Machine Translated by Google

Preuve de travail optique

Michael Dubrovsky1 , Marshall Ball2 , et Bogdan Penkovsky1

1PoWx, Cambridge, MA, États-Unis. Courriel : mike@PoWx.org, bogdan@PoWx.org
2Columbia University, New York, NY, États-Unis. Courriel : marshall@cs.columbia.edu

Résumé — La plupart des crypto-monnaies s'appuient sur le « minage » de preuve de travail (PoW) pour résister aux attaques Sybil et à double dépense, ainsi qu'à un mécanisme d'émission de devises. PoW (Hashcash) basé sur SHA256 a réussi à sécuriser le réseau Bitcoin depuis sa création. Cependant, à mesure que le réseau s'est étendu pour prendre en charge un stockage de valeur et un volume de transactions supplémentaires, la forte dépendance de Bitcoin PoW à l'égard de l'électricité a créé des problèmes d'évolutivité, des préoccupations environnementales et systémiques. des risques. Les efforts miniers se sont concentrés dans les zones où les coûts d'électricité sont faibles, créant ainsi des points de défaillance uniques. Bien que les propriétés de sécurité du PoW reposent sur l'imposition d'un coût économique trivialement vérifiable aux mineurs, il n'y a aucune raison fondamentale pour qu'il soit principalement constitué du coût de l'électricité. Pour faire évoluer des systèmes comme Bitcoin jusqu'à 10 à 100 fois sa taille actuelle, les auteurs proposent un nouvel algorithme PoW, Optical Proof of Work (oPoW), pour éliminer l'énergie comme coût principal du minage. La preuve de travail optique impose des difficultés économiques aux mineurs, cependant, le coût est concentré dans le matériel (dépenses en capital – CAPEX) plutôt que dans l'électricité (dépenses d'exploitation – OPEX). Le schéma oPoW implique des modifications minimes aux schémas PoW de type Hashcash et hérite ainsi de nombreuses propriétés de ces schémas, y compris la sûreté/sécurité de base de SHA ou d'une fonction de hachage similaire.

La croissance et l'amélioration rapides de la photonique sur silicium au cours des deux dernières décennies ont récemment conduit à la commercialisation de coprocesseurs photoniques sur silicium (qui sont basés sur des circuits intégrés utilisant des photons au lieu d'électrons pour effectuer des tâches informatiques spécialisées) pour les applications en profondeur à faible énergie. apprentissage des calculs. oPoW est optimisé pour une version simplifiée de cette technologie, de sorte que les mineurs soient incités à utiliser une photonique spécialisée et hautement économe en énergie pour le calcul.

En plus de permettre des économies d'énergie, oPoW a le potentiel d'améliorer l'évolutivité du réseau, de permettre une exploitation minière décentralisée en dehors des zones à faible coût de l'électricité et de démocratiser l'émission. La décentralisation géographique rendra l'écosystème minier oPoW plus résistant à la censure, avec une exposition réduite aux attaques de partition et aux réglementations régionales. De plus, en raison de la domination du CAPEX sur les coûts miniers, le hashrate oPoW sera nettement moins sensible à la baisse sous-jacente du prix des pièces. Dans cet article, nous fournissons un aperçu du concept, de l'algorithme et du matériel oPoW.

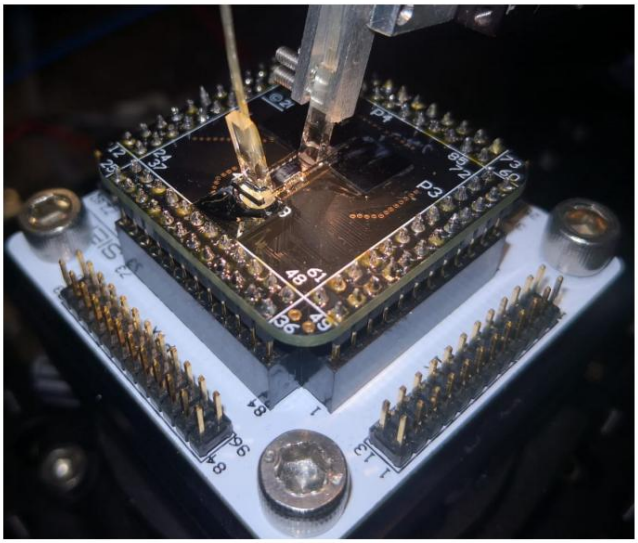

Figure 1. Prototype de mineur photonique au silicium oPoW

I. INTRODUCTION

La fonction principale des réseaux publics de crypto-monnaie, tels que Bitcoin, est de maintenir un registre électronique décentralisé des transactions. Il est essentiel que cela nécessite qu'il n'y ait pas d'autorité unique, telle qu'une banque, contrôlant ou validant le contenu du grand livre. Une conception naïve de ce type de réseau peut être obtenue si les utilisateurs publient leurs transactions publiquement via des messages signés (en utilisant la cryptographie à clé publique), et une transaction n'est considérée comme terminée que lorsque la majorité des nœuds du réseau l'ont acceptée. Cependant, si le réseau doit être sans confiance/sans autorisation et résistant aux acteurs malveillants, un mécanisme doit exister pour empêcher les attaques Sybil1 et les doubles dépenses2 .

Bien qu'il y ait eu des tentatives antérieures de systèmes de paiement électronique, l'architecture de Bitcoin (décrite dans le livre blanc original de Nakamoto [1]) a été la première à résoudre les problèmes de double dépense et d'attaque Sybil grâce à une utilisation intelligente de Hashcash [2] Preuve du travail (PoW). L'idée clé de Nakamoto était que les preuves de travail permettent aux systèmes distribués d'imposer automatiquement des coûts trivialement vérifiables aux nœuds participants, permettant un accord byzantin [3] dans des paramètres auparavant considérés comme insolubles, avec la fonctionnalité supplémentaire de créer un mécanisme de distribution pour la crypto-monnaie, c'est-à-dire les nœuds sont rémunérés pour leur « travail » en utilisant la crypto-monnaie elle-même. Cela a conduit à l'incroyable essor du Bitcoin et d'autres crypto-monnaies, créant la possibilité d'un accès sans précédent à la liberté financière et aux droits de propriété à l'échelle mondiale.

A. Preuve de travail dans le contexte des blockchains

Les systèmes de preuve de travail, ou fonctions de tarification, ont été initialement proposés à Crypto 1992 par Cynthia Dwork et Moni Naor pour diverses tâches telles que la lutte contre le courrier indésirable [4]. Une « preuve de travail » est une solution à un défi informatique spécifique qui nécessite inévitablement une certaine quantité de calcul.

1Plusieurs nœuds contrôlés par un acteur malveillant

2Faire deux achats avec la même pièce en réécrivant le grand livre supprimer la première transaction

Machine Translated by Google

travailler à résoudre. Ce défi s'appelle un cryptopuzzle et est conçu de telle manière qu'il ne peut être forcé qu'en vérifiant toutes les solutions possibles une par une jusqu'à ce qu'une solution valable soit trouvée. Cela garantit que les solutions sont relativement rares.
La résolution de ces énigmes dans le contexte de la cryptomonnaie est communément connue sous le nom de « mining », car une solution réussie rapporte des récompenses (appelées « récompenses de bloc »). D'un autre côté, il est facile de vérifier que n'importe quelle solution est correcte, ne nécessitant qu'un seul cycle de calcul. Par conséquent, une preuve de travail fournit une garantie trivialement vérifiable qu'un certain nombre de calculs ont été effectués pour la produire.

Dans Bitcoin, les transactions sont enregistrées en blocs, et une séquence liée de ces blocs est appelée chaîne de blocs. Une fois qu'un dispositif minier (mineur) compile un bloc de transactions, il mélange les valeurs aléatoires d'une entrée spéciale (nonce) dans le bloc jusqu'à ce que le hachage cryptographique du bloc soit inférieur à un seuil prédéterminé. Les propriétés de sécurité des fonctions de hachage obligent un mineur à tester les noms occasionnels par force brute jusqu'à ce qu'un bloc satisfaisant soit trouvé. Un tel bloc constitue une solution au cryptopuzzle et est en soi la preuve du travail. Une fois le bloc publié, chacun peut facilement vérifier que le travail a été effectué en calculant le hachage cryptographique du bloc et en vérifiant qu'il est bien en dessous du seuil prédéterminé3 Bitcoin utilise le hachage cryptographique SHA-256(NIST), mais divers hachages les fonctions sont utilisées par différents réseaux blockchain. Chaque type impose une charge différente sur le processeur et la mémoire de l'appareil informatique d'un mineur, mais ils utilisent tous les mêmes principes. Ethereum, par exemple, utilise un hachage cryptographique nommé Ethash, qui nécessite de plus grandes exigences en mémoire [5].

En conséquence, la validité d'une blockchain repose sur un travail informatique préalablement effectué. Cela signifie également que la chaîne la plus longue, correspondant implicitement à la quantité de travail la plus élevée, peut être automatiquement considérée comme l'historique des transactions valide (puisqu'elle accumule la majorité des ressources informatiques). La modification d'un seul bloc nécessite une grande quantité de calcul4 , ce qui devient rapidement impossible sans contrôler plus de la moitié de la puissance de calcul du réseau (c'est ce qu'on appelle une attaque à 51 %, voir Section II-D). De plus, toute transaction à double dépense devient impossible puisque seule la plus longue des deux blockchains nouvellement créées sera reconnue comme valide. PoW a également été appliqué à des registres décentralisés à haut débit (en transactions par seconde) plus complexes où les blocs sont dans un graphe acyclique dirigé, et pas simplement dans une chaîne [6], [7]. Les systèmes PoW ont d'excellents antécédents en matière de garantie de l'irréversibilité des transactions sur le réseau Bitcoin. Cependant, la preuve de travail s'est heurtée à de graves problèmes de mise à l'échelle qui pourraient éventuellement nuire à la croissance de Bitcoin.

B. Défis rencontrés par l'écosystème de preuve de travail de Bitcoin

Alors que Bitcoin est passé au cours de la dernière décennie d'un petit réseau géré par des amateurs à une monnaie mondiale, le protocole de preuve de travail sous-jacent n'a pas été mis à jour. Initialement envisagées comme un réseau décentralisé mondial (« un processeur, une voix »), les transactions Bitcoin sont aujourd'hui sécurisées par un petit groupe d'entreprises. En raison de l'augmentation de la valeur marchande des récompenses minières au fil du temps et de la concurrence entre les mineurs, la difficulté du minage de Bitcoin a augmenté de façon exponentielle, conduisant à l'industrialisation du minage. L'énorme et croissante5 consommation d'énergie du Proof of Work a conduit à une centralisation géographique du minage dans des centres de données spécialement construits, situés dans des régions à très faibles coûts énergétiques et excluant les petites entités de l'écosystème minier.

Bien que les chiffres exacts soient contestés, la consommation d'énergie du Bitcoin a augmenté régulièrement avec sa valeur marchande et, aujourd'hui, on estime que le Bitcoin consomme plus de 75 térawattheures par an [8]. Étant donné que cela représente plus que la consommation électrique de l'Autriche [9], le minage de Bitcoin favorise fortement les économies d'échelle. En fait, cela n'est réalisable que pour les entités capables de garantir un accès à une énergie abondante et peu coûteuse [10]. L'économie de l'exploitation minière limite la rentabilité à des pays comme l'Islande et l'ouest de la Chine. Outre les externalités environnementales négatives, qui peuvent être importantes, l'exploitation minière est aujourd'hui principalement réalisée avec le consentement (et dans de nombreux cas, le partenariat) des grands services publics et des gouvernements qui les contrôlent. Même si cela ne pose peut-être pas de problème à court terme, à long terme, cela risque d'éroder la résistance à la censure et la sécurité du Bitcoin et d'autres blockchains publiques par le biais d'attaques potentielles de réglementation ou de partitionnement6 [13] .

Une conséquence supplémentaire de l'économie énergétique de la preuve de travail est la sensibilité du hashrate au blocage de la valeur de la récompense. Si la valeur monétaire des récompenses globales diminue ou si les prix de l'électricité augmentent, les mineurs peu rentables sont obligés d'arrêter leurs machines pour éviter de fonctionner à perte. Cela conduit à une instabilité indésirable de la sécurité du réseau, notamment en période de volatilité.

Il est important de noter que, d'un point de vue algorithmique, la consommation d'énergie du Bitcoin est une fonctionnalité et non un bug. Le réseau est conçu pour encourager automatiquement une augmentation du minage de PoW à mesure qu'il s'agrandit afin de maintenir un niveau de sécurité proportionnellement plus élevé. La valeur monétaire des récompenses minières augmente (par conception) avec la valeur marchande de la pièce, ce qui conduit les mineurs à dépenser plus de ressources en compétition pour les récompenses minières (qui sont libellées en Bitcoin) et donc à utiliser plus d'énergie. Cela permet à Bitcoin d'augmenter le coût d'une attaque de 51 % à mesure que la récompense associée à une attaque réussie augmente. L'algorithme Bitcoin n'a pas d'accès direct aux informations sur la valeur marchande du Bitcoin, mais il peut indirectement déduire une augmentation de la valeur à partir d'une augmentation du hashrate7. Un algorithme alternatif de récompense minière peut être ima

3Ce seuil est automatiquement ajusté par le système de telle sorte qu'un seul bloc soit trouvé toutes les 10 minutes ; plus le seuil est bas, plus il est improbable de trouver une solution. Par exemple : un hachage SHA256 produit 256 bits, si le paramètre de difficulté nécessite que le mineur trouve un nom occasionnel qui mène à un hachage de bloc avec 40 zéros non significatifs, alors statistiquement 2 essais seront nécessaires pour trouver l'un des noms occasionnels « acceptables ».

4Les preuves de travail pour tous les blocs suivant le bloc modifié doivent être recalculées.

5Le taux de hachage, et donc la consommation d'énergie, est conçu pour croître avec la valeur du réseau afin de maintenir un coût de double dépense irréalisable par rapport à la valeur globale d'une attaque à double dépense réussie.

6Une censure à cette échelle n'est pas aussi improbable qu'on pourrait le penser [11], [12], cependant, une grande partie du risque peut être atténuée en répartissant l'exploitation minière à l'échelle mondiale.

7Bien que ce ne soit pas parfait car le hashrate a tendance à augmenter en raison des améliorations matérielles.

Machine Translated by Google

la récompense de bloc à mesure que le hashrate augmente, limitant ainsi l'incitation des mineurs à dépenser plus de ressources et d'énergie8 .
Cela dissocierait effectivement la consommation d'énergie du réseau de la valeur totale stockée et de la valeur marchande de chaque pièce, mais cela signifierait que le coût d'une attaque contre le réseau n'augmenterait plus avec l'incitation à le faire.

donc.

De nouveaux mécanismes de consensus ont été proposés comme moyen de sécuriser les crypto-monnaies tout en réduisant les coûts énergétiques, tels que diverses formes de Proof of Stake9 et de Proof of Space-Time [15], [16] mises en œuvre par Chia et Spacemesh.
Même si bon nombre de ces mécanismes alternatifs offrent des garanties convaincantes, ils nécessitent généralement de nouvelles hypothèses de sécurité, qui n'ont pas été testées par des déploiements réels à une échelle adéquate. Par conséquent, nous avons encore relativement peu de connaissances empiriques sur leur sécurité. Changer complètement le paradigme du bitcoin est susceptible d'introduire de nouveaux problèmes imprévus. Nous pensons que les problèmes majeurs évoqués ci-dessus peuvent être résolus en améliorant plutôt qu'en éliminant la couche de sécurité fondamentale de Bitcoin : la preuve de travail.

C. Une preuve de travail de nouvelle génération

Au lieu de concevoir une nouvelle architecture consensuelle pour résoudre les problèmes de mise à l'échelle, nous réfléchissons aux moyens de modifier l'économie du PoW. Comme il est utilisé dans des systèmes de type Bitcoin, PoW permet à des réseaux comme Bitcoin de parvenir à un consensus via les difficultés économiques imposées aux mineurs. Il n'est toutefois pas nécessaire que le coût financier soit concentré sur l'électricité. En fait, la situation peut être considérablement améliorée en réduisant les dépenses d'exploitation (OPEX) – l'énergie – en tant que coût important de l'exploitation minière. Ensuite, en déplaçant le coût vers les dépenses en capital (CAPEX) – matériel minier – la dynamique de l'écosystème minier devient beaucoup moins dépendante des prix de l'électricité, et beaucoup moins d'électricité est consommée dans son ensemble. De plus, cela conduit automatiquement à une exploitation minière géographiquement répartie, car l'exploitation minière devient rentable même dans les régions où l'électricité est chère. Enfin, une consommation d'énergie plus faible élimine les problèmes de chauffage rencontrés par les opérations minières d'aujourd'hui, ce qui réduit encore davantage les coûts d'exploitation ainsi que le bruit associé aux ventilateurs et aux systèmes de refroidissement. Tout cela signifie que les particuliers et les petites entités pourraient entrer dans l'écosystème minier simplement pour le prix d'un mineur, sans avoir au préalable accès à une énergie bon marché et à un centre de données dédié à température contrôlée. Dans une certaine mesure, les schémas PoW gourmands en mémoire comme Cuckoo Cycle [17], qui augmentent l'utilisation de SRAM au lieu du calcul pur, poussent le rapport CAPEX/OPEX dans la bonne direction en occupant la zone de la puce ASIC avec de la mémoire.

Pour maximiser le ratio CAPEX/OPEX du coût minier, nous étudions des algorithmes alternatifs de preuve de travail et des paradigmes de matériel informatique complémentaires qui sont difficiles/coûteux à produire mais atteignent une efficacité énergétique élevée.
On peut observer que le matériel d'intelligence artificielle (IA) l'industrie converge vers un objectif similaire alors que de nombreuses entreprises tentent de commercialiser des architectures exotiques pour l'informatique à faible consommation d'énergie10 . L'une des approches prometteuses commercialisées pour l'IA est le calcul optique, en particulier les coprocesseurs photoniques. En raison de sa faisabilité commerciale et de son potentiel à long terme pour une consommation d'énergie ultra-faible, nous avons conclu que l'informatique optique est une plate-forme prometteuse pour une preuve de travail à faible consommation d'énergie.

D. Informatique optique Alors

que dans le matériel numérique traditionnel, nous comptons sur les courants électriques, l'informatique optique utilise la lumière comme base de ses opérations. Cette approche existe depuis des décennies, mais les progrès récents dans le secteur des télécommunications et dans l'intelligence artificielle (IA) ont contribué de manière significative au développement de l'informatique optique. En effet, les chercheurs prévoient que l'intégration du traitement optique, en commençant par le routage du signal sur puce et en terminant par les accélérateurs optiques pour l'IA, peut augmenter considérablement la vitesse de traitement, tout en maintenant les niveaux de consommation d'énergie aussi bas que possible. De plus, l'industrie des semi-conducteurs a presque atteint ses limites fondamentales, ce qui signifie que les ordinateurs numériques ne peuvent pas continuer à s'améliorer sur la même trajectoire qu'ils suivent depuis cinquante ans [19]. Cela signifie également que le progrès technologique continu nécessitera des méthodes informatiques et du matériel alternatifs. Les avantages de l'utilisation de la lumière pour le traitement de l'information peuvent être mieux illustrés par l'adoption de l'optique dans l'industrie des télécommunications. En effet, le remplacement des câbles de cuivre par des fibres optiques a transformé les communications intercontinentales, y compris Internet, qui est devenu exponentiellement plus rapide et plus efficace.

L'informatique optique a une histoire riche qui remonte au traitement de Fourier dans les années 1940 (Duffieux 1946), aux premiers réseaux de neurones optiques dans les années 1980 (Psalti 1984), aux travaux des années 1980 sur le transistor optique aux Bell Labs et aux travaux modernes sur les réseaux de neurones optiques. informatique de réservoir et informatique quantique optique. La recherche en informatique optique aux Bell Labs a inspiré l'informatique optique/photonique moderne de l'IA, tandis que les ordinateurs holographiques et les communications de chaos optique ont influencé différentes sortes d'informatique à réservoir optique.

Le Reservoir Computing (RC) a été initialement conçu au début des années 2000 pour tenter de simplifier la formation récurrente des réseaux de neurones [20], [21].11 Entraîné de manière supervisée en créant une simple lecture linéaire à partir d'un état de grande dimension. Dans l'espace, les systèmes RC sont capables de résoudre les problèmes de reconnaissance de formes et de prédiction de séries chronologiques [23], [24] et sont rapidement devenus populaires pour l'informatique in-materio avec divers substrats physiques tels que l'eau (d'où « réservoir ») [25] .

Les chercheurs ont montré qu'en utilisant des systèmes optiques pour le calcul, la recherche photonique RC peut produire un fonctionnement à grande vitesse et une faible consommation d'énergie. À titre de comparaison, une configuration RC utilisant un équipement optique disponible dans le commerce effectue des tâches de reconnaissance vocale.

8La réduction de moitié de la subvention globale de Bitcoin permet d'atteindre cet objectif dans une certaine mesure, mais l'argument courant est que les frais de transaction paieront pour la sécurité une fois la subvention globale épuisée.

9Il existe de nombreuses tentatives de mise en œuvre, notamment les efforts jusqu'ici infructueux d'Ethereum pour mettre en œuvre une forme de PoS sur son réseau principal. Ces programmes introduisent également de nouveaux défis [14].

10La demande en matière de calcul pour l'IA croît de façon exponentielle et ne peut être prise en charge par le matériel conventionnel sans une consommation d'énergie massive [18].

11Une méthode apparentée a été proposée encore plus tôt en neurosciences cognitives [22].

Machine Translated by Google

environ trois fois plus rapide qu'un Google TPU [26]. Un autre travail récent implémente la RC photonique avec un système spatialement étendu [27]. Ce système RC, basé sur des modulateurs spatiaux de lumière et des réseaux de micromiroirs, permet facilement un traitement massivement parallèle des informations par des centaines de nœuds non linéaires.

Informatique IA par apprentissage profond Bien que l'objectif initial de l'informatique inspirée du cerveau était d'imiter le comportement de populations de neurones biologiques à l'aide de circuits analogiques intégrés, ces dernières années, les implémentations photoniques de réseaux neuronaux profonds12 ont gagné du terrain . En conséquence, plusieurs nouvelles stratégies matérielles optiques ont été développées pour effectuer la multiplication matrice-vecteur [29], [30]. Les approches plus anciennes reposaient sur des modulateurs spatiaux lents de la lumière [31], tandis que les implémentations récentes, qui sont maintenant commercialisées, utilisent des circuits photoniques intégrés en silicium basés sur des résonateurs à micro-anneaux [29] et des réseaux d'interféromètres de Mach-Zehnder [30].

Malgré des démonstrations réussies de calcul optique sous diverses formes au fil des années, le facteur limitant l'adoption commerciale a toujours été le coût et la difficulté de fabriquer le matériel à grande échelle. Les ordinateurs numériques concurrents ont bénéficié d'améliorations continues de la technologie de fabrication et d'une chaîne d'approvisionnement sans usine pour les nouveaux produits13 .

L'avènement relativement récent de la photonique sur silicium, compatible avec les processus de fabrication de puces standards utilisés pour l'électronique numérique, a ouvert la possibilité de fabriquer des coprocesseurs optiques évolutifs et reproductibles. Dans les deux sous-sections suivantes, nous fournissons un bref aperçu de la photonique sur silicium et de son application au traitement de l'IA par apprentissage profond.

De plus, dans la section II-B, nous expliquons brièvement les principes de fonctionnement de la multiplication matrice-vecteur dans les circuits photoniques.

E. Photonique sur silicium

Traditionnellement, les systèmes optiques nécessitent un alignement précis et des composants en vrac coûteux et soigneusement fabriqués. Les progrès récents dans les circuits intégrés photoniques (PIC) ont résolu ces problèmes avec succès en portant des systèmes optiques massifs sur des circuits de guide d'ondes à l'échelle d'une puce. Les circuits intégrés photoniques sont produits en modelant de fines tranches diélectriques ou semi-conductrices à l'aide d'un traitement micro/nano, en tirant parti de l'incroyable et toujours croissante précision de la lithographie pour garantir l'alignement et permettre une production de masse à moindre coût. Jusqu'au début des années 2000, les PIC étaient fabriqués à partir de matériaux III-V coûteux. Malgré les propriétés optiques intrinsèquement sous-optimales du silicium (pas de lasers au silicium commerciaux, pas d'effet électro-optique), son utilisation omniprésente en électronique a créé un énorme écosystème de fabrication qui a rendu avantageux de contourner les problèmes et de s'appuyer sur- composants optiques en silicium à puce. Après des percées dans la conception de composants photoniques en silicium (Si)14 tels que des coupleurs fibre optique à puce à faible perte [32], des modulateurs électro-optiques rapides [33] et des photodétecteurs sur puce au germanium [34], il est devenu possible de tirer parti des incroyables développements de la technologie silicium CMOS15 au cours des six dernières décennies pour produire des circuits photoniques dans des processus de fonderie électronique réutilisés. L'un des éléments fondamentaux des circuits photoniques en Si est le guide d'onde en Si à l'échelle nanométrique. Les figures 2 et 3 représentent des guides d'ondes typiques produits dans une plaquette de silicium sur isolant, qui confinent la lumière dans le circuit photonique via une réflexion interne totale (le même effet utilisé pour guider la lumière dans les fibres optiques).

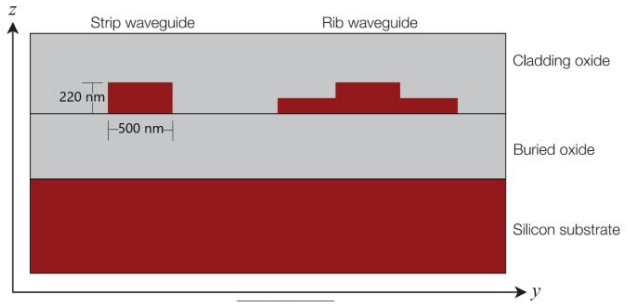

Figure 2. Coupe transversale de silicium sur des guides d'ondes isolants

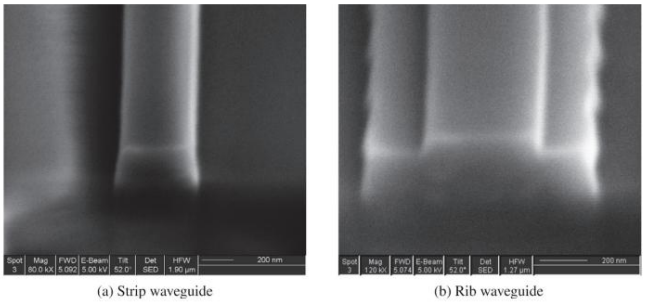

Figure 3. Image MEB du silicium sur des guides d'ondes isolants [35]

Les circuits intégrés photoniques au silicium ont connu un succès commercial en tant qu'émetteurs-récepteurs pour diverses applications de communication de données [36]. Aujourd'hui, des millions d'émetteurs-récepteurs photoniques au silicium (fabriqués par des sociétés telles que Luxtera, IBM et Intel) font circuler les informations entre les racks de serveurs des centres de données. De plus, plusieurs entreprises commercialisent désormais la photonique sur silicium pour le LIDAR et la biodétection. Surtout, les principales fonderies de micropuces (dont Global Foundries et TSMC) proposent des photoniques au silicium ou sont en train de lancer des lignes de fabrication de photoniques sur silicium. Ces dernières années, cette disponibilité de fabrication photonique commerciale sur silicium a stimulé les efforts visant à commercialiser des puces photoniques sur silicium pour un calcul massivement parallèle, conduisant à l'émergence de coprocesseurs photoniques pour l'IA.

Coprocesseurs photoniques intégrés pour l'IA : en raison du succès récent des algorithmes d'IA d'apprentissage en profondeur, la demande de quantités massives de traitement de multiplication et d'accumulation (MAC) a conduit à de lourds investissements dans le processeur MAC.

Les architectures 12DNN n'imitent pas directement l'architecture cérébrale, même si elles ont conservé le terme « neurone ». Même s'il existe des implémentations photoniques neuromorphiques qui produisent un traitement d'intégration et de déclenchement de type neurone [28], elles ne sont pas proches de la commercialisation.

13Les entreprises qui commercialisent des puces peuvent travailler avec des fonderies comme TSMC et Global Foundries, plutôt que de créer leurs propres opérations de fabrication.

14Voir https://youtu.be/csHshgggAdw la conférence de Michal Lipson sur l'histoire de la photonique Si

15Le procédé métal-oxyde-semi-conducteur complémentaire (CMOS) est le procédé de fabrication nanoélectronique qui a réussi à réduire le coût et la taille des transistors de plus d'un facteur 106 au cours des 60 dernières années. Cette technologie constitue la base des circuits numériques modernes, notamment des processeurs informatiques et de la mémoire.

Machine Translated by Google

recherche ainsi que de nombreux efforts commerciaux pour produire des processeurs spécialisés qui effectuent ces calculs plus efficacement du point de vue des coûts et de l'énergie. Parallèlement aux développements en cours des fabricants de GPU comme NVIDIA et Google (TPU), plusieurs sociétés telles que Groq (numérique), Graphcore (numérique), ainsi que Mythic (analogique) et Synthiant (analogique) recherchent des architectures électroniques innovantes pour MAC.

Les architectures d'IA ont été explorées dans les systèmes optiques en espace libre [27], [37], et plusieurs sociétés telles que LightOn, Fathom et Optalysis travaillent sur la mise en œuvre commerciale de tels systèmes. Cependant, plus récemment, grâce aux progrès réalisés par le laboratoire de photonique neuromorphique de Princeton [38] ainsi que par les recherches du MIT [30] et d'autres institutions académiques, plusieurs startups ont vu le jour, dont Lightel-ligence [39], Lightmatter [40] , et Luminous [41], qui appliquent des conceptions photoniques sur silicium pour les télécommunications et le traitement de l'information quantique afin de construire des circuits photoniques de traitement MAC. La promesse de la technologie, telle que détaillée par Nahmias et al. [42], vise à offrir aux MAC une efficacité énergétique supérieure de 2 à 3 ordres de grandeur par rapport aux processeurs électroniques, et à terme des gains encore plus importants car le calcul optique a des limites théoriques très élevées en matière d'efficacité énergétique [43]. Dans une comparaison des performances du GPU de pointe avec un modèle de processeur électronique-photonique basé sur des composants de fonderie disponibles dans le commerce, il a été constaté une accélération de 2,8 à 14x pour la même consommation d'énergie lors de l'exécution de calculs CNN. 44]. Une estimation des coprocesseurs photoniques par Lima et al. prédit 10fJ/MAC pour une puce à 128 canaux contre 1pJ/MAC pour le Google TPU [45] et Nahmias et al. [42] prédisent que les performances peuvent être poussées à 2,1fJ/MAC. Ces développements passionnants dans les coprocesseurs photoniques au silicium ont créé une opportunité d'appliquer la technologie sous-jacente à des applications à faible consommation d'énergie en dehors du traitement de l'IA.

F. Preuve de travail optique

Inspirés par les progrès récents de la photonique sur silicium pour le calcul à faible énergie, nous envisageons un système PoW pratique conçu pour compléter le calcul optique. L'objectif principal d'une telle approche PoW est de réaliser des économies d'énergie drastiques. Bien qu'à long terme, il soit concevable que certains mineurs soient construits sur la base d'autres architectures analogiques, nous considérons que les coprocesseurs photoniques détiennent le plus grand potentiel en termes d'efficacité énergétique élevée, combiné à une disponibilité commerciale à court terme.
En conséquence, nous proposons une preuve de travail optique (oPoW), un algorithme PoW optimisé pour l'accélération avec des coprocesseurs photoniques intégrés.

II. POUVOIR À FAIBLE ÉNERGIE

Plutôt que d'essayer de calculer un algorithme PoW existant à l'aide de matériel photonique16, nous avons choisi de construire un PoW modifié pour favoriser les conceptions de coprocesseurs photoniques existantes.

16Il existe déjà d'énormes incitations financières à le faire : de nombreux experts en informatique optique ont étudié la possibilité d'utiliser la photonique pour l'extraction de bitcoins, mais les algorithmes PoW existants sont mal adaptés à l'informatique analogique.
Les hachages comme SHA256 sont spécialement conçus pour être implémentés efficacement par les processeurs numériques.

Nous décrirons ici brièvement la co-conception d'un prototype de coprocesseur photonique et d'un algorithme PoW construit pour atteindre notre objectif PoW à faible consommation d'énergie.

Il convient de noter que presque toutes les tentatives précédentes visant à modifier les algorithmes PoW pour favoriser un paradigme matériel spécifique se sont concentrées sur la résistance ASIC, ce qui signifie que plutôt que de privilégier le matériel spécialisé, l'objectif est d'exclure le matériel spécialisé au profit des GPU ou des CPU17. Les exemples incluent Scrypt, Cryptonight, Equihash et, plus récemment, ProgPoW.
Outre ProgPoW, qui n'a pas encore été implémenté, ces expériences ont plus ou moins échoué en raison des avantages inhérents au matériel spécialisé. Une excellente discussion sur ce sujet peut être trouvée dans The State of Cryptocurrency Mining [46], où l'auteur conclut que :

> « Pour tout algorithme, il y aura toujours une voie que les ingénieurs en matériel personnalisé pourront emprunter pour battre le matériel à usage général. C'est une limitation fondamentale du matériel à usage général.

Le PoW optique est fondamentalement un problème d'ingénierie plus simple que le PoW résistant aux ASIC. Il est conçu pour être le plus efficace sur le matériel photonique intégré, donnant ainsi un avantage à une classe d'ASIC par rapport à une autre, plutôt que d'essayer de limiter l'avantage du matériel spécialisé par rapport au matériel général.

A. HeavyHash

Notre objectif dans la conception d'oPoW était d'imiter la construction Bitcoin PoW (HashCash), en maintenant la sécurité cryptographique tout en garantissant que le puzzle cryptographique PoW est optimisé pour notre « paradigme cible » (coprocesseurs photoniques). Comme le coût majeur du PoW réside dans l'évaluation de la fonction de hachage choisie, la solution naïve serait de trouver un hachage optiquement calculable. Cependant, un choix de conception a été fait dès le début pour éviter les hachages entièrement optiques et les fonctions physiques unidirectionnelles - en raison de problèmes de répétabilité [47] et de leurs propriétés de sécurité mal comprises. La création d'un nouveau hachage optimisé pour le traitement photonique n'a pas non plus été envisagée en raison de la complexité et du risque de déploiement d'une fonction de hachage non testée, voir le fiasco IOTA [48]. Cela conduit à la sélection d'une conception hybride qui compose un hachage numérique avec une multiplication de matrice vectorielle de faible précision (destinée à l'accélération photonique) pour produire du HeavyHash. HeavyHash est une composition itérée d'une fonction de hachage existante, c'est-à-dire SHA256, et d'une fonction de pondération telle que le coût d'évaluation de HeavyHash est dominé par le calcul de la fonction de pondération. Si la fonction de pondération est dominée par l'évaluation d'une multiplication vecteur-matrice de taille suffisante (et de préférence unitaire), elle peut être mise en œuvre avec une très grande efficacité par des coprocesseurs photoniques [30]. Le rapport entre le coût de calcul des hachages et celui de la fonction de pondération est réglable dans une large plage en raison de leurs différents ordres de grandeur de complexité18).

Machine Translated by Google

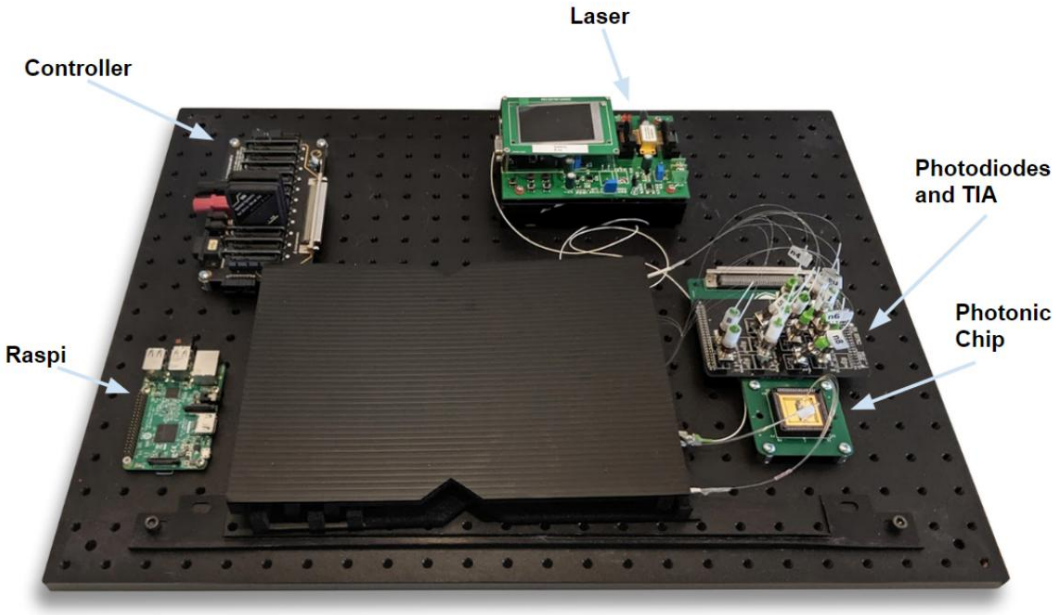

Figure 4. Configuration du prototype de mineur. Câblage exclu - le Raspberry Pi communique avec le Qontrol via USB, qui à son tour est connecté au PCB qui porte la puce et le TIA.

B. Prototype PoW optique

Dans sa forme la plus simple, oPoW est l'algorithme Hashcash [2] avec notre fonction de hachage personnalisée, HeavyHash, conçue spécifiquement pour fonctionner efficacement sur les accélérateurs optiques tout en préservant toutes les propriétés de sécurité cryptographiques nécessaires au PoW. Un prototype d'implémentation matérielle et logicielle de PoW optique (un fork Bitcoin oPoW et un prototype de mineur photonique de silicium oPoW) a été développé dans le but de tester la fonctionnalité de bout en bout. Le remplacement de la fonction de hachage dans le code PoW de Bitcoin est simple, nous nous concentrons donc ici sur le matériel prototype. Vous trouverez ci-dessous une brève description du système, du circuit intégré photonique au silicium en son cœur et du principe de fonctionnement du calcul analogique.

Système : Il existe plusieurs architectures connues pour la mise en œuvre d'un multiplicateur matrice-vecteur analogique utilisant des composants photoniques au silicium standard. Les deux principaux types d'approches sont (1) l'architecture de banc de filtres en anneau développée au laboratoire de photonique neuromorphique de Princeton [29] et (2) divers maillages d'interféromètre MZI tels que le maillage triangulaire utilisé dans le très cité Shen et al. [30] article du MIT.

Notre multiplicateur matrice-vecteur photonique analogique implémente tation est un maillage de coupleur directionnel rectangulaire19. Comme le montre la figure 4, une carte RasPi exécutant notre logiciel de nœud fork Bitcoin est associée à une carte pilote fabriquée par Qontrol, qui communique avec une carte de circuit imprimé personnalisée, TIA (pour amplifier le signal des photodétecteurs) et un interposeur sur lequel le silicium photonique la puce est montée20. Un gros plan de la puce emballée peut être vu sur les figures 1 et 5 montrant une vue de haut en bas de la puce nue. Le RasPi effectue la partie numérique du HeavyHash et décharge la partie analogique vers la puce photonique via le contrôleur Qontrol.

Puce photonique au silicium : ci-dessous, dans la figure 5, se trouve la disposition de notre prototype de puce photonique. La puce se compose d'une entrée de coupleur à réseau de surface unique, divisée en 16 sorties. Chaque sortie est modulée (selon les données fournies par le RasPi) individuellement par un modulateur thermique Mach-Zehnder équilibré21. · Les sorties des modulateurs sont ensuite introduites dans le maillage du coupleur directionnel de multiplication matricielle22, et les sorties du réseau de multiplication matricielle sont collectées. en fibres via des coupleurs de réseau et convertis en signaux électriques par le

17L'objectif final étant la démocratisation de l'offre matérielle plutôt que l'efficacité énergétique ou la décentralisation géographique.

18Une augmentation N de la taille de sortie du hachage, correspondant à une augmentation N du coût de calcul du hachage, entraîne une augmentation N2 du coût de calcul de la fonction de pondération en raison des propriétés de multiplication matricielle.

19La conception du maillage a été générée à l'aide d'un algorithme fourni par Sunil Pai basé sur ses travaux à Stanford [49].

20Le PCB, le TIA et la puce photonique au silicium ont été fabriqués en partenariat avec SiEPIC kits, une société d'ingénierie photonique intégrée affiliée à l'Université de la Colombie-Britannique.

21Une brève explication du MZM est donnée à la section 2.2.3. Pour plus de détails, un excellent tutoriel sur les composants photoniques sur silicium typiques peut être trouvé dans Silicon Photonics Design: From Devices to Systems de Lukas Chrostowski et Michael Hochberg [35]

22Une brève explication des coupleurs directionnels est donnée en 2.2.3.

Machine Translated by Google

photodiodes et TIA. Dans une configuration commerciale, les photodétecteurs seraient sur puce, ce qui rendrait l'ensemble beaucoup plus simple et éliminerait le besoin de connexions par fibre optique (une entrée laser peut être couplée via une liaison flip-chip).

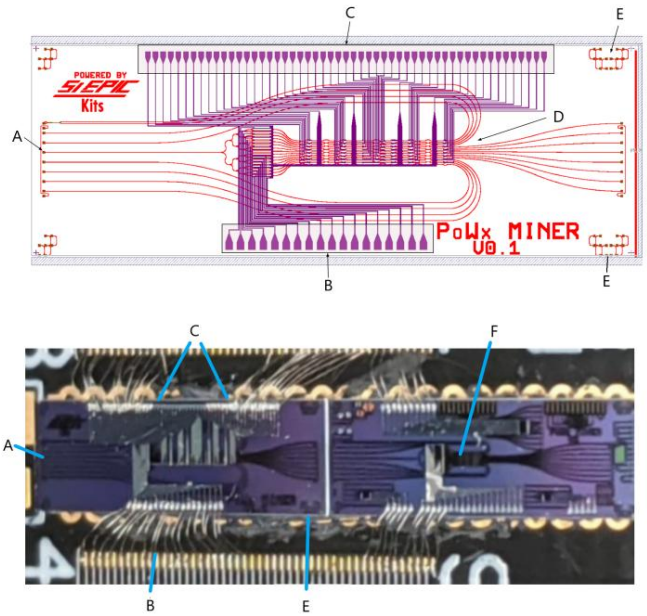

Figure 5. HAUT : Schéma du circuit photonique, A. Entrée laser (1 550 nm, longueur d'onde commune des télécommunications) B. Patins métalliques pour contrôler les modulateurs afin de transduire les données électriques en optique C. Patins métalliques pour régler le maillage des coupleurs directionnels D. Le signal optique sort ici contenant les résultats du calcul et sont transmis aux fibres via un coupleur de réseau à l'extrémité de chaque guide d'ondes.
E. Circuit d'alignement pour aligner l'étage de couplage de fibre. Puce prototype de mineur oPoW nue avant la liaison des fils et des fibres. Sur le côté gauche de la matrice se trouvent les structures de test, le mineur oPoW est à droite. AE inférieur : identique à TOP F. Circuits de test

Principe de fonctionnement de la multiplication matricielle unitaire dans un maillage de coupleurs directionnels : Une discussion généralisée sur les configurations de multiplication matricielle unitaire utilisant la photonique/ l'interférence peut être trouvée dans Reck et al. et Russell et al. [50], [51]. Dans cette section, nous fournirons une intuition de base du principe de fonctionnement de l'approche que nous avons utilisée.

Comme le montre la figure 6, une seule entrée laser est divisée uniformément en plusieurs guides d'ondes, chaque guide d'ondes alimentant un modulateur qui peut diminuer l'intensité de la lumière.

Nous avons choisi un modulateur Mach-Zender, comme le montre la figure 7, qui divise la lumière d'entrée en deux guides d'ondes et les recombine à nouveau avec un déphasage. Le déphasage est réalisé à l'aide d'un élément chauffant23 qui modifie l'indice de réfraction de l'un des guides d'ondes du modulateur.

23Il existe des déphaseurs basés sur des jonctions PN offrant une vitesse et une efficacité bien meilleures.

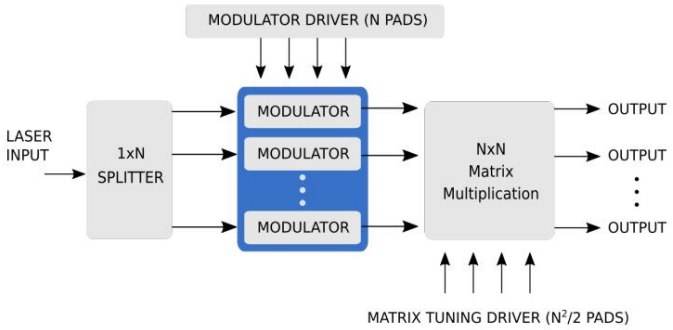

Figure 6. Schéma fonctionnel général des composants de l'appareil (métal en bleu).
N = 16 dans notre conception et les plots de connexion métalliques fournissent un accès électrique aux modulateurs MZM. Un deuxième ensemble de coussinets permet d'accéder au réglage des éléments chauffants dans le maillage du coupleur directionnel.

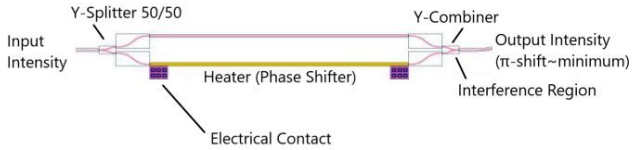

Figure 7. Modulateur Mach-Zender

Dans un appareil parfait, un décalage π complet entraîne une interférence destructrice complète, et des décalages plus petits peuvent être utilisés pour obtenir une interférence destructrice partielle. C'est ainsi qu'un signal numérique utilisé pour piloter le modulateur peut être converti en une intensité optique analogique. Par exemple, dans un système à 4 bits, un décalage π correspondrait à 0000 et un déphasage nul correspondrait à 1111, une interférence partielle fournissant les niveaux intermédiaires. Les sorties des modulateurs sont ensuite introduites dans un maillage de coupleurs directionnels (voir Figure 8 ci-dessous), dont les rapports de division dépendent des phases φ et φ de la lumière entrant à chaque entrée et de la géométrie optique effective de la région de couplage24 .

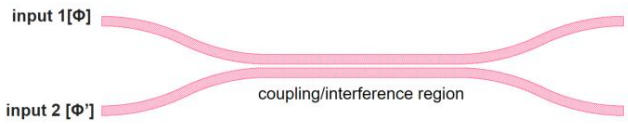

Figure 8. Conception de base du coupleur directionnel

En ajustant les retards de phase de chaque guide d'onde au niveau de chaque couche du maillage du coupleur directionnel et la longueur optique effective de la région de couplage à l'aide d'éléments chauffants, il devrait être possible d'obtenir une matrice de transfert unitaire arbitraire25. Si l'on appelle le vecteur des amplitudes et des phases sortant de chaque modulateur

24Cela dépend de la géométrie physique (longueur du coupleur et écart entre les guides d'ondes) ainsi que de l'indice de réfraction qui peut être réglé avec un élément chauffant).

25En pratique, notre prototype ne peut réaliser qu'un sous-ensemble de matrices unitaires, en raison du nombre limité d'entrées électriques, mais cela ne constitue pas un problème fondamental pour les systèmes commerciaux.

Machine Translated by Google

le vecteur d'entrée [I]26, et la matrice de transfert du maillage [U], la sortie est mathématiquement égale à l'opération matrice-vecteur [U]*[I]. Cependant, le signal réel détecté par les photodétecteurs correspond à l'intensité de la lumière et non à la phase. Par conséquent, le signal électrique analogique détecté renvoie en fait la valeur absolue du vecteur de sortie [O]. Paï et coll. a récemment publié une discussion détaillée de cette architecture et de plusieurs autres architectures similaires avec des compromis différents [49]. L'avantage d'utiliser la photonique pour effectuer cette opération, en supposant qu'une conversion AD-DA de faible précision soit compatible avec le cas d'utilisation, est ici énorme : tous les faisceaux lumineux effectuent un traitement intrinsèquement parallèle.

Nous prévoyons que l'adoption d'un algorithme PoW conçu pour le matériel photonique offrira aux réseaux blockchain divers avantages, tels qu'une meilleure sécurité (résistance aux attaques plus élevée de 51 %) et une consommation globale d'énergie du réseau inférieure pour des réseaux équivalents. Bien qu'une analyse détaillée des implications économiques et sécuritaires d'un PoW dominé par les CAPEX soit publiée séparément, dans les sections suivantes, nous fournissons un bref résumé.

C. Économies d'énergie

La consommation totale d'énergie d'une blockchain PoW ne dépend pas du coût énergétique d'un seul hachage/essai mais de la quantité totale d'énergie utilisée par les mineurs effectuant des travaux dans le système. Par exemple, si SHA256 était remplacé par un hachage présentant une difficulté de calcul moindre (et donc une consommation d'énergie par hachage inférieure), mais le même paradigme matériel optimal (ASIC), alors les mineurs seraient simplement obligés d'effectuer plus de hachages via un ajustement de difficulté.

Cependant, si le coût du calcul PoW est orienté vers un paradigme matériel plus économe en énergie (mais peut être plus coûteux en termes de coût matériel), une blockchain construite sur un tel schéma PoW sera globalement plus économe en énergie même si , quelque peu paradoxalement, un hachage individuel coûte plus cher en termes de calcul. La raison pour laquelle cela est possible est que la difficulté du PoW s'ajuste de telle sorte que le coût relatif par bloc des schémas soit équivalent, même si le coût par évaluation unique de la fonction de hachage sous-jacente est significativement différent. Étant donné que le coût global des systèmes dépend de la valeur de la récompense de bloc, et non du nombre de hachages requis pour obtenir la récompense, nous pouvons comparer directement les facteurs relatifs qui composent le coût de chaque système de hachage (coût énergétique, OPEX, et dépréciation du matériel, CAPEX).27

Tant que le paradigme matériel le plus économe en énergie offre un avantage de coût marginal par rapport aux autres, nous supposons que les agents rationnels adopteront ce paradigme pour maximiser leur utilité dans un écosystème minier donné. En résumé, un PoW à faible consommation d'énergie peut être obtenu en adaptant un algorithme PoW à un paradigme matériel avec un coût par hachage/essai dominé par les CAPEX.

D. Implications sur le budget de sécurité

Le réseau Bitcoin paie aux mineurs plus de 5 milliards de dollars par an pour sécuriser son grand livre. En fin de compte, ce coût est supporté par le détenteurs de Bitcoin via l'inflation. Lors de l'analyse d'un algorithme de sécurité/consensus proposé pour les crypto-monnaies décentralisées, la question clé est la suivante : quel niveau de sécurité réelle le budget de sécurité permet-il d'acheter ?

Pour examiner la sécurité économique de la mise en œuvre d'oPoW dans un protocole blockchain, nous considérons l'attaque classique de 51 % [1], ainsi que le comportement de hachage au fil du temps.

1) Cinquante et un pour cent de sécurité d'attaque dans un PoW à faible OPEX : dans l'attaque à 51 %, un adversaire souhaite acquérir plus de la moitié de la puissance de hachage du système afin de briser le consensus, de construire sa propre chaîne parallèle et faire des choses comme des paiements en double ou censurer des paiements spécifiques en réécrivant l'historique de la blockchain au sein de leur chaîne secrète. Le coût d'une telle attaque serait d'égaler (et de dépasser) le CAPEX total (matériel contrôlé par des nœuds honnêtes) du système et de payer le coût OPEX (énergie) pour la durée de l'attaque. La sécurité de tout système de blockchain PoW repose sur le coût élevé d'une telle attaque.

En supposant qu'un seul système utilise une implémentation particulière de l'algorithme oPoW28, un attaquant désireux d'acquérir 51 % du hashrate pour une attaque ne pourra probablement pas louer le matériel nécessaire à cette attaque. Il est peu probable que les mineurs du système louent simultanément une si grande partie de leur hashrate29 et comme aucun , autre système n'utilise le matériel, il n'y a pas de source secondaire (un système doté de matériel générique, tel que des GPU, n'a pas cet avantage). Ainsi l'attaquant doit acheter près du CAPEX total du système pour gagner 51% de la puissance de calcul. Notez qu'en attaquant le système, l'attaquant rend potentiellement négligeable la valeur de revente du matériel.

Cette analyse est également vraie pour Bitcoin. Bien que Bitcoin ait des OPEX élevés, le coût d'une attaque courte (de l'ordre de quelques jours/ semaines) est dominé par le coût d'acquisition du matériel nécessaire. Dans l'ensemble, l'oPoW offre en fait une sécurité supérieure de 51 % à celle d'un PoW lourd en OPEX à long terme, car il entraîne une croissance plus rapide du hashrate et une plus grande résilience du hashrate face à la diminution de la valeur des récompenses de bloc.30

2) Croissance du hashrate et résilience dans un PoW à faible OPEX : le déplacement des coûts miniers d'OPEX vers CAPEX augmente l'investissement effectif total réalisé par le réseau (via les récompenses de bloc et les frais de transaction) dans la sécurité à long terme. Les coûts OPEX supportés par les mineurs ne contribuent pas à la croissance du hashrate et donc à la sécurité à long terme. L'OPEX est un mal nécessaire. À mesure que davantage de fonds sont investis dans les CAPEX, le réseau constitue un cache de plus en plus important de matériel de sécurité spécialisé, ce qui rend la barrière aux attaques plus élevée. Dans le cadre d'un effet positif connexe de la domination des CAPEX, les mineurs utilisant du matériel à faible OPEX

26De par leur conception, les phases d'entrée sont toutes les mêmes.

27Nous supposons ici que le hashrate sera ajusté par les forces du marché de sorte que le coût relatif du minage est identique dans les deux cas.

28L'analyse se complique si plusieurs réseaux utilisent le même Algorithme PoW, car les mineurs de l'un peuvent attaquer l'autre.

29Bien que cela ne soit pas impossible, un effort coordonné visant à louer environ la moitié du matériel d'un réseau serait difficile à dissimuler et les propriétaires de matériel sont incités à ne pas louer à des attaquants, car le matériel risque de perdre de la valeur si le réseau est détruit. attaqué.

30Il convient de noter que dans certains cas, le coût de l'énergie pourrait être partiellement CAPEX plutôt que totalement OPEX si le mineur investit réellement dans les infrastructures. C'est certainement meilleur en termes de stabilité du hashrate tant que l'infrastructure ne peut pas être réutilisée, mais l'infrastructure énergétique est volumineuse et immobile par rapport au matériel informatique et nécessite plus d'entretien.

Machine Translated by Google

n'avez aucune raison de l'éteindre lorsque le prix des pièces (et donc la valeur de la récompense minière) ou le prix de l'électricité fluctue.
La croissance du hashrate de Bitcoin n'est pas aussi impressionnante qu'elle le paraît si l'on prend en compte les améliorations des performances matérielles. L'analyse d'une mesure plus nuancée, peut-être le taux de hachage spécifique (nous pouvons définir vaguement le taux de hachage spécifique comme le hashrate divisé par le coût en dollars de la réalisation d'un seul hachage), montre que la sécurité du Bitcoin est très sensible au prix. Au quatrième trimestre 2018, les prix du Bitcoin étaient volatils et la pièce a temporairement perdu environ 45 % de sa valeur marchande. À la suite du fait que les mineurs ont éteint leurs machines pour éviter de payer l'électricité, le hashrate est passé de 60 EH/s à 35 EH/s [52] (bien que Bitmain ait lancé un nouveau mineur 7 nm haute performance [53] et que d'autres fabricants de matériel aient rejoint le groupe). combat). L'économie d'oPoW peut créer une communauté de mineurs à croissance plus rapide, plus stable et plus engagée.

III. CONSIDÉRATIONS POUR UNE MISE EN ŒUVRE PRATIQUE D' OPOW

Ci-dessous, nous discutons de certains des facteurs de base requis pour une mise en œuvre réussie d'oPoW dans le monde réel. Nous ne prétendons pas que cette liste soit exhaustive, mais soulignons plutôt certaines des considérations clés.

A. Propriétés de sécurité de HeavyHash

HeavyHash tire sa sécurité cryptographique du hachage (tel que SHA256), qui est composé avec la fonction de pondération pour créer la construction HeavyHash. Tant que la fonction de pondération préserve l'entropie de la sortie de hachage initiale, les propriétés de sécurité Oracle aléatoires du hachage sont héritées. Afin de donner aux coprocesseurs photoniques un avantage dans l'évaluation de HeavyHash, la fonction de pondération doit non seulement être optimisée pour les coprocesseurs photoniques, mais elle doit également être numériquement difficile dans la plupart des cas, de sorte qu'il n'y ait pas de meilleur algorithme pour évaluer l'ensemble du HeavyHash dans ASIC numériques plutôt que de calculer directement l'intégralité du HeavyHash pour chaque nouvel essai/nonce. Nous appelons ce concept la dureté effective minimale. Au-delà de ces intuitions, les spécificités de l'algorithme et une preuve détaillée de sa sécurité seront publiées dans un manuscrit séparé. [54]

B. Économies d'énergie

Pour qu'une mise en œuvre d'oPoW génère des économies d'énergie drastiques par rapport aux blockchains de preuve de travail conventionnelles équivalentes, deux exigences clés devront être satisfaites :

1) Les mineurs utilisant des coprocesseurs photoniques doivent avoir un coût total par hachage (CAPEX amorti + OPEX) inférieur à celui du matériel concurrent (c'est-à-dire ASIC, GPU).
2) Le rapport CAPEX/OPEX dans le coût par hachage pour les mineurs photoniques oPoW doit être d'un ordre de grandeur supérieur à celui des ASIC et des GPU fonctionnant actuellement sur des réseaux comme Bitcoin et Ethereum.

Sur la base d'une ingénierie interne et de discussions approfondies avec des chercheurs et des fabricants de matériel informatique travaillant dans le domaine de l'informatique photonique, nous pensons que ces objectifs sont réalisables compte tenu de l'état de l'art actuel. Toutefois, une implémentation en direct d'oPoW fournira un test empirique.

C. Décentralisation

En supposant que des économies d'énergie drastiques soient réalisées, on peut affirmer que la décentralisation minière en serait nécessairement une conséquence directe. Nous abordons ci-dessous brièvement deux aspects de la question.

1) Décentralisation géographique : Même s'il y aura toujours un faible coût énergétique, et donc une certaine sorte d'économies associées à l'exploitation dans des régions à énergie bon marché, l'énergie ne sera plus le facteur décisif de rentabilité.
Il existe une demande refoulée de participation minière dans les grandes villes et dans d'autres régions où l'énergie est chère mais où les lois sont favorables à la cryptographie (par exemple, Malte). Actuellement, les mineurs potentiels de ces zones n'ont aucun moyen d'obtenir un retour sur capital car leurs coûts d'exploitation seraient supérieurs à la valeur des récompenses en cryptomonnaies qu'ils pourraient obtenir via le minage. oPoW démocratisera l'exploitation minière et offrira aux mineurs la possibilité d'opérer dans des juridictions plus favorables à la cryptographie avec moins de risques, l'état de droit et des coûts de capital inférieurs.

Nous nous attendons à voir les grands mineurs des régions à faible énergie continuer à extraire des pièces PoW conventionnelles, où ils auront moins de concurrence, à mesure que de nouveaux acteurs émergeront dans d'autres régions pour exploiter sur les réseaux oPoW.

2) Décentralisation de la fabrication du matériel : en plus de l'efficacité énergétique, la photonique sur silicium en tant que plate-forme présente l'avantage de réduire les NRE (dépenses d'ingénierie non récurrentes) car les circuits photoniques sur silicium sont fabriqués à l'aide de nœuds de processus plus anciens (c'est-à-dire 200 nm SOI [55] , 90 nm SOI [56] contre 7 nm pour les ASIC Bitcoin [57]). Les faibles NRE contribueront à réduire les barrières à l'entrée et à garantir un marché de fournisseurs sain et compétitif pour les mineurs d'oPoW à long terme. De plus, comme oPoW est basé sur une architecture de coprocesseur photonique qui est appliquée plus généralement au traitement de l'IA, nous nous attendons à une forte concurrence entre les fournisseurs dans le domaine du matériel minier oPoW. Non seulement de nombreuses entreprises commercialisent des coprocesseurs photoniques d'IA, comme indiqué dans l'introduction, mais d'autres approches de multiplication analogique matrice-vecteur sont également étudiées, telles que les réseaux de memristors crossbar et d'autres architectures électroniques inspirées du cerveau qui pourraient éventuellement offrir des performances concurrentes. mineurs au marché. Une intuition plus large qui mérite d'être mentionnée : il est beaucoup plus facile pour un seul fabricant de dominer le marché d'un hachage comme SHA256 qui n'a pas de cas d'utilisation du calcul haute performance en dehors de la cryptomonnaie, que pour un seul fabricant de dominer le marché du calcul d'un plus grand nombre de crypto-monnaies. opération générale utilisée au-delà du PoW d'une pièce particulière.

IV. PERSPECTIVES À LONG TERME

Crypto-monnaie Les crypto-monnaies ont progressé au cours des cinq dernières années, depuis le stade du concept jusqu'au début de la commercialisation.
Il est difficile d'estimer le véritable potentiel à long terme de cette technologie, mais il est clair qu'il existe une opportunité d'accroître l'efficacité et l'équité du système financier mondial. L'accès aux marchés des cryptomonnaies peut agir comme une soupape de sécurité dans les situations de crise, et nous avons déjà vu cela se produire lorsque les krachs de monnaies fiduciaires dans des pays comme le Zimbabwe et le Venezuela ont entraîné une hausse locale de la demande de Bitcoin.

À mesure que les crypto-monnaies deviendront plus stables, fonctionnelles et conviviales, elles seront en mesure de concurrencer plus largement les services financiers traditionnels.

Machine Translated by Google

Coprocesseurs photoniques sur silicium Il y a beaucoup d'espoir dans l'industrie photonique que le succès de la photonique sur silicium dans les communications de données se traduira par des cas d'utilisation informatique.
Il est clair que l'informatique avec des photons plutôt qu'avec des électrons offre des avantages fondamentaux intéressants, mais de nombreux défis d'ingénierie pratiques doivent être relevés pour appliquer l'informatique optique à grande échelle. Tirer parti de la chaîne d'approvisionnement standard de fabrication de semi-conducteurs en utilisant la photonique sur silicium résout bon nombre des problèmes majeurs, mais il en reste quelques-uns, comme l'absence de source laser au silicium31. Dans le cas du traitement de l'IA, des composants optiques non linéaires appropriés Les composants compatibles avec les fonderies de semi-conducteurs constituent un domaine de recherche actif, mais pas encore disponibles dans le commerce. De plus, les composants des circuits photoniques au silicium sont généralement réglés pour s'adapter aux variations de fabrication à l'aide de microchauffeurs, ce qui entraîne une augmentation de la consommation d'énergie globale de tout circuit photonique32. Nous prévoyons que la simplicité du cas d'utilisation de la preuve de travail optique (calcul par force brute conçu pour la photonique, avec presque aucun besoin de mémoire ni variabilité) se révélera être un excellent tremplin pour la technologie des coprocesseurs photoniques sur la voie d'une commercialisation grand public.

PoW optique La mise à l'échelle des crypto-monnaies à réserve de valeur, Bitcoin et autres, pour répondre à la demande mondiale nécessitera des innovations à la fois techniques et sociales. De nombreux chercheurs et développeurs travaillent à apporter des améliorations via des développements hors chaîne tels que Lightning Network33 et des innovations fondamentales en matière de blockchain telles que MimbleWimble / Zcash / Monero (confidentialité) et DAG (évolutivité). Les entrepreneurs améliorent l'intégration des nouveaux utilisateurs et facilitent généralement l'expérience des utilisateurs non techniques. Cependant, outre des efforts intéressants (bien que très centralisés) pour utiliser les énergies renouvelables pour le minage de Bitcoin, la preuve de travail n'a pas connu beaucoup d'innovation depuis l'avènement des ASIC de minage de Bitcoin en 2012.

Notre objectif chez PoWx est de changer cela en tirant parti de l'informatique de nouvelle génération. Un changement fondamental dans l'écosystème PoW est nécessaire pour soutenir une autre augmentation d'un ordre de grandeur de la réserve de valeur décentralisée. Tout en nécessitant des modifications minimes des systèmes de preuve de travail existants et en héritant ainsi des propriétés de sécurité souhaitables, la preuve de travail optique a le potentiel de résoudre certains des problèmes les plus profonds rencontrés aujourd'hui par Bitcoin et d'autres crypto-monnaies. oPoW a la promesse de dissocier les crypto-monnaies des centrales électriques, permettant ainsi un minage géographiquement décentralisé et donc une sécurité améliorée avec des avantages supplémentaires tels que l'élimination de la sensibilité du hashrate au prix des pièces et la démocratisation de l'émission. La mise en œuvre d'oPoW contribuera à accélérer le développement de coprocesseurs photoniques économes en énergie, agissant comme un tremplin vers d'autres applications.

31Il y a eu beaucoup de succès avec les lasers hybrides silicium III-V [58], [59] ainsi que des tentatives plus exotiques de lasers silicium [60], [61].

32De nombreux travaux intéressants sont en cours pour remplacer les microchauffeurs, tels que le réglage des matériaux à changement de phase non volatils [62].

33Lightning est un cadre permettant d'augmenter les transactions traitées par seconde pour le réseau Bitcoin via des canaux de paiement hors chaîne qui finissent par régler leurs totaux finaux sur la blockchain Bitcoin.

REMERCIEMENTS

Les auteurs reconnaissent le soutien financier partiel de PoWx. Nous remercions Sunil Pai (Stanford) pour son aide dans la conception de prototypes de puces et Mustafa Hamood, Stephen Lin et Jaspreet Joha (SiEPIC/Université de la Colombie-Britannique) pour leur aide dans la fabrication et les tests de prototypes. Nous tenons également à remercier Guy Corem (Beam), Bram Cohen (Chia), Tom Brand (Starkware), Yichen Shen (Lightelligence), Mitchell Nahmias (Luminous Computing), Yonatan Sampolin-sky (DAGlabs) et John Tromp (Grin) pour des discussions et des commentaires utiles.

Machine Translated by Google

LES RÉFÉRENCES

[1] Satoshi Nakamoto. Bitcoin : Un système de paiement électronique peer-to-peer. https://bitcoin.org/bitcoin.pdf, 2008.

[2] Adam de retour. Hashcash : une contre-mesure par déni de service. http://www.hashcash.org/papers/hashcash.pdf, 2002.

[3] Leslie Lamport, Robert E. Shostak et Marshall C. Pease. Le problème des généraux byzantins. ACM Trans. Programme. Lang. Syst., 4(3):382-401, 1982.

[4] Cynthia Dwork et Moni Naor. Tarification via le traitement ou la lutte contre le courrier indésirable. Dans CRYPTO, volume 740 de Notes de cours en informatique, pages 139-147. Springer, 1992.

[5] Wiki Ethereum. https://github.com/ethereum/wiki/wiki/Ethash. Archivé sur http://archive.is/ZvgcL.

[6] Iddo Bentov, Pavel Hubacek, Tal Moran et Asaf Nadler. Consensus des tortues et des lièvres : le cadre meshcash pour des crypto-monnaies évolutives et compatibles avec les incitations. Archives ePrint de cryptologie IACR, 2017 : 300, 2017.

[7] Yonatan Sompolinsky. Phantom , ghostdag : Deux protocoles blockdag évolutifs, 2018. ePrint https://eprint.iacr.org/2018/104.

[8] Indice énergétique Bitcoin de Cambridge. https://www.cbeci.org/.

[9] AIE. Statistiques énergétiques de l'IEA. www.iea.org/statistics/electricity. Archivé sur http://archive.is/wqJr0.

[10] Kyle Torpey. Blockstream révèle une opération minière massive. https://www.forbes.com/sites/ktorpey/2019/08/08/blockstream-reveals-massive-bitcoin-mining-facilities-fidelity-an-early-customer/. Archivé sur http://archive.is/YeDwh.

[11] Zak Doffman. Poutine signe la « loi russe sur l'Internet » pour déconnecter la Russie du World Wide Web. https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web, mai 2019 . Archivé sur http://archive.is/oQ8LT.

[12] Brenda Goh. La Chine veut interdire le minage de Bitcoin. https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4, avril 2019. Archivé sur http://archive.is/E4Rzc.

[13] Maria Apostolaki, Aviv Zohar et Laurent Vanbever. Détournement de Bitcoin : routage d'attaques sur les cryptomonnaies. Au Symposium IEEE 2017 sur la sécurité et Confidentialité (SP), pages 375 à 392. IEEE, 2017.

[14] Peter Gazi, Aggelos Kiayias et Alexander Russell. Attaques par stake-bleeding sur les blockchains de preuve de participation. Dans CVCBT, pages 85 à 92. IEEE, 2018.

[15] Hamza Abusalah, Joel Alwen, Bram Cohen, Danylo Khilko, Krzysztof Pietrzak et Leonid Reyzin. Au-delà des compromis temps-mémoire de Hellman avec des applications aux preuves d'espace. Dans ASIACRYPT (2), volume 10625 de Lecture Notes in Computer Science, pages 357-379. Springer, 2017.

[16] Tal Moran et Ilan Orlov. Preuves simples d'espace-temps et preuves rationnelles de stockage. Dans CRYPTO (1), volume 11692 de Notes de cours en informatique Sciences, pages 381 à 409. Springer, 2019.

[17] John Tromp. Cycle de coucou : une preuve de travail basée sur la théorie des graphes liée à la mémoire. Notes de cours sur la cryptographie financière et la sécurité des données en informatique Sciences, pages 49 à 62, 2015.

[18] Dario Amodei. IA et calcul. https://openai.com/blog/ai-and-compute/, octobre 2019. Archivé sur http://archive.is/gUXwr.

[19] B. Marr, B. Degnan, P. Hasler et D. Anderson. Mise à l'échelle de l'énergie par opération via un pipeline asynchrone. Transactions IEEE à très grande échelle Systèmes d'intégration (VLSI), 21(1):147-151, janvier 2013.

[20] Herbert Jaeger. L'approche « état d'écho » pour analyser et former les réseaux de neurones récurrents. Centre national allemand de recherche sur l'information Rapport technique Technology GMD, 148:34, 2001.

[21] Wolfgang Maass, Thomas Natschlager et Henry Markram. Calcul temps réel sans états stables : un nouveau cadre pour le calcul neuronal basé sur les perturbations. Calcul neuronal, 14 : 2531-2560, 2002.

[22] Peter Ford Dominey. Apprentissage de séquences sensori-motrices complexes basé sur la représentation d'états récurrents et l'apprentissage par renforcement. Cybernétique biologique, 73 : 265-274, 1995.

[23] Iulian Ilies, Herbert Jaeger, Olegas Kosuchinas et Monserrat Rincon. Aller de l'avant à travers les échos du passé : prévoir avec l'état d'écho réseaux. Rapport technique, Université Jacobs, 2007.

[24] Azarakhsh Jalalvand, Glenn Van Wallendael et Rik Van De Walle. Systèmes basés sur réseau de calcul de réservoir en temps réel pour les tâches de détection sur les contenus visuels. 7e Conférence internationale sur l'intelligence informatique, les systèmes et réseaux de communication (CICSyN), pages 146-151, 2015.

[25] Chrisantha Fernando et Sampsa Sojakka. Reconnaissance de formes dans un seau. Dans ECAL, volume 2801 des Notes de cours en informatique, pages 588-597. Springer, 2003. ,

[26] Laurent Larger, Antonio Baylon-Fuentes, Romain Martinenghi, Vladimir S. Udaltsov, Yanne K. Chembo et Maxime Jacquot. Calcul de réservoir photonique à grande vitesse utilisant une architecture basée sur le délai : classification en millions de mots par seconde. Examen physique X, 7(1):011015, 2017.

[27] J. Bueno, S. Maktoobi, L. Froehly, I. Fischer, M. Jacquot, L. Larger et D. Brunner. Apprentissage par renforcement dans un réseau neuronal photonique récurrent à grande échelle. Optique, 5(6):756, 2018.

[28] Paul R. Prucnal, Bhavin J. Shastri et Malvin Carl Teich. Photonique neuromorphique. Presse CRC, 2017.

[29] Alexander N. Tait, Thomas Ferreira De Lima, Ellen Zhou, Allie X. Wu, Mitchell A. Nahmias, Bhavin J. Shastri et Paul Richard Prucnal. Réseaux photoniques neuromorphiques utilisant des banques de poids photoniques au silicium. Rapports scientifiques, 7(1), 12 2017.

[30] Yichen Shen, Nicholas C. Harris, Scott Skirlo, Dirk Englund et Marin Soljacic. Apprentissage profond avec des circuits nanophotoniques cohérents. Série de réunions thématiques d'été (SUM) de l'IEEE Photonics Society 2017, 2017.

[31]Steven Cartwright. Nouveau multiplicateur matrice-vecteur optique. Optique appliquée, 1984.

[32] T. Shoji. Convertisseur de taille de mode à faible perte à partir de guides d'ondes en fil SI carré de 0,3 µm vers des fibres monomodes. Lettres électroniques, 38 : 1669-1670(1), décembre 2002.

[33] Qianfan Xu, Bradley Schmidt, Sameer Pradhan et Michal Lipson. Modulateur électro-optique en silicium à l'échelle micrométrique. Nature, 435(7040):325-327, 2005.

[34] Long Chen et Michal Lipson. Photodétecteurs au germanium à très faible capacité et haute vitesse sur silicium. Opter. Express, 17(10):7901-7906, mai 2009.

[35] Lukas Chrostowski et Michael E. Hochberg. Conception photonique au silicium. Presse de l'Universite de Cambridge, 2015.

[36] La photonique sur silicium atteint un point critique, avec des émetteurs-récepteurs expédiés en volume. http://www.semiconductor-today.com/news items/2018/jan/yole 220118.shtml. Archivé sur http://archive.is/qtusc.

[37] A Saadé, F Caltagirone, I Carron, L Daudet, A. Dremeau, S Gigan et F Krzakala. Projections aléatoires par diffusion optique multiple : Rapprocher les noyaux à la vitesse de la lumière. Dans ICASSP, Conférence internationale de l'IEEE sur l'acoustique, la parole et le traitement du signal - Actes, volume 2016-mai, pages 6215-6219, 2016.

[38] Mitchell Nahmias Prucnal, Paul R. et Bhavin J. Shastri. Photonique neuromorphique. Presse CRC, 2017.

[39] Kyle Wiggers. Lightelligence publie un prototype de sa puce d'accélérateur optique d'IA. https://venturebeat.com/2019/04/15/lightelligence-releases-prototype-of-its-optical-ai-accelerator-chip/, avril 2019. Archivé sur http://archive.is/l8A8H.

[40] SPIE Europe Ltd. Lightmatter décroche 33 millions de dollars pour marier la photonique avec l'IA. http://optics.org/news/10/2/32. Archivé sur http://archive.is/jUNjG.

[41] Bill Gates, néo, gigafund soutenant lumineux dans le moonshot du superordinateur photonique. https://techcrunch.com/2019/06/04/bill-gates-neo-gigafund-backing-luminous-in-photonics-supercomputer-moonshot/, juin 2019. Archivé sur http://archive.is/29Nb8.

[42] Mitchell A. Nahmias, Thomas Ferreira De Lima, Alexander N. Tait, Hsuan-Tung Peng, Bhavin J. Shastri et Paul R. Prucnal. Opérations photoniques de multiplication-accumulation pour les réseaux de neurones. Journal IEEE de sujets sélectionnés en électronique quantique, pages 1–1, 2019.

Machine Translated by Google

[43] David AB Miller. Optoélectronique Attojoule pour le traitement de l'information et les communications à faible consommation d'énergie. Journal de la technologie des ondes lumineuses, 35(3):346-396, 2017.

[44] Viraj Bangari, Bicky A Marquez, Heidi B Miller, Alexander N Tait, Mitchell A Nahmias, Thomas Ferreira de Lima, Hsuan-Tung Peng, Paul R Prucnal et Bhavin J Shastri. Electronique numérique et photonique analogique pour les réseaux de neurones convolutifs (DEAP-CNN). Préimpression arXiv arXiv : 1907.01525, 2019.

[45] Thomas Ferreira de Lima, Hsuan-Tung Peng, Alexander N. Tait, Mitchell A. Nahmias, Heidi B. Miller, Bhavin J. Shastri et Paul R. Prucnal. Apprentissage automatique avec photonique neuromorphique. J. Lightwave Technol., 37(5):1515-1534, mars 2019.

[46] David Vorick. L'état de l'exploitation minière de crypto-monnaie par David Vorick. https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b. Archivé à http://archive.is/SIA9a.

[47] Ravikanth Pappu, Ben Recht, Jason Taylor et Neil Gershenfeld. Fonctions physiques à sens unique. Science, 297(5589) :2026-2030, 2002.

[48] Ethan Heilman, Neha Narula, Thaddeus Dryja et Madars Virza. Rapport de vulnérabilité Iota : Cryptanalyse de la fonction de hachage curl permettant des attaques de contrefaçon de signature sur la crypto-monnaie iota. Rapport technique, MIT Media Lab, 2017.

[49] Sunil Pai, Ben Bartlett, Olav Solgaard et David AB Miller. Optimisation matricielle sur les dispositifs photoniques unitaires universels. Examen physique appliqué, 11(6):064044, 2019.

[50] Michael Reck, Anton Zeilinger, Herbert J. Bernstein et Philip Bertani. Réalisation expérimentale de tout opérateur unitaire discret. Lettres d'examen physique, 73(1):58-61, avril 1994.

[51] Nicholas J Russell, Levon Chakhmakhchyan, Jeremy L O'Brien et Anthony Laing. Composition directe de matrices unitaires aléatoires haar. Nouveau Journal of Physics, 19(3):033007, mars 2017.

[52] Graphique de hachage Bitcoin par rapport au prix en USD. https://bitinfocharts.com/comparison/hashrate-price-btc.html. Archivé sur http://archive.is/RJaxR.

[53] Marie Huillet. Chine : le géant minier Bitcoin bitmain lance un nouveau matériel antiminer 7 nm. https://cointelegraph.com/news/china-bitcoin-mining-behemoth-bitmain-releases-new-7nm-antminer-hardware, février 2019. Archivé sur http://archive.is/YxXKZ.

[54] Michael Dubrovsky et Marshall Ball. Vers une preuve optique du travail ; OPow. Manuscrit non publié, 2019.

[55] Objectif fonderie photonique. http://www.aimphotonics.com/, mai 2019.

[56] Fonderies mondiales. Fonderies mondiales de photonique sur silicium. https://www.globalfoundries.com/technology-solutions/silicon-photonics, 2019. Archivé sur http://archive.is/CfczY.

[57] Actualités Bitcoin. Bitmain annonce une nouvelle puce minière Bitcoin de 7 nm avec une efficacité 29 % plus élevée. https://news.bitcoin.com/bitmain-announces-new-7nm-bitcoin-mining-chip-with-29-more-efficiency/, février 2019.

[58] X. Sun, J. Liu, LC Kimerling et J. Michel. Vers un laser au germanium pour la photonique intégrée au silicium. Journal IEEE de sujets sélectionnés dans Quantum Electronics, 16(1):124-131, janvier 2010.

[59] Alexander W. Fang, Oded Cohen, Richard Jones, Mario J. Paniccia et John E. Bowers. Laser évanescent hybride algainas-silicium à pompage électrique, Octobre 2006.

[60] Nils T Otterstrom, Ryan O Behunin, Eric A Kittlaus, Zheng Wang et Peter T Rakich. Un laser Brillouin au silicium. Science, 360(6393) :1113-1116, 2018.

[61] Haisheng Rong, Ansheng Liu, Richard Jones, Oded Cohen, Dani Hak, Remus Nicolaescu, Alexander Fang et Mario Paniccia. Un raman entièrement en silicium laser. Nature, 433(7023):292, 2005.

[62] Yifei Zhang, Jeffrey B. Chou, Mikhail Shalaginov, Carlos Rios, Christopher Roberts, Paul Robinson, Bridget Bohlin, Qingyang Du, Qihang Zhang, Junying Li, Myungkoo Kang, Claudia Gonçalves, Kathleen Richardson, Tian Gu, Vladimir Liberman et Juejun Hu. Remodeler la lumière : photonique reconfigurable rendue possible par des matériaux à changement de phase optique à large bande et à faible perte. Dans Thomas George et M. Saif Islam, éditeurs, Micro- and Nanotechnology Sensors, Systems, and Applications XI, volume 10982, pages 98 – 105. Société internationale d'optique et de photonique, SPIE, 2019.