce parcours de conceptualisation du minage et de l'énergie par les mots m'a permis de vous en parler en alternant les exemples concrets et des réflexions abstraites.

J'espère qu'il vous aura intéressé et qu'il ouvrira une conversation qui serait, pour vous et moi, une continuation de notre apprentissage.

« Si vous voulez trouver les secrets de l'univers, pensez en termes d'énergie, de fréquence, d'information et de vibration »

- Nikola Tesla

Pour aller plus loin :

Dans ce témoignage terrain à contrepied du discours établi, Sébastien Gouspillou livre ses réflexions sur les opportunités et les défis du mining.

Minage et énergie sur Bitcoin

Par @tomily_jones et @dario_nakamoto de *Numeraire Bitcoin*.

L'énergie, face cache de la monnaie par Pierre Noizat

What is the Bitcoin Network's Real Hashrate?

https://mempool.space/fr/docs/faq#what-is-a-mempool

GUIDE MINING

The Real-World Costs of the Digital Race for Bitcoin

Hashrate Index 2024 Bitcoin Mining Year in Review (ANALYSE EXHAUSTIVE)

Séries video Pôle Léonard de Vinci (CONSENSUS DE NAKAMOTO)

Leveraging bitcoing mining to improve grid resilience in Africa

A Primer on Bitcoin Mining

The Environmental Cost of Gold Mining

Revolutionizing Bitcoin Mining: The Power of Three-Phase Systems

Bitcoin Mining for EU Electricity Grids: An Energy Supply Management Tools

https://www.linkedin.com/posts/danielsbatten_can-bitcoin-mining-empower-energy-transition-activity-7269533381158154241-OJfE/

https://www.linkedin.com/pulse/l%25C3%25A9quation-qui-rend-bitcoin-si-simple-et-fort-nicolas-cantu-vrume/

https://www.youtube.com/watch?v=gAQ9KHkDngA

https://x.com/Melt_Dem/status/1881877219762696609/photo/1

https://batcoinz.com/why-climate-action-doesnt-just-benefit-from-bitcoin-mining-it-requires-it/

Bitcoin and Energy Transition: From Risk to Opportunity

BITCOIN METRICS:

https://bitcoin.sipa.be/

https://www.blockchain.com/fr/explorer/charts/pools

https://www.dsn.kastel.kit.edu/bitcoin/#propdelaytx

https://charts.checkonchain.com/

MEMPOOL explorer :

https://txcity.io/v/eth-btc
https://bits.monospace.live/