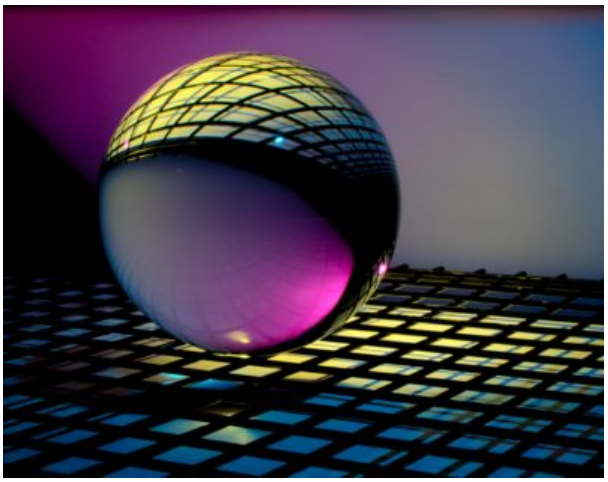
Les startups blockchain de la Silicon Valley innovantes en matière de nouveaux algorithmes de consensus



L’importance de l’écosystème startup dans l’essor de la blockchain

Depuis leur apparition en 2008, les blockchains suscitent un intérêt grandissant à travers le monde, comme en témoigne le fait que 81 des 100 plus grandes multinationales [1] s’intéressent à la technologie des blockchains. Pour autant, pour que l’adoption des blockchains par les entreprises leur soit réellement bénéfique, une analyse fine de ses processus est requise. En effet, tous les types d’entreprises n’ont pas intérêt à y avoir recours, et pas forcément de la même manière [2]. Un entrepreneur travaillant dans la baie de San Francisco que nous avons interviewé est persuadé que l’impulsion de la « révolution Blockchain » viendra des startups. Notons que cette révolution est déjà plus ou moins en marche, notamment dans certains secteurs (FinTech, gaming). Mais il est fort possible que d’ici quelques années, cette technologie soit le support d’une refonte globale du fonctionnement d’un grand nombre de secteurs comme les banques, les assurances, l’internet social, le développement des smart cities, l’internet des objets, etc.

Si la baie de San Francisco n'est pas l'unique écosystème startup en matière de blockchain, il y existe une grande effervescence. Facebook a ainsi lancé l'association *Diem* (anciennement *Libra*, nom de la blockchain associée) qui vise à « construire un réseau financier fiable et innovant, doté de contrôles solides pour protéger les consommateurs et lutter contre la criminalité financière ». Parallèlement, le CEO Mark Zuckerberg a annoncé vouloir être connu comme la société qui a développé le « Métavers ». Les technologies qui vivent sur la blockchain sont donc au cœur des aspirations de Facebook – renommé *Meta* le 28 octobre pour marquer sa polarisation vers le Métavers. Du côté des startups, la baie a vu naître près de 500 startups focalisées sur les blockchains [3]. Trois d'entre elles sont devenues publiques, et cinq autres sont des licornes (startup évaluée à plus d'un milliard de dollars) [4].

La blockchain : un partage décentralisé de l'information

La blockchain (littéralement : chaîne de blocs) désigne, par abus de langage, un ensemble de technologies communément utilisées pour construire des **registres partagés et décentralisés** qui permettent à des participants n'ayant **pas de relation de confiance** entre eux de réaliser des transactions sans l'intervention d'un tiers.

Concrètement, chaque bloc de la chaîne est constitué d'une **clé de hachage** (identifiant du bloc), de la **clé de hachage du bloc précédent** (qui permet de relier les blocs entre eux et de vérifier que la chaîne n'a pas été compromise grâce au consensus, expliqué ci-après), d'un **horodatage** (date d'ajout du bloc à la chaîne) et d'un certain nombre de données correspondant à **des transactions**. Une transaction correspond à toute donnée ayant une valeur : cela peut être un échange de crypto-monnaies, un brevet, une commande de satellites ou des informations

d’identification personnelle comme un permis de conduire.

Chaque utilisateur possède sa propre copie de l’ensemble de la blockchain (registre partagé). Il peut donc vérifier à tout moment que les transactions enregistrées sur la blockchain sont correctes (transparence). Contrairement à une banque qui possède des serveurs sur lesquels sont stockées toutes les données des utilisateurs, avec la blockchain, les informations se trouvent à la fois sur tous les nœuds du réseau, que sont les ordinateurs des utilisateurs (registre décentralisé).

Il existe deux grandes familles de blockchains :

- **Les blockchains publiques** – qui sont ouvertes à tous les utilisateurs sans autorisation ou authentification préalable ; elles sont nécessairement accompagnées d’un système de token (jeton) ou d’une crypto-monnaie. Les plus connues sont Bitcoin et Ethereum.
- **Les blockchains privées, pour lesquelles une autorisation est nécessaire pour participer** – différentes sous-catégories existent ; elles sont par exemple utilisées au sein d’une société ou pour qu’une entreprise échange avec ses partenaires. La blockchain la plus utilisée est Hyperledger (IBM, Walmart, Amazon, Nestle, etc.).

Des algorithmes de consensus qui sont au cœur du fonctionnement des blockchains

Contrairement à ce que le nom de la technologie peut laisser penser, la nouveauté de la technologie blockchain n’est pas tant dans la structure en chaîne de blocs que dans les algorithmes de consensus qui permettent à toutes les entités du réseau de parvenir à un accord sur la fiabilité des informations présentes dans la base de données sans nécessiter une relation de confiance. Réussir à atteindre un consensus

est un problème qui est connu depuis longtemps dans le monde de l'informatique et des systèmes distribués, les premiers travaux datant de la fin des années 1970. Dans les systèmes centralisés, les milliers de serveurs des centres de données doivent par exemple être en accord sur la valeur d'une transaction. Dans ces systèmes, le nombre de participants (les serveurs) est connu et ils sont tous autorisés préalablement pour rejoindre le réseau (grâce à une clé cryptographique qui leur permet de s'inter-identifier).

Cependant, dans les systèmes décentralisés, la difficulté de ce problème augmente considérablement car le nombre de participants n'est pas nécessairement connu, et, suivant le type de blockchain, ces derniers peuvent écrire sur la blockchain sans avoir à s'authentifier au préalable. Dans de telles conditions, un des risques les plus évidents est « l'attaque de Sybil » qui consiste pour un même utilisateur à créer une quantité très importante de fausses identités afin d'obtenir une importance disproportionnée au sein du réseau.

En 2008, l'article original présentant le Bitcoin a proposé la "Proof-of-Work" (« preuve de travail » en français) pour contrecarrer ce stratagème. Il s'agit de demander aux utilisateurs validant les transactions de résoudre un problème algorithmique qui nécessite une charge de calcul importante. Créer un grand nombre de fausses identités devient ainsi beaucoup plus complexe car la puissance de calcul nécessaire devient en principe trop difficile à obtenir pour un seul utilisateur au point d'inverser le rapport coût/bénéfice. Une autre méthode de consensus couramment utilisée (dans Ethereum ou Cardano par exemple) est la Proof-Of-Stake (preuve d'enjeu). Comme pour la Proof-of-Work, cette méthode ne vise pas à empêcher avec certitude qu'une transaction fallacieuse soit acceptée par le consensus à tort mais de rendre la probabilité que cela arrive tellement faible que l'on peut considérer le réseau sécurisé.

Une grande émulation en matière de nouvelles méthodes de consensus dans

la Silicon Valley

Ces deux méthodes de consensus sont quasiment les deux seules qui sont connues du grand public car elles sont utilisées par les crypto-monnaies les plus répandues : Proof-of-Work pour Bitcoin, Proof-of-Stake pour Ethereum et Cardano. Cependant, l'utilisation des blockchains ne se limite pas aux cryptomonnaies et ces deux algorithmes ne sont pas les seuls existants.

En effet, un certain nombre de startups de la baie de San Francisco développent des méthodes de consensus qui s'accordent exactement avec leur cas d'usage. Helium en est certainement l'exemple le plus parlant avec sa Proof-of-Coverage (preuve de couverture). Fondée en 2013 à San Francisco, Helium est une plateforme qui vise au développement de l'Internet of Things (IoT). En effet, de nombreux freins compliquent le passage à l'échelle de l'IoT : trop coûteux, pas assez régulé, pas assez sécurisé, sont certains des arguments évoqués. Helium propose ainsi un réseau physique sans fil et sécurisé dont le succès repose sur la quantité de couverture fiable créée par et pour ses utilisateurs. Pour sa mise en place, un nouvel algorithme de consensus a été créé : la Proof of Coverage (PoC), basée sur l'utilisation des radiofréquences [5].

Avec Helium, les nœuds du réseau sont les participants qui mettent à disposition des antennes qui servent de "Hotspots" pour les objets connectés. Les participants sont alors récompensés pour leur participation à l'agrandissement du réseau (en fournissant de la connexion) et à la preuve de travail.

En effet, grâce au fait qu'un signal radio ne peut être reçu que dans un rayon limité et qu'il se propage à la vitesse de la lumière, la blockchain interroge constamment les Hotspots à l'aide d'un mécanisme connu sous le nom de « PoC Challenge ». La force de la preuve de couverture réside dans le fait que les données générées par les preuves en cours et stockées dans la blockchain Helium constituent une vérification définitive de la couverture sans fil fournie par les points d'accès au réseau.

Développer de nouvelles méthodes de consensus permet également de rendre les blockchains plus adaptées à une utilisation massive. Le passage à l'échelle est souvent présenté comme le plus gros enjeu lié à cette technologie. Le réseau bitcoin est capable de traiter entre 5 et 7 transactions par seconde, Ethereum en traite 30. Dans les deux cas, cela reste peu pour répondre aux besoins mondiaux (à titre de comparaison, Visa assure 24 000 transactions par seconde).

La blockchain Solana, en développant sa Proof-of-History (preuve par l'historique) [6], permet de pallier ce manque d'efficacité. La startup, fondée à San Francisco en 2017, a développé le réseau décentralisé le plus efficace au monde puisqu'avec 200 nœuds physiquement distincts, Solana supporte un débit soutenu pouvant dépasser les 50 000 transactions par seconde.

Au lieu de se fier à l'horodatage des transactions, Proof-Of-History se base sur le fait qu'il est possible de prouver qu'une transaction s'est produite avant ou après un événement. En pratique, toutes les transactions faites sur Solana sont enchaînées les unes aux autres : leur fonction de hachage est générée avec les données de la transaction en elle-même et le résultat de l'encryptage de la transaction précédente. Ce processus crée donc une longue chaîne ininterrompue de transactions hachées. Comme il est très difficile de prédire les résultats des hachages, le réseau est sécurisé. Cela permet aussi de créer une séquence claire et vérifiable de transactions qu'un validateur ajoute à un bloc, sans avoir besoin d'ajouter un horodatage conventionnel.

La Proof-of-History a un grand potentiel, elle est économe en énergie et extrêmement efficace. Mais comme tout algorithme de consensus, elle présente aussi des inconvénients. Par exemple, pour devenir validateur de la blockchain Solana (contrairement aux blockchains utilisant la Proof-Of-Stake par exemple), le matériel informatique doit répondre à des exigences de performance très strictes, ce qui limite la décentralisation du réseau. Par ailleurs, une telle vitesse de transaction engendre des quantités de données colossales. Comme chaque utilisateur possède une copie de l'ensemble de la blockchain localement, cela nécessite une grande capacité de stockage. Pour l'instant, la barrière d'entrée dans Solana reste donc

assez haute, et les équipes de la startup cherchent à l'abaisser.

Du point de vue des recherches académiques, la Proof-of-Luck, présentée par University of California, Berkeley en 2016 est très prometteuse car extrêmement sécurisée et peu coûteuse en énergie [7]. Elle présente cependant elle aussi une barrière d'entrée parce qu'elle nécessite un jeu d'instruction appelé SGX qui est développé sur les processeurs Intel récents. Ces derniers offrent un environnement très sécurisé et non modifiable par les systèmes d'exploitation. Avec la Proof-of-Luck, les participants choisissent des nombres aléatoires appelés *chance* et celui qui choisit le nombre le plus élevé est considéré comme le *gagnant* – et peut ajouter le bloc à la chaîne. Aucune application industrielle de ce consensus n'est connue.

De très nombreuses méthodes de consensus sont développées par les startups dans la Silicon Valley et dans les universités dans la région. Nous avons cité la Proof-of-Work, la Proof-of-Stake, la Proof-of-Coverage, la Proof-of-History ou encore la Proof-of-Luck mais bien d'autres existent. Cette diversité et multiplicité des protocoles de consensus développés dans la baie témoigne d'une innovation qui se concentre non pas seulement sur l'application des blockchains à un secteur économique en particulier, mais sur le cœur de leur fonctionnement pour obtenir des blockchains capables d'être les supports du monde de demain.

Rédacteurs:

Alice Joyeux, service scientifique de San Francisco. E-mail: analyst-sf at ambascience-usa.org

Jean-Baptiste Bordes, service scientifique de San Francisco. E-mail: attache-stic.sf at ambascience-usa.org

[1] Schweiger L. (22 septembre 2021), *81 of the Top 100 Public Companies are using blockchain technology,*

Blockdata https://www.blockdata.tech/blog/general/81-of-the-top-100-public-companies-are-using-blockchain-technology

[2] Blockchain Working Group (Juillet 2020), *Blockchain in California, A Roadmap*, page 32 – 34

[3] Crunchbase, Consulté le 26 octobre 2021 à l'adresse https://www.crunchbase.com/hub/san-francisco-bay-area-blockchain-companies

[4] Analyses réalisées à partir du site Crunchbase et de la plateforme de recherche de CBInsight

[5] Helium, Consulté le 27 octobre 2021 à l'adresse https://docs.helium.com/blockchain/proof-of-coverage/

[6] Yakovenko A., *Solana: A new architecture for a high performance blockchain v0.8.13*, Consultable à l'adresse https://solana.com/solana-whitepaper.pdf

[7] Mitar Milutinovic, Warren He et al. (December 2016), *Proof of Luck: An Efficient Blockchain Consensus Protocol*